

FUNDAÇÃO BIBLIOTECA NACIONAL

Estudo Técnico Preliminar 45/2026**1. Informações Básicas**

Número do processo: 01430.000105/2026-17

2. Descrição da necessidade

A aquisição de **2 (duas) licenças de Certificado Digital Secure Sockets Layer (SSL), com validade de 36 (trinta e seis) meses**, visa garantir a segurança, autenticidade e confidencialidade das comunicações realizadas pelos servidores web utilizados pela Coordenação de Tecnologia da Informação (COTI) da Fundação Biblioteca Nacional (FBN).

Esses certificados são essenciais para assegurar a proteção das informações trafegadas entre usuários e os sistemas institucionais, por meio da criptografia de dados, prevenindo acessos não autorizados, interceptações indevidas e riscos à integridade das aplicações disponibilizadas na internet.

O quantitativo informado reflete a necessidade de manutenção da infraestrutura de segurança digital dos serviços web institucionais, garantindo a continuidade operacional, a confiabilidade dos acessos e a conformidade com boas práticas e requisitos de segurança da informação aplicáveis aos serviços de TIC da FBN.

3. Área requisitante

Área Requisitante	Responsável
Núcleo de Suporte e Infraestrutura/COTI	Hugo Cezar Christino de Paiva
COTI	Fabio Biangolino Teixeira Lima

4. Necessidades de Negócio

A presente contratação decorre da necessidade de garantir a continuidade, a segurança e a confiabilidade dos serviços institucionais prestados pela Fundação Biblioteca Nacional, os quais dependem diretamente da disponibilidade, integridade e proteção da infraestrutura de Tecnologia da Informação.

A utilização de certificados digitais Secure Sockets Layer (SSL) é essencial para assegurar comunicações seguras entre os servidores web institucionais e seus usuários, garantindo a criptografia das informações trafegadas, a autenticação dos domínios institucionais e a proteção contra acessos indevidos, interceptações e ataques cibernéticos.

A contratação de empresa especializada para fornecimento de 2 (duas) licenças de Certificado Digital SSL, com validade de 36 (trinta e seis) meses, visa atender às demandas operacionais da instituição, proporcionando maior segurança, confiabilidade e conformidade com as boas práticas de segurança da informação aplicáveis aos serviços digitais disponibilizados pela Fundação Biblioteca Nacional.

Dessa forma, a contratação contribui para:

- A continuidade dos serviços digitais essenciais da instituição;

- A proteção das informações trafegadas nos sistemas e portais institucionais;
- O aumento da segurança das comunicações entre usuários e servidores web;
- A redução de riscos de ataques cibernéticos e acessos não autorizados;
- A melhoria da confiabilidade e credibilidade dos serviços disponibilizados na internet;
- O atendimento às necessidades atuais e futuras de segurança da informação da organização;
- A conformidade com requisitos e boas práticas de segurança aplicáveis à infraestrutura de TIC.

5. Necessidades Tecnológicas

A presente contratação tem por objetivo atender às necessidades da Coordenação de Tecnologia da Informação da Fundação Biblioteca Nacional, por meio da disponibilização de solução de Tecnologia da Informação e Comunicação (TIC) voltada à segurança dos serviços digitais institucionais.

A solução consiste na contratação de empresa especializada para fornecimento de 2 (duas) licenças de Certificado Digital Secure Sockets Layer (SSL), com validade de 36 (trinta e seis) meses, destinadas à proteção dos servidores web institucionais, assegurando a criptografia das comunicações, a autenticação dos domínios e a integridade das informações trafegadas entre usuários e sistemas.

A contratação justifica-se pela necessidade de garantir a continuidade, a confiabilidade e a segurança dos serviços digitais disponibilizados pela Fundação Biblioteca Nacional, mitigando riscos relacionados a interceptação de dados, acessos não autorizados e vulnerabilidades nas comunicações eletrônicas.

Nesse contexto, a solução de TIC contribui para:

- Garantir a disponibilidade e a segurança dos serviços digitais institucionais;
- Proteger a confidencialidade e integridade das informações trafegadas nos ambientes web;
- Assegurar a autenticidade dos domínios institucionais perante os usuários;
- Reduzir riscos de incidentes de segurança da informação;
- Atender às boas práticas e diretrizes de segurança aplicáveis à Administração Pública Federal;
- Sustentar o adequado funcionamento dos sistemas utilizados pelas áreas administrativas e finalísticas da instituição.

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

Requisitos de Capacitação

Não faz parte do escopo da contratação a realização de capacitação técnica, considerando que a equipe da Coordenação de Tecnologia da Informação (COTI) possui conhecimento técnico suficiente para instalação, configuração, validação e gerenciamento dos certificados digitais SSL nos servidores web institucionais.

Requisitos Legais

A contratação deverá observar a legislação vigente aplicável, especialmente a Constituição Federal, a Lei nº 14.133/2021, a Instrução Normativa SGD/ME nº 94/2022, a Instrução Normativa SEGES/ME nº 65/2021, a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), a Portaria SGD/MGI nº 5.950/2023 e demais normativos pertinentes às contratações de soluções de Tecnologia da Informação e Comunicação (TIC).

Requisitos de Sustentabilidade

A contratada deverá atender, no que couber, aos critérios de sustentabilidade previstos no Decreto nº 7.404/2010, na IN SLTI/MP nº 1/2010 e no Decreto nº 7.746/2012, priorizando práticas que reduzam impactos ambientais, considerando que a solução é de natureza digital e não envolve fornecimento de bens físicos.

Requisitos de Conformidade Técnica

Os certificados digitais SSL fornecidos deverão atender aos padrões internacionais de segurança da informação e criptografia aplicáveis, incluindo conformidade com normas reconhecidas pelo mercado e compatibilidade com os principais navegadores e servidores web, bem como demais requisitos técnicos pertinentes à certificação digital e segurança das comunicações eletrônicas.

7. Estimativa da demanda - quantidade de bens e serviços

A estimativa da demanda para contratação de Certificados Digitais Secure Sockets Layer (SSL) foi definida a partir de levantamento técnico realizado pela Coordenação de Tecnologia da Informação (COTI) da Fundação Biblioteca Nacional (FBN), considerando o cenário atual dos serviços digitais institucionais e a necessidade de garantir comunicações seguras nos servidores web da instituição.

O quantitativo previsto contempla:

- a proteção criptográfica das comunicações realizadas por meio dos portais e sistemas web institucionais;
- a garantia de autenticidade dos domínios institucionais perante os usuários externos e internos;
- a manutenção da disponibilidade e confiabilidade dos serviços digitais disponibilizados pela FBN;
- a mitigação de riscos relacionados a interceptação de dados, ataques cibernéticos e vulnerabilidades nas conexões web;
- a continuidade operacional dos serviços digitais essenciais suportados pela infraestrutura de Tecnologia da Informação e Comunicação (TIC).

A definição das quantidades foi baseada em análise técnica dos servidores web ativos, dos domínios institucionais que demandam certificação digital e da necessidade de redundância operacional para assegurar a continuidade dos serviços críticos.

ITEM	ESPECIFICAÇÃO	CATMAT	UNIDADE DE MEDIDA	QUANT	VALOR UNITÁRIO	VALOR TOTAL
1	Certificado Digital Secure Sockets Layer (SSL) para servidores web, incluindo emissão, validação e suporte técnico, com validade de 36 (trinta e seis) meses, compatível com os principais navegadores e servidores web do mercado	27502	Unidade (UN)	2	-	-

Observação: Os valores unitário e total serão definidos posteriormente com base na pesquisa de preços a ser realizada pela Divisão de Compras, Patrimônio e Almoxarifado (DCPA/COAD).

Dessa forma, a contratação da solução proposta busca garantir a segurança, autenticidade e confiabilidade das comunicações digitais da Fundação Biblioteca Nacional, assegurando a continuidade dos serviços institucionais disponibilizados por meio da internet.

8. Levantamento de soluções

Para atendimento da necessidade identificada, foram analisadas possíveis soluções disponíveis no mercado capazes de garantir a segurança, autenticidade e confiabilidade das comunicações realizadas pelos serviços digitais da Coordenação de Tecnologia da Informação (COTI) da Fundação Biblioteca Nacional (FBN).

Durante o levantamento, foram consideradas as seguintes alternativas:

a) Manutenção da utilização de certificados expirados ou utilização de conexões sem certificação digital válida

Consiste na continuidade da operação dos serviços web institucionais sem a utilização de certificados digitais válidos ou com certificados expirados.

Entretanto, essa alternativa mostrou-se inviável, considerando que a ausência de certificação SSL válida compromete a segurança das comunicações, gera alertas de navegação insegura nos navegadores, reduz a confiabilidade dos serviços institucionais e expõe informações trafegadas a riscos de interceptação e ataques cibernéticos.

b) Utilização de certificados digitais gratuitos

Foi avaliada a utilização de certificados digitais gratuitos disponíveis no mercado.

Essa alternativa não se mostrou plenamente adequada, considerando limitações relacionadas ao ciclo reduzido de validade, necessidade de renovações frequentes, maior esforço operacional para gerenciamento contínuo e ausência de garantias formais de suporte técnico e níveis de serviço compatíveis com ambientes institucionais da Administração Pública.

c) Contratação de licenças de Certificado Digital Secure Sockets Layer (SSL) com validade estendida (Solução adotada)

A contratação de licenças de certificados digitais SSL foi identificada como a solução mais adequada, por possibilitar:

- criptografia segura das comunicações entre usuários e servidores web institucionais;
- autenticação dos domínios institucionais, garantindo confiabilidade aos acessos;
- redução de riscos relacionados a interceptação de dados e ataques cibernéticos;
- maior estabilidade operacional, com validade estendida e menor necessidade de intervenções administrativas;
- suporte técnico especializado e conformidade com boas práticas de segurança da informação;
- melhor relação custo-benefício no médio e longo prazo.

Além disso, a contratação permite maior previsibilidade operacional e alinhamento às diretrizes de segurança da informação aplicáveis à Administração Pública Federal.

Dessa forma, conclui-se que a contratação de **2 (duas) licenças de Certificado Digital Secure Sockets Layer (SSL), com validade de 36 (trinta e seis) meses**, representa a solução mais eficiente, segura e economicamente viável para atendimento da demanda apresentada.

9. Análise comparativa de soluções

Com base no levantamento de soluções realizado, procedeu-se à análise comparativa das alternativas identificadas, considerando critérios de viabilidade técnica, econômica e operacional, bem como a capacidade de atendimento às necessidades da Coordenação de Tecnologia da Informação (COTI) da Fundação Biblioteca Nacional (FBN).

As soluções avaliadas foram comparadas conforme os aspectos abaixo:

a) Manutenção dos equipamentos atualmente existentes

- **Vantagens:**
 - ausência de investimento inicial imediato.

- **Desvantagens:**

- comprometimento da segurança das comunicações eletrônicas;
- exibição de alertas de navegação insegura nos navegadores;
- risco de interceptação de dados e ataques cibernéticos;
- perda de confiabilidade dos serviços institucionais disponibilizados ao público.

Conclusão: alternativa tecnicamente inadequada, por não atender aos requisitos mínimos de segurança da informação e confiabilidade dos serviços digitais institucionais.

b) Utilização de certificados digitais gratuitos

- **Vantagens:**

- inexistência de custo direto para aquisição das licenças;
- rápida disponibilização inicial.

- **Desvantagens:**

- prazos curtos de validade, exigindo renovações frequentes;
- maior esforço operacional para gestão e acompanhamento das renovações;
- ausência de garantias formais de suporte técnico e níveis de serviço;
- maior risco operacional decorrente de falhas no processo de renovação.

Conclusão: alternativa tecnicamente viável, porém operacionalmente menos adequada para ambiente institucional da Administração Pública, em razão da menor previsibilidade e confiabilidade operacional.

c) Contratação de licenças de Certificado Digital Secure Sockets Layer (SSL) com validade estendida (Solução escolhida)

Vantagens:

- criptografia segura das comunicações entre usuários e servidores web;
- autenticação dos domínios institucionais, aumentando a confiança dos usuários;
- redução de riscos de incidentes de segurança da informação;
- menor necessidade de intervenções administrativas devido à validade estendida;
- suporte técnico especializado;
- melhor relação custo-benefício no médio e longo prazo.

- **Desvantagens:**

- necessidade de investimento inicial para contratação das licenças.

Conclusão: solução que apresenta melhor equilíbrio entre segurança, eficiência operacional e viabilidade econômica, atendendo plenamente às necessidades institucionais.

Diante da análise comparativa realizada, conclui-se que a contratação de **2 (duas) licenças de Certificado Digital Secure Sockets Layer (SSL), com validade de 36 (trinta e seis) meses**, constitui a alternativa mais vantajosa para a Administração Pública, por atender aos requisitos técnicos, operacionais e de segurança da informação da Fundação Biblioteca Nacional, garantindo a continuidade e a confiabilidade dos serviços digitais institucionais.

10. Registro de soluções consideradas inviáveis

Durante o processo de análise das alternativas para atendimento da necessidade identificada, foram avaliadas soluções que, após estudo técnico e operacional, mostraram-se inviáveis para a realidade da Coordenação de Tecnologia da Informação (COTI) da Fundação Biblioteca Nacional (FBN).

Destacam-se as seguintes soluções consideradas inviáveis:

a) Continuidade da utilização de serviços web sem certificação digital válida ou com certificados expirados

A manutenção da operação dos serviços institucionais sem certificados digitais válidos foi considerada inviável, tendo em vista os riscos relacionados à segurança da informação e à confiabilidade dos serviços disponibilizados pela instituição.

A permanência dessa solução poderia ocasionar:

- aumento do risco de interceptação de dados trafegados nas comunicações eletrônicas;
- exibição de alertas de conexão insegura nos navegadores dos usuários;
- comprometimento da credibilidade institucional dos serviços digitais;
- possibilidade de indisponibilidade ou bloqueio de acesso por mecanismos de segurança dos navegadores modernos.

b) Utilização exclusiva de certificados digitais gratuitos

A alternativa de utilização de certificados digitais gratuitos foi considerada inviável sob o ponto de vista operacional e de gestão, uma vez que:

- exige renovações frequentes devido ao curto período de validade;
- aumenta o risco operacional decorrente de eventual falha no processo de renovação;
- não assegura níveis formais de suporte técnico compatíveis com ambiente institucional;
- reduz a previsibilidade operacional necessária à Administração Pública.

Dessa forma, conclui-se que as soluções acima descritas não atendem de maneira satisfatória aos princípios da economicidade, eficiência, segurança da informação e continuidade do serviço público, sendo descartadas no âmbito deste Estudo Técnico Preliminar.

11. Análise comparativa de custos (TCO)

A análise comparativa de custos foi realizada considerando o Custo Total de Propriedade (Total Cost of Ownership – TCO) das soluções avaliadas, abrangendo não apenas o custo inicial de contratação, mas também os custos associados à operação, gestão, suporte e continuidade dos serviços digitais ao longo do período de utilização.

Foram considerados, para fins de comparação, os seguintes elementos:

- custo de aquisição ou contratação das licenças;
- custos operacionais relacionados à gestão e renovação dos certificados;
- impacto financeiro decorrente de eventuais indisponibilidades dos serviços web;
- necessidade de suporte técnico especializado;
- prazo de validade das licenças;
- esforço operacional da equipe técnica interna para manutenção da solução.

a) Utilização de serviços web sem certificação digital válida ou com certificados expirados

Embora não exija investimento financeiro imediato, essa alternativa apresenta elevados custos indiretos, decorrentes de riscos de segurança da informação, perda de confiabilidade dos serviços institucionais e possíveis indisponibilidades causadas por bloqueios de navegação ou incidentes de segurança.

O TCO dessa solução torna-se elevado ao longo do tempo, considerando os potenciais impactos operacionais, institucionais e de segurança.

b) Utilização de certificados digitais gratuitos

Essa alternativa reduz o custo direto de contratação, porém implica custos operacionais indiretos relacionados à necessidade de renovações frequentes, monitoramento constante da validade dos certificados e maior risco de interrupção dos serviços em caso de falhas no processo de renovação.

O custo total acumulado tende a aumentar em função do esforço operacional contínuo e da menor previsibilidade da solução, especialmente em ambiente institucional que demanda alta disponibilidade.

c) Contratação de licenças de Certificado Digital Secure Sockets Layer (SSL) com validade de 36 meses (Solução adotada)

A contratação das licenças apresenta custo inicial definido, porém proporciona redução significativa dos custos operacionais ao longo do período contratual, considerando:

- validade estendida das licenças, reduzindo a necessidade de renovações frequentes;
- maior estabilidade e previsibilidade operacional;
- suporte técnico especializado;
- redução de riscos de indisponibilidade dos serviços digitais;
- menor esforço administrativo e técnico da equipe interna;
- maior confiabilidade e segurança das comunicações institucionais.

Sob a perspectiva do TCO, esta alternativa demonstra melhor relação custo-benefício no médio e longo prazo, garantindo sustentabilidade financeira e eficiência operacional para a Administração Pública.

Diante da análise realizada, conclui-se que a contratação de 2 (duas) licenças de Certificado Digital Secure Sockets Layer (SSL), com validade de 36 (trinta e seis) meses, representa a solução economicamente mais vantajosa, alinhada aos princípios da economicidade, eficiência, segurança da informação e continuidade do serviço público.

12. Descrição da solução de TIC a ser contratada

A solução de Tecnologia da Informação e Comunicação (TIC) a ser contratada consiste na **aquisição de 2 (duas) licenças de Certificado Digital Secure Sockets Layer (SSL), com validade de 36 (trinta e seis) meses**, destinadas a garantir a segurança, autenticidade e confiabilidade das comunicações realizadas pelos servidores web da Fundação Biblioteca Nacional (FBN), sob gestão da Coordenação de Tecnologia da Informação (COTI).

As licenças a serem contratadas têm como finalidade assegurar a criptografia das comunicações eletrônicas, protegendo a transmissão de dados entre usuários e os sistemas institucionais disponibilizados na internet, bem como garantindo a autenticidade dos domínios institucionais.

A solução contempla o fornecimento de certificados digitais compatíveis com a infraestrutura tecnológica existente, observando requisitos técnicos de segurança da informação, interoperabilidade e conformidade com padrões internacionais, permitindo:

- proteção das comunicações por meio de criptografia segura (HTTPS);
- autenticação dos serviços web institucionais perante os usuários;
- prevenção contra interceptação e adulteração de dados trafegados;
- melhoria da confiabilidade e credibilidade dos serviços digitais da instituição;
- redução de riscos de indisponibilidade decorrentes de alertas de segurança em navegadores;
- suporte à continuidade operacional dos sistemas e serviços digitais da FBN.

Os certificados digitais deverão ser emitidos por Autoridade Certificadora reconhecida internacionalmente, compatíveis com os principais navegadores e servidores web utilizados no ambiente institucional, garantindo plena integração à infraestrutura tecnológica existente.

A contratação compreende exclusivamente o fornecimento das licenças dos certificados digitais SSL, incluindo suporte técnico do fornecedor durante o período de validade, conforme especificações técnicas a serem detalhadas no Termo de Referência, não envolvendo prestação continuada de serviços de operação.

Dessa forma, a solução proposta visa assegurar níveis adequados de segurança da informação, disponibilidade e confiabilidade dos serviços digitais institucionais, atendendo às necessidades atuais e futuras da Fundação Biblioteca Nacional.

13. Estimativa de custo total da contratação

Valor (R\$): 1,00

Em conformidade com o fluxograma de tramitação da Fundação Biblioteca Nacional (FBN), no âmbito do presente Estudo Técnico Preliminar, a estimativa de preços será oportunamente elaborada pela Divisão de Compras, Patrimônio e Almoxarifado (DCPA/COAD), unidade responsável pela realização da pesquisa de preços e pela devida instrução dos autos com os resultados obtidos.

14. Justificativa técnica da escolha da solução

A escolha pela contratação de **licenças de Certificado Digital Secure Sockets Layer (SSL)** fundamenta-se em análise técnica realizada pela Coordenação de Tecnologia da Informação (COTI) da Fundação Biblioteca Nacional (FBN), considerando critérios de segurança da informação, confiabilidade, economicidade e continuidade dos serviços institucionais disponibilizados em ambiente web.

A solução selecionada demonstrou-se tecnicamente mais adequada por garantir a proteção das comunicações eletrônicas, assegurando a criptografia dos dados trafegados entre os usuários e os servidores institucionais, bem como a autenticação dos domínios da instituição perante os navegadores e sistemas clientes.

A alternativa adotada possibilita:

- implementação de comunicação segura por meio do protocolo HTTPS;
- autenticação dos serviços digitais institucionais, aumentando a confiança dos usuários;
- proteção contra interceptação, adulteração e acesso indevido às informações trafegadas;
- redução de riscos de indisponibilidade decorrentes de alertas de segurança em navegadores;
- conformidade com boas práticas e requisitos de segurança da informação aplicáveis a serviços públicos digitais;
- autonomia da equipe técnica interna para instalação, configuração e gestão dos certificados digitais.

Além disso, conforme análise comparativa realizada no presente Estudo Técnico Preliminar, verificou-se que a contratação de certificados digitais com validade de 36 (trinta e seis) meses apresenta melhor relação custo-benefício no médio prazo quando comparada à utilização de certificados gratuitos com renovações frequentes ou à ausência de certificação adequada, que pode gerar riscos operacionais e institucionais.

Dessa forma, a solução escolhida atende plenamente às necessidades técnicas e operacionais da FBN, estando alinhada aos princípios da eficiência, economicidade, segurança da informação e continuidade do serviço público, previstos na legislação vigente aplicável às contratações públicas.

15. Justificativa econômica da escolha da solução

A escolha pela contratação de licenças de Certificado Digital Secure Sockets Layer (SSL) apresenta-se economicamente mais vantajosa para a Fundação Biblioteca Nacional (FBN), conforme análise realizada no presente Estudo Técnico Preliminar, especialmente sob a perspectiva do custo total de propriedade.

Embora a solução adotada demande investimento para aquisição das licenças com validade de 36 (trinta e seis) meses, verificou-se que essa alternativa proporciona maior previsibilidade orçamentária e redução de custos operacionais ao longo do período contratado, quando comparada às demais soluções avaliadas.

A utilização de certificados gratuitos ou de curta duração tende a gerar aumento de custos indiretos relacionados à necessidade de renovações frequentes, maior esforço operacional da equipe técnica e riscos associados à expiração inadvertida dos certificados, podendo ocasionar indisponibilidade dos serviços institucionais.

Por sua vez, a contratação de soluções terceirizadas mais abrangentes, envolvendo serviços contínuos de segurança ou hospedagem com certificação inclusa, implicaria custos recorrentes superiores, além de criar dependência contratual permanente sem benefício proporcional às necessidades institucionais.

A contratação direta das licenças de certificados digitais SSL apresenta vantagens econômicas relevantes, tais como:

- redução da necessidade de renovações frequentes durante o período de vigência;
- diminuição do risco de indisponibilidade dos serviços web por expiração de certificados;
- previsibilidade orçamentária durante os 36 meses de validade;
- redução do esforço operacional da equipe técnica interna;
- melhoria da confiabilidade dos serviços digitais sem custos recorrentes adicionais de serviços continuados.

Dessa forma, conclui-se que a solução escolhida representa a alternativa economicamente mais eficiente e sustentável para a Administração Pública, garantindo equilíbrio entre investimento, segurança da informação e continuidade dos serviços de Tecnologia da Informação e Comunicação da FBN.

16. Benefícios a serem alcançados com a contratação

A contratação visa assegurar uma infraestrutura de Tecnologia da Informação adequada às necessidades da Fundação Biblioteca Nacional (FBN), garantindo a confidencialidade, integridade, disponibilidade, autenticidade e segurança das informações trafegadas nos sistemas e serviços digitais institucionais, em observância ao princípio da economicidade.

Como benefícios esperados, destacam-se:

- fortalecimento da segurança das comunicações realizadas por meio dos servidores web institucionais;
- garantia de criptografia dos dados trafegados entre usuários e sistemas da instituição;
- aumento da confiabilidade e credibilidade dos serviços digitais disponibilizados ao público interno e externo;
- redução de riscos de interceptação, adulteração ou exposição indevida de informações;
- diminuição da possibilidade de indisponibilidade dos serviços decorrente de certificados expirados ou inválidos;
- suporte às demandas atuais e futuras de segurança da informação da instituição.

Dessa forma, a contratação contribuirá para o fortalecimento da segurança dos serviços digitais e para a continuidade das atividades institucionais da Fundação Biblioteca Nacional.

17. Providências a serem Adotadas

Todos os recursos necessários ao fornecimento das licenças de Certificado Digital Secure Sockets Layer (SSL), incluindo emissão, validação, disponibilização e garantia durante o período de vigência, serão de responsabilidade da empresa CONTRATADA, conforme as especificações técnicas estabelecidas no Termo de Referência.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

A contratação mostra-se viável sob os aspectos técnico e econômico, uma vez que há soluções amplamente disponíveis no mercado capazes de atender integralmente aos requisitos de segurança e confiabilidade necessários aos serviços web institucionais, garantindo a continuidade e a proteção das comunicações digitais da Fundação Biblioteca Nacional.

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](#).

HUGO CESAR CHRISTINO DE PAIVA

Equipe de Planejamento



Assinou eletronicamente em 09/04/2026 às 10:58:41.

FABIO BIANGOLINO TEIXEIRA LIMA

Equipe de Planejamento



Assinou eletronicamente em 08/04/2026 às 17:30:48.