



Ministério da Justiça e Segurança Pública - MJSP
Conselho Administrativo de Defesa Econômica - CADE

SEPN 515, Conjunto D, Lote 4, Edifício Carlos Taurisano, - Bairro Asa Norte, Brasília/DF, CEP 70770-504
Telefone: - www.gov.br/cade

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

PROCESSO Nº 08700.003021/2026-49

INTRODUÇÃO

O Estudo Técnico Preliminar - ETP é o documento constitutivo da primeira etapa do planejamento de uma contratação, que caracteriza o interesse público envolvido e a sua melhor solução. Ele serve de base ao Termo de Referência a ser elaborado, caso se conclua pela viabilidade da contratação.

O ETP tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Formalização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação

Referência: Art. 11 da IN SGD/ME nº 94/2022.

1. INFORMAÇÕES BÁSICAS

- ID PCA no PNCP: 00418993000116-0-000001/2026
- Data de publicação no PNCP: 21/03/2025
- Id do item no PCA: 90
- Classe/Grupo: 167 - SERVIÇOS DE EMISSÃO DE CERTIFICADOS DIGITAIS
- Identificador da Futura Contratação: 303001-86/2026

O objeto da contratação também está alinhado com a Estratégia de Governo Digital 2025 e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2025-2028 do Conselho Administrativo de Defesa Econômica:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS

ID	Objetivos Estratégicos
OE8	OE8: Potencializar a atuação do Cade por meio da transformação digital e do uso intensivo de dados

ALINHAMENTO AO PDTIC <2025-2028>

ID	Ação do PDTIC	ID	Meta do PDTIC associada
OE5	Garantir a Segurança da Informação e Comunicação	23	Aquisição de Certificado Digital

ALINHAMENTO AO PAC <2026>

Item	Descrição
90	167 - SERVIÇOS DE EMISSÃO DE CERTIFICADOS DIGITAIS

2. DESCRIÇÃO DA NECESSIDADE

A contratação pretendida têm a finalidade de suprir a necessidade do Conselho Administrativo de Defesa Econômica - Cade, quanto a aquisição e renovação do certificado de assinatura digital SSL/TLS, no intuito de manter a continuidade dos equipamentos servidores e dos serviços que fazem uso de certificado digital como método de autenticação. O Cade lida diariamente com documentos digitais e sistemas, cuja autenticidade precisa ser comprovada. Essa comprovação ocorre através do uso de certificados digitais.

É preciso contemplar a contratação do serviço de emissão continuada do Certificado de assinatura digital para Servidor, SSL/TLS Wildcard - OV para o domínio *cade.gov.br, para garantir a continuidade, segurança e conformidade legal dos serviços digitais prestados pelo Conselho Administrativo de Defesa Econômica.

2.1 Motivação/Justificativa

Um dos requisitos fundamentais para a segurança das aplicações web do Cade é a utilização de certificados digitais SSL/TLS, que permitem a criptografia das comunicações entre servidores e usuários. Essa tecnologia impede a interceptação indevida de dados, assegurando que as informações transmitidas sejam acessíveis apenas por usuários legítimos e autorizados. O Certificado Digital SSL/TLS Wildcard OV, possibilita a segurança criptográfica para todos os subdomínios do Cade dentro do domínio principal.

Os certificados para equipamentos servidores são necessários para garantir a identidade de forma segura e inequívoca, e a garantia da autenticidade, preservando a continuidade operacional dos sistemas de informática do Cade. Por meio do certificado de equipamentos servidores pode-se garantir que um servidor (site, portal ou

aplicação) pertence realmente ao órgão a que se refere. O certificado digital é, também, um recurso utilizado no esquema de segurança para evitar que sejam cometidas fraudes por meio da utilização de sites falsos contra os usuários.

A licença do certificado digital WILDCARD, adquirida por esta Autarquia em agosto de 2025, processo SEI nº 08700.007701/2025-51, tem como prazo de vigência até 06/08/2026. Considerando que a não contratação deste certificado, afetará diretamente todos os processos administrativos, sobretudo o sistema SEI e as aplicações web que dependam do protocolo SSL/TLS, e inviabilizará a integridade e a autenticidade das informações deste Conselho Administrativo, esta contratação se faz necessária.

3. ÁREA REQUISITANTE	
Identificação da Área Requisitante	Nome do Responsável
Coordenação-Geral de Tecnologia da Informação	Vinícius Eloy dos Reis
Serviço de Infraestrutura de Tecnologia	Thiago Nogueira de Oliveira

4. NECESSIDADES DE NEGÓCIO
A contratação visa atender às seguintes necessidades: a) Garantir a integridade e a confiabilidade das informações; b) Garantir a segurança em transações feitas em meios eletrônicos, dos dados e das informações transmitidas entre o site (domínio Cade) e os usuários; c) Proteção adicional de segurança do domínio e dos subdomínios de internet do Cade; d) Permitir o acesso seguro, por meio de um canal criptografado, dos usuários de sistemas e serviços, que utilizam certificado digital do tipo Wildcard SSL/TLS; e) Evitar avisos de sites não seguros; f) Maior proteção contra ataques de phishing.

5. NECESSIDADES TECNOLÓGICAS	
Descrição do Serviço	Requisitos tecnológicos
Certificado Digital SSL/TLS Wildcard OV para servidor	1. Certificado tipo WILDCARD, que permite certificar um único domínio e infinitos subdomínios; 2. Certificado SSL/TLS de validação de empresa (OV); 3. Dever possuir raiz internacional e ser compatíveis com os principais navegadores do mercado, sem a necessidade de instalação manual de cadeia de certificados. 4. Instalação em servidor adicional sem custo e ilimitado; 5. Licença de uso do mesmo certificado em ilimitados servidores e/ou equipamentos; 6. Reemissão ilimitada durante o período de validade do certificado; 7. Utilizar algoritmo de criptografia SHA-2 de 256 bits; 8. Suportar chaves RSA com 2048 bits; 9. Ser compatível com o protocolo SSL/TLS-Secure Socket Layer, versões SSL/TLSv2, SSL/TLSv3, TLS - Transport Layer Security na versão TLSvI (SSL/TLSv3. I) e HTTPS; 10. Compatível com todos os servidores web que suportem os protocolos SSL/TLS e TLS 11. Ser reconhecido por todos os navegadores web que suportem certificados SSL/TLS/TLS, sem a necessidade de nenhuma intervenção manual do usuário ou instalação de cadeias adicionais; 12. Compatível com dispositivos móveis, celulares, smartphones e tablets; 13. Possuir selo de segurança; 14. Verificação do status do Certificado em tempo real (OCSP); 15. Possuir conformidade WebTrust; 16. Garantia de reposição do Certificado ou a correção da solicitação pendente, em caso de constatação de erro técnico no CSR, no prazo máximo de 02 (dois) dias após a emissão; 17. Caso necessite de visita presencial para validação e fornecimento do Certificado, os custos se darão por conta da contratada.

6. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC
6.1 Requisitos Legais • Lei nº 14.133 de 1º de abril de 2021 - Lei de Licitações e Contratos Administrativos.

- Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022 (Normas para Contratação de Soluções de TIC pelos órgãos integrantes do SISP);
- Lei 12.846/2013-Lei anticorrupção.
- Decreto nº 11.878, de 9 de janeiro de 2024 (Normas para o funcionamento do Sistema de Cadastramento Unificado de Fornecedores - SICAF);
- Decreto nº 7.174, de 12 de maio de 2010 (Normas para Contratação de Bens e Serviços de TIC);
- Decreto nº 9.507, de 21 de setembro de 2018;
- Portaria do Cade nº 488, de 10 de outubro de 2023 (Normas sobre a Gestão de Contratos no Âmbito do Cade [1295970](#));
- Instrução Normativa nº 65, de 07 de julho de 2021, da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia;
- Instrução Normativa SEGES/ME Nº 98/2022, que estabelece regras e diretrizes para o procedimento de contratação de serviços sob o regime de execução indireta de que dispõe a Lei nº 14.133, de 1º de abril de 2021, no âmbito da Administração Pública federal direta, autárquica e fundacional;
- Instrução Normativa SEGES/ME nº 5/2017 (Atualizada), que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional; Portaria do Cade nº 405/2019 - Segurança de Informação.
- Lei nº 12.527/2011- Lei de Acesso à Informação
- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

6.2 Requisitos de Segurança da Informação e Privacidade

Na execução dos serviços contratados a CONTRATADA deve zelar, no que for de sua competência, pela garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações custodiadas. Além disso, a CONTRATADA deve adotar e se responsabilizar por medidas efetivas quanto ao seguinte:

- Evitar vazamento de dados e fraudes digitais nos ambientes gerenciados sob sua responsabilidade técnica;
- Garantir a rastreabilidade das ações realizadas nos ambientes gerenciados sob sua responsabilidade técnica, mantendo trilha(s) de auditoria de segurança da informação;
- Assegurar e responsabilizar-se pela continuidade do negócio implementado pelos ambientes gerenciados sob sua responsabilidade técnica;
- Assegurar o adequado tratamento de dados pessoais e informações classificadas dos quais venha a ter conhecimento ou manusear em razão da execução do objeto do contrato, nos termos da Lei Federal nº 13.709/2018 e em aderência aos requisitos de segurança da informação vigentes no ambiente do CONTRATANTE;
- Observar a Medida Provisória nºs 2.200-2/2001, Portaria do Cade nºs 79/2012 e 88/2016 e do Ministério da Justiça 3.530/2013, NBR 27002, 15999-1 e 22301.
- A Contratada deverá se comprometer a guardar sigilo absoluto por tempo indeterminado sobre quaisquer dados, informações, sistemas, *softwares*, documentos, especificações técnicas e comerciais, metodologias, inovações e demais informações da contratante de que venha a ter conhecimento durante a execução dos trabalhos, não podendo sob qualquer pretexto divulgar, revelar, reproduzir ou utilizar, sob pena de lei.
- Conforme legislação em vigor, a Contratada responderá caso ocorra divulgação ou uso de informação sigilosa a que tenha tido acesso em virtude do contrato.
- Para a formalização desta contratação, faz-se necessário que seja exigida a assinatura de termo de responsabilidade e sigilo das informações trocadas entre Fornecedor e Cade. Tal termo deve exigir manifestação da contratada quanto à guarda, privacidade e o sigilo, em razão do exercício de suas atividades bem como das informações disponibilizadas pela entidade contratante.
- Prever os requisitos da LGPD aplicáveis à contratação.

6.3 Requisitos de Garantia e Manutenção

- O certificado digital terá garantia durante toda a sua vigência.
- A Contratada deverá garantir o funcionamento dos certificados digitais durante todo prazo de validade, bem como a reemissão durante o período de vigência do contrato, sem custo adicional.
- Os serviços de suporte deverão ser disponibilizados por meio de canais eletrônicos, pode ser telefone, e-mail, chat e/ou website. Devendo prever mecanismos de acompanhamento das solicitações registradas pelos usuários.
- As solicitações de suporte deverão contemplar situações relacionadas à emissão, instalação, utilização, renovação, revogação ou eventual indisponibilidade dos certificados digitais.
- A Contratada deverá realizar, sem custos adicionais, a reemissão de certificados nos casos de falha técnica atribuível à própria solução ou à Autoridade Certificadora.
- Os atendimentos deverão ser realizados em prazo compatível com a criticidade do serviço, observado o limite máximo de 2 (dois) dias úteis para solução de ocorrências que impeçam a utilização do certificado digital.

6.4 Requisitos Temporais

- A CONTRATADA receberá as informações por e-mail e ficará responsável por iniciar a certificação, no prazo máximo de 02 (dois) dias, a contar do recebimento da Ordem de Serviço (OS), emitida pela Contratante.
- A emissão dos certificados deverá ocorrer preferencialmente de forma remota, em até 10 (dez) dias corridos após o registro da solicitação (Ordem de Serviço). Caso seja necessária validação presencial, esta deverá ocorrer na sede do Cade, em data a ser definida pelo gestor do contrato, sendo os custos da visita e dos procedimentos de responsabilidade da Contratada.
- A solução deverá garantir cobertura contínua durante os 36 (trinta e seis) meses de vigência contratual, incluindo substituições programadas por vencimento, reemissões por mudanças técnicas ou operacionais, e atualizações exigidas por boas práticas de segurança. A substituição de certificados deverá ocorrer com antecedência mínima de 15 (quinze) dias do vencimento, assegurando tempo hábil para testes, homologações e aplicação controlada nas camadas de infraestrutura do Cade.
- A Contratada deverá disponibilizar mecanismo automatizado de notificação à Contratante com, no mínimo, 15 (quinze) dias de antecedência do vencimento do certificado digital emitido no âmbito deste contrato. O lembrete deverá ser enviado por e-mail institucional da CGTI previamente indicado pelo Cade, contendo as informações necessárias para identificação do certificado prestes a expirar, incluindo domínio, data de vencimento e orientações para renovação. O objetivo é assegurar tempo hábil para a emissão de novo certificado, realização de testes e substituição segura, conforme previsto neste Termo de Referência.
- A prestação dos serviços em parcela única corresponde ao fornecimento, instalação e configuração do certificado, que será válido pelo prazo de vigência da contratação, de 36 (trinta e seis) meses, incluindo a reemissão do certificado de acordo com os prazos de validade técnica definidos pelo [CA/Browser Forum](#): a cada 199 dias, a cada 100 dias em 2027 e a cada 47 dias a partir de 2029, ou de acordo com os prazos estabelecidos pelo CAB Forum. As reduções progressivas no prazo de validade dos certificados nos próximos anos, fazem parte de um plano global de reforço na segurança digital do [CA/Browser Forum](#).

6.5 Demais Requisitos necessários

- Com objetivo de prestar todo suporte técnico necessário e eficiente à contratante, a contratada deverá garantir que o profissional designado para o atendimento a esta Autarquia possua experiência e todos os requisitos de qualificação técnica necessários.
- A Contratada deve estar vinculada à Autoridade Certificadora (AC), a qual deve possuir certificação válida do programa de auditoria *Webtrust Certification Authority*. A comprovação deve ser enviada por meio das informações divulgadas no sítio eletrônico da Autoridade Certificadora e/ou através de relatórios de auditoria elaborados por auditor independente, certificações, normas de segurança, relatórios públicos de compliance ou em seção análoga.
- Considerando que as ACs privadas ou próprias (não públicas) não atendem ao requisito WebTrust para SSL/TLS público, a AC emissora do certificado deve ser membro do CA/Browser Fórum, e ser uma das autoridades reconhecidas mundialmente, por exemplo: *Sectigo (Comodo)*, *DigiCert*, *GlobalSign*, *Entrust*, entre outras.

7. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

7.1 Quantitativo detalhado motivado

Item	Descrição	Unidade de Medida	Quantidade	Motivação e Justificativa da Demanda inclusive quanto a Memória de Cálculo
01	Certificado de assinatura digital para Servidor, SSL/TLS Wildcard - OV	Unidade	01	O certificado SSL/TLS garante aos usuários e clientes uma troca segura de informações, minimizando os riscos de os dados trafegados sofrerem intervenções maliciosas, garantindo a identificação, a privacidade e a integridade dos dados que trafegam entre o navegador do usuário e o servidor web. Ou seja, ele servirá para atestar a integridade e autenticidade dos serviços hospedados no domínio *.cade.gov.br. Ademais, diferentemente de outros tipos de certificado em que é necessária a emissão individual e / ou manual de certificados para cada sistema ou endereço, o certificado Wildcard possibilita a segurança SSL/TLS em ilimitados websites e servidores, desde que façam parte de subdomínios do mesmo domínio. A Validação da Organização (OV) possui Nível de segurança intermediário, recomendado para empresas e organizações que precisam de um nível de confiança maior. A licença do certificado digital <i>wildcard</i>, adquirida por esta Autarquia em agosto de 2025, processo SEI 08700.007701/2025-51, tem como prazo de vigência até o dia 06/08/2026. Considerando que a não contratação deste certificado, ora pleiteado afetará diretamente todos os processos administrativos, sobretudo o sistema SEI e as aplicações web que dependam do protocolo SSL/TLS, e inviabilizará a integridade e a autenticidade das informações deste Conselho Administrativo, esta contratação se faz necessária.

7.2 Metodologia de cálculo da volumetria estimada

Para elaboração da memória de cálculo, foram considerados os processos [08700.007701/2025-51](#), [08700.003112/2024-12](#), realizados pelo Cade nos últimos 2 anos para contratação do certificado de servidor SSL/TLS Wildcard, com validade de 12 meses.

8. LEVANTAMENTO DE SOLUÇÕES

A análise comparativa de soluções, nos termos do inc. II do art. 11 da IN 94/2022/SGD, visa a elencar as alternativas de atendimento à demanda considerando, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

- **Disponibilidade do produto similar em outro órgão ou entidade da Administração Pública e as soluções adotadas.**

ID	Solução	Entidade	Contratação	Valor
01	Contratação de serviços de emissão de 1 (um) certificado digital SSL/TLS Wildcard para validação de organização (OV) com validade de 1 ano.	PODER JUDICIÁRIO Tribunal Regional Federal 4ª Região	Dispensa de Licitação Nº 90022/2025	R\$ 1.350,00
02	Contratação de serviço continuado de validação e emissão de certificados digitais do tipo Wildcard OV com validade de 1 ano	JUSTIÇA DO TRABALHO Tribunal Regional do Trabalho da 12ª Região	PE 9134/2025 TERMO DE CONTRATO 12039/2025	R\$ 1.312,00

- **Alternativas no mercado**

Há no mercado, diversas empresas que fornecem a solução.

- **Existência de softwares disponíveis conforme descrito na Portaria STI/MP nº 46/2016, que dispõe sobre a disponibilização de Software Público Brasileiro e dá outras providências.**

Requisito	Sim	Não	Não se Aplica	Justificar quando não aplicável
A Solução está disponível no Portal do Software Público Brasileiro(SPB)?			X	

- **Necessidades de adequação do ambiente para viabilizar a execução contratual**

Id	Tipo de Necessidade	Necessidade
1	Infraestrutura tecnológica	Equipamentos com processador e memória que atendam aos requisitos de instalação de certificados digitais
2	Infraestrutura elétrica	Não aplicável para essa contratação
3	Logística	Não aplicável para essa contratação
4	Espaço físico	Não aplicável para essa contratação
5	Mobiliário	Não aplicável para essa contratação
6	Recursos Humanos	Não aplicável para essa contratação
7	Telefonia	Não aplicável para essa contratação

- **Possibilidade de aquisição na forma de bens ou contratação como serviço**

Requisito	Sim	Não	Não se Aplica	Justificativa (se couber)
Existe a possibilidade de aquisição na forma de bens ou contratação como serviço?	X			

- **Diferentes modelos de prestação do serviço**

Requisito	Sim	Não	Não se Aplica	Justificativa (se couber)
Existem diferentes modelos de prestação de serviços?	X			

- **Diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes**

Requisito	Sim	Não	Não se Aplica	Justificativa (se couber)
Existe diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes?	X			

• **Ampliação ou substituição da solução implantada**

Requisito	Sim	Não	Não se Aplica	Justificativa (se couber)
O objeto dessa contratação é ampliação ou substituição da solução implantada?	X			O certificado do Cade Wildcard OV irá expirar em agosto de 2026.

• **Diferentes métricas de prestação do serviço e de pagamento**

Requisito	Sim	Não	Não se Aplica	Justificativa (se couber)
Existem Diferentes métricas de prestação do serviço e de pagamento	X			

• **Identificação das Soluções**

Em se tratando dos certificados digitais para servidor, apenas um tipo de certificado, o SSL/TLS é compatível com as necessidades do Cade.

Solução	Descrição da solução (ou cenário)
1	Certificados SSL/TLS Gratuitos
2	Contratação de Certificado SSL/TLS - Wildcard OV

9. Análise Comparativa de Soluções

A análise comparativa de soluções, nos termos do inc. II do art. 11 da IN 94/2022/SGD, visa a elencar as alternativas de atendimento à demanda considerando, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

Cenário	Descrição do Cenário
1	Certificados SSL/TLS Gratuitos Descrição: Certificados SSL/TLS gratuitos, utilizados por diversos serviços online e oferecem criptografia para a comunicação entre cliente e servidor. Características: Curto prazo de validade (90 dias) – Requer renovação constante, aumentando o risco de falhas operacionais e a carga de trabalho da equipe técnica; Ausência de validação organizacional (OV) – Não há um processo formal de verificação da identidade do Cade, permitindo a possibilidade de ataques de spoofing e phishing; Dificuldade na gestão de múltiplos certificados – Cada subdomínio exigiria um certificado próprio, dificultando a administração e aumentando a vulnerabilidade a erros de renovação; Falta de suporte técnico especializado – Não há assistência técnica em caso de falhas ou problemas na implementação.
2	Contratação de Certificado para Servidor SSL/TLS Wildcard OV Descrição: Consiste na realização de contratação por dispensa eletrônica, permitindo a aquisição de um Certificado Digital SSL/TLS Wildcard OV, mantendo os padrões de segurança necessários ao CADE. Características: Atende aos requisitos técnicos e de segurança, garantindo criptografia forte e validação organizacional (OV); Cobre todos os subdomínios de primeiro nível (*.cade.gov.br), reduzindo a necessidade de múltiplos certificados; A validade do contrato pode ser de 12, 24 ou 36 meses, minimizando renovações constantes; Garantia de suporte técnico especializado, essencial para resolução de incidentes. Conclusão: Viável. Essa alternativa atende plenamente aos requisitos de segurança, validação e gestão do Cade, garantindo uma solução escalável e confiável para os serviços web institucionais.

• **Quadro para comparação de requisitos entre as Soluções identificadas**

Comparação dos requisitos entre as Soluções identificadas.

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1	X		
	2	X		
A Solução encontra-se implantada em outro órgão ou entidade da Justiça Federal?	1	X		
	2	X		

A Solução está disponível no Portal do Software Público Brasileiro?	1		X	
	2			
A Solução é um software livre ou software público?	1		X	
	2		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	1			NA
	2			NA
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1	X		
	2	X		
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	1	X		
	2	X		

10. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Solução: 1

Descrição da solução: Certificados SSL/TLS Gratuitos

Justificativa: Solução inviável. Apesar do custo zero, essa opção não atende aos requisitos mínimos de segurança, validação e eficiência operacional exigidos para os serviços do Cade, tendo em vista que não previne ataques de spoofing e phishing. Além de não possuir suporte técnico. Cada subdomínio exigiria outro certificado, dificultando a administração e aumentando vulnerabilidades e erros, além da necessidade de renovação e alteração constante pela equipe de TI do Cade.

11. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

Após análise das opções, conclui-se que a melhor solução para o Cade é a contratação de um Certificado Digital SSL/TLS Wildcard OV via dispensa eletrônica, pois essa alternativa:

- Garante a segurança dos serviços web do Cade;
- Mantém a validação organizacional (OV), protegendo contra falsificações;
- Evita a necessidade de múltiplos certificados, simplificando a administração;
- Atende plenamente aos requisitos técnicos, operacionais e de conformidade legal;
- Permite maior competitividade e vantajosidade na escolha do fornecedor.

Apenas 1 (uma) solução se mostrou viável, porém será realizada a comparação de custos entre os cenários, conforme demonstrado a seguir.

11.1 Cálculo dos Custos Totais de Propriedade

Foi realizada a pesquisa de preços no mercado, em sites especializados no fornecimento de certificados digitais SSL/TLS para servidor, ACTIVEWEB e SSL DRAGON. Dessa forma, foi possível fazer a análise comparativa de custos - TCO, de acordo com as durações disponíveis de 12, 24 e 36 meses, considerando que os preços representam o custo total em cada período.

ActiveWeb

Visualizar carrinho

Página Inicial

Comprar

Contato

Minha Conta

Categorias

Certificados SSL/TLS

Backup de E-mails

Backup de Sites

Certificado para Email S/MIME

Certificados Code Signing

Certificados de Marca

SiteLock - Segurança de Sites

Configurar

Configure as opções desejadas e depois continue.

DigiCert OV Wildcard SSL

Escolha o ciclo de pagamento

R\$ 5.373,00 Trienal

R\$ 1.990,00 Anual

R\$ 3.781,00 Bienal

R\$ 5.373,00 Trienal

Informações Adicionais

Resumo do Pedido

DigiCert OV Wildcard SSL

Certificados SSL/TLS

DigiCert OV Wildcard SSL

Trienal

R\$ 5.373,00

R\$ 5.373,00

R\$ 5.373,00

Total a pagar agora

Continuar

Sectigo OV Wildcard

Protege um domínio e todos os subdomínios

SECTIGO®

Perfeito para lojas on-line, comércio eletrônico, organizações

SSL Dragon

Certificados SSLProdutos de segurançaRecursosSobre

criptografá-los. Com esse certificado, você economizará tempo e dinheiro durante a instalação e a renovação.

Validação de negócios

Emissão em 1 a 2 dias úteis

Protege as versões com e sem www

Compatível com dispositivos móveis

Reedições gratuitas e ilimitadas

Garantia de US \$1.000.000

Selo de site dinâmico gratuito

Criptografia de até 256 bits

Licenças de servidor ilimitadas e gratuitas

Acelere com o LEI: Validação rápida

Métodos de validação: DV (EMAIL, DNS) e BV

Algoritmo de hash disponível: RSA e ECC

Informações

Recursos

Benefícios do certificado Sectigo OV Wildcard

R\$ 159 07

Faturado R\$6,477.23 para 3 anos

Compre agora

Quer mais barato?
Comprar vários anos

Duração

Preço

Você economiza

1 ano

R\$2.590,89

2 anos

R\$4.663,60

R\$518,18

3 anos

R\$6.477,23

R\$1.295,44

11.2 Mapa comparativo dos cálculos totais de propriedade (TCO)

Certificado OV Wildcard SSL/TLS (valores unitários)		
Período	ACTIVEWEB	SSL DRAGON
12 meses	R\$ 1.990,00	R\$ 2.590,89
24 meses	R\$ 3.781,00	R\$ 4.663,60
36 meses	R\$ 5.373,00	R\$ 6.477,23

Custo Médio Mensal:

Período	SSL DRAGON (R\$/mês)	ACTIVEWEB (R\$/mês)
12 meses	R\$ 215,91	R\$ 165,83
24 meses	R\$ 194,32	R\$ 157,54
36 meses	R\$ 179,92	R\$ 149,25

Conforme análise do mapa comparativo do TCO, quanto maior o prazo de vigência de contratação do certificado, menor o custo mensal médio. O ganho financeiro cresce com o tempo, sendo que a economia acumulada é maior em 36 meses.

12. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

A única alternativa viável identificada foi a contratação do Certificado Digital SSL/TLS Wildcard OV, com reemissão de acordo com as regras vigentes dos navegadores e normas internacionais -CAB/fórum, garantindo a continuidade da segurança e proteção digital dos sistemas do Cade e adequação aos padrões globais de segurança da informação. Analisando as alternativas disponíveis quanto aos prazos de validade, e que atendam à necessidade do Cade, considerando a viabilidade técnica e econômica demonstrada na análise comparativa de custos, a equipe de planejamento da contratação sugere a vigência inicial de 3 anos, podendo ser prorrogada por até 10 anos, possibilitando maior previsibilidade, eficiência na gestão contratual e economicidade para a Administração.

A caracterização dos serviços emissão de certificados digitais, objeto deste Estudo como sendo de prestação continuada se deve ao fato de se tratar de serviço essencial às atividades do Cade, de caráter permanente, e sua interrupção resultaria em comprometimento da prestação do serviço público à sociedade, uma vez que tem relação direta com a infraestrutura de segurança digital do Cade, sendo essencial para a proteção dos serviços web institucionais, bem como para o recebimento e acesso de informações. Esse serviço vem sendo contratado anualmente através dos processos SEI nº 08700.007701/2025-51 e 08700.003112/2024-12.

Tendo em vista o valor estimado, a solução deverá ser contratada por **dispensa de licitação** com fulcro no art. 75, II, da lei 14.133/21, permitindo a participação de diferentes fornecedores.

Registra-se que o objeto da contratação NÃO incide nas hipóteses vedadas pelos artigos 3º e 4º da IN SGD/ME nº 94/2022.:

Art. 3º Não poderão ser objeto de contratação:

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

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

Parágrafo único. O apoio técnico aos processos de gestão, de planejamento e de avaliação da qualidade das soluções de

Estudo Técnico Preliminar da Contratação 1720530 SEI 08700.003021/2020-49 7 pg. 6

TIC poderá ser objeto de contratação, desde que sob supervisão exclusiva de servidores do órgão ou entidade.

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

A solução não está presente nos Catálogos de Soluções de TIC com Condições Padronizadas publicados pelo Órgão Central do SISP.

Conforme disposto no ANEXO II da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, consideram-se soluções de TIC os bens e/ou serviços que se adequam à definição de pelo menos uma das categorias a seguir:

1.5. INFRAESTRUTURA DE TIC

a) São considerados recursos de TIC os serviços associados ao conjunto de componentes técnicos, hardware, software, bancos de dados implantados, procedimentos e documentação técnica usados para disponibilizar informações, incluindo serviços de segurança digital (controle lógico e biométrico), **certificação digital**, operação e suporte técnico;

Não será admitida nesta licitação a participação de empresas que estejam reunidas em consórcio e sejam controladoras, coligadas ou subsidiárias entre si, qualquer que seja sua forma de constituição, haja vista que o objeto a ser executado não apresenta vulto ou complexidade que tornem restrito o universo de possíveis licitantes.

Item	Descrição	Especificação
1	Certificado de assinatura digital para Servidor, SSL/TLS Wildcard (OV), com período de cobertura de 36 meses	Emissão de Certificado digital SSL/TLS de raiz internacional do tipo WILDCARD OV para servidores: a) certificado digital internacional SSL/TLS do tipo OV para domínio, com Nível de segurança intermediário, assegurando que todos os sistemas acessíveis sob o domínio *.cade.gov.br sejam oficialmente reconhecidos como pertencentes ao Cade, evitando ataques de spoofing e phishing. b) certificado de validação completa do tipo SSL/TLS OV (Organization Validated), validação a nível da organização, para atestar a integridade e autenticidade dos serviços hospedados no domínio *.cade.gov.br. c) O certificado deve possuir conformidade WebTrust, com os padrões globais de segurança digital, como CA/Browser Forum, criptografia SHA-2, suporte a TLS 1.2 e TLS 1.3, garantindo aderência às melhores práticas para a proteção de dados sensíveis. d) licença de uso do mesmo certificado em ilimitados servidores e/ou equipamentos, instalação em servidor adicional sem custo e ilimitada; e) reemissão ilimitada durante o período de validade do certificado; f) utilizado para uma quantidade ilimitada de subdomínios vinculados ao domínio principal, válido para um domínio principal e seus subdomínios (no mínimo 100 subdomínios); g) utilizar algoritmo de criptografia SHA-256; h) suportar chaves RSA com 2048 bits; i) ser compatível com o protocolo SSL/TLS- Secure Sockets Layer, versões SSL/TLSv2, SSL/TLSv3, TLS — Transport Layer Security na versão TLSv1 (SSL/TLSv3.1) e HTTPS; j) compatível com 100% dos servidores WEB que suportem os protocolos SSL/TLS e TLS k) ser reconhecido por todos os navegadores web que suportem certificados SSL/TLS/TLS, sem a necessidade de nenhuma intervenção manual do usuário ou instalação de cadeias adicionais; l) O certificado deverá ser compatível com todas as infraestruturas utilizadas pelo Cade, incluindo servidores, além de ser reconhecido automaticamente pelos principais navegadores e dispositivos móveis celulares, smartphones e tablets, sem necessidade de intervenções manuais m) possuir selo de segurança Site Seguro; n) verificação do status do Certificado em tempo real (OCSP); o) O fornecedor deverá garantir a verificação completa da identidade institucional do Cade, conforme exigências das Autoridades Certificadoras (CA) reconhecidas pelo CA/Browser Forum; p) incluir prestação de suporte técnico remoto, via telefone, e-mail, chat e/ou website, por equipe de técnicos especializados, para esclarecimento de dúvidas técnicas e cadastrais, tais como: geração do CSR, validação da solicitação de compra, instalação do certificado e selo do site seguro e outras necessárias à perfeita execução do objeto contratado; q) garantia de reposição do Certificado ou a correção da solicitação pendente, em caso de constatação de erro técnico no CSR, no prazo máximo de 02 (dois) dias após a emissão do mesmo; r) não serão aceitos certificados de autoridades certificadoras descredenciadas pela Apple, Microsoft, Mozilla e Google; s) O certificado deve ser emitido exclusivamente para o domínio principal do Cade e abranger todos os subdomínios de primeiro nível sem necessidade de configurações adicionais. Conforme decisão do CA/Browser Forum, que estabelece as regras globais para certificados públicos na internet, a validade máxima dos certificados SSL/TLS/TLS publicamente confiáveis foi reduzida para aproximadamente 199 dias em março de 2026, exigindo reemissões dentro do período contratado. Essa medida faz parte de um plano global de reforço na segurança digital, que prevê reduções progressivas no prazo de validade dos certificados nos próximos anos, para 100 dias a partir de 2027 e para 47 dias em 2029, conforme divulgado nos sites: https://www.digicert.com/faq/tls-SSL/TLS-certificate-validity?utm_source=chatgpt.com. e https://cabforum.org/working-groups/server/baseline-requirements/requirements/#632-certificate-operational-periods-and-key-pair-usage-periods. Portanto, inicialmente, o certificado terá a validade técnica de 199 dias, sendo necessária a reemissão do certificado dentro da mesma ordem de serviço para completar o prazo de 36 meses. Não haverá cobrança adicional por esse serviço. O fornecedor deverá informar na proposta que disponibiliza método de notificação pelo menos 15 dias antes do vencimento, e a reemissão com a cobertura total de 36 meses.

13. ESTIMATIVA DO CUSTO TOTAL DA CONTRATAÇÃO

Para cálculo do Custo Total desta solução, foi utilizada a seguinte metodologia: Realização de pesquisa no Sistema de Preços do Portal de Compras Governamentais, de soluções similares contratadas por outros Órgãos no sistema do banco de preços, em sites de domínio público / especializados, e com fornecedores . O documento SEI 1727041 detalhada a metodologia utilizada para a composição da pesquisa de preços.

Item	Descrição	Qtd.	CAT SER	Unidade de medida	Valor unitário (R\$)	Valor Total (R\$)
1	Emissão de Certificado de assinatura digital para Servidor, SSL/TLS Wildcard - Validação da Organização (OV) para o domínio *cade, com período de cobertura de 03 anos.	1	2717 0	Certificado emitido	R\$ 5.387,33	R\$ 5.387,33
Valor total:			R\$ 5.387,33			

14. JUSTIFICATIVA TÉCNICA DA ESCOLHA DA SOLUÇÃO

A contratação do Certificado Digital SSL/TLS Wildcard OV visa garantir a segurança, confiabilidade e integridade das comunicações eletrônicas realizadas nos sistemas web do Cade. O certificado será adquirido em conformidade com os padrões globais de segurança digital, como CA/B Forum, criptografia SHA-2, suporte a TLS 1.2 e TLS 1.3, garantindo aderência às melhores práticas recomendadas para a proteção de dados sensíveis.

Existe a necessidade de contratação de autoridade especializada na prestação de serviço contínuo, sem dedicação exclusiva de mão de obra, para execução de serviços de emissão de certificados digitais. A empresa certificadora será contratada de forma contínua para que a instituição disponha de serviço de emissão de certificados e não haja descontinuidade, considerando que este tipo de serviço será sempre necessário a fim de manter as atividades do Cade, o objeto enquadra-se como serviço de natureza continuada.

O contrato firmado entre a CONTRATANTE e a CONTRATADA terá vigência de 03 anos, a partir da data de sua assinatura. Poderá ser admitida a sua prorrogação até o limite de 10 (dez) anos, a critério das partes e mediante termo aditivo, observado os artigos 106 e 107 da Lei nº 14.133/2021, desde que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação para a manutenção e eventual restabelecimento do equilíbrio econômico-financeiro do CONTRATO, aos preços efetivamente praticados no mercado, à época da eventual prorrogação.

A Contratada deve estar vinculada à Autoridade Certificadora (AC), a qual deve possuir certificação válida do programa de auditoria *Webtrust Certification Authority*. A comprovação deve ser enviada por meio das informações divulgadas no sítio eletrônico da Autoridade Certificadora e/ou através de relatórios de auditoria elaborados por auditor independente, certificações, normas de segurança, relatórios públicos de compliance ou em seção análoga. O WebTrust for Certification Authorities é um programa internacional de auditoria independente, é o padrão exigido pelos principais navegadores (Chrome, Edge, Firefox, Safari).

A AC emissora do certificado deve ser membro do CA/Browser Forum, e ser uma autoridade pública, reconhecida mundialmente, por exemplo: *Sectigo (Comodo), DigiCert, GlobalSign, Entrust, entre outras*. Pois, as AC's privadas ou próprias (não públicas) não atendem ao requisito WebTrust para SSL/TLS público.

15. JUSTIFICATIVA ECONÔMICA DA ESCOLHA DA SOLUÇÃO

Para o presente objeto, a pesquisa de preços está de acordo com o Art. 5º, da IN nº 65/2021 SEGES/ME, em que foram realizadas buscas no sistema governamental de preços, de contratações similares de outros entes públicos, em sites de domínio amplo, e com fornecedores, com o intuito de determinar o valor estimado da contratação. A pesquisa de mercado e a análise comparativa de custos demonstraram que a contratação planejada seguirá o princípio da economicidade, garantindo a melhor relação custo-benefício para o Cade, conforme as diretrizes da Lei nº 14.133/2021.

Com a aquisição do Certificado Digital SSL/TLS Wildcard OV, o Cade garantirá um ambiente digital seguro, confiável e eficiente, protegendo as informações institucionais e promovendo uma melhor experiência para servidores, e usuários que acessam seus serviços online. O certificado será reemitido pelo fornecedor sem custo adicional, antes do seu vencimento. Diferente dos certificados gratuitos e individuais, que demandam alterações constantes e gerenciamento complexo, o uso de um certificado Wildcard OV permitirá a proteção de múltiplos subdomínios com um único certificado, reduzindo custos operacionais e facilitando a administração da infraestrutura digital do Cade.

A contratação será realizada de acordo com a Lei nº 14.133/2021, permitindo contratos contínuos com vigência inicial de até 3 anos, prorrogáveis por até 10 anos. Isso trará maior previsibilidade e estabilidade na gestão da segurança digital do Cade.

O pagamento da contratação do serviço de Certificado Digital SSL/TLS/TLS OV Wildcard, será feito em parcela única, para o período de 03 anos, porém, o certificado deverá ser reemitido, dentro da mesma ordem de serviço, sem custos adicionais para o Cade. Por questões de segurança da informação, de acordo com as regras vigentes dos navegadores e normas internacionais do CAB/fórum, a Contratada deverá reemitir o certificado, fornecido com validade inicial de 199 dias, e prosseguir com a renovação 15 dias antes do seu vencimento, a cada 100 dias a partir de 15 de março de 2027 e a cada 47 dias a partir de 15 de março de 2029, sucessivamente até completar o prazo contratado de 36 meses.

16. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

- A contratação do Certificado Digital SSL/TLS Wildcard OV visa garantir a segurança, confiabilidade e integridade das comunicações eletrônicas realizadas nos sistemas web do Cade.
- A renovação do certificado digital permitirá a proteção ininterrupta dos serviços web institucionais, assegurando a criptografia de ponta a ponta das informações trafegadas entre servidores e usuários.

- Garantia de autenticidade e confiabilidade das aplicações web: O Certificado SSL/TLS Wildcard OV possui validação organizacional (OV), assegurando que todos os sistemas acessíveis sob o domínio *.cade.gov.br sejam oficialmente reconhecidos como pertencentes ao Cade, evitando ataques de spoofing e phishing.
- Simplificação da gestão de certificados digitais: Diferente dos certificados gratuitos e individuais, que demandam renovações constantes e gerenciamento complexo, o uso de um certificado Wildcard OV permitirá a proteção de múltiplos subdomínios com um único certificado, reduzindo custos operacionais e facilitando a administração da infraestrutura digital do Cade.
- Atendimento às diretrizes e padrões de segurança da informação: O certificado será adquirido em conformidade com os padrões globais de segurança digital, como CA/B Forum, criptografia SHA-2, suporte a TLS 1.2 e TLS 1.3, garantindo aderência às melhores práticas recomendadas para a proteção de dados sensíveis.

17. PROVIDÊNCIAS A SEREM ADOTADAS

Não são necessárias providências.

18. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

Considerando as informações apresentadas no presente documento, verifica-se que o objeto desta contratação se mostra viável em termos de disponibilidade de mercado, forma de prestação do serviço/fornecimento de bens e competitividade, não sendo possível observar óbices ao prosseguimento da presente contratação.

Ressalta-se que o objeto dessa contratação possui padrões de desempenho e qualidade que podem ser objetivamente definidos por Edital, por meio de especificações usuais de mercado.

Certificamos que os serviços a serem contratados se enquadram como atividades materiais acessórias, instrumentais ou complementares aos assuntos que constituem área de competência legal do Conselho Administrativo de Defesa Econômica - CADE, em conformidade com o art. 3º, inciso I, da Instrução Normativa SGD/ME nº 94, de 2022.

Por tudo o que foi apresentado, a equipe de planejamento conclui este Estudo Técnico Preliminar declara viabilidade da contratação.

19. RESPONSÁVEIS

A Equipe de Planejamento da Contratação designada pelo Despacho Decisório 310 ([1754862](#)) aprova e assina este Estudo Técnico Preliminar da Contratação, conforme o determina o § 2º do Art. 11 da Instrução Normativa SGD/ME nº 94/2022.

EQUIPE DE PLANEJAMENTO		
INTEGRANTE REQUISITANTE	INTEGRANTE TÉCNICA SUBSTITUTA	INTEGRANTE ADMINISTRATIVO
Thiago Nogueira de Oliveira (Assinado eletronicamente)	Débora Maria de Souza Reis (Assinado eletronicamente)	Erika Aparecida Bastos Veríssimo (Assinado eletronicamente)

20. APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

Em conformidade com o §2º e §3º do Art. 11 da Instrução Normativa SGD/ME nº 94/2022, declaro que a Autoridade máxima da área de TIC não está compondo a Equipe de Planejamento da Contratação. Dessa forma, aprovo o presente Estudo Técnico e declaro a viabilidade da contratação.

AUTORIDADE MÁXIMA DA ÁREA DE TIC
ANA PAULA PESSOA MELLO Coordenadora Geral de Tecnologia da Informação Substituta (Assinado eletronicamente)



Documento assinado eletronicamente por **Débora Maria de Souza Reis, Integrante Técnico**, em 01/06/2026, às 16:35, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.



01/06/2026, às 22:23, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.



Documento assinado eletronicamente por **Erika Aparecida Bastos Veríssimo, Integrante Administrativo**, em 02/06/2026, às 14:02, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.



Documento assinado eletronicamente por **Ana Paula Pessoa Mello, Coordenadora-Geral substituta**, em 11/06/2026, às 10:28, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.



A autenticidade deste documento pode ser conferida no site <https://sei.cade.gov.br/autentica>, informando o código verificador **1726950** e o código CRC **4353E213**.

Referência: Processo nº 08700.003021/2026-49

SEI nº 1726950