AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Estudo Técnico Preliminar 23/2026

1. Informações Básicas

Número do processo: 00261.002282/2026-56

2. Descrição da necessidade

2.1 Introdução

Este Estudo Técnico Preliminar — ETP integra a fase de planejamento da contratação e tem por finalidade caracterizar a necessidade administrativa, analisar as alternativas disponíveis no mercado e demonstrar a viabilidade técnica, econômica, administrativa e ambiental da solução pretendida, nos termos do art. 18 da Lei nº 14.133, de 1º de abril de 2021, e do art. 11 da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

A elaboração deste ETP observa as normas aplicáveis às contratações de soluções de Tecnologia da Informação e Comunicação — TIC, especialmente a Lei nº 14.133/2021, a Instrução Normativa SGD/ME nº 94/2022, a Instrução Normativa SEGES nº 58/2022 e, quanto à formação do valor estimado, a Instrução Normativa SEGES/ME nº 65/2021, sem prejuízo das normas técnicas aplicáveis aos certificados digitais públicos SSL/TLS.

A solução analisada compreende a contratação de até 2 (dois) serviços de certificação digital pública SSL/TLS do tipo Wildcard, com validação organizacional — OV, cada um com cobertura contínua durante 36 (trinta e seis) meses.

A primeira unidade será destinada à proteção do domínio curinga `*.anpd.gov.br` e ao atendimento do domínio raiz `anpd.gov.br`. A segunda unidade será destinada a outro domínio institucional sob gestão da ANPD, a ser formalmente indicado quando caracterizada a necessidade, observadas as mesmas características técnicas, o mesmo período de cobertura e o mesmo preço unitário.

A solução destina-se à autenticação de servidores e à proteção criptográfica das comunicações realizadas por meio do protocolo HTTPS. Não se trata de certificado ICP-Brasil destinado à assinatura digital, à autenticação pessoal ou à representação de pessoa física ou jurídica.

O período de 36 (trinta e seis) meses corresponde à duração da cobertura de cada serviço, e não à validade de uma única emissão de certificado. Considerando que a validade técnica individual dos certificados públicos SSL/TLS será inferior ao período contratado, cada serviço deverá incluir todas as validações, emissões sucessivas, renovações, reemissões, revogações, atividades de gerenciamento e suporte técnico necessárias à manutenção ininterrupta da cobertura, sem cobrança adicional por certificado, emissão ou evento.

O presente estudo subsidiará a definição do objeto, o dimensionamento da demanda, o levantamento das soluções disponíveis, a comparação dos custos, a escolha da solução, a estimativa do valor da contratação e o tratamento dos riscos, em observância aos princípios da eficiência, da economicidade, da continuidade do serviço público e da segurança da informação.

2.2 Necessidade

A ANPD, na condição de autarquia de natureza especial responsável pela proteção de dados pessoais no Brasil, necessita assegurar que seus serviços digitais sejam disponibilizados de forma segura, confiável e contínua.

A Agência mantém portais, sistemas e outros serviços digitais acessíveis pela internet, os quais demandam a utilização do protocolo HTTPS e de certificados digitais públicos SSL/TLS emitidos por Autoridade Certificadora reconhecida pelos principais navegadores e sistemas operacionais.

A necessidade compreende a manutenção de até 2 (duas) coberturas HTTPS Wildcard distintas, cada uma pelo período de 36 (trinta e seis) meses.

A primeira unidade será destinada ao domínio curinga `*.anpd.gov.br` e ao domínio raiz `anpd.gov.br`. A cobertura Wildcard permitirá proteger os subdomínios de primeiro nível existentes e aqueles que forem criados ou substituídos durante a vigência, sem exigir a contratação de certificados individuais ou a manutenção de uma lista fechada de subdomínios.

A segunda unidade será destinada a outro domínio institucional sob gestão da ANPD, a ser formalmente indicado quando caracterizada a necessidade. Essa unidade permitirá atender tempestivamente outro domínio institucional que necessite de proteção HTTPS durante a vigência, sem a necessidade de iniciar uma nova contratação para solução com as mesmas características técnicas.

O quantitativo de 2 (dois) serviços representa duas coberturas Wildcard distintas. Não representa duas emissões sucessivas do mesmo certificado. A primeira unidade possui destinação definida, enquanto a segunda deverá ser acionada mediante indicação formal do domínio institucional, conforme procedimento a ser estabelecido no Termo de Referência.

A notação Wildcard `*.dominio.gov.br`, isoladamente, não abrange tecnicamente o respectivo domínio raiz `dominio.gov.br`. Por essa razão, em cada unidade o respectivo domínio raiz deverá constar expressamente no campo Subject Alternative Name — SAN do mesmo certificado Wildcard, sem cobrança adicional.

Na primeira unidade, o certificado deverá contemplar `*.anpd.gov.br` e `anpd.gov.br`. Na segunda, deverá contemplar o nome Wildcard e o domínio raiz correspondente ao domínio institucional que vier a ser indicado pela ANPD.

A existência de soluções com essa configuração foi verificada no mercado. Há autoridades certificadoras que documentam a inclusão do domínio-base como SAN em certificados Wildcard e soluções comerciais que informam a proteção conjunta do domínio principal e dos respectivos subdomínios. Essa verificação demonstra a disponibilidade e a exequibilidade do requisito, sem implicar indicação de marca ou direcionamento da contratação.

A inclusão do domínio raiz como SAN não transforma o objeto, por si só, em certificado Multi-Domain/SAN destinado à proteção de uma lista ampla de domínios distintos. Trata-se de mecanismo técnico complementar necessário para que o mesmo certificado atenda ao nome Wildcard e ao respectivo domínio raiz.

O certificado Wildcard abrangerá os subdomínios de primeiro nível. Assim, `*.anpd.gov.br` poderá abranger nomes como `portal.anpd.gov.br`, mas não abrangerá nomes situados em nível adicional, como `sistema.interno.anpd.gov.br`.

Como a validade técnica individual dos certificados públicos SSL/TLS será inferior ao período total de 36 meses, serão necessárias emissões sucessivas durante a execução. Todas as validações, emissões, renovações, reemissões, revogações, atividades de gerenciamento e suporte necessárias à manutenção ininterrupta de cada cobertura deverão integrar o respectivo serviço e preço unitário, sem cobrança adicional por certificado, emissão ou evento.

A necessidade possui prioridade alta, conforme registrado no Documento de Formalização da Demanda — DFD. A ausência, a expiração, a revogação ou a emissão inadequada de certificados pode:

- provocar alertas de “site não seguro” nos navegadores;
- impedir ou desencorajar o acesso dos usuários aos serviços digitais;
- comprometer a confidencialidade e a integridade das comunicações;
- aumentar os riscos de interceptação, falsificação de identidade, adulteração de conteúdo, spoofing e phishing;
- causar indisponibilidade prática dos serviços;
- afetar a imagem, a reputação e a confiança institucional; e
- expor indevidamente as informações transmitidas.

O encerramento do acordo de cooperação com o Ministério da Justiça e Segurança Pública — MJSP reforça a necessidade de a ANPD assegurar diretamente a continuidade dessa proteção.

Nesse contexto, a contratação pretende:

- manter o acesso HTTPS confiável e contínuo aos serviços digitais da ANPD;
- proteger a confidencialidade e a integridade dos dados transmitidos;
- autenticar os domínios e os serviços digitais institucionais;
- atender ao domínio raiz e aos subdomínios de primeiro nível;
- permitir a criação ou substituição de subdomínios durante a vigência;
- prevenir alertas decorrentes de certificado inválido ou expirado;
- reduzir os riscos de interceptação, falsificação de identidade, spoofing e phishing;
- assegurar autonomia operacional à ANPD;
- preservar a confiança dos usuários nos serviços digitais da Agência; e
- evitar a realização de nova contratação para outro domínio institucional que demande solução equivalente durante a vigência.

2.3 Motivação e justificativa

A contratação é motivada pela necessidade de preservar a segurança, a confiabilidade e a continuidade dos serviços digitais disponibilizados pela ANPD, assegurando a utilização de conexões HTTPS baseadas em certificados públicos reconhecidos pelos principais navegadores e sistemas operacionais.

Os certificados SSL/TLS contribuem para proteger a confidencialidade e a integridade dos dados transmitidos, autenticar os serviços acessados pelos usuários e reduzir os riscos de interceptação, adulteração de tráfego e falsificação da identidade dos serviços digitais.

A indisponibilidade, a expiração ou a emissão inadequada de certificados pode provocar alertas de segurança nos navegadores, indisponibilidade prática de acesso, perda de confiança dos usuários, danos à imagem institucional e aumento da exposição a ataques de interceptação, spoofing e phishing.

A validação organizacional — OV foi adotada para que, além da comprovação do controle do domínio, seja realizada a validação da identidade da organização responsável pelo serviço. A necessidade e a proporcionalidade desse requisito são analisadas nas seções de levantamento de mercado e comparação das soluções.

A adoção da cobertura Wildcard possibilita proteger os subdomínios de primeiro nível presentes e futuros sem exigir certificado individual para cada nome. Entretanto, como o nome Wildcard não abrange tecnicamente o respectivo domínio raiz, a solução deverá incluir expressamente esse domínio no campo SAN do mesmo certificado.

A contratação de até 2 (dois) serviços decorre da necessidade de manter duas coberturas Wildcard distintas. A primeira possui aplicação definida em `*.anpd.gov.br` e `anpd.gov.br`. A segunda permitirá atender outro domínio institucional sob gestão da ANPD que venha a necessitar da mesma proteção durante a vigência.

A previsão da segunda unidade busca conferir tempestividade ao atendimento da necessidade, reduzir o risco de descontinuidade e evitar a realização de novo procedimento de contratação para solução de mesma natureza e características técnicas. Seu acionamento dependerá da indicação formal do domínio institucional e da efetiva caracterização da necessidade.

O Termo de Referência deverá estabelecer o procedimento de acionamento da segunda unidade, o momento de indicação do domínio, o marco inicial da respectiva cobertura de 36 meses e as condições de faturamento e pagamento, de modo que somente sejam remunerados os serviços efetivamente acionados e prestados.

O prazo de 36 (trinta e seis) meses refere-se à duração da cobertura de cada unidade e não à validade de uma única emissão. Todas as emissões sucessivas, validações, renovações, reemissões, revogações, atividades de gerenciamento e suporte necessárias durante esse período deverão estar incluídas no preço unitário contratado.

A solução é de certificação digital pública para servidores e não se confunde com certificado ICP-Brasil destinado à assinatura digital, à autenticação pessoal ou à identificação de pessoa física ou jurídica.

Conforme registrado no DFD, a demanda possui prioridade alta em razão do encerramento do acordo de cooperação com o Ministério da Justiça e Segurança Pública — MJSP e do risco de descontinuidade operacional.

A demanda encontra-se prevista no PCA 2026, alinhada ao Planejamento Estratégico da ANPD 2024–2027 e vinculada, no PDTIC 2025–2028, ao OE03, ao OE06, à ação A061 e à meta M5.

3. Área requisitante

Área Requisitante	Responsável
Coordenação-Geral de Tecnologia da Informação	Igor de Moura Leite Moreira
Coordenação de Governança de Tecnologia da Informação	Rodrigo Vaz dos Santos

4. Necessidades de Negócio

4. Necessidades de negócio

A ANPD necessita assegurar que seus serviços digitais sejam disponibilizados de forma segura, confiável e contínua, em conformidade com as boas práticas de segurança da informação e com a proteção dos dados transmitidos no exercício de suas competências institucionais.

A ausência, a expiração, a revogação ou a emissão inadequada de certificados digitais públicos SSL/TLS pode:

- provocar alertas de “site não seguro” nos navegadores;
- comprometer ou desencorajar o acesso dos usuários aos serviços digitais;
- causar indisponibilidade prática dos portais e sistemas;
- aumentar os riscos de interceptação, falsificação de identidade e adulteração de conteúdo;
- elevar o risco de exposição indevida das informações transmitidas;

- facilitar ataques de spoofing e phishing; e
- afetar negativamente a imagem, a reputação e a confiança institucional.

Dessa forma, a contratação deverá atender às seguintes necessidades de negócio:

1. Manter acesso HTTPS confiável e contínuo aos serviços digitais institucionais durante 36 (trinta e seis) meses por unidade contratada.

2. Proteger a confidencialidade e a integridade dos dados transmitidos entre os usuários e os serviços digitais da ANPD.

3. Autenticar os domínios e serviços digitais institucionais perante cidadãos, agentes regulados, servidores e demais usuários.

4. Manter cobertura contínua para o domínio curinga `*.anpd.gov.br` e para o domínio raiz `anpd.gov.br`.

5. Assegurar que o domínio raiz `anpd.gov.br` conste expressamente no campo Subject Alternative Name — SAN do mesmo certificado destinado a `*.anpd.gov.br`.

6. Permitir a criação ou substituição de subdomínios de primeiro nível durante a vigência, sem a necessidade de contratar certificados individuais ou alterar uma lista fechada de subdomínios.

7. Possibilitar o atendimento de outro domínio institucional sob gestão da ANPD mediante a segunda unidade, quando a necessidade for formalmente caracterizada.

8. Assegurar que a segunda unidade contemple o nome Wildcard e o respectivo domínio raiz como SAN no mesmo certificado, observadas as mesmas condições técnicas da primeira unidade.

9. Evitar a realização de nova contratação para solução de mesma natureza caso outro domínio institucional necessite de cobertura durante a vigência.

10. Evitar alertas de certificado inválido ou expirado, indisponibilidade prática dos serviços e perda de confiança dos usuários.

11. Reduzir os riscos de interceptação, falsificação de identidade, adulteração de conteúdo, spoofing e phishing.

12. Preservar a imagem, a reputação e a confiabilidade institucional da Agência.

13. Assegurar autonomia operacional à ANPD após o encerramento do acordo de cooperação com o Ministério da Justiça e Segurança Pública — MJSP.

14. Obter previsibilidade dos custos durante o período contratado, sem faturamento adicional por validação, emissão, renovação, reemissão ou revogação.

15. Dispor de suporte técnico e gerenciamento do ciclo de vida dos certificados durante todo o período contratado.

A quantidade máxima de 2 (dois) serviços representa duas coberturas Wildcard distintas, cada uma mantida durante 36 (trinta e seis) meses, e não duas emissões sucessivas do mesmo certificado.

A primeira unidade será destinada a `*.anpd.gov.br`, incluindo `anpd.gov.br` como SAN. A segunda unidade será destinada a outro domínio institucional sob gestão da ANPD, a ser formalmente indicado quando caracterizada a necessidade.

Como a validade técnica individual dos certificados será inferior ao período de cobertura, todas as validações, emissões sucessivas, renovações, reemissões, revogações, atividades de gerenciamento e suporte necessárias deverão integrar o preço unitário de cada serviço. Essas atividades não constituirão unidades adicionais de fornecimento, consumo, faturamento ou pagamento.

O Termo de Referência deverá disciplinar o procedimento de acionamento da segunda unidade, a indicação formal do domínio, o início da respectiva cobertura de 36 meses e as condições de faturamento e pagamento, de modo que somente sejam remunerados os serviços efetivamente acionados e prestados.

Assim, a disponibilização contínua de certificados SSL/TLS válidos para até duas coberturas institucionais constitui condição necessária para a operação segura, confiável e contínua dos serviços digitais da ANPD.

5. Necessidades Tecnológicas

Para atender à demanda da ANPD, a solução deverá contemplar até 2 (dois) serviços de certificação digital pública SSL/TLS do tipo Wildcard, com validação organizacional — OV, cada um com cobertura contínua durante 36 (trinta e seis) meses.

Os certificados deverão ser emitidos por Autoridade Certificadora — AC cuja cadeia de certificação integre os programas de confiança dos principais navegadores e sistemas operacionais utilizados no mercado, garantindo o reconhecimento e a validação pelos clientes de acesso.

A primeira unidade será destinada ao domínio curinga `*.anpd.gov.br` e ao domínio raiz `anpd.gov.br`. A segunda unidade será destinada a outro domínio institucional sob gestão da ANPD, a ser formalmente indicado quando caracterizada a necessidade.

As duas unidades deverão observar os mesmos requisitos técnicos, de segurança, compatibilidade, emissão, gerenciamento e suporte.

5.1 Padrões de certificação e criptografia

A solução deverá atender aos seguintes requisitos:

- certificado digital público SSL/TLS do tipo Wildcard com validação organizacional — OV;
- emissão por Autoridade Certificadora cuja cadeia de certificação esteja presente nos programas de confiança dos navegadores e sistemas operacionais amplamente utilizados;
- conformidade com as Baseline Requirements vigentes do CA/Browser Forum;
- utilização de chave RSA de, no mínimo, 2.048 bits ou de algoritmo de criptografia de curva elíptica — ECC compatível com a infraestrutura da ANPD e admitido pelas normas aplicáveis;
- cobertura dos subdomínios de primeiro nível abrangidos pelo nome Wildcard;
- inclusão obrigatória do respectivo domínio raiz no campo Subject Alternative Name — SAN do mesmo certificado;
- ausência de cobrança adicional pela inclusão do domínio raiz como SAN; e
- emissão de certificado e utilização de chave privada próprios para cada uma das duas coberturas contratadas.

Na primeira unidade, o certificado deverá contemplar:

- `*.anpd.gov.br`; e
- `anpd.gov.br`, incluído expressamente no campo SAN.

Na segunda unidade, o certificado deverá contemplar:

- o nome Wildcard correspondente ao domínio institucional formalmente indicado pela ANPD; e
- o respectivo domínio raiz, incluído expressamente no campo SAN.

A inclusão do domínio raiz como SAN não representa a contratação de dois certificados independentes para a mesma unidade nem transforma o objeto, por si só, em certificado Multi-Domain/SAN destinado a uma lista ampla de domínios distintos. Trata-se de mecanismo técnico complementar necessário ao atendimento conjunto do nome Wildcard e do respectivo domínio raiz.

O nome Wildcard abrangerá somente os subdomínios de primeiro nível. Assim, `*.anpd.gov.br` poderá abranger nomes como `portal.anpd.gov.br` e `sistemas.anpd.gov.br`, mas não abrangerá nomes situados em nível adicional, como `sistema.interno.anpd.gov.br`.

A compatibilidade com TLS 1.2 e TLS 1.3 dependerá da configuração dos servidores, dos aplicativos e das cifras utilizadas pela infraestrutura da ANPD. O certificado deverá ser tecnicamente compatível com esses ambientes, mas a habilitação e a configuração dos protocolos permanecerão sob responsabilidade da ANPD.

5.2 Processo de geração e validação

O processo de geração, validação e emissão deverá observar os seguintes requisitos:

- geração da solicitação de assinatura do certificado — Certificate Signing Request — CSR pela infraestrutura da ANPD;
- geração e custódia da chave privada exclusivamente em ambiente controlado pela ANPD;
- vedação à geração, ao armazenamento ou ao acesso à chave privada pela contratada ou pela Autoridade Certificadora;
- utilização de CSR e chave privada próprios para cada cobertura;
- validação organizacional da ANPD com base no CNPJ e em outras fontes oficiais admitidas pela Autoridade Certificadora;
- validação do controle dos domínios por método admitido pelas Baseline Requirements do CA/Browser Forum, preferencialmente mediante DNS;
- realização de nova validação sempre que exigida pelas normas vigentes ou pela política da Autoridade Certificadora;
- emissão em conformidade com as Baseline Requirements e com as políticas de certificação e declarações de práticas da Autoridade Certificadora;
- inclusão expressa, no certificado emitido, do nome Wildcard e do respectivo domínio raiz; e

- comprovação do atendimento mediante documentação oficial da Autoridade Certificadora e inspeção dos campos do certificado após cada emissão ou reemissão.

A indicação do domínio da segunda unidade deverá ocorrer antes do início do respectivo processo de validação e emissão.

5.3 Compatibilidade

Os certificados emitidos no âmbito dos serviços deverão ser compatíveis com:

- servidores Linux e Windows Server;
- servidores web Apache, NGINX e IIS;
- navegadores Chrome/Chromium, Firefox, Edge e Safari;
- dispositivos móveis e clientes padrão de internet;
- formatos de certificado e de cadeia de confiança utilizados pela infraestrutura da ANPD; e
- ambientes configurados para TLS 1.2 e TLS 1.3.

A compatibilidade deverá abranger o certificado do servidor, os certificados intermediários e a respectiva cadeia de confiança.

5.4 Gestão do ciclo de vida

Cada unidade deverá assegurar cobertura contínua durante 36 (trinta e seis) meses. Esse prazo corresponde à duração do serviço e não à validade de uma única emissão de certificado.

O preço unitário de cada serviço deverá incluir todas as atividades necessárias à manutenção da respectiva cobertura durante os 36 meses, incluindo:

- validações iniciais e periódicas;
- emissões sucessivas;
- renovações;
- reemissões;
- revogações;
- substituições decorrentes de alteração técnica, erro de emissão ou comprometimento de chave;
- gerenciamento do ciclo de vida; e
- suporte técnico.

Essas atividades não poderão gerar cobrança adicional por certificado, emissão, renovação, reemissão, revogação ou evento.

Cada certificado deverá observar o limite máximo de validade vigente na data de sua emissão. Conforme as Baseline Requirements do CA/Browser Forum vigentes na elaboração deste ETP:

- certificados emitidos de 15/03/2026 até 14/03/2027 não poderão possuir validade superior a 200 dias;
- certificados emitidos de 15/03/2027 até 14/03/2029 não poderão possuir validade superior a 100 dias; e
- certificados emitidos a partir de 15/03/2029 não poderão possuir validade superior a 47 dias.

Os limites deverão ser observados conforme a versão vigente das Baseline Requirements na data de cada emissão. Eventual redução posterior da validade máxima não poderá gerar cobrança adicional, pois todas as emissões necessárias estão compreendidas no serviço contratado.

A contratada deverá disponibilizar:

- o certificado emitido;
- os certificados intermediários;
- a cadeia de confiança correspondente;
- os arquivos em formatos interoperáveis adequados à infraestrutura da ANPD;
- orientações para instalação e validação da cadeia;
- mecanismos de consulta ao estado de revogação por OCSP e/ou CRL, conforme as políticas da Autoridade Certificadora; e
- suporte técnico para validação, emissão, instalação, renovação, reemissão, revogação e tratamento de falhas durante toda a cobertura.

O início da cobertura da segunda unidade será definido conforme o acionamento formal previsto no Termo de Referência.

5.5 Segurança

A solução deverá observar os seguintes requisitos de segurança:

- geração e custódia das chaves privadas exclusivamente pela ANPD;
- utilização de chave privada distinta para cada unidade;
- vedação ao compartilhamento da chave privada entre as duas coberturas;
- proteção das chaves privadas por controles de acesso compatíveis com sua criticidade;
- integridade e autenticidade das informações utilizadas na validação organizacional e dos domínios;

- atendimento às boas práticas de segurança aplicáveis aos certificados digitais públicos utilizados em ambientes web;
- revogação e reemissão tempestivas, sem custo adicional, em caso de comprometimento ou suspeita de comprometimento da chave;
- reemissão sem custo adicional em caso de erro de emissão, alteração técnica justificada ou necessidade de substituição do algoritmo;
- disponibilização de informações suficientes para verificação da validade, da cadeia de confiança e do estado de revogação dos certificados; e
- comprovação, após cada emissão, de que o certificado contém o nome Wildcard e o respectivo domínio raiz no campo SAN.

Limite do Wildcard e atendimento obrigatório do domínio raiz: o nome `*.dominio.gov.br` cobre os subdomínios de primeiro nível, mas não cobre, isoladamente, o domínio raiz `dominio.gov.br` nem nomes situados em níveis adicionais. Por essa razão, em cada unidade o respectivo domínio raiz deverá constar expressamente no campo SAN do mesmo certificado Wildcard, sem cobrança adicional.

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

Para assegurar aderência às necessidades da ANPD e conformidade com os padrões aplicáveis à certificação digital pública, os até 2 (dois) serviços SSL/TLS Wildcard OV deverão observar os requisitos complementares descritos nesta seção.

Cada unidade deverá proporcionar cobertura durante 36 (trinta e seis) meses. A primeira será destinada a `*.anpd.gov.br`, incluindo `anpd.gov.br` como SAN. A segunda será destinada a outro domínio institucional sob gestão da ANPD, a ser formalmente indicado quando caracterizada a necessidade, observadas as mesmas condições técnicas e o mesmo preço unitário.

6.1 Requisitos de capacitação

Não há necessidade de capacitação formal ou presencial para usuários finais, pois os certificados serão instalados e administrados pela equipe técnica da ANPD.

A contratada deverá disponibilizar instruções e orientações suficientes para:

- geração da solicitação de assinatura de certificado — CSR;
- validação organizacional;
- validação do controle dos domínios;
- emissão;
- instalação;
- renovação;
- reemissão;
- revogação; e
- verificação da cadeia de confiança.

As orientações essenciais e o atendimento deverão ser disponibilizados em língua portuguesa.

Será admitida documentação técnica complementar em inglês quando se tratar de material padronizado da Autoridade Certificadora, desde que o suporte prestado permita sua adequada compreensão e utilização pela equipe da ANPD.

Deverão ser disponibilizados, quando existentes, guias aplicáveis aos servidores Apache, NGINX e IIS, sem prejuízo de a instalação, a configuração e a administração da infraestrutura permanecerem sob responsabilidade da ANPD.

6.2 Requisitos legais e normativos

A contratação deverá observar, no que for aplicável:

- a Lei nº 14.133/2021;
- a Instrução Normativa SGD/ME nº 94/2022;
- a Instrução Normativa SEGES nº 58/2022;
- a Instrução Normativa SEGES/ME nº 65/2021;
- a Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais — LGPD;
- as Baseline Requirements vigentes do CA/Browser Forum; e
- as demais normas aplicáveis ao objeto.

A solução deverá atender às Baseline Requirements vigentes do CA/Browser Forum, especialmente quanto aos procedimentos de validação, emissão, validade, revogação e gerenciamento de certificados públicos SSL/TLS.

A Autoridade Certificadora deverá manter publicamente disponíveis e atualizadas sua Política de Certificação — Certificate Policy — CP e sua Declaração de Práticas de Certificação — Certification Practice Statement — CPS.

Por não se tratar de certificado destinado à assinatura digital, à autenticação pessoal ou à representação de pessoa física ou jurídica, não será exigida emissão no âmbito da ICP-Brasil. A referência à ICP-Brasil constante da Instrução Normativa SGD/ME nº 94/2022 será observada somente quando aplicável à natureza do objeto.

6.3 Requisitos de manutenção e continuidade

A contratada deverá fornecer as orientações, as correções e o suporte necessários à emissão, à instalação e ao gerenciamento do ciclo de vida dos certificados durante todo o período de cobertura de cada unidade.

A configuração dos servidores, das aplicações, dos protocolos e das cifras permanecerá sob responsabilidade da ANPD.

A Autoridade Certificadora deverá disponibilizar mecanismos de verificação de revogação por Online Certificate Status Protocol — OCSP e/ou Certificate Revocation List — CRL, conforme suas políticas CP/CPS e as Baseline Requirements aplicáveis.

A contratada deverá comunicar tempestivamente à ANPD as indisponibilidades programadas de que tenha conhecimento e que possam afetar:

- os serviços de emissão ou validação;
- os mecanismos de verificação do estado de revogação;
- os repositórios dos certificados intermediários;
- a cadeia de confiança; ou
- outra infraestrutura necessária à execução do serviço.

Os prazos e os canais para essas comunicações deverão ser detalhados no Termo de Referência.

Cada unidade deverá ser mantida durante 36 meses, independentemente da quantidade de emissões tecnicamente necessárias. A redução da validade máxima dos certificados não poderá provocar descontinuidade da cobertura nem cobrança adicional.

6.4 Requisitos temporais

Cada serviço deverá assegurar cobertura contínua durante 36 (trinta e seis) meses. Esse período corresponde à duração da prestação do serviço, e não à validade de uma única emissão de certificado.

Para a primeira unidade, o marco inicial da cobertura será definido no Termo de Referência e no instrumento contratual. Para a segunda unidade, o prazo de cobertura será contado conforme o acionamento formal e o marco inicial estabelecido no Termo de Referência.

O preço unitário de cada serviço deverá incluir todas as:

- validações;
- emissões sucessivas;
- renovações;
- reemissões;
- revogações;
- atividades de gerenciamento; e
- atividades de suporte

necessárias à manutenção ininterrupta da respectiva cobertura durante 36 meses, sem cobrança adicional por certificado, emissão ou evento.

Cada certificado deverá observar a validade máxima estabelecida nas Baseline Requirements vigentes do CA/Browser Forum. Na data de elaboração deste ETP, estão previstos os seguintes limites:

- até 200 dias para certificados emitidos de 15/03/2026 até 14/03/2027;
- até 100 dias para certificados emitidos de 15/03/2027 até 14/03/2029; e
- até 47 dias para certificados emitidos a partir de 15/03/2029.

Deverá prevalecer o limite máximo vigente na data de cada emissão. Eventual alteração normativa que reduza a validade dos certificados não poderá gerar cobrança adicional nem afastar a obrigação de manutenção contínua da cobertura durante os 36 meses.

A emissão deverá ocorrer em até 5 (cinco) dias úteis, contados da conclusão, pela ANPD, de todas as providências, do fornecimento das informações e das validações sob sua responsabilidade, desde que não exista pendência externa devidamente comprovada.

A reemissão e o atendimento das solicitações de suporte deverão ocorrer em até 2 (dois) dias úteis, observada a criticidade do incidente e os níveis de atendimento a serem detalhados no Termo de Referência.

Os prazos de 5 e 2 dias úteis deverão ser confirmados pela equipe técnica antes da aprovação do Termo de Referência, especialmente quanto ao marco inicial de contagem, às hipóteses de suspensão justificável e ao tratamento de incidentes críticos.

Em caso de comprometimento ou suspeita de comprometimento da chave, erro de emissão, alteração da infraestrutura, substituição de algoritmo ou outra necessidade tecnicamente justificada, a reemissão e, quando cabível, a revogação deverão ocorrer sem custo adicional durante o período de cobertura.

6.5 Requisitos sociais, ambientais e culturais

Sustentabilidade

O serviço deverá ser solicitado, emitido, entregue e gerenciado eletronicamente, sem utilização de mídia física, embalagem ou geração direta de resíduos eletrônicos.

Eficiência logística

A validação, a emissão, a renovação, a reemissão, a revogação e o suporte deverão ser realizados remotamente, evitando deslocamentos e transporte de mídias.

Idioma e acessibilidade da informação

O atendimento e as orientações essenciais deverão ser disponibilizados em língua portuguesa.

Documentação técnica complementar padronizada poderá ser fornecida em inglês, desde que o suporte permita sua compreensão e utilização adequada pela equipe técnica da ANPD.

Inclusão e confiança digital

A utilização de conexões HTTPS com certificados públicos válidos deverá contribuir para a segurança, a acessibilidade e a confiança dos usuários nos serviços digitais da Agência.

6.6 Requisitos de garantia e suporte

A contratada será responsável pelo cumprimento das obrigações de validação, emissão, renovação, reemissão, revogação, gerenciamento e suporte durante os 36 meses de cobertura de cada unidade.

A atuação de revendedora, representante ou Autoridade Certificadora não afastará a responsabilidade integral da contratada perante a ANPD.

A contratada não responderá por falhas comprovadamente decorrentes exclusivamente de:

- configuração inadequada da infraestrutura pela ANPD;
- falhas nos servidores ou nas aplicações da ANPD;
- utilização indevida do certificado pela ANPD; ou
- comprometimento causado exclusivamente por descumprimento dos procedimentos de custódia da chave privada sob responsabilidade da ANPD.

Essa exclusão não afastará a obrigação de a contratada prestar orientação e suporte para diagnóstico, revogação e reemissão quando o evento estiver abrangido pelo objeto.

Falhas imputáveis à contratada, à Autoridade Certificadora ou à cadeia de fornecimento deverão ser corrigidas sem custo adicional e dentro dos prazos estabelecidos.

O suporte deverá abranger orientação técnica para:

- solicitação;
- validação organizacional;
- validação dos domínios;
- emissão;
- instalação;
- verificação da cadeia de confiança;
- renovação;
- reemissão;
- revogação; e
- tratamento de incidentes relacionados aos certificados ou aos mecanismos de verificação de seu estado.

Os canais, horários, níveis de prioridade, prazos de resposta e prazos de solução deverão ser definidos no Termo de Referência.

6.7 Requisitos de segurança e privacidade

Geração e custódia das chaves privadas

A CSR e a respectiva chave privada deverão ser geradas exclusivamente em infraestrutura controlada pela ANPD.

A chave privada permanecerá sob domínio integral da Agência e não poderá ser gerada, armazenada, copiada, manipulada ou acessada pela contratada ou pela Autoridade Certificadora.

Cada unidade deverá possuir CSR, certificado e chave privada próprios. Não será permitido compartilhar a mesma chave privada entre as duas coberturas distintas.

A ANPD será responsável pelo armazenamento protegido, pelo controle de acesso, pelo inventário, pela distribuição, pela rotação e pela resposta a eventual comprometimento das chaves privadas.

Criptografia robusta

O certificado deverá admitir chave RSA de, no mínimo, 2.048 bits ou algoritmo ECC equivalente, compatível com a infraestrutura da ANPD e admitido pelas normas vigentes.

A solução não poderá exigir algoritmo ou tamanho de chave obsoleto ou incompatível com a infraestrutura da Agência.

Validação organizacional — OV

A contratada deverá viabilizar a validação da identidade organizacional da ANPD mediante consulta ao CNPJ e às demais fontes oficiais admitidas pela Autoridade Certificadora.

A validação do controle dos domínios deverá utilizar método previsto nas Baseline Requirements vigentes do CA/Browser Forum, preferencialmente mediante DNS e sem exigir o fornecimento das chaves privadas.

Para a primeira unidade, a validação deverá abranger `*.anpd.gov.br` e `anpd.gov.br`. Para a segunda, deverá abranger o nome Wildcard e o domínio raiz formalmente indicados pela ANPD.

Atendimento obrigatório do domínio raiz

Em cada unidade, o respectivo domínio raiz deverá constar expressamente no campo Subject Alternative Name — SAN do mesmo certificado Wildcard, sem cobrança adicional.

A contratada deverá comprovar esse atendimento:

- por documentação oficial da Autoridade Certificadora; e
- após cada emissão ou reemissão, pela inspeção dos campos do certificado emitido.

Proteção das comunicações

O certificado deverá viabilizar a autenticação dos serviços e o estabelecimento de conexões HTTPS protegidas quanto à confidencialidade e à integridade, contribuindo para mitigar os riscos de interceptação, adulteração de tráfego, falsificação de identidade, spoofing e phishing.

A efetiva segurança das conexões também dependerá da correta configuração dos servidores, das aplicações, dos protocolos e das cifras pela ANPD.

Tratamento de dados pessoais

Não se prevê tratamento de dados pessoais sensíveis, utilização de biometria ou realização de procedimento presencial para a execução ordinária do objeto.

Os eventuais dados pessoais de representantes, responsáveis ou contatos necessários à validação deverão:

- limitar-se ao mínimo necessário;
- ser utilizados exclusivamente para a execução do objeto;
- ser protegidos contra acessos indevidos;
- ser mantidos somente pelo período necessário; e
- ser tratados em conformidade com a LGPD e com as demais normas aplicáveis.

Revogação e resposta a incidentes

Em caso de suspeita ou confirmação de comprometimento da chave privada, emissão incorreta, alteração relevante das informações validadas ou outro evento previsto nas políticas da Autoridade Certificadora, a contratada deverá orientar e viabilizar a revogação e a reemissão tempestivas, sem custo adicional.

Os prazos e os procedimentos para incidentes críticos deverão ser detalhados no Termo de Referência.

Segregação e controle de acesso

As solicitações, aprovações e instalações deverão ser executadas por agentes autorizados pela ANPD, com aplicação do princípio do menor privilégio e registro das operações relevantes, conforme os controles internos da Agência.

Padrões de segurança

A infraestrutura da ANPD deverá operar com TLS 1.2 ou TLS 1.3, mantendo desabilitados protocolos e cifras obsoletos.

A contratada deverá fornecer certificados e cadeias de confiança compatíveis com esses ambientes, sem que isso transfira a ela a responsabilidade pela configuração ou pela segurança integral dos servidores e das aplicações da ANPD.

6.8 Requisitos de qualidade e padronização

A solução deverá assegurar:

- compatibilidade com Linux e Windows Server;
- compatibilidade com Apache, NGINX e IIS;
- compatibilidade com Chrome/Chromium, Firefox, Edge e Safari;
- compatibilidade com dispositivos móveis e clientes padrão de internet;
- conformidade com as Baseline Requirements vigentes do CA/Browser Forum;
- conformidade com as políticas CP/CPS da Autoridade Certificadora;
- disponibilidade dos mecanismos de verificação de revogação previstos nas normas e nas políticas públicas da Autoridade Certificadora;
- disponibilização dos certificados intermediários e da cadeia de confiança;
- fornecimento em formatos interoperáveis adequados à infraestrutura da ANPD;
- inclusão do respectivo domínio raiz como SAN no mesmo certificado Wildcard;
- aplicação dos mesmos requisitos de qualidade às duas unidades; e
- ausência de limitação indevida do número de emissões necessárias durante os 36 meses.

6.9 Outros requisitos

Responsabilidade integral

Será admitido que a contratada atue como revendedora ou representante de Autoridade Certificadora.

Essa relação comercial não afastará a responsabilidade integral da contratada perante a ANPD pelo cumprimento do objeto e pela coordenação da cadeia de fornecimento.

Correção de falhas

Os procedimentos executados em desacordo com as condições pactuadas deverão ser repetidos ou corrigidos às expensas da contratada, sem custo adicional para a ANPD.

Segregação de funções

As solicitações e as aprovações de emissão deverão ser realizadas por servidores ou agentes autorizados pela ANPD, conforme seus controles internos.

Segunda unidade

A segunda unidade será destinada a outro domínio institucional sob gestão da ANPD, formalmente indicado antes do início da validação e da emissão.

O Termo de Referência deverá disciplinar:

- o procedimento de acionamento;
- a indicação formal do domínio;
- o marco inicial da cobertura de 36 meses;
- os responsáveis pela autorização;
- as condições de faturamento; e
- as condições de pagamento.

Competitividade

Não será exigida marca ou Autoridade Certificadora específica.

Os requisitos deverão ser aferidos pelo resultado técnico pretendido, incluindo:

- validação organizacional — OV;
- confiança pública da cadeia de certificação;
- cobertura Wildcard;
- inclusão do respectivo domínio raiz no campo SAN do mesmo certificado;
- compatibilidade;
- continuidade da cobertura durante 36 meses; e

- suporte e gerenciamento do ciclo de vida.

A indicação de fabricantes ou autoridades certificadoras na pesquisa de mercado e na Nota Técnica possui finalidade exclusivamente referencial e demonstrativa da disponibilidade da solução, não constituindo direcionamento da contratação

7. Estimativa da demanda - quantidade de bens e serviços

A ANPD necessita contratar até 2 (dois) serviços de certificação digital pública SSL/TLS do tipo Wildcard, com validação organizacional — OV, cada um com cobertura contínua durante 36 (trinta e seis) meses.

A primeira unidade será destinada à proteção do domínio curinga `*.anpd.gov.br` e do domínio raiz `anpd.gov.br`.

A segunda unidade será destinada a outro domínio institucional sob gestão da ANPD, a ser formalmente indicado quando caracterizada a necessidade, observadas as mesmas características técnicas, o mesmo período de cobertura e o mesmo preço unitário da primeira unidade.

Cada serviço deverá contemplar todas as validações, emissões sucessivas, renovações, reemissões, revogações, atividades de gerenciamento e suporte necessárias à manutenção ininterrupta da respectiva proteção HTTPS durante os 36 meses.

A cobertura Wildcard abrangerá os subdomínios de primeiro nível existentes e aqueles que forem criados ou substituídos durante o período de cobertura, sem limitação a uma lista fechada de nomes e sem cobrança adicional por subdomínio abrangido.

A relação de subdomínios eventualmente existente possui natureza meramente operacional e poderá ser alterada durante a execução. Ela não integra uma lista fechada de Subject Alternative Names — SAN nem constitui parâmetro para a quantidade contratada.

O nome Wildcard não cobre tecnicamente, por si só, o respectivo domínio raiz. Por essa razão, em cada unidade o domínio raiz deverá constar expressamente no campo SAN do mesmo certificado, sem cobrança adicional.

Na primeira unidade, o certificado deverá contemplar `*.anpd.gov.br` e `anpd.gov.br`. Na segunda unidade, deverá contemplar o nome Wildcard e o respectivo domínio raiz formalmente indicados pela ANPD.

Nomes situados em níveis adicionais, como `sistema.interno.anpd.gov.br`, não são abrangidos pelo nome Wildcard `*.anpd.gov.br` e não integram automaticamente a cobertura.

Em razão da redução progressiva da validade máxima dos certificados públicos TLS, serão necessárias múltiplas emissões durante os 36 meses. Conforme as Baseline Requirements vigentes do CA/Browser Forum na data de elaboração deste ETP, os certificados estarão sujeitos aos limites máximos de 200, 100 ou 47 dias, a depender da data de emissão.

Não é possível nem adequado fixar antecipadamente a quantidade exata de emissões, pois ela dependerá:

- da data de início da cobertura de cada unidade;
- das regras vigentes na data de cada emissão;
- da duração efetivamente atribuída pela Autoridade Certificadora;
- das validações exigidas;
- de eventual comprometimento da chave privada;
- de erros de emissão;
- de alterações justificadas da infraestrutura; e
- de outras hipóteses de revogação ou reemissão previstas nas normas ou nas políticas da Autoridade Certificadora.

Por essa razão, o quantitativo foi dimensionado pelo número máximo de coberturas Wildcard distintas, e não pelo número de certificados tecnicamente emitidos durante a execução.

Item	Descrição	Métrica	Qtd.	Vigência
1	Serviço SSL/TLS Wildcard OV para *.anpd.gov.br e anpd.gov.br, incluindo todas as emissões sucessivas, atividades de gerenciamento e suporte	Serviço	2	36 meses

7.1 Memória do quantitativo

Cobertura contínua de `*.anpd.gov.br` e `anpd.gov.br` × período total de 36 meses = 2 serviços completos.

Todas as emissões técnicas necessárias integram o preço global.

O quantitativo de 2 (dois) serviços representa o resultado completo a ser mantido durante o período total de 36 (trinta e seis) meses e serve de base para o planejamento e a formação do preço referencial. Não corresponde a uma franquia de certificados nem a uma estimativa de consumo de emissões.

A emissão, a validação, a renovação, a reemissão e a revogação ocorrerão conforme a necessidade técnica para assegurar a continuidade da proteção criptográfica, sem alterar a quantidade contratada ou gerar cobrança adicional.

A cobertura obrigatória compreende o domínio raiz `anpd.gov.br` e os subdomínios de primeiro nível presentes ou futuramente criados sob `*.anpd.gov.br`, sem limitação a uma lista fechada de FQDNs.

A raiz poderá ser incluída como SAN adicional no mesmo certificado Wildcard, conforme a solução ofertada. Nomes em níveis mais profundos não integram o objeto.

A especificação por requisitos de validação OV, confiança pública, compatibilidade, cobertura Wildcard e atendimento ao domínio raiz preserva a competitividade, sem indicação de marca ou de Autoridade Certificadora específica.

8. Levantamento de soluções

O levantamento de mercado considerou alternativas disponíveis para emissão e gerenciamento de certificados digitais públicos SSL/TLS, avaliando:

- os níveis de validação;
- as formas de cobertura dos domínios;
- os modelos operacionais de prestação;
- a compatibilidade com a infraestrutura da ANPD;
- o esforço de implantação e gerenciamento;
- os riscos de indisponibilidade;
- a necessidade de emissões sucessivas;
- o período de cobertura de 36 meses;
- a possibilidade de atendimento de até duas coberturas distintas; e
- os custos diretos e indiretos associados a cada alternativa.

A primeira cobertura será destinada ao domínio curinga `*.anpd.gov.br` e ao domínio raiz `anpd.gov.br`. A segunda será destinada a outro domínio institucional sob gestão da ANPD, a ser formalmente indicado quando caracterizada a necessidade.

Em cada unidade, o respectivo domínio raiz deverá constar no campo Subject Alternative Name — SAN do mesmo certificado Wildcard, sem cobrança adicional.

8.1. Alternativas avaliadas

Solução 1 — Certificado SSL/TLS DV

O certificado SSL/TLS com validação de domínio — DV comprova o controle do domínio e permite o estabelecimento de conexões HTTPS protegidas.

Entretanto, essa alternativa não realiza a validação da identidade organizacional do solicitante. Considerando que a solução definida neste ETP exige validação organizacional — OV, o certificado DV não atende integralmente aos requisitos estabelecidos.

A não escolha dessa alternativa decorre da diferença no nível de validação, e não de insuficiência dos mecanismos criptográficos empregados pelos certificados DV.

Solução 2 — Certificados individuais OV

Os certificados individuais OV realizam a validação organizacional e poderiam proteger separadamente o domínio raiz e cada subdomínio institucional.

Contudo, essa alternativa exigiria certificado, chave privada, validação, instalação, monitoramento, renovação e controle separados para cada nome protegido.

Além de aumentar o esforço operacional, a alternativa não oferece cobertura automática para novos subdomínios. A criação de cada novo nome poderia exigir nova emissão, instalação e gerenciamento individualizado, tornando a solução menos flexível e mais complexa que a cobertura Wildcard.

Solução 3 — Certificado Multi-Domain/SAN OV

O certificado Multi-Domain/SAN OV realiza validação organizacional e permite reunir vários nomes de domínio totalmente qualificados — FQDNs — em uma lista explícita no mesmo certificado.

A alternativa poderia atender aos nomes conhecidos no momento da emissão. Entretanto, a inclusão ou a substituição de subdomínios exigiria alteração da lista de SANs e reemissão do certificado.

Esse modelo apresenta menor flexibilidade para ambientes em que novos subdomínios de primeiro nível podem ser criados ou substituídos durante a vigência.

A inclusão do respectivo domínio raiz como SAN no certificado Wildcard não transforma a solução escolhida, por si só, em certificado Multi-Domain/SAN destinado a uma lista ampla ou fechada de domínios distintos. Nesse caso, o SAN é utilizado como mecanismo técnico complementar para atendimento do domínio raiz, que não é abrangido isoladamente pelo nome Wildcard.

Solução 4 — Serviço SSL/TLS Wildcard OV por 36 meses

O serviço SSL/TLS Wildcard OV realiza validação organizacional e protege os subdomínios de primeiro nível abrangidos pelo nome Wildcard, inclusive aqueles que forem criados ou substituídos durante o período de cobertura.

Para atender integralmente à necessidade, o respectivo domínio raiz deverá constar expressamente no campo Subject Alternative Name — SAN do mesmo certificado Wildcard, sem cobrança adicional.

A solução permitirá a contratação de até 2 (dois) serviços, cada um com cobertura contínua durante 36 (trinta e seis) meses:

- a primeira unidade será destinada a `*.anpd.gov.br`, incluindo obrigatoriamente `anpd.gov.br` como SAN; e
- a segunda unidade será destinada ao nome Wildcard e ao respectivo domínio raiz de outro domínio institucional sob gestão da ANPD, a ser formalmente indicado quando caracterizada a necessidade.

A quantidade máxima de 2 (dois) serviços representa duas coberturas Wildcard distintas, e não duas emissões sucessivas do mesmo certificado.

Cada unidade deverá incluir, em seu preço unitário para 36 meses, todas as validações, emissões sucessivas, renovações, reemissões, revogações, atividades de gerenciamento e suporte necessárias à manutenção ininterrupta da respectiva cobertura.

O período de 36 meses corresponde à duração da cobertura de cada serviço e não à validade de uma única emissão. Considerando que a validade técnica individual dos certificados será inferior a esse período, deverão ser realizadas todas as emissões sucessivas necessárias, sem cobrança adicional por certificado, emissão ou evento.

Nomes situados em níveis adicionais, como `sistema.interno.anpd.gov.br`, não são automaticamente abrangidos pelo nome `*.anpd.gov.br` e não integram a cobertura dessa unidade.

A primeira unidade possui destinação definida. A segunda deverá ser acionada mediante indicação formal do domínio institucional, conforme procedimento, marco inicial da cobertura e condições de pagamento estabelecidos no Termo de Referência.

Essa é a solução escolhida.

Solução 5 — Certificado SSL/TLS EV

O certificado SSL/TLS com validação estendida — EV adota procedimento ampliado de verificação da identidade e da existência da organização solicitante.

Essa alternativa acrescenta requisitos, tempo de validação e custos sem benefício proporcional demonstrado para a necessidade analisada.

Além disso, certificados EV não admitem nomes Wildcard nas condições aplicáveis aos certificados públicos TLS. Por essa razão, a alternativa não atende ao requisito de cobertura de `*.anpd.gov.br` nem à cobertura Wildcard prevista para a segunda unidade.

Diante da incompatibilidade com o núcleo funcional do objeto e da ausência de vantagem proporcional, a alternativa não foi escolhida.

Solução 6 — Certificados DV automatizados e gratuitos

Soluções automatizadas e gratuitas, como Let's Encrypt, podem emitir certificados publicamente confiáveis e automatizar processos de emissão e renovação, inclusive em determinados cenários Wildcard mediante validação por DNS.

Essas soluções são tecnicamente capazes de estabelecer conexões HTTPS protegidas. Entretanto, utilizam validação de domínio — DV — e não realizam a validação da identidade organizacional do solicitante.

A adoção dessa alternativa também dependeria da avaliação, implantação e manutenção de mecanismos internos de automação, gerenciamento de credenciais, publicação de registros DNS, monitoramento, tratamento de falhas e resposta a incidentes.

Considerando o requisito de validação organizacional — OV estabelecido neste ETP, a alternativa DV automatizada não atende integralmente à solução definida pela ANPD.

A não escolha decorre do nível de validação e do modelo operacional, e não do caráter gratuito da solução ou de insuficiência de seus mecanismos criptográficos.

Solução 7 — Serviço gerenciado associado a plataforma de borda ou hospedagem

Serviços de borda, CDN, nuvem ou hospedagem podem incluir a emissão e o gerenciamento de certificados para os sistemas integrados à respectiva plataforma.

Essa alternativa pode reduzir o esforço operacional de emissão e renovação quando todos os serviços digitais estão hospedados ou integrados à mesma plataforma.

Contudo, sua adoção depende da arquitetura de hospedagem e segurança utilizada pela ANPD, pode introduzir dependência tecnológica adicional e pode limitar a portabilidade dos certificados ou sua utilização fora da respectiva plataforma.

Não foi demonstrado que uma única plataforma gerenciada seja compatível com todos os serviços e ambientes que deverão ser protegidos, nem que possa fornecer, de forma independente, as duas coberturas Wildcard OV pretendidas.

Por essas razões, a alternativa não foi escolhida para o cenário atual.

Considerações sobre a prospecção de mercado

A prospecção considerou:

- necessidades similares identificadas em contratações de outros órgãos;
- alternativas disponíveis no mercado;
- diferentes níveis de validação;
- diferentes modelos de cobertura;
- diferentes formas de prestação e pagamento;
- referências de contratações públicas; e
- preços publicados em sítios oficiais de autoridades certificadoras e canais especializados.

A pesquisa formal foi materializada na Pesquisa de Preços nº 123/2026, UASG 302122, e na respectiva Nota Técnica.

Foram analisadas contratações públicas obtidas no Compras.gov.br e, de forma complementar, preços publicados nos sítios da Sectigo Brasil, SSL.com e DigiCert, nos termos do art. 5º, inciso III, da Instrução Normativa SEGES/ME nº 65/2021.

A consulta aos fornecedores possui finalidade de levantamento de mercado e formação do valor estimado. A menção às empresas não representa indicação de marca, direcionamento ou restrição à participação de outras autoridades certificadoras, representantes ou revendedores que atendam integralmente aos requisitos.

Caso tenha sido realizada e documentada consulta ao Catálogo de Soluções de TIC com Condições Padronizadas do SISP, poderá ser registrado o seguinte:

Em consulta realizada ao Catálogo de Soluções de TIC com Condições Padronizadas do SISP, não foi localizada solução padronizada correspondente ao objeto. A data e o resultado da consulta encontram-se registrados nos autos.

Esse parágrafo somente deverá ser mantido se a consulta e sua data estiverem comprovadas no processo.

Não são necessárias obras, aquisição de equipamentos, adequações elétricas, mídia física ou instalação presencial para a execução do objeto.

A ANPD deverá manter capacidade operacional para:

- gerar as CSRs;
- gerar e custodiar as chaves privadas;
- manter chave privada distinta para cada unidade;
- publicar os registros DNS necessários à validação;
- instalar os certificados e as respectivas cadeias de confiança;
- controlar o acesso às chaves privadas;
- monitorar a validade e o funcionamento dos certificados;
- solicitar emissões, reemissões e revogações; e
- acompanhar a execução dos dois serviços.

8.2 Justificativa preliminar da solução escolhida

A alternativa mais aderente à necessidade é a contratação de até 2 (dois) serviços SSL/TLS Wildcard com validação organizacional — OV, cada um com cobertura contínua durante 36 (trinta e seis) meses.

A primeira unidade será destinada a `*.anpd.gov.br`, incluindo obrigatoriamente `anpd.gov.br` no campo SAN do mesmo certificado.

A segunda unidade será destinada ao nome Wildcard e ao respectivo domínio raiz de outro domínio institucional sob gestão da ANPD, a ser formalmente indicado quando caracterizada a necessidade.

A solução foi escolhida porque:

- realiza validação organizacional — OV;
- permite verificar, durante o processo de emissão, a identidade da organização responsável pelos domínios;
- possui cadeia de certificação integrante dos programas de confiança dos principais navegadores e sistemas operacionais;
- cobre os subdomínios de primeiro nível existentes e aqueles criados durante o período de cobertura;
- não depende de uma lista fechada de subdomínios;
- inclui obrigatoriamente o respectivo domínio raiz como SAN no mesmo certificado;
- reduz a quantidade de certificados, chaves, validações, instalações e controles separados em comparação com certificados individuais;
- permite atender outro domínio institucional por meio da segunda unidade;
- inclui todas as validações, emissões sucessivas, renovações, reemissões e revogações necessárias durante os 36 meses;
- inclui gerenciamento e suporte durante todo o período de cobertura;
- estabelece preço unitário por serviço para os 36 meses;
- evita cobrança adicional em razão da quantidade de emissões tecnicamente necessárias;
- proporciona previsibilidade de custos;
- atende às Baseline Requirements vigentes do CA/Browser Forum; e
- apresenta relação adequada entre aderência funcional, segurança, esforço operacional e custo.

A validação OV não elimina, isoladamente, os riscos de falsificação de identidade, spoofing ou phishing. A mitigação desses riscos depende da combinação entre validação organizacional, controle dos domínios, configuração segura dos servidores, proteção das chaves privadas, segurança do DNS, monitoramento e demais controles adotados pela ANPD.

A quantidade máxima de 2 (dois) serviços representa duas coberturas Wildcard distintas, e não duas emissões sucessivas do mesmo certificado.

Cada unidade deverá possuir certificado, CSR e chave privada próprios. Todas as emissões tecnicamente necessárias durante os 36 meses deverão integrar o preço unitário, sem cobrança adicional por emissão ou evento.

A segunda unidade dependerá de acionamento e indicação formal do domínio institucional. O Termo de Referência deverá estabelecer o procedimento de acionamento, o marco inicial da cobertura e as condições de faturamento e pagamento.

A escolha não indica marca nem Autoridade Certificadora específica. A solução deverá ser avaliada pelo atendimento aos requisitos objetivos de:

- confiança pública da cadeia de certificação;
- validação organizacional — OV;
- cobertura Wildcard;
- inclusão obrigatória do respectivo domínio raiz como SAN;
- compatibilidade;
- segurança;
- continuidade da cobertura;
- gerenciamento do ciclo de vida; e
- suporte técnico.

9. Análise comparativa de soluções

A análise comparativa foi realizada considerando critérios de segurança, nível de validação, conformidade, interoperabilidade, confiança pública, cobertura funcional, esforço operacional, custo e adequação ao contexto tecnológico da ANPD.

Também foram considerados:

- a necessidade de até duas coberturas Wildcard distintas;
- a inclusão obrigatória do respectivo domínio raiz como SAN;
- o período de cobertura de 36 meses por unidade;
- a necessidade de emissões sucessivas;
- o gerenciamento do ciclo de vida;
- a compatibilidade com a infraestrutura existente; e
- a previsibilidade dos custos.

Como o nível de validação e o modelo de cobertura representam dimensões diferentes da solução, a análise foi dividida em duas matrizes.

9.1. Matriz comparativa dos níveis de validação

Critério	DV	OV — escolhido	EV
Validação do controle do domínio	Realiza	Realiza	Realiza
Validação da identidade organizacional	Não realiza	Realiza	Realiza de forma ampliada
Atendimento ao requisito institucional da ANPD	Não atende	Atende	Excede o necessário
Contribuição para autenticação institucional e mitigação de falsificação de identidade	Limitada à posse do domínio	Adequada ao identificar a organização	Ampliada, sem benefício proporcional demonstrado
Compatibilidade com navegadores modernos	Atende	Atende	Atende
Compatibilidade com cobertura Wildcard	Admite, conforme a solução	Admite	Não admite para o objeto
Custo relativo esperado	Baixo	Moderado	Alto
Resultado	Inviável por não validar a organização	Viável e escolhido	Inviável por custo, excesso de requisitos e incompatibilidade com Wildcard

A validação OV apresenta equilíbrio entre validação da identidade organizacional, compatibilidade, custo e aderência à necessidade definida pela ANPD.

A validação DV comprova o controle do domínio e permite o estabelecimento de conexões HTTPS protegidas, mas não realiza a validação da organização solicitante. Por essa razão, não atende integralmente ao requisito estabelecido neste ETP.

A validação EV acrescenta verificações, tempo de processamento e custos sem benefício proporcional demonstrado para o caso. Além disso, certificados EV não admitem nomes Wildcard, o que impede o atendimento ao núcleo funcional do objeto.

A validação OV não elimina, isoladamente, os riscos de falsificação de identidade, spoofing ou phishing. Sua contribuição ocorre por meio da verificação da organização durante o processo de emissão e deve ser combinada com controles de DNS, proteção das chaves privadas, configuração segura dos servidores, monitoramento e resposta a incidentes.

9.2. Matriz comparativa dos modelos de cobertura e prestação

Critério	OV individual	OV Multi-Domain/SAN	OV Wildcard — escolhido	DV automatizado	Serviço gerenciado de plataforma
Cobertura dos subdomínios atuais	Atende mediante múltiplos certificados	Atende mediante lista explícita	Atende aos subdomínios de primeiro nível	Atende tecnicamente, sem OV	Depende da plataforma
Novos subdomínios de primeiro nível sem alteração de lista	Não atende	Não atende	Atende	Pode atender mediante automação	Depende da plataforma
Atendimento ao respectivo domínio raiz	Exige certificado próprio	Atende mediante inclusão na lista de SANs	Atende mediante inclusão obrigatória da raiz como SAN no mesmo certificado	Pode atender tecnicamente, sem OV	Depende da plataforma

Validação organizacional — OV	Atende	Atende	Atende	Não atende	Não demonstrada para todos os ambientes
Necessidade de lista fechada de nomes	Sim, por certificado	Sim	Não para os subdomínios de primeiro nível	Não necessariamente	Depende da plataforma
Esforço operacional	Alto	Médio	Moderado e centralizado	Baixo após implantação da automação	Pode ser baixo, com dependência da plataforma
Isolamento de chaves entre subdomínios	Alto	Baixo quando utilizado certificado único	Baixo dentro de cada cobertura Wildcard	Pode ser alto	Depende da arquitetura
Isolamento de chaves entre as duas unidades	Possível	Possível	Obrigatório: cada unidade terá chave própria	Possível	Depende da plataforma
Cobertura por 36 meses	Exigiria múltiplos certificados e controles	Possível, sujeita à gestão da lista	Atende com todas as emissões sucessivas incluídas	Possível mediante automação, mas sem OV	Não demonstrada de forma independente
Previsibilidade do custo	Menor, devido à multiplicidade de certificados	Sujeita à quantidade de nomes e alterações	Preço unitário por cobertura para 36 meses	Baixo custo de emissão, com custos internos de automação	Vinculada ao modelo comercial da plataforma
Atendimento de até duas coberturas distintas	Exigiria várias unidades	Possível mediante listas separadas	Atende mediante duas unidades Wildcard independentes	Possível tecnicamente, sem OV	Depende da arquitetura
Aderência às referências pesquisadas	Parcial	Parcial	Maior aderência	Não comparável quanto à validação OV	Não comparável por vinculação à plataforma
Resultado	Não escolhido por maior complexidade operacional	Não escolhido por depender de lista fechada	**Viável e escolhido**	Não escolhido por ausência de OV	Não escolhido no cenário atual

Os certificados individuais OV são tecnicamente capazes de atender aos nomes conhecidos, mas exigiriam múltiplos certificados, chaves, validações, instalações, monitoramentos e renovações.

O certificado Multi-Domain/SAN OV também é tecnicamente possível, mas depende de uma lista explícita de nomes. A inclusão ou substituição de subdomínios exigiria alteração da lista e reemissão.

A solução OV Wildcard permite cobrir os subdomínios de primeiro nível presentes e futuros sem manter lista fechada. O respectivo domínio raiz deverá ser incluído obrigatoriamente como SAN no mesmo certificado.

A inclusão da raiz como SAN não transforma, por si só, a solução em certificado Multi-Domain/SAN destinado a uma lista ampla de domínios distintos. O SAN é utilizado como mecanismo complementar para atender ao domínio raiz que não é abrangido isoladamente pelo nome Wildcard.

9.3. Conclusão da análise comparativa

A combinação entre validação organizacional — OV e cobertura Wildcard é a alternativa que melhor equilibra validação da organização, confiança pública, compatibilidade, flexibilidade, esforço operacional e custo para o contexto da ANPD.

A solução permitirá a contratação de até 2 (dois) serviços distintos, cada um com cobertura durante 36 (trinta e seis) meses:

- primeira unidade: `*.anpd.gov.br`, com inclusão obrigatória de `anpd.gov.br` como SAN no mesmo certificado; e
- segunda unidade: nome Wildcard e respectivo domínio raiz de outro domínio institucional sob gestão da ANPD, a ser formalmente indicado.

Cada unidade deverá possuir CSR, certificado e chave privada próprios. Não será permitido utilizar a mesma chave privada para as duas coberturas distintas.

Dentro de cada unidade, o certificado Wildcard poderá ser instalado nos servidores que hospedem os subdomínios abrangidos. Essa característica exige controles de inventário, distribuição, armazenamento, acesso, rotação, monitoramento e revogação da chave privada.

A quantidade máxima de 2 (dois) serviços representa duas coberturas Wildcard distintas, e não duas emissões sucessivas do mesmo certificado.

O período de 36 meses corresponde à duração da cobertura de cada unidade. Como a validade técnica individual dos certificados será inferior, todas as validações, emissões sucessivas, renovações, reemissões, revogações, atividades de gerenciamento e suporte necessárias deverão estar incluídas no preço unitário de cada serviço, sem cobrança adicional por certificado, emissão ou evento.

A segunda unidade será acionada mediante indicação formal do domínio institucional. O Termo de Referência deverá estabelecer o procedimento de acionamento, o marco inicial da cobertura e as condições de faturamento e pagamento.

A validação OV contribui para a governança do processo de emissão ao incluir a verificação da identidade organizacional do solicitante. Entretanto, a proteção contra falsificação de identidade, spoofing e phishing depende da atuação conjunta de outros controles, incluindo:

- segurança do DNS;
- validação adequada dos domínios;
- configuração segura dos servidores;
- proteção das chaves privadas;
- controle de acesso;
- inventário das instalações;
- monitoramento;
- rotação das chaves; e
- revogação e reemissão tempestivas em caso de comprometimento.

Com base na análise comparativa, a solução OV Wildcard mostra-se a mais aderente aos requisitos definidos pela ANPD, sem indicação de marca ou Autoridade Certificadora específica.

10. Registro de soluções consideradas inviáveis

Após a análise técnica e funcional, foram registradas como não escolhidas ou inviáveis para o atendimento integral da necessidade específica da ANPD as soluções descritas a seguir.

A classificação refere-se ao conjunto de requisitos deste ETP e não significa que essas tecnologias sejam inadequadas para todos os cenários.

10.1. Certificados SSL/TLS DV

Os certificados DV asseguram a criptografia da comunicação e validam o controle do domínio, mas não realizam a validação da identidade organizacional da entidade solicitante.

Como a necessidade definida neste ETP inclui a validação organizacional — OV, a alternativa não atende integralmente ao problema de negócio.

A não escolha decorre da diferença no nível de validação, e não de insuficiência dos mecanismos criptográficos utilizados pelos certificados DV.

10.2. Certificados DV automatizados e gratuitos

Soluções como Let’s Encrypt oferecem automação e criptografia adequadas a cenários em que a validação do domínio seja suficiente, inclusive para determinadas coberturas Wildcard.

Entretanto, não realizam validação organizacional — OV. Sua adoção também exigiria a implantação e a manutenção de mecanismos internos de automação, gerenciamento de credenciais, validação por DNS, monitoramento e tratamento de falhas.

A não escolha decorre da ausência do nível de validação requerido e das condições operacionais envolvidas, e não do caráter gratuito ou automatizado da solução.

10.3. Certificados SSL/TLS EV

Embora apresentem validação ampliada, os certificados EV possuem requisitos e custos adicionais sem benefício proporcional demonstrado para o perfil dos serviços da ANPD.

Além disso, não admitem nomes Wildcard nas condições aplicáveis aos certificados públicos TLS, impossibilitando a cobertura de `*.anpd.gov.br` e a cobertura Wildcard prevista para a segunda unidade.

10.4. Certificados individuais OV

Os certificados individuais atendem à validação organizacional e podem proteger separadamente o domínio raiz e os subdomínios institucionais.

Entretanto, exigiriam múltiplas unidades, chaves privadas, validações, instalações, monitoramentos, renovações e controles. Cada novo subdomínio poderia demandar nova emissão e gerenciamento individualizado, elevando o esforço operacional.

Para atender às duas coberturas institucionais pretendidas, seria necessário administrar separadamente todos os certificados relativos aos domínios e subdomínios abrangidos.

A alternativa é tecnicamente possível, mas não oferece a mesma flexibilidade e simplicidade operacional da solução Wildcard.

10.5. Certificado Multi-Domain/SAN OV

O certificado Multi-Domain/SAN atende à validação organizacional e pode proteger vários nomes de domínio totalmente qualificados — FQDNs, incluindo o domínio raiz e os subdomínios expressamente incluídos.

Contudo, utiliza uma lista explícita de nomes, de modo que cada inclusão ou substituição de subdomínio exige alteração da lista e reemissão. Assim, não atende com a mesma flexibilidade à necessidade de incorporar subdomínios de primeiro nível presentes ou futuros.

A inclusão obrigatória do respectivo domínio raiz como SAN no certificado Wildcard não se confunde com a adoção de certificado Multi-Domain/SAN destinado a uma lista ampla ou fechada de domínios distintos.

Na solução escolhida, o SAN é utilizado como mecanismo técnico complementar para atendimento ao domínio raiz, que não é abrangido isoladamente pelo nome Wildcard.

10.6. Serviço gerenciado associado a plataforma de borda ou hospedagem

Essa alternativa pode reduzir o esforço operacional quando os serviços estão integralmente hospedados ou integrados à plataforma correspondente.

Não foi escolhida porque depende da arquitetura específica de hospedagem e segurança, pode introduzir dependência tecnológica e operacional adicional, restringir a portabilidade e limitar a utilização dos certificados fora da respectiva plataforma.

Também não foi demonstrado que uma única plataforma seja compatível com todo o ambiente da ANPD ou que possa fornecer, de forma independente, as duas coberturas Wildcard OV pretendidas.

11. Análise comparativa de custos (TCO)

A análise comparativa de custos considera somente as soluções técnica e funcionalmente aderentes, conforme o art. 11, inciso III e § 1º, da Instrução Normativa SGD/ME nº 94/2022.

Após a comparação dos níveis de validação e dos modelos de cobertura, o serviço SSL/TLS Wildcard OV foi considerado a solução plenamente aderente ao conjunto de requisitos estabelecidos neste ETP.

As alternativas DV, EV, OV individual, Multi-Domain/SAN e os serviços vinculados a plataformas específicas não foram escolhidas pelas razões apresentadas nas Seções 9 e 10 e, por isso, não foram submetidas ao cálculo de TCO.

11.1. Definição dos cenários que integram o TCO

Cenário	Resultado da análise técnica e funcional	Integra o TCO?	Fundamento
Cenário	Resultado da análise técnica e funcional	Integra o TCO?	Fundamento
DV	Não atende integralmente	Não	Não realiza validação organizacional
DV automatizado	Não atende integralmente	Não	Não realiza validação organizacional e depende da implantação e manutenção de automação própria
OV individual	Menor aderência	Não	Exige múltiplos certificados, chaves, instalações e controles e não oferece cobertura automática para novos subdomínios
Multi-Domain /SAN OV	Menor aderência	Não	Depende de lista explícita de nomes e de reemissão quando houver alteração
EV	Não atende ao objeto	Não	Não admite cobertura Wildcard e possui requisitos adicionais sem benefício proporcional demonstrado
Serviço associado a plataforma	Não escolhido no cenário atual	Não	Depende de arquitetura específica e não teve demonstrada compatibilidade com todo o ambiente da ANPD

Wildcard OV	Viável e escolhido	Sim	Atende à validação OV, à cobertura Wildcard, à inclusão do respectivo domínio raiz como SAN e ao período de 36 meses

Como somente o cenário Wildcard OV foi considerado plenamente aderente ao conjunto dos requisitos, a análise de TCO concentra-se nessa solução.

A solução compreende até 2 (dois) serviços, cada um correspondente a uma cobertura Wildcard distinta durante 36 (trinta e seis) meses.

A primeira unidade será destinada a `*.anpd.gov.br`, incluindo obrigatoriamente `anpd.gov.br` no campo SAN do mesmo certificado. A segunda será destinada ao nome Wildcard e ao respectivo domínio raiz de outro domínio institucional sob gestão da ANPD, a ser formalmente indicado.

A tabela não substitui as justificativas detalhadas constantes das Seções 9 e 10.

11.2. Pesquisa de preços

A estimativa foi elaborada com fundamento na Lei nº 14.133/2021, na Instrução Normativa SEGES/ME nº 65/2021 e no art. 20 da Instrução Normativa SGD/ME nº 94/2022.

A pesquisa formal foi registrada como Pesquisa de Preços nº 123/2026, UASG 302122, acompanhada do relatório do Compras.gov.br, da memória de cálculo e da Nota Técnica de análise crítica.

O relatório do Compras.gov.br apresentou 4 (quatro) referências de contratações públicas. Após a análise dos documentos, foram equalizadas para 36 meses as referências do Conselho Administrativo de Defesa Econômica — CADE, da Agência Nacional de Vigilância Sanitária — Anvisa e do Tribunal Regional Eleitoral da Bahia — TRE/BA.

A referência da Secretaria da Segurança Pública do Estado de São Paulo — SSP/SP foi mantida no quadro histórico da pesquisa, mas não integrou o cálculo ajustado, pois não foi possível confirmar o período de cobertura correspondente ao preço registrado.

Com fundamento no art. 5º, inciso III, da Instrução Normativa SEGES/ME nº 65/2021, a pesquisa foi complementada com preços publicados nos sítios eletrônicos da Sectigo Brasil, SSL.com e DigiCert.

Os preços publicados em moeda estrangeira foram inicialmente calculados para 36 meses em sua moeda original e, em seguida, convertidos para reais pela cotação de venda PTAX de R$ 5,1527 por US$ 1,00. O arredondamento para centavos foi realizado somente após a conversão final.

A amostra combinada e equalizada para 36 meses foi composta pelas seguintes referências:

Referência	Valor para 36 meses
TRE/BA	R$ 2.334,00
Anvisa	R$ 4.200,00
SSL.com	R$ 4.621,97
CADE	R$ 4.660,00
Sectigo Brasil	R$ 6.237,00
DigiCert	R$ 17.993,23

A consolidação estatística apresentou os seguintes resultados:

Medida	Valor
Quantidade de referências	6
Menor preço	R$ 2.334,00
Média	R$ 6.674,3667
Mediana adotada	R$ 4.640,99
Maior preço	R$ 17.993,23
Desvio padrão populacional	R$ 5.188,7576
Coeficiente de variação	77,7416%

A Nota Técnica adotou a mediana de R$ 4.640,99 por serviço com cobertura de 36 meses.

A utilização da mediana reduz a influência dos valores extremos, especialmente do preço superior da DigiCert, e representa o centro da série ordenada formada pelas referências comparáveis.

11.3. Memória de cálculo

O valor unitário estimado para cada serviço com cobertura durante 36 meses é de:

R$ 4.640,99.

Considerando a quantidade máxima de 2 (dois) serviços, a memória de cálculo é:

2 serviços × R$ 4.640,99 = R$ 9.281,98.

Assim, o valor máximo estimado da contratação é de **R$ 9.281,98 (nove mil duzentos e oitenta e um reais e noventa e oito centavos)**.

A primeira unidade será destinada a `*.anpd.gov.br` e `anpd.gov.br`. A segunda será destinada a outro domínio institucional sob gestão da ANPD, a ser formalmente indicado.

A quantidade 2 representa duas coberturas Wildcard distintas e não duas emissões sucessivas do mesmo certificado.

A redução progressiva da validade técnica dos certificados não multiplica o preço unitário de cada serviço. Todas as validações, emissões sucessivas, renovações, reemissões, revogações, atividades de gerenciamento e suporte necessárias durante os 36 meses integram o respectivo serviço.

Essas atividades não constituem unidades adicionais de fornecimento, consumo, faturamento ou pagamento e não poderão gerar cobrança adicional.

O valor máximo de R$ 9.281,98 considera o acionamento das duas unidades. O Termo de Referência deverá disciplinar o acionamento, o marco inicial da cobertura, o faturamento e o pagamento da segunda unidade.

11.4. Custos diretos e indiretos

O TCO considera o custo direto de até 2 (dois) serviços durante 36 (trinta e seis) meses de cobertura por unidade.

O custo direto unitário estimado é de R$ 4.640,99, e o custo direto máximo para as duas unidades é de R$ 9.281,98.

Não haverá aquisição de equipamentos, licenças acessórias, mídia física, frete, capacitação formal obrigatória ou manutenção física.

As atividades internas de geração e custódia das chaves privadas, publicação dos registros DNS, instalação dos certificados, monitoramento e fiscalização serão executadas pelas equipes da ANPD no curso ordinário de suas atribuições.

Não foi identificado desembolso incremental mensurável relacionado a essas atividades internas. Por essa razão, não foram adicionados custos indiretos estimados sem documentação que permita sua mensuração.

Cada unidade deverá possuir CSR, certificado e chave privada próprios. Todas as emissões e atividades necessárias à manutenção da cobertura deverão estar incluídas no preço unitário do respectivo serviço.

Assim, o custo total de propriedade máximo estimado para a solução é de R$ 9.281,98 (nove mil duzentos e oitenta e um reais e noventa e oito centavos), correspondente ao acionamento das duas unidades.

Caso apenas uma unidade seja efetivamente acionada, o valor correspondente será de R$ 4.640,99, observadas as condições de execução, faturamento e pagamento estabelecidas no Termo de Referência.

Conforme registrado na Nota Técnica, as referências utilizadas foram equalizadas para o período comum de 36 meses e analisadas quanto à aderência ao serviço SSL/TLS Wildcard OV. A inclusão obrigatória do respectivo domínio raiz como SAN deverá ser observada na proposta contratada.

12. Descrição da solução de TIC a ser contratada

A solução de TIC a ser contratada consiste na prestação de até 2 (dois) serviços de certificação digital pública SSL/TLS Wildcard com validação organizacional — OV, cada um com cobertura durante 36 (trinta e seis) meses.

A primeira unidade será destinada à proteção dos subdomínios de primeiro nível abrangidos por `*.anpd.gov.br` e ao atendimento do domínio raiz `anpd.gov.br`.

A segunda unidade será destinada ao nome Wildcard e ao respectivo domínio raiz de outro domínio institucional sob gestão da ANPD, a ser formalmente indicado quando caracterizada a necessidade.

A contratação será realizada por preço unitário por serviço para 36 meses. Cada unidade deverá abranger todas as validações, emissões sucessivas, renovações, reemissões, revogações, atividades de gerenciamento e suporte necessárias à manutenção contínua da respectiva cobertura, sem cobrança adicional por certificado, emissão ou evento.

O escopo de cada unidade compreende:

- validação organizacional da ANPD mediante fontes oficiais;
- validação do controle do nome Wildcard e do respectivo domínio raiz por método admitido pelas Baseline Requirements vigentes do CA/Browser Forum, preferencialmente mediante DNS;
- emissão de certificado digital público SSL/TLS Wildcard OV por Autoridade Certificadora cuja cadeia de certificação integre os programas de confiança dos principais navegadores e sistemas operacionais;
- inclusão obrigatória do respectivo domínio raiz no campo Subject Alternative Name — SAN do mesmo certificado Wildcard;
- todas as emissões sucessivas necessárias à manutenção contínua da cobertura durante 36 meses;
- renovação, reemissão e revogação sem custo adicional por certificado ou evento;
- disponibilização do certificado, dos certificados intermediários e da respectiva cadeia de confiança em formatos interoperáveis;
- suporte aos mecanismos de verificação de revogação por OCSP e/ou CRL, conforme as políticas da Autoridade Certificadora;
- gerenciamento do ciclo de vida e suporte técnico para solicitação, validação, emissão, instalação, renovação, reemissão, revogação e tratamento de incidentes; e
- orientações e documentação suficientes em língua portuguesa, admitida documentação técnica complementar em inglês.

Para a primeira unidade, o certificado deverá contemplar `*.anpd.gov.br` e `anpd.gov.br`. Para a segunda unidade, deverá contemplar o nome Wildcard e o respectivo domínio raiz formalmente indicados pela ANPD.

A CSR e a chave privada de cada unidade serão geradas e permanecerão sob controle exclusivo da ANPD. A contratada e a Autoridade Certificadora não poderão gerar, armazenar, copiar, manipular ou acessar as chaves privadas.

Cada unidade deverá possuir CSR, certificado e chave privada próprios. Não será permitido o compartilhamento da mesma chave privada entre as duas coberturas distintas.

A cobertura Wildcard abrangerá os subdomínios de primeiro nível presentes e futuros sob o respectivo nome curinga.

Como o nome Wildcard não cobre tecnicamente o domínio raiz, este deverá constar expressamente no campo SAN do mesmo certificado, sem cobrança adicional.

Essa configuração não representa a contratação de dois certificados independentes para a mesma unidade nem transforma o objeto, por si só, em certificado Multi-Domain/SAN destinado a uma lista ampla ou fechada de domínios distintos.

Nomes situados em níveis adicionais, como `sistema.interno.anpd.gov.br`, não são automaticamente abrangidos pelo nome `*.anpd.gov.br` e não integram a cobertura dessa unidade.

A prestação ocorrerá de forma digital e remota, sem utilização de mídia física ou realização de procedimento presencial obrigatório.

Os certificados e as respectivas cadeias deverão ser compatíveis com Linux, Windows Server, Apache, NGINX, IIS e os principais navegadores, sistemas operacionais, dispositivos móveis e clientes padrão de internet utilizados pela ANPD.

Será admitido que a contratada atue como revendedora ou representante de Autoridade Certificadora, permanecendo integralmente responsável perante a ANPD pelo cumprimento das obrigações e pela coordenação da cadeia de fornecimento.

Não será exigida marca ou Autoridade Certificadora específica. A solução será avaliada pelo atendimento aos requisitos técnicos, de confiança pública, validação organizacional, compatibilidade, cobertura, segurança, gerenciamento e suporte definidos neste ETP e no Termo de Referência.

O período de 36 (trinta e seis) meses corresponde à duração da cobertura de cada unidade, e não à validade de uma única emissão de certificado.

Cada certificado deverá observar o limite técnico vigente na data de sua emissão. Como a validade individual será inferior ao período de cobertura, serão necessárias emissões sucessivas ao longo dos 36 meses.

A redução da validade máxima ou o aumento da quantidade de emissões necessárias não alterarão a unidade contratada nem gerarão pagamento adicional.

A quantidade máxima de 2 (dois) serviços representa duas coberturas Wildcard distintas, e não duas emissões sucessivas do mesmo certificado.

A primeira unidade possui destinação definida. A segunda unidade dependerá de acionamento e indicação formal do domínio institucional.

O Termo de Referência deverá estabelecer o procedimento de acionamento da segunda unidade, o marco inicial de sua cobertura de 36 meses e as condições de faturamento e pagamento, de modo que somente sejam remunerados os serviços efetivamente acionados e prestados.

13. Estimativa de custo total da contratação

Valor (R$): 9.281,98

O valor máximo estimado da contratação é de **R$ 9.281,98 (nove mil duzentos e oitenta e um reais e noventa e oito centavos)**, correspondente à contratação de até 2 (dois) serviços de certificação digital pública SSL/TLS Wildcard com validação organizacional — OV, cada um com cobertura durante 36 (trinta e seis) meses.

A primeira unidade será destinada à proteção de `*.anpd.gov.br`, incluindo obrigatoriamente o domínio raiz `anpd.gov.br` no campo SAN do mesmo certificado.

A segunda unidade será destinada ao nome Wildcard e ao respectivo domínio raiz de outro domínio institucional sob gestão da ANPD, a ser formalmente indicado quando caracterizada a necessidade.

A estimativa foi obtida por meio da Pesquisa de Preços nº 123/2026, UASG 302122, e da respectiva Nota Técnica de análise crítica.

O relatório do Compras.gov.br apresentou 4 (quatro) referências de contratações públicas. Após a análise dos documentos, foram equalizadas para 36 meses as referências do Conselho Administrativo de Defesa Econômica — CADE, da Agência Nacional de Vigilância Sanitária — Anvisa e do Tribunal Regional Eleitoral da Bahia — TRE/BA.

A referência da Secretaria da Segurança Pública do Estado de São Paulo — SSP/SP foi mantida no quadro histórico, mas não integrou o cálculo ajustado, pois não foi possível confirmar o período de cobertura correspondente ao preço registrado.

Com fundamento no art. 5º, inciso III, da Instrução Normativa SEGES/ME nº 65/2021, a pesquisa foi complementada com preços publicados nos sítios eletrônicos da Sectigo Brasil, SSL.com e DigiCert.

As referências incluídas na amostra ajustada foram:

Referência	Valor para 36 meses
TRE/BA	R$ 2.334,00
Anvisa	R$ 4.200,00
SSL.com	R$ 4.621,97
CADE	R$ 4.660,00
Sectigo Brasil	R$ 6.237,00
DigiCert	R$ 17.993,23

Para os preços publicados em dólares, primeiro foi calculado o total correspondente aos 36 meses na moeda original. Em seguida, o resultado foi convertido para reais pela cotação de venda PTAX de R$ 5,1527 por US$ 1,00, com arredondamento para centavos somente após a conversão final.

A consolidação dos preços apresentou os seguintes resultados:

- quantidade de referências: 6;
- menor preço: R$ 2.334,00;
- média: R$ 6.674,3667;
- mediana: R$ 4.640,99;
- maior preço: R$ 17.993,23;
- desvio padrão populacional: R$ 5.188,7576; e
- coeficiente de variação: 77,7416%.

Para a definição do valor estimado, adotou-se a mediana de **R$ 4.640,99 por serviço com cobertura de 36 meses**.

A mediana corresponde ao centro da série ordenada e reduz a influência dos valores extremos, especialmente da referência superior da DigiCert, conforme fundamentação constante da Nota Técnica.

Considerando a quantidade máxima de 2 (dois) serviços, foi aplicada a seguinte memória de cálculo:

2 serviços × R$ 4.640,99 = R$ 9.281,98.

A estimativa da contratação fica assim consolidada:

Item	Descrição	Quantidade máxima	Vigência por unidade	Valor unitário	Valor total máximo
	Serviço de certificação digital pública SSL/TLS				

1	Wildcard OV, incluindo o respectivo domínio raiz como SAN, todas as validações, emissões sucessivas, renovações, reemissões, revogações, atividades de gerenciamento e suporte	2 serviços	36 meses	R$ 4.640,99	**R$ 9.281,98**

O valor unitário de R$ 4.640,99 corresponde à cobertura completa de uma unidade durante 36 meses, e não ao valor anual nem ao preço de uma única emissão.

A quantidade máxima de 2 (dois) serviços representa duas coberturas Wildcard distintas. Não representa duas emissões sucessivas do mesmo certificado.

Todas as validações, emissões, renovações, reemissões, revogações, atividades de gerenciamento e suporte necessárias à manutenção contínua de cada cobertura deverão integrar o respectivo preço unitário, sem cobrança adicional por certificado, emissão, evento ou subdomínio abrangido pelo Wildcard.

A redução progressiva da validade técnica dos certificados ou o aumento da quantidade de emissões necessárias não multiplicará o valor unitário nem alterará a unidade contratada, pois essas emissões constituem atividades integrantes do serviço.

O valor máximo de R$ 9.281,98 considera o acionamento das duas unidades. Caso somente uma unidade seja efetivamente acionada, o valor correspondente será de R$ 4.640,99.

O Termo de Referência deverá estabelecer o procedimento de acionamento da segunda unidade, o marco inicial da respectiva cobertura de 36 meses e as condições de faturamento e pagamento.

O filtro temporal de 12 meses utilizado no Compras.gov.br refere-se exclusivamente ao período de busca das contratações públicas recentes. Ele não se confunde com o período de cobertura da solução nem com a validade técnica individual dos certificados.

O relatório da pesquisa, a memória de cálculo, os registros das consultas aos sítios eletrônicos e a análise crítica dos preços constam da Pesquisa de Preços nº 123/2026 e da respectiva Nota Técnica.

14. Justificativa técnica da escolha da solução

A solução SSL/TLS Wildcard OV foi escolhida por atender às necessidades técnicas e funcionais definidas neste ETP, pelos seguintes motivos:

- viabiliza a confidencialidade e a integridade das comunicações HTTPS e a autenticação dos serviços digitais abrangidos, em conjunto com a configuração segura da infraestrutura da ANPD;
- realiza a validação organizacional da Agência durante o processo de emissão, acrescentando a verificação da identidade da organização à validação do controle do domínio;
- contribui para a governança e a segurança do processo de emissão, em conjunto com os demais controles de DNS, servidores, aplicações, chaves privadas, monitoramento e resposta a incidentes;
- cobre os subdomínios de primeiro nível presentes e futuros sob o respectivo nome Wildcard, sem lista fechada de subdomínios e sem necessidade de contratar certificado individual para cada novo nome;
- inclui obrigatoriamente o respectivo domínio raiz no campo Subject Alternative Name — SAN do mesmo certificado Wildcard;
- permite atender até duas coberturas Wildcard institucionais distintas;
- assegura compatibilidade com os principais navegadores, sistemas operacionais, dispositivos móveis e servidores web utilizados pela ANPD;
- permite a manutenção contínua de cada cobertura durante 36 (trinta e seis) meses;
- inclui todas as validações, emissões sucessivas, renovações, reemissões, revogações, atividades de gerenciamento e suporte no preço unitário de cada serviço;
- reduz o esforço operacional associado à administração de múltiplos certificados individuais ou à manutenção de listas de SANs; e
- atende às Baseline Requirements e às demais práticas aplicáveis do CA/Browser Forum para certificados públicos TLS.

A solução compreende até 2 (dois) serviços, cada um correspondente a uma cobertura Wildcard distinta durante 36 meses.

A primeira unidade será destinada a `*.anpd.gov.br`, incluindo obrigatoriamente o domínio raiz `anpd.gov.br` no campo SAN do mesmo certificado.

A segunda unidade será destinada ao nome Wildcard e ao respectivo domínio raiz de outro domínio institucional sob gestão da ANPD, a ser formalmente indicado quando caracterizada a necessidade.

O nome curinga `*.dominio.gov.br` não abrange tecnicamente, por si só, o respectivo domínio raiz `dominio.gov.br`. Por essa razão, o atendimento ao domínio raiz integra obrigatoriamente cada unidade e deverá ocorrer mediante sua inclusão expressa no campo SAN do mesmo certificado Wildcard, sem cobrança adicional.

Essa configuração não representa a contratação de dois certificados independentes para a mesma unidade nem transforma o objeto, por si só, em certificado Multi-Domain/SAN destinado a uma lista ampla ou fechada de domínios distintos.

Nomes situados em níveis adicionais, como `sistema.interno.anpd.gov.br`, não são automaticamente abrangidos pelo nome `*.anpd.gov.br` e não integram a cobertura dessa unidade.

O período de 36 (trinta e seis) meses corresponde à duração da cobertura de cada serviço e não se confunde com a validade técnica de uma única emissão de certificado.

Como a validade individual será inferior ao período de cobertura, serão necessárias emissões sucessivas durante a execução. Todas essas emissões deverão integrar o preço unitário do respectivo serviço, sem cobrança adicional por certificado, emissão ou evento.

A redução da validade máxima dos certificados ou o aumento da quantidade de emissões necessárias não alterará o quantitativo contratado nem o preço unitário para 36 meses.

A quantidade máxima de 2 (dois) serviços representa duas coberturas Wildcard distintas e não duas emissões sucessivas do mesmo certificado.

Cada unidade deverá possuir CSR, certificado e chave privada próprios. Não será permitido utilizar a mesma chave privada para as duas coberturas distintas.

Dentro de cada unidade, o certificado Wildcard poderá ser instalado em diferentes servidores que hospedem os subdomínios abrangidos. A utilização da mesma chave privada em múltiplos servidores reduz a segregação criptográfica e amplia o impacto de eventual comprometimento.

Esse risco é conhecido e não inviabiliza a solução, mas exige a adoção de controles compensatórios pela ANPD, incluindo:

- geração e custódia das chaves privadas exclusivamente pela Agência;
- utilização de chave distinta para cada unidade;
- inventário dos servidores e das instalações;
- distribuição restrita das chaves;
- aplicação do princípio do menor privilégio;
- armazenamento protegido;
- registro das operações relevantes;
- monitoramento;
- rotação das chaves; e
- revogação e reemissão tempestivas em caso de suspeita ou confirmação de comprometimento.

A validação OV não elimina, isoladamente, os riscos de falsificação de identidade, spoofing ou phishing. A mitigação desses riscos depende da atuação conjunta da validação organizacional, da segurança do DNS, da configuração dos servidores e aplicações, da proteção das chaves privadas, do monitoramento e dos demais controles adotados pela ANPD.

A segunda unidade dependerá de indicação formal do domínio institucional e de acionamento conforme as condições estabelecidas no Termo de Referência.

Consideradas a cobertura necessária, a validação organizacional, a compatibilidade, a continuidade operacional, o gerenciamento do ciclo de vida e os controles de segurança previstos, o serviço SSL/TLS Wildcard OV apresenta a alternativa tecnicamente mais adequada ao contexto da ANPD.

15. Justificativa econômica da escolha da solução

Sob o aspecto econômico, o serviço SSL/TLS Wildcard OV apresenta relação adequada entre custo, benefício e aderência ao conjunto de requisitos, pelos seguintes motivos:

- evita os requisitos e custos adicionais da validação EV, que não apresenta benefício proporcional demonstrado e não é compatível com a cobertura Wildcard requerida;
- substitui a contratação e a administração de múltiplos certificados individuais por até 2 (dois) serviços, cada um correspondente a uma cobertura Wildcard distinta;
- permite cobrir os subdomínios de primeiro nível presentes e futuros sob cada nome Wildcard, sem contratação de certificado individual para cada subdomínio;
- inclui obrigatoriamente o respectivo domínio raiz no campo SAN do mesmo certificado, sem cobrança adicional;
- elimina a necessidade de alterações comerciais decorrentes da inclusão ou substituição de nomes em uma lista fechada de subdomínios;
- inclui no preço unitário de cada serviço todas as validações, emissões sucessivas, renovações, reemissões, revogações, atividades de gerenciamento e suporte necessárias durante 36 meses;

- evita pagamentos imprevisíveis vinculados à redução da validade técnica dos certificados ou ao aumento da quantidade de emissões;
- reduz o esforço administrativo associado a contratações anuais repetidas e ao gerenciamento de múltiplos certificados individuais;
- possibilita atender outro domínio institucional por meio da segunda unidade, sem necessidade de iniciar nova contratação para solução equivalente;
- proporciona previsibilidade orçamentária para o período de cobertura; e
- não exige aquisição de equipamentos, mídia física, frete, capacitação formal obrigatória ou manutenção física.

A Pesquisa de Preços nº 123/2026 e a respectiva Nota Técnica adotaram a mediana de **R$ 4.640,99 (quatro mil seiscentos e quarenta reais e noventa e nove centavos)** por serviço com cobertura de 36 meses.

A mediana foi calculada a partir de 6 (seis) referências comparáveis, equalizadas para o período de 36 meses, compostas por três contratações públicas e três preços publicados em sítios eletrônicos especializados.

O valor máximo estimado para até 2 (dois) serviços foi calculado da seguinte forma:

2 serviços × R$ 4.640,99 = R$ 9.281,98.

Assim, o custo total de propriedade máximo estimado é de **R$ 9.281,98 (nove mil duzentos e oitenta e um reais e noventa e oito centavos)**, sem custos incrementais adicionais mensuráveis.

A primeira unidade será destinada a `*.anpd.gov.br`, incluindo obrigatoriamente `anpd.gov.br` no campo SAN do mesmo certificado.

A segunda unidade será destinada ao nome Wildcard e ao respectivo domínio raiz de outro domínio institucional sob gestão da ANPD, a ser formalmente indicado quando caracterizada a necessidade.

O valor unitário de R$ 4.640,99 considera a continuidade de uma cobertura durante 36 meses, e não a aquisição de um único certificado com essa validade.

Todas as validações, emissões sucessivas, renovações, reemissões, revogações, atividades de gerenciamento e suporte exigidas durante o período deverão estar incluídas no preço unitário de cada serviço.

A redução da validade técnica dos certificados ou o aumento da quantidade de emissões necessárias não poderá gerar cobrança adicional.

O valor máximo de R$ 9.281,98 considera o acionamento das duas unidades. Caso somente uma unidade seja efetivamente acionada, o valor correspondente será de R$ 4.640,99, observadas as condições estabelecidas no Termo de Referência.

A previsão da segunda unidade oferece benefício econômico e administrativo ao permitir o atendimento tempestivo de outro domínio institucional com necessidade equivalente, evitando a realização de novo procedimento de contratação durante a vigência.

A redução dos riscos de indisponibilidade também produz benefício econômico indireto ao evitar retrabalho, atendimento emergencial, perda de produtividade e impactos decorrentes da expiração ou invalidade dos certificados, embora esses benefícios não tenham sido monetizados no cálculo do custo total de propriedade.

Dessa forma, a contratação de até 2 (dois) serviços SSL/TLS Wildcard OV, cada um com cobertura durante 36 meses, representa a alternativa economicamente mais vantajosa para a ANPD, observados os princípios da economicidade, eficiência, continuidade dos serviços e segurança da informação.

16. Benefícios a serem alcançados com a contratação

A contratação visa assegurar a proteção das comunicações eletrônicas realizadas entre os usuários e os sistemas, portais e serviços digitais disponibilizados pela ANPD, mediante até 2 (duas) coberturas SSL/TLS Wildcard OV distintas, cada uma mantida durante 36 (trinta e seis) meses.

A primeira unidade será destinada ao domínio curinga `*.anpd.gov.br` e ao domínio raiz `anpd.gov.br`. A segunda será destinada ao nome Wildcard e ao respectivo domínio raiz de outro domínio institucional sob gestão da ANPD, a ser formalmente indicado quando caracterizada a necessidade.

São esperados os seguintes benefícios:

- garantia da confidencialidade das informações transmitidas por meio de conexões HTTPS;
- preservação da integridade dos dados durante a transmissão;
- validação da identidade organizacional da ANPD no processo de emissão dos certificados;
- ampla compatibilidade e reconhecimento pelos principais navegadores, sistemas operacionais e clientes de acesso;
- redução dos riscos de interceptação, adulteração de tráfego e alertas decorrentes de certificado inválido ou expirado;

- contribuição para a mitigação dos riscos de falsificação de identidade, spoofing e phishing, em conjunto com os demais controles de segurança;
- continuidade, disponibilidade prática e maior confiabilidade dos serviços públicos digitais;
- inclusão obrigatória do respectivo domínio raiz no campo SAN do mesmo certificado Wildcard;
- cobertura flexível dos subdomínios de primeiro nível presentes e futuros, sem manutenção de lista fechada e sem contratação de certificado individual para cada nome;
- possibilidade de atendimento tempestivo de outro domínio institucional mediante a segunda unidade;
- manutenção ininterrupta de cada cobertura durante 36 meses;
- inclusão de todas as validações, emissões sucessivas, renovações, reemissões e revogações necessárias, sem cobrança adicional por certificado ou evento;
- atendimento às Baseline Requirements vigentes do CA/Browser Forum e às boas práticas de certificação digital e segurança da informação;
- redução dos riscos operacionais, institucionais e reputacionais;
- melhoria da experiência e da confiança dos usuários no acesso aos serviços digitais da ANPD;
- simplificação do gerenciamento, do faturamento e da fiscalização do ciclo de vida dos certificados;
- previsibilidade do preço unitário de cada cobertura durante 36 meses, independentemente da quantidade de emissões tecnicamente necessárias;
- redução do esforço administrativo relacionado à realização de contratações anuais sucessivas; e
- redução da necessidade de novo procedimento de contratação caso outro domínio institucional necessite de solução equivalente durante a vigência.

A validação OV não elimina, isoladamente, os riscos de spoofing ou phishing. A mitigação desses riscos depende da atuação conjunta da validação organizacional, da segurança do DNS, da configuração dos servidores e aplicações, da proteção das chaves privadas, do monitoramento e dos demais controles adotados pela ANPD.

Os benefícios deverão ser acompanhados durante a execução contratual por meio:

- do monitoramento da validade e do funcionamento dos certificados;
- da verificação da presença do nome Wildcard e do respectivo domínio raiz no campo SAN;
- do acompanhamento das emissões, renovações, reemissões e revogações;
- do registro dos incidentes relacionados à emissão, validação ou funcionamento dos certificados;
- da verificação do atendimento aos prazos contratuais;
- do acompanhamento da continuidade de cada cobertura; e
- da fiscalização das condições de acionamento, faturamento e pagamento da segunda unidade.

Para a primeira unidade, deverá ser monitorada a manutenção contínua da cobertura de `*.anpd.gov.br` e `anpd.gov.br`.

Para a segunda unidade, caso acionada, deverá ser monitorada a manutenção contínua do nome Wildcard e do respectivo domínio raiz formalmente indicados pela ANPD, durante todo o período de cobertura.

5:02 PM

17. Providências a serem Adotadas

Antes da celebração do contrato e do início da execução, a ANPD deverá confirmar a titularidade e a governança interna do domínio `anpd.gov.br`, bem como identificar os responsáveis pela administração do domínio e do respectivo DNS.

A relação dos subdomínios de primeiro nível abrangidos por `*.anpd.gov.br` possui natureza operacional e não constitui lista fechada de nomes. Novos subdomínios de primeiro nível poderão ser criados ou substituídos durante o período de cobertura sem alteração do objeto ou cobrança adicional.

O domínio raiz `anpd.gov.br` não é abrangido automaticamente pelo nome curinga `*.anpd.gov.br`. Por essa razão, deverá constar obrigatoriamente no campo SAN do mesmo certificado Wildcard, sem cobrança adicional. Nomes situados em níveis adicionais, como `sistema.interno.anpd.gov.br`, não são automaticamente abrangidos por essa cobertura.

Para a segunda unidade, a ANPD deverá confirmar previamente a titularidade e a governança do domínio institucional que vier a ser indicado. O certificado deverá contemplar o nome Wildcard e o respectivo domínio raiz no campo SAN, observadas as mesmas características técnicas aplicáveis à primeira unidade.

Deverão ser definidos os servidores responsáveis por autorizar e acompanhar as solicitações de validação, emissão, renovação, reemissão e revogação. Também será necessária articulação com a equipe responsável pela administração do DNS para garantir a publicação tempestiva dos registros exigidos no procedimento de validação do controle dos domínios.

A geração das CSRs e das respectivas chaves privadas deverá ocorrer exclusivamente em infraestrutura controlada pela ANPD. Cada unidade deverá possuir CSR, certificado e chave privada próprios, não sendo permitido utilizar a mesma chave privada para as duas coberturas distintas.

Deverão ser estabelecidos procedimentos internos de custódia, controle de acesso, armazenamento, distribuição, inventário, rotação, cópia de segurança e resposta a eventual comprometimento das chaves privadas, preservando-se a segregação de funções e o controle institucional sobre os ativos criptográficos.

A equipe técnica deverá organizar calendário de acompanhamento e configurar alertas compatíveis com os limites máximos de validade estabelecidos nas Baseline Requirements vigentes do CA/Browser Forum.

Essa providência permitirá planejar as emissões sucessivas com antecedência suficiente e manter cada cobertura HTTPS de forma ininterrupta durante 36 (trinta e seis) meses, apesar da redução progressiva da validade técnica dos certificados públicos.

O Termo de Referência deverá refletir a contratação de 2 (dois) serviços SSL/TLS Wildcard OV, cada um com cobertura durante 36 (trinta e seis) meses e preço unitário.

A primeira unidade será destinada a `*.anpd.gov.br`, incluindo obrigatoriamente `anpd.gov.br` como SAN. A segunda unidade será destinada ao nome Wildcard e ao respectivo domínio raiz de outro domínio institucional sob gestão da ANPD, a ser formalmente indicado.

O Termo de Referência deverá estabelecer o procedimento de acionamento da segunda unidade, os responsáveis pela autorização, a forma de indicação do domínio, o marco inicial da cobertura de 36 meses e as condições de faturamento e pagamento.

O escopo de cada unidade deverá incluir todas as validações, emissões, renovações, reemissões, revogações, atividades de gerenciamento e suporte técnico necessárias durante o período de cobertura, sem cobrança adicional por certificado, emissão ou evento.

Também deverá ser realizada conferência final para assegurar que os requisitos permaneçam relacionados à certificação digital pública SSL/TLS e que não sejam incluídas exigências alheias ao objeto ou condições que restrinjam indevidamente a competitividade.

Deverão ser juntados aos autos a Pesquisa de Preços nº 123/2026, o relatório extraído do Compras.gov.br, os documentos utilizados para confirmação dos períodos das contratações públicas, a memória de cálculo, os registros das consultas aos sítios eletrônicos especializados e a respectiva Nota Técnica.

O Mapa de Gerenciamento de Riscos deverá ser atualizado para refletir a quantidade máxima de 2 (dois) serviços, a indicação futura do domínio da segunda unidade, o acionamento separado das unidades, a inclusão obrigatória do domínio raiz como SAN, a utilização de chaves privadas distintas e a necessidade de emissões sucessivas durante os 36 meses.

A ANPD deverá designar e orientar os responsáveis pela gestão e fiscalização contratual. Não se identifica necessidade de capacitação formal específica, desde que os agentes designados conheçam as características do objeto, os controles internos aplicáveis e as obrigações estabelecidas no contrato.

Quanto ao parcelamento, a contratação em item único, com quantidade máxima de 2 (duas) unidades e preço unitário por serviço, mostra-se técnica e economicamente adequada, nos termos da Lei nº 14.133/2021 e da Instrução Normativa SGD/ME nº 94/2022.

As duas unidades possuem as mesmas características técnicas e diferem apenas quanto ao domínio institucional protegido. A adjudicação em item único preserva a padronização, o gerenciamento e a responsabilidade contratual, sem impedir o faturamento separado das unidades efetivamente acionadas.

Não se recomenda a fragmentação de cada unidade por domínio raiz, subdomínio, emissão, renovação ou período anual. Esses componentes integram uma única cobertura por 36 meses, e sua separação ampliaria a complexidade operacional, fragmentaria responsabilidades e poderia comprometer a continuidade e a padronização da solução.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Com base nos levantamentos realizados no âmbito deste Estudo Técnico Preliminar, conclui-se que a contratação de serviço de certificação digital SSL/TLS Wildcard OV com inclusão do domínio raiz como SAN mostra-se tecnicamente viável, necessária e adequada ao atendimento das demandas institucionais da ANPD.

Verifica-se, ainda, que a contratação atende ao interesse público, uma vez que contribuirá para o fortalecimento da segurança da informação, proteção das comunicações eletrônicas, confiabilidade dos serviços digitais e continuidade operacional dos sistemas institucionais.

Sob o aspecto operacional, não foram identificados impedimentos relevantes à implantação da solução, sendo plenamente possível sua integração aos ambientes tecnológicos existentes.

Quanto aos aspectos econômicos, a contratação apresenta relação custo-benefício favorável em comparação com alternativa EV e mostra-se mais aderente ao problema institucional do que alternativas DV, desde que a pesquisa de preços confirme os valores referenciais e a equivalência técnica das amostras utilizadas.

19. 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.

KAROLINA MARTINS MILANO

Integrante Técnico

Assinou eletronicamente em 23/09/2026 às 14:50:55.

RODRIGO VAZ DOS SANTOS

Integrante Requisitante

Assinou eletronicamente em 23/09/2026 às 14:40:37.