SUBSECRETARIA DE TECNOLOGIA E INOVAÇAO/MME

Estudo Técnico Preliminar 2/2026

1. Informações Básicas

Número do processo: 48330.000004/2026-20

2. Descrição da necessidade

Contratação de serviço de fornecimento de Certificado de assinatura Digital SSL/TLS, do tipo *wildcard*, com Validação Organizacional (OV) e cadeia de confiança (raiz) internacional.

2.1. A **Subsecretaria de Tecnologia e Inovação (STI)** do Ministério de Minas e Energia (MME), em conformidade com suas atribuições institucionais, é responsável por **garantir a infraestrutura tecnológica, a segurança da informação e o suporte aos sistemas e serviços digitais essenciais** ao funcionamento da Pasta, observando as diretrizes de governança, conformidade e proteção dos serviços públicos digitais.

2.2. No atual contexto de intensificação das ameaças cibernéticas, a autenticação confiável de pessoas, serviços e organizações em transações eletrônicas constitui requisito crítico para **assegurar a integridade, a confidencialidade e a disponibilidade das informações**. Nesse cenário, certificados digitais SSL/TLS desempenham papel fundamental ao viabilizar a autenticação de origem, a criptografia de dados “em trânsito” e a mitigação de riscos associados a interceptação, adulteração e fraudes em comunicações eletrônicas.

2.3. A presente contratação fundamentase na necessidade de manter, de forma contínua e segura, a **confiabilidade das comunicações** estabelecidas pelos sistemas, portais, sítios eletrônicos e aplicações web institucionais vinculados ao domínio ***.mme.gov.br**, utilizados por públicos internos e externos. Esses serviços digitais dão suporte a atividades administrativas e à prestação de serviços públicos eletrônicos, muitos dos quais envolvem **informações sensíveis** e, frequentemente, dados pessoais, exigindo mecanismos técnicos robustos para assegurar a proteção na camada de transporte e preservar a confiança dos usuários nos canais oficiais da Administração Pública.

2.4. A proteção criptográfica adequada e a autenticação de domínio para serviços web são obtidas mediante a adoção de **certificados digitais SSL/TLS** e do protocolo **HTTPS**, o que garante:

i. criptografia ponta a ponta das comunicações; e
ii. validação do domínio perante navegadores, aplicativos e dispositivos.

2.5. Atualmente, o MME utiliza um **Certificado Digital SSL/TLS** do tipo **Wildcard, com Validação Organizacional (OV) e cadeia de confiança internacional,** cujo período de validade **expira em 27 de março de 2026**. Para assegurar a continuidade da proteção criptográfica e evitar riscos operacionais, tornase necessária a contratação tempestiva de novo certificado SSL/TLS com as mesmas características, abrangendo o domínio institucional e seus subdomínios.

2.6. Diversos sistemas críticos e amplamente utilizados dependem diretamente da validade e disponibilidade do certificado digital, entre os quais se destacam:

- SEI – Sistema Eletrônico de Informações;
- CONSULTA PÚBLICA – Sistema de participação social;
- SAPED – Sistema de Arrecadação para Pesquisa e Desenvolvimento;

- DDIG – Declaração Digital de Necessidade de Compra de Energia Elétrica;
- SREIDI – Sistema do Regime Especial de Incentivos ao Desenvolvimento da Infraestrutura;
- LPT – Sistema de acompanhamento do Programa Luz para Todos;
- SCAEE – Sistema de Controle de Acesso à Energia Elétrica;
- PROJETEEE – Sistema de Projetos de Edificações Energeticamente Eficientes;
- VPN corporativa;
- Web Application Firewalls (WAFs);
- Portal de autenticação da rede WiFi institucional;
- dentre outros serviços hospedados sob o domínio institucional.

2.7. A solução requerida consiste na **Contratação de serviço de emissão de Certificado de assinatura Digital SSL /TLS, compatível com certificação de subdomínios (*wildcard*), de tipo Validação Organizacional (OV) e cadeia de confiança (raiz) internacional.** Os principais requisitos técnicos justificam-se da seguinte forma:

- **Validação Organizacional (OV)**: eleva o nível de segurança ao incluir verificação da identidade institucional, mitigando riscos de fraude, falsificação de identidade digital e ataques de phishing.
- **Certificação de subdomínios (*Wildcard)***: assegura cobertura a múltiplos subdomínios com um único certificado, simplificando a gestão, reduzindo custos e minimizando riscos operacionais decorrentes de manuseio de múltiplos certificados independentes.
- **Cadeia de confiança (raiz) internacional**: garante ampla compatibilidade com navegadores, sistemas operacionais e dispositivos móveis, evitando alertas, bloqueios ou restrições de acesso que prejudiquem a disponibilidade dos serviços digitais.

2.8. Considerando que o certificado atualmente implantado encontrase próximo do término de sua vigência, a aquisição tornase **urgente** para prevenir **riscos associados** à expiração, tais como:

- **indisponibilidade ou degradação** de acesso a sistemas devido a alertas de segurança emitidos por navegadores;
- **redução da confiança** dos usuários nos serviços digitais do MME, com potencial impacto reputacional;
- **aumento da superfície de ataque** e exposição a vulnerabilidades decorrentes da quebra de confiança na camada de transporte;
- **prejuízos operacionais** e interrupções em serviços digitais essenciais.

2.9. Assim, a contratação revela-se necessária e atende ao interesse público ao garantir continuidade, disponibilidade e confiabilidade dos serviços digitais do Ministério, bem como a proteção das informações trafegadas.

2.10. Ademais, contribui para a adequada fundamentação técnica do processo de contratação, em conformidade com a lógica do Estudo Técnico Preliminar estabelecida nas normas vigentes, subsidiando a elaboração do Termo de Referência e demais documentos instrutórios.

3. Área requisitante

Área Requisitante	Responsável
Coordenador-Geral de Governança e Serviços de Tecnologia (CGST)	Ricardo Leopoldino Abreu

4. Necessidades de Negócio

4.1. Para atender plenamente a necessidade do Órgão, é essencial a adoção de tecnologia que garanta **autenticação institucional inequívoca**, **criptografia forte** e **estabelecimento de canais seguros de comunicação**. Nesse sentido, a solução que se mostra adequada e necessária consiste na contratação de um **certificado digital SSL/TLS do tipo Wildcard com Validação Organizacional (OV)**, emitido por **Autoridade Certificadora de raiz internacional amplamente reconhecida**, garantindo aceitação automática pelos principais navegadores, sistemas operacionais e dispositivos móveis utilizados pelos usuários.

4.2. A utilização de certificado ***Wildcard*** é indispensável para abranger, sob um único certificado, todos os subdomínios associados ao domínio institucional, permitindo a expansão estruturada de serviços digitais, a padronização de mecanismos de autenticação e a simplificação da gestão tecnológica. A característica **OV**, por sua vez, assegura a verificação da existência jurídica e da legitimidade do órgão perante a Autoridade Certificadora. reforçando a confiança do usuário e mitigando riscos de ataques baseados em falsificação de identidade digital (phishing, spoofing, etc.).

4.3. Adicionalmente, destaca-se que o certificado atualmente em uso aproximase do término de sua vigência (27/03 /2026), e a descontinuidade desse serviço configura risco crítico para a operação digital do Ministério de Minas e Energia (MME). A expiração do certificado implicaria imediatamente:

- Exibição de **alertas de segurança** em todos os navegadores ao acessar sistemas e portais;
- **Interrupção de conexões seguras (HTTPS)**, com impacto direto na experiência do usuário e no cumprimento das políticas de segurança da informação;
- **Comprometimento de integrações sistêmicas**, incluindo integrações do **SEI** com outras instituições;
- **Interrupção de serviços dependentes de túnel seguro**, como VPNs corporativas;
- Possibilidade de **paralisação total ou parcial** de sistemas essenciais;
- Riscos à proteção de dados pessoais, em desacordo com a **LGPD**;
- Exposição da Administração a riscos reputacionais, operacionais e legais.

4.4. Nesse contexto, fica evidente que os certificados digitais compõem **infraestrutura crítica** para o funcionamento das soluções de TI do MME, servindo de base para a execução, coordenação e supervisão de políticas públicas, bem como para a oferta de serviços digitais ao cidadão e a interoperabilidade com demais órgãos da Administração Pública. A ausência ou inadequação dessa infraestrutura expõe o órgão a vulnerabilidades significativas, fragiliza a confiança no governo digital e compromete diretamente a efetividade das entregas institucionais.

4.5. Portanto, ainda que o certificado digital não represente uma ação finalística do MME, sua contratação é **instrumento imprescindível de sustentação tecnológica**, garantindo segurança, continuidade, autenticidade das aplicações web e conformidade com a **Lei nº 14.133/2021**, a **Lei nº 13.709/2018 (LGPD)**, a **Política de Segurança da Informação (POSIN), conforme portaria MME Nº 887, de 15 de dezembro de 2025**. Assim, a solução proposta atende ao interesse público ao proteger dados, assegurar a prestação ininterrupta de serviços digitais e sustentar a confiança do cidadão na atuação institucional.

5. Necessidades Tecnológicas

5.1. As necessidades tecnológicas do MME para a contratação de certificados digitais SSL/TLS abrangem a compatibilidade com seus ambientes computacionais, garantindo que a solução possa ser implementada e utilizada de forma consistente, replicando as configurações de segurança para assegurar a estabilidade e a proteção dos serviços em seu ambiente final.

5.2. É fundamental que os certificados sejam emitidos no formato **OV (Organization Validation)**, uma escolha tecnológica alinhada com a política de segurança do Ministério, que busca transmitir um nível elevado de confiança aos usuários através de um processo de validação de identidade mais rigoroso por parte da Autoridade Certificadora. Esta validação reduz riscos de falsificação de identidade digital, ataques de phishing e redirecionamentos maliciosos.

5.3. Observar-se ainda que o certificado deve ser do tipo "curinga", ***Wildcard,*** para ser seja possível realizar a proteção simultânea do domínio principal e de todos os seus subdomínios, conferindo abrangência e eficiência operacional ao processo de segurança digital.

5.4. Ademais, faz-se necessário que o certificado seja de **cadeia de confiança (raiz) internacional** para assegura compatibilidade automática com navegadores modernos e sistemas operacionais, evitando alertas de segurança que podem gerar indisponibilidade prática e perda de confiança do usuário. A escolha por padrão internacional fundamentase nos seguintes aspectos:

I. A ICPBrasil (Infraestrutura de Chaves Públicas Brasileira) utiliza raiz de certificação própria, com compatibilidade reduzida junto a navegadores e dispositivos que não reconhecem automaticamente essa cadeia de confiança.
II. A Resolução CG/ICP-Brasil nº 209/2024 encerrou a emissão de certificados SSL/TLS para websites no âmbito da ICPBrasil, devido à baixa interoperabilidade desses certificados com navegadores amplamente utilizados.
III. A Resolução CG/ICP-Brasil nº 211/2024 tornou facultativa a adoção dos requisitos WebTrust Baseline, permitindo às Autoridades Certificadoras adoção de padrões internacionais como os do CA/Browser Forum.
IV. Certificados OV *Wildcard* destinam-se exclusivamente à autenticação de servidores e criptografia HTTPS, não sendo utilizados para assinatura digital de documentos, o que dispensa aderência à infraestrutura da ICPBrasil.

5.5. A solução deve ainda implementar **padrões reconhecidos internacionalmente**, incluindo:

- chaves criptográficas de 2048 ou 4096 bits;
- criptografia forte de 256 ou 512 bits;
- conformidade plena com versões atuais do protocolo SSL/TLS (Secure Socket Layer / Transport Layer Security), garantindo sigilo, integridade e proteção contra ataques de interceptação ou adulteração.

5.6. Para garantir máxima interoperabilidade, o certificado deve ser automaticamente reconhecido por:

- 100% dos navegadores modernos (Chrome, Firefox, Edge, Safari, Opera);
- Sistemas operacionais amplamente utilizados (Windows, Linux);
- Dispositivos móveis (Android, iOS);
- Servidores web utilizados pelo MME (Apache, Nginx, IIS, Tomcat), além de outras aplicações que utilizem padrões **SSL/TLS** e o formato **x509 v3**.

5.7. Essa compatibilidade é necessária para garantir o funcionamento seguro, eficiente e ininterrupto dos serviços disponibilizados à sociedade e aos servidores.

5.8. Ademais, os padrões elencados nesta sessão refletem práticas recomendadas por instituições internacionais de segurança cibernética e asseguram resiliência frente às ameaças contemporâneas.

5.9. É essencial que o referido serviço seja prestado de forma continuada tendo em vista que este é necessário para proporcionar mecanismos de segurança adequadosdos aos serviços de TIC do Ministério que estão expostos na internet.

5.10. Diante do exposto, apresenta-se a seguir as características técnicas mínimas que o certificado deve possuir:

- Certificado digital para servidores Web aderente ao padrão internacional X.509;
- Permitir estabelecimento de sessões com protocolo SSL (Security Socket Layer) e TLS (Transport Layer Security);
- Conter chaves para criptografia assimétrica baseada no algoritmo RSA. O tamanho das chaves deve ser, no mínimo, 2048 bits;
- Permitir a utilização de criptografia simétrica com chaves de, no mínimo, 256 bits;
- Ser instalável em Microsoft Internet Information Server (IIS) versão 8.5 ou posterior e servidor Web Apache versão 2.2.x, ou posterior);
- Possuir nível de validação do tipo *Organization Validation* – OV;
- Suportar ilimitados subdomínios – *Wildcard*.

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

6.1. Além dos requisitos já mencionados na sessão anterior, o certificado deve abarcar:

- **reemissão gratuita e ilimitada durante a vigência** — importante para contingências e incidentes operacionais;
- **licenciamento para uso em múltiplos servidores sem custo adicional** — compatível com arquiteturas distribuídas e com o ambiente de produção/contingência do Ministério de Minas e Energia (MME);
- **processo de validação concluído em até 2 dias úteis**, reduzindo a janela de risco de expiração do certificado vigente;
- **validade de 12 meses**, prorrogados por 1 (um) período igual, preferencialmente com mecanismos de aviso antecipado e possibilidade de renovação planejada.
- **Suporte Técnico** da autoridade certificadora ou distribuidor com atendimento em português.

6.2. Ademais, a validação da propriedade do domínio deve ocorrer preferencialmente por meio de **registro DNS do tipo TXT**, método amplamente reconhecido por sua segurança, rastreabilidade e facilidade de auditoria, alinhado aos requisitos de governança e integridade das operações de TIC no setor público.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. A estimativa da demanda do certificado SSL baseou-se na quantidade de domínio que o Ministério de Minas e Energia possui e necessita manter.

7.2. Será necessário 1 (um) Certificado digital do tipo *Wildcard* SSL OV (Organizational Validation) dado que a Pasta possui apenas um domínio registrado, a saber: mme.gov.br, conforme apresenta-se abaixo:

PRODUTO	UNIDADE	QUANTIDADE
Certificado digital SSL Wildcard OV - raiz internacional	un	1

8. Levantamento de soluções

8.1. Necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas:

8.1.1. Investigamos necessidades similares em outros órgãos ou entidades da Administração Pública, analisando as soluções adotadas por eles, conforme pode ser verificado na pesquisa de preços anexadas a este documento.

8.2. As alternativas do mercado:

8.2.1. Pesquisamos e avaliamos as alternativas disponíveis no mercado para atender à necessidade de certificado digital wildcard para o domínio *.mme.gov.br, em que foi encontrado diversos fornecedores, os quais parte foi apresentado no Anexo 1 - Pesquisa de Preços, deste documento.

8.3. A existência de Software público brasileiro:

8.3.1. Não se aplica.

8.4. Políticas, modelos e padrões de governo:

8.4.1. Alinhamos a busca às políticas, modelos e padrões de governo, incluindo ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, sendo aplicável em especial o ICP-Brasil, o qual foi considerado como alternativa de solução.

8.5. Necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual:

8.5.1. Considerando que trata-se da continuidade do serviço de certificação Digital do tipo servidor, o qual já está implantado e em uso pelo MME, não há necessidade de realizar qualquer adequação do ambiente, desde que seja fornecido o item contratado conforme descrito nas especificações do objeto, mantendo o padrão usado atualmente.

8.6. Os diferentes modelos de prestação do serviço:

8.6.1. Não existem diferentes modelos de prestação de serviços, os certificados digitais para servidor, são comercializados como serviço e tempo determinado (1 ano, 2 anos, 3 anos, dentre outros).

8.7. Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes:

8.7.1. Os certificados podem ser adquiridos no modelo SSL padrão (protege um único domínio e não abrange os subdomínios) ou do modelo SSL Wildcard (protege um domínio principal e o número ilimitado de seus subdomínios).

8.7.2. O MME utiliza a solução para toda a gama de URLs descritas abaixo:

EXTERNAS
acessovpn.mme.gov.br
waf.mme.gov.br
dlpt.mme.gov.br
hlpt.mme.gov.br
hluzparatodos.mme.gov.br
jump.mme.gov.br
dsaped.mme.gov.br
saped.mme.gov.br
consultas-publicas.mme.gov.br
dluzparatodosapi.mme.gov.br
hsei.mme.gov.br
meu.mme.gov.br
paineis.mme.gov.br
petrvs-hmg.mme.gov.br
petrvs-dev.mme.gov.br
petrvs.mme.gov.br
projeteee.mme.gov.br
omne.mme.gov.br
suporte.mme.gov.br
dadosabertos.mme.gov.br
sei.mme.gov.br
sreidi.mme.gov.br
www.mme.gov.br
correio.mme.gov.br

antigo.mme.gov.br

INTERNAS
zabbix.mme.gov.br
suporte.mme.gov.br
correio.mme.gov.br
admin-sso.mme.gov.br
auth.mme.gov.br
cofre.mme.gov.br
consultas-publicas.mme.gov.br
dadosabertos.mme.gov.br
docflow.mme.gov.br
grafana.mme.gov.br
grafana-k8s.mme.gov.br
ipam.mme.gov.br
jump.mme.gov.br
meu.mme.gov.br
navegador.mme.gov.br
navegadorseguro.mme.gov.br
nessus.mme.gov.br
netbox.mme.gov.br
nexus.mme.gov.br
omne.mme.gov.br
openvas.mme.gov.br
paineis.mme.gov.br
petrvs.mme.gov.br
projeteee.mme.gov.br
projetos.mme.gov.br
rabbitmq.mme.gov.br
rancher.mme.gov.br
saped.mme.gov.br
scaee.mme.gov.br
sei.mme.gov.br
siem.mme.gov.br
sim.mme.gov.br
soar.mme.gov.br
sq.mme.gov.br
sreidi.mme.gov.br
sreidimin.mme.gov.br
sso.mme.gov.br
storage-api.mme.gov.br
taiga.mme.gov.br
vault.mme.gov.br
wiki.mme.gov.br

www.mme.gov.br
dauth.mme.gov.br
dconsultas-publicas.mme.gov.br
dlpt.mme.gov.br
dluzparatodos.mme.gov.br
dluzparatodosapi.mme.gov.br
dprojeteee.mme.gov.br
drabbitmq.mme.gov.br
dsaped.mme.gov.br
dscaee.mme.gov.br
dsreidi.mme.gov.br
dstorage-api.mme.gov.br
petrvs-dev.mme.gov.br
hadmin-sso.mme.gov.br
hauth.mme.gov.br
hconsultas-publicas.mme.gov.br
hlpt.mme.gov.br
hlpt-rabbitmq.mme.gov.br
hluzparatodos.mme.gov.br
hprojeteee.mme.gov.br
hrabbitmq.mme.gov.br
hrancher.mme.gov.br
hsaped.mme.gov.br
hscaee.mme.gov.br
hsei.mme.gov.br
hsreidi.mme.gov.br
hsso.mme.gov.br
hstorage-api.mme.gov.br
hsuporte.mme.gov.br
htaiga.mme.gov.br
hvault.mme.gov.br
petrvs-hmg.mme.gov.br
portalh.mme.gov.br

8.7.3. Assim, considerando a quantidade expressiva de subdominios do domínio principal existente no MME, entende-se ser adequado o uso do modelo *Wildcard* (curinga), dado que abarca toda a necessidade com uso de um único certificado na raiz (domínio).

8.8. A possibilidade de aquisição na forma de bens ou contratação como serviço:

8.8.1. A necessidade da presente contratação só é comercializada na forma de serviço.

8.9. A ampliação ou substituição da solução implantada:

8.9.1. A presente contratação trata-se da continuidade de uma solução já utilizada/implantada, em consequência da expiração da validade do certificado de servidor atualmente utilizado.

8.9.2. No entanto, vale ressaltar que o fornecedor/ CA - Autoridade Certificadora do certificado a ser contratado, poderá ser diferente do atual sem quer haja impactos na continuidade dos serviços que utilizam a solução.

8.10. As diferentes métricas de prestação do serviço e de pagamento:

10.1. Os certificados são metrificados por unidade, ou seja, uma unidade de certificado é emitido para um tempo pré determinado.

8.11. ALTERNATIVAS DE SOLUÇÕES

8.11.1. Diante do exposto, considerando os requisitos básicos e os levantamentos acima, as alternativas de soluções são elencadas considerando as variações dos Certificados de assinatura Digital SSL/TLS que seriam compatíveis com certificação de subdomínios (*wildcard*) existentes no mercado, bem como sua adoção em outros órgãos ou entidades da Administração Pública, a saber:

ID	DESCRIÇÃO DA ALTERNATIVA DE SOLUÇÃO
1	Contratação de empresa para prestação de serviço de emissão de Certificado SSL Wildcard OV emitidos por autoridades de raiz internacional
2	Contratação de empresa para prestação de serviço de emissão de Certificados SSL Wildcard OV emitidos por autoridades nacionais (ICP-Brasil)
3	Emissão de Certificados SSL *Wildcard* gratuitos por emitidos por meio de autoridades certificadoras abertas.

9. Análise comparativa de soluções

9.1. Foram consideradas as seguintes alternativas de soluções para atendimento das necessidades do MME:

9.2. Alternativa 1 – Certificado SSL Wildcard OV emitidos por autoridades de raiz internacional

9.2.1. Descrição da solução: Consiste na contratação, por meio de fornecedor qualificado, de certificado digital **SSL/TLS Wildcard** com **Validação Organizacional (OV)**, emitido por **Autoridade Certificadora de raiz internacional**, reconhecida automaticamente pela totalidade dos navegadores modernos e dispositivos móveis. Este tipo de certificado possibilita a autenticação institucional e a proteção simultânea de todos os subdomínios ligados ao domínio **mme.gov.br**, garantindo criptografia robusta e compatibilidade universal.

9.2.2. Solução baseada em ACs globais reconhecidas (ex.: DigiCert, Sectigo, GlobalSign), com ampla compatibilidade, validação OV e suporte estruturado.

9.2.3. Pontos positivos:

- Alta compatibilidade e confiança;
- Validação organizacional, reduzindo o risco de fraude;
- Documentação;
- Suporte técnico do fornecedor.

9.2.4. Pontos negativos:

- Custo superior quando comparado ao modelo de certificado DV (Domain Validated);
- Validação pode ser mais demorada (1 a 3 dias, pois requer verificação manual).

9.3. Alternativa 2 – Certificados SSL Wildcard OV emitidos por autoridades nacionais (ICP-Brasil)

9.3.1. Descrição da solução: Consiste na contratação de certificados digitais emitidos no âmbito da **ICPBrasil**, infraestrutura oficial brasileira. Embora amplamente reconhecida em aplicações nacionais, essa alternativa enfrenta limitações relevantes para uso em HTTPS e proteção de múltiplos subdomínios do MME.

9.3.2. Recentemente, a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) decidiu interromper a emissão de certificados digitais SSL/TLS, aqueles que mostram o "cadeado" na barra de endereço de sites. Essa mudança foi regulamentada pela **Resolução CG ICP-Brasil nº 209/2024**, e afeta apenas os certificados SSL /TLS usados em websites, comuns para a navegação na internet.

9.3.3. Certificados vinculados à infraestrutura nacional, podendo apresentar restrições de compatibilidade universal em navegadores e menor oferta de Wildcard conforme mercado.

9.3.4. Pontos positivos:

- Alinhamento à infraestrutura nacional de chaves públicas;
- Respaldo regulatório local.

9.3.5. Pontos negativos:

- Possíveis limitações de compatibilidade global;
- Oferta/aderência a *Wildcard* possivelmente limitada.
- Certificados SSL/TLS ICP-Brasil não geram mais "cadeado" confiável em browsers comuns;
- Resolução nº 209/2024 restringe o uso apenas para ambientes fechados, como redes corporativas, Open Banking e SPB.

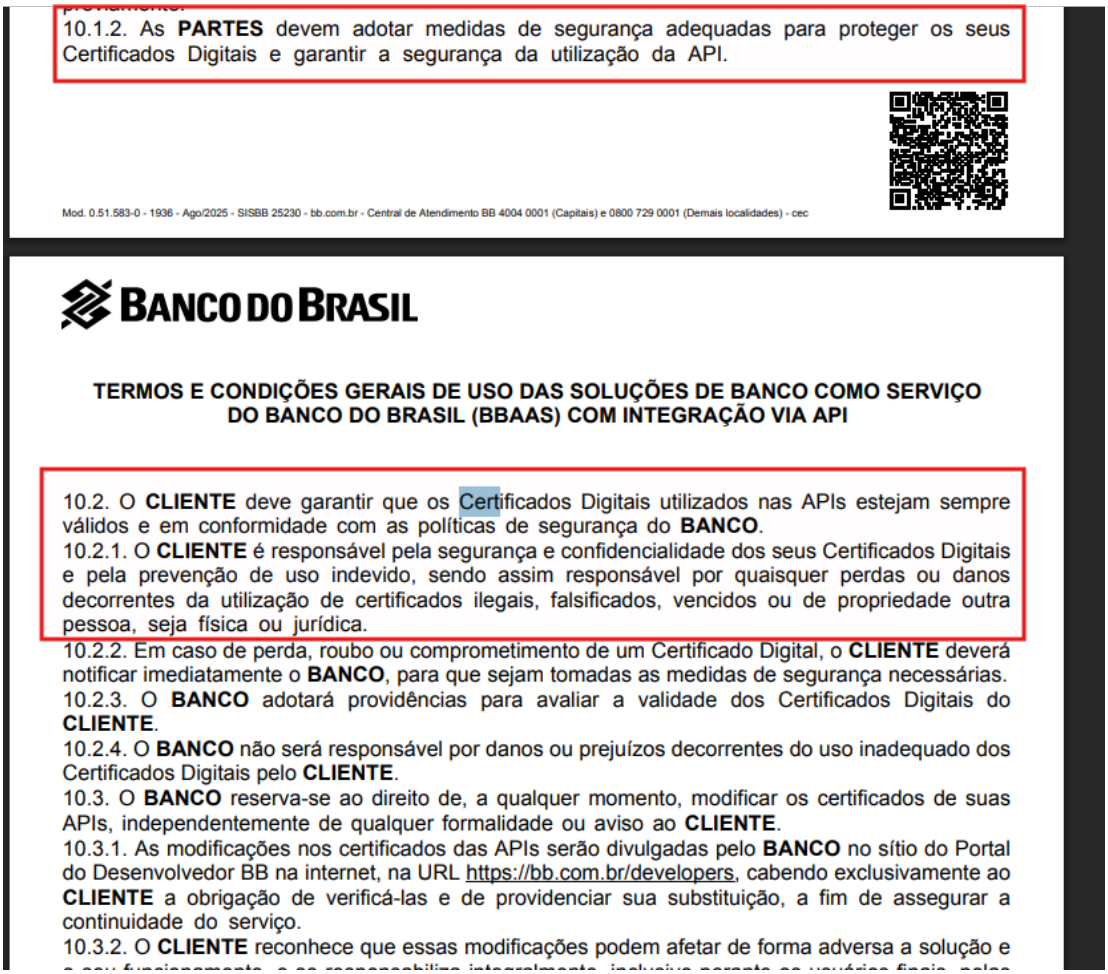
9.4. Alternativa 3 – Certificados SSL *Wildcard* emitidos por autoridades certificadoras abertas

9.4.1. Descrição da solução: Consiste na emissão de certificados digitais do tipo *Wildcard* por meio de Autoridade Certificadora (AC) gratuita, automatizada e aberta (exemplo: https://letsencrypt.org). Os quais possuem validade máxima de 90 dias e validação do tipo Domain Validated (DV), método de validação inferior ao previsto neste Estudo Técnico Preliminar (Organization Validated).

9.4.2. Por se tratar de certificados gratuitos com processo de emissão automatizado, não possuem padrões em total conformidade com as boas práticas de segurança da informação. Não oferecem também suporte ao produto, sendo este baseado na documentação publicada na Internet e nos fóruns da comunidade de usuários.

9.4.3. Além do mais, pelo curto prazo de validade, a Autoridade Certificadora recomenda atualização automática a cada 60 dias, o que implica no aumento do esforço na gestão dos certificados digitais pelas diferentes equipes responsáveis pela sua administração e aumenta também o risco de incidentes relacionados à não atualização tempestiva de todos os servidores de aplicação.

9.4.4. Por fim, vale observar que o MME possui um importante sistema que envolve transação financeira, o Sistema de Arrecadação para Pesquisa e Desenvolvimento - SAPED possui integração com o banco do brasil, usa a API MME para dar baixa em boletos. Os documentos Termos e condições do uso das APIs do BB deixa expresso a preocupação com o certificado digital utilizado. Vide abaixo:



10.1.2. As **PARTES** devem adotar medidas de segurança adequadas para proteger os seus Certificados Digitais e garantir a segurança da utilização da API.

Mod. 0.51.583-0 - 1936 - Ago/2025 - SISBB 25230 - bb.com.br - Central de Atendimento BB 4004 0001 (Capitais) e 0800 729 0001 (Demais localidades) - cec

BANCO DO BRASIL

TERMOS E CONDIÇÕES GERAIS DE USO DAS SOLUÇÕES DE BANCO COMO SERVIÇO DO BANCO DO BRASIL (BBAAS) COM INTEGRAÇÃO VIA API

10.2. O **CLIENTE** deve garantir que os Certificados Digitais utilizados nas APIs estejam sempre válidos e em conformidade com as políticas de segurança do **BANCO**.
10.2.1. O **CLIENTE** é responsável pela segurança e confidencialidade dos seus Certificados Digitais e pela prevenção de uso indevido, sendo assim responsável por quaisquer perdas ou danos decorrentes da utilização de certificados ilegais, falsificados, vencidos ou de propriedade outra pessoa, seja física ou jurídica.
10.2.2. Em caso de perda, roubo ou comprometimento de um Certificado Digital, o **CLIENTE** deverá notificar imediatamente o **BANCO**, para que sejam tomadas as medidas de segurança necessárias.
10.2.3. O **BANCO** adotará providências para avaliar a validade dos Certificados Digitais do **CLIENTE**.
10.2.4. O **BANCO** não será responsável por danos ou prejuízos decorrentes do uso inadequado dos Certificados Digitais pelo **CLIENTE**.
10.3. O **BANCO** reserva-se ao direito de, a qualquer momento, modificar os certificados de suas APIs, independentemente de qualquer formalidade ou aviso ao **CLIENTE**.
10.3.1. As modificações nos certificados das APIs serão divulgadas pelo **BANCO** no sítio do Portal do Desenvolvedor BB na internet, na URL https://bb.com.br/developers, cabendo exclusivamente ao **CLIENTE** a obrigação de verificá-las e de providenciar sua substituição, a fim de assegurar a continuidade do serviço.
10.3.2. O **CLIENTE** reconhece que essas modificações podem afetar de forma adversa a solução e

fonte: https://publicador.developers.bb.com.br/bucket/termos_e_condicoes_gerais_de_uso_das_apis_4f2be9c744.pdf

9.4.5. Pontos positivos:

- Sem custo de aquisição.

9.4.6. Pontos negativos:

- Não possuem padrões em total conformidade com as boas práticas de segurança da informação
- Não atende requisito de OV - Validação Organizacional e Garantia de Identidade;
- Não possui Acordo de Nível de Serviço (SLA) e Responsabilidade Legal;
- Risco Operacional devido ao baixo período de validade;
- Dependência de automação de renovação;
- Suporte limitado.

9.5. Análise comparativa das Alternativas de Soluções levantadas:

REQUISITO	SOLUÇÃO 1	SOLUÇÃO 2	SOLUÇÃO 3
Garantir validação do tipo Organization Validated (OV)	Atende	Atende	Não Atende
Suportar ilimitados subdomínios – *Wildcard*	Atende	Atende	Atende
Conservar raiz internacional	Atende	Não Atende	Atende

Possuir compatibilidade com os principais navegadores do mercado sem a necessidade de instalação manual de cadeia de certificados.	Atende	Não Atende	Atende
Possuir validade mínima de 12 (doze) meses.	Atende	Atende	Não Atende
Possuir suporte técnico especializado	Atende	Atende	Não Atende
RESULTADO	**Viável**	**Não Viável**	**Não Viável**

10. Registro de soluções consideradas inviáveis

10.1. Registra-se a seguir as alternativas de soluções que foram consideradas, após análise apresentada na sessão anterior, como inviáveis:

10.2. Alternativa 2 – Certificados SSL Wildcard OV emitidos por autoridades nacionais (ICP-Brasil)

10.2.1. Justificativa da inviabilidade:

10.2.1.1. Devido a a falta de interoperabilidade dos certificados ICP-Brasil com os principais navegadores do mercado, o que gerava problemas de confiabilidade e segurança para os usuários, o Comitê Gestor da ICP-Brasil publicou a Resolução CG/ICP-Brasil nº 209/2024, de 7/8/2024, que encerrou a emissão de certificados SSL/TLS para websites.

10.2.1.2. A Resolução CG/ICP-BRASIL nº 211 de 31/10/2024, estabeleceu que a adesão , aos requisitos WebTrust Baseline para a emissão de certificados SSL/TLS não é mais obrigatória.

10.2.1.3. Dessa forma, as Autoridades Certificadoras que desejarem emitir certificados SSL/TLS podem optar por seguir as normas da ICP-Brasil ou as de outros padrões internacionais, como o CA/Browser Forum.

10.2.1.4. Como o certificado SSL Wildcard OV é destinado para à proteção de tráfego web (criptografia HTTPS) e à autenticação do servidor, e não para assinatura digital de documentos, a aderência à ICPBrasil não é um requisito funcional direto para o seu uso.

10.2.1.5. Ademais, a garantia de uma experiência de navegação segura e sem problemas de interoperabilidade é um requisito essencial para a presente contratação, o que denota a inviabilidade da presente alternativa de solução para a contratação pleiteada.

10.3. Alternativa 3 – Certificados SSL *Wildcard* emitidos por autoridades certificadoras abertas

10.3.1. Justificativa da inviabilidade:

10.3.1.1. Como uma possível solução temporária ou plano de contingência, o certificado Let's Encrypt poderia ser considerado para garantir a criptografia básica (HTTPS) nos subdomínios do MME de forma rápida e gratuita em situações emergenciais, dada a sua facilidade de emissão e renovação automatizada.

10.3.1.2. No entanto, é fundamental reconhecer que, por oferecer apenas validação de domínio (DV) e possuir uma validade mais curta, o Let's Encrypt não atende ao requisito essencial de validação organizacional (OV) exigido para a contratação principal, nem oferece as garantias e o suporte de um certificado comercial, tornando-o uma solução inviável para substituir a necessidade de um certificado Wildcard OV no longo prazo.

11. Análise comparativa de custos (TCO)

11.1. A construção de um quadro comparativo de requisitos de negócio e tecnológicos objetiva viabilizar a classificação das alternativas do ponto devista qualitativo.

11.2. Após a realização da prospecção das soluções candidatas e a análise técnica e funcional dos cenários possíveis, procedeu-se a análise comparativa de custos das soluções viáveis (Solução Viável 1 - Contratação de empresa para prestação de serviço de emissão de Certificado SSL Wildcard OV emitidos por autoridades de raiz internacional).

11.3. O custo total de propriedade, do inglês (TCO), é um método utilizado para calcular o custo global de um produto ouTotal Cost of Ownershsipserviço ao longo de seu ciclo de vida, considerando custos diretos e indiretos.

11.4. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE (TCO)

11.4.1. O cálculo dos custos totais de propriedade refere-se à estimativa dos custos dos cenários projetados ao longo do uso da solução, possibilitando uma análise mais precisa e abrangente economicamente, e, por conseguinte, é necessário estimar os custos de bens e serviços para cada cenário viável, caso haja mais de um cenário viável.

11.4.2. Nesse caso, foi encontrada apenas uma solução viável para atender as necessidades requeridas pelo MME, a saber, Solução Viável 1 - Contratação de empresa para prestação de serviço de emissão de Certificado SSL Wildcard OV emitidos por autoridades de raiz internacional.

11.4.3. A Tabela a seguir apresenta o cálculo do TCO da Solução Viável 1.

Solução Viável 1 – Contratação de empresa para prestação de serviço de emissão de Certificado SSL Wildcard OV emitidos por autoridades de raiz internacional	
ANO	**ANO 1**
ITEM	
emissão de Certificado SSL Wildcard OV emitidos por autoridades de raiz internacional	R$ 1.175,00

11.4.4. Para estimar o custo médio da alternativa de solução da presente contratação, foi realizada pesquisa de preços e análise de preços em consonância com os parâmetros dispostos no Artigo 5º da Instrução Normativa SEGES/ME nº 65, de 07 de julho de 2021, e suas atualizações, que versa sobre o procedimento para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional, conforme apresenado no Anexo I - Pesquisa de Preços do presente Estudo Técnico Preliminar.

11.4.5. Por fim, registra-se que o TCO estimado da Solução viável 1 foi de **R$ 1.175,00 (mil cento e setenta e cinco reais)** .

12. Descrição da solução de TIC a ser contratada

12.1. Contratação de serviço de emissão de Certificado de assinatura Digital SSL/TLS, compatível com certificação de subdomínios (*wildcard*), de tipo Validação Organizacional (OV) e cadeia de confiança (raiz) internacional.

12.2. A solução de TIC a ser contratada consiste na aquisição de um **Certificado Digital SSL/TLS do tipo Wildcard com Validação Organizacional (OV)**, emitido por **Autoridade Certificadora (AC) de raiz internacional** amplamente reconhecida pelos principais navegadores, sistemas operacionais e dispositivos móveis. Esse certificado constitui componente crítico da infraestrutura de segurança do Ministério de Minas e Energia (MME), responsável por garantir a confidencialidade, a integridade e a autenticidade das comunicações estabelecidas entre usuários, sistemas e serviços vinculados ao domínio institucional ***.mme.gov.br**.

12.3. O certificado Wildcard OV a ser contratado utiliza **protocolos criptográficos padrão internacional (TLS)** e arquitetura de certificação baseada em **x.509 v3**, com chaves criptográficas robustas (2048 ou 4096 bits) e criptografia forte. A solução permite proteger, por meio de um único certificado, todos os subdomínios vinculados ao domínio institucional, assegurando interoperabilidade, padronização técnica e gerenciamento centralizado, reduzindo riscos de inconsistência e falhas associadas à gestão de múltiplos certificados distintos.

12.4. A emissão por AC internacional garante não apenas a aceitação automática e global da cadeia de confiança, mas também assegura que os usuários internos e externos não enfrentarão alertas de segurança, bloqueios ou mensagens de site inseguro, circunstâncias que impactariam diretamente a continuidade e a credibilidade dos serviços digitais do Ministério.

12.5. Como a Solução Atende às Necessidades Identificadas:

12.5.1. Proteção criptográfica robusta

12.5.1.1 A solução oferece criptografia de ponta a ponta em todas as transações estabelecidas entre servidores, sistemas e usuários, prevenindo acessos indevidos, interceptações, adulterações de informações e ataques “maninthemiddle”. Essa proteção é essencial para serviços que tratam informações sensíveis e dados pessoais, em consonância com a LGPD.

12.5.2. Garantia de autenticidade institucional

12.5.2.1. A modalidade **OV (Organization Validation)** atesta formalmente a identidade do MME, informando aos usuários que o domínio acessado pertence, de fato, à instituição — mecanismo essencial para prevenir ataques de phishing, falsificação de páginas e fraudes digitais que exploram a confiança do cidadão.

12.5.3. Cobertura integral de múltiplos subdomínios

15.5.3.1. Por se tratar de certificado **Wildcard**, a proteção se estende a todos os subdomínios de ***.mme.gov.br**, viabilizando a expansão de novos serviços digitais, sem necessidade de múltiplos certificados individuais. Essa cobertura reduz riscos operacionais, facilita a gestão, evita descompassos de validade e fortalece a governança tecnológica.

12.5.4. Máxima compatibilidade e interoperabilidade

15.5.4.1. A solução é automaticamente reconhecida por 100% dos navegadores modernos (Chrome, Firefox, Edge, Safari, Opera), sistemas operacionais amplamente utilizados (Windows, Linux) e dispositivos móveis (Android, iOS), sem necessidade de instalação manual de certificados intermediários. Isso garante a plena funcionalidade de conexões HTTPS, inclusive para usuários externos e transfronteiriços.

12.5.5. Conformidade com requisitos legais e normativos

12.5.5.1. A contratação está alinhada:

- à **Lei nº 14.133/2021**, que exige planejamento prévio, mitigação de riscos e aderência ao interesse público;
- à **IN SGD/ME nº 94/2022**, que determina a descrição clara da solução tecnológica e sua adequação às necessidades de negócio;
- à **LGPD (Lei nº 13.709/2018)**, que exige proteção de dados pessoais em trânsito;
- ao **Decreto nº 10.046/2019**, que disciplina a governança e integridade de dados;
- às políticas internas de segurança da informação.

12.5.6. Suporte técnico especializado e confiável

12.5.6.1. Sendo emitido por autoridade certificadora internacional de alta reputação, o certificado conta com suporte técnico estruturado, documentação detalhada e mecanismos de atendimento adequados para instalação, renovação, reemissão e resolução de incidentes.

12.5.7. Durabilidade, renovação eficiente e governança

15.5.7.1. Os certificados de raiz internacional apresentam ciclo de atualização compatível com os padrões modernos de segurança, fornecem mecanismos de renovação clara e alertas de expiração, e permitem **reemissão ilimitada** durante a validade contratual — garantindo continuidade dos serviços e mitigação de riscos.

12.6. Conclusão

12.6.1. A solução de TIC proposta — Certificado Digital SSL/TLS Wildcard OV, de raiz internacional — atende integralmente aos requisitos tecnológicos, operacionais, normativos e de negócio identificados no Ministério de Minas e Energia. Ela se alinha às melhores práticas de segurança da informação, garante continuidade de serviços públicos digitais, protege dados sensíveis, reduz riscos operacionais e jurídicos, e materializa infraestrutura crítica de apoio às políticas públicas e às atividades finalísticas do órgão.

13. Estimativa de custo total da contratação

Valor (R$): 1.175,00

13.1. O valor total estimado da contratação é de **R$ 1.175 (um mil e cento e setenta e cinco reais)**, definido de acordo com a tabela a seguir:

ID	CATMAT/ CARTSER	DESCRIÇÃO	QUANT.	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
Item1	27170	Certificado Digital SSL Wildcard, com Validação da Organização (OV), padrão internacional, com vigência de 12 meses.	01	R$ 1.175,00	R$ 1.175,00

13.2. A metodologia utilizada para estimativa do valor da contratação bem como os documentos que lhes dão suporte estão indicados no Relatório da Pesquisa de Preços, disponível no Anexo I deste ETP.

14. Justificativa técnica da escolha da solução

Como a solução escolhida atende melhor às especificações da demanda:

Critério/Especificação	Atendimento pela Solução Escolhida
Proteção de múltiplos subdomínios	Certificado SSL Wildcard cobre todos os subdomínios do domínio principal, simplificando a gestão e ampliando o escopo de proteção.

Validação organizacional (OV)	Garante a verificação da existência e legitimidade da instituição, aumentando a confiança dos usuários.
Reconhecimento internacional da raiz	Compatibilidade universal com browsers, sistemas e dispositivos diversos, inclusive em contextos internacionais.
Conformidade normativa e legal	Atenda a todos os requisitos legais (Lei 14.133/2021, LGPD, etc.) e padrões técnicos estabelecidos para o setor público. Portaria Nº 887, de 15 de dezembro de 2025 - Política de Segurança da Informação do Ministério de Minas e Energia (POSIN-MME)
Garantia de integridade, autenticidade e confidencialidade	Criptografia robusta e validação institucional oferecem proteção abrangente aos dados trafegados; Redução de riscos.
Suporte técnico e documentação	Fornecedores internacionais oferecem suporte qualificado e documentação clara para todos os estágios da implementação e manutenção.

.

15. Justificativa econômica da escolha da solução

15.1. A escolha pela aquisição de certificados digitais do tipo Wildcard SSL com validação organizacional (OV) fundamenta-se em critérios técnicos alinhados aos princípios da economicidade, eficiência administrativa e mitigação de riscos operacionais e de segurança da informação.

15.2. Durante a etapa de pesquisa de preços, verificou-se a existência de diversos fornecedores que ofertam o referido serviço no mercado, o que demonstra a ampla competitividade da solução, bem como a disponibilidade de alternativas com condições comerciais similares.

15.3. A análise comparativa dos preços coletados evidenciou que os valores unitários praticados para certificados com vigência anual apresentam baixa dispersão entre os fornecedores, mantendo-se dentro de uma faixa de similaridade compatível com os parâmetros de mercado. Tal cenário indica que a realização da contratação por meio de dispensa eletrônica de licitação, com disputa de lances, tende a estimular a competitividade entre os participantes, possibilitando a obtenção da proposta mais vantajosa para a Administração.

15.4. Adicionalmente, a adoção de certificados Wildcard SSL permite a proteção de múltiplos subdomínios vinculados a um mesmo domínio principal, reduzindo a necessidade de aquisição de certificados individuais e, consequentemente, otimizando custos de contratação, gestão e renovação, além de simplificar a administração da infraestrutura de segurança digital.

15.5. Dessa forma, conclui-se que a contratação pretendida configura solução economicamente vantajosa, tecnicamente adequada e operacionalmente eficiente, atendendo às necessidades institucionais e justificando sua adoção como estratégia mais apropriada para a Administração.

16. Benefícios a serem alcançados com a contratação

16.1. A contratação do certificado digital SSL/TLS Wildcard OV, com raiz internacional, permitirá ao Ministério de Minas e Energia alcançar um conjunto robusto de benefícios técnicos, operacionais, normativos e estratégicos, garantindo maior maturidade em segurança da informação, continuidade dos serviços digitais e atendimento pleno ao interesse público.

16.2. Fortalecimento da segurança da informação e da confiança institucional

- Elevação do nível de proteção criptográfica, assegurando comunicações seguras entre servidores, aplicações e usuários.
- Validação Organizacional (OV) reforça a identidade institucional do MME, mitigando riscos de ataques de phishing, spoofing e falsificação de páginas.
- Redução de riscos de interceptação, adulteração de tráfego e ataques maninthemiddle.

16.2.1. Impacto esperado: melhora significativa no nível de segurança cibernética, requisito essencial em ambientes que tratam dados pessoais, informações sensíveis e conteúdos oficiais.

16.3. Garantia de continuidade operacional e estabilidade dos serviços digitais

- Prevenção de interrupções causadas por certificados expirados ou incompatíveis.
- Evita notificações de “site não seguro” e bloqueios automáticos de navegadores.
- Mantém operantes integrações críticas, como VPNs, serviços internos e conexões com sistemas de outros órgãos (ex.: integrações SEISEI).

16.3.1. Impacto esperado: continuidade ininterrupta dos serviços digitais essenciais do MME.

16.4. Simplificação da gestão de certificados e redução de riscos administrativos

- Centralização da proteção de múltiplos subdomínios por meio de um único certificado Wildcard.
- Redução de incidentes de expiração decorrentes da gestão fragmentada de diversos certificados isolados.
- Menor carga operacional para equipes de TIC, reduzindo retrabalho e falhas humanas.

16.4.1. Impacto esperado: governança mais eficiente e diminuição de vulnerabilidades operacionais.

16.5. Ampliação da compatibilidade e interoperabilidade

- Reconhecimento automático em 100% dos navegadores modernos, sistemas operacionais e dispositivos móveis.
- Eliminação de mensagens de alerta e barreiras de uso para cidadãos, servidores e parceiros institucionais.
- Maior aderência a ambientes híbridos, distribuídos ou multi-cloud.

16.5.1. Impacto esperado: experiência do usuário maximizada, com acessos estáveis e seguros em qualquer contexto.

16.6. Conformidade legal, regulatória e alinhamento às melhores práticas

- Atende integralmente à **Lei nº 14.133/2021**, garantindo planejamento, análise e mitigação de riscos.
- Suporta obrigações da **LGPD**, assegurando confidencialidade de dados pessoais em trânsito.
- Está alinhado às diretrizes de segurança da informação, governança digital e padrões internacionais de criptografia.
- Contribui para a conformidade com recomendações técnicas do ITI, práticas internacionais e normativos internos.

16.6.1. Impacto esperado: redução de riscos institucionais, legais e de responsabilização administrativa.

16.7. Melhoria da experiência do usuário e fortalecimento da confiança pública

- Elimina avisos de “site inseguro”, que comprometem a percepção de qualidade e credibilidade.
- Garante acesso seguro e fluido aos serviços digitais, promovendo confiança no Ministério.
- Eleva a qualidade de serviços orientados ao cidadão e aos servidores.

16.7.1. Impacto esperado: maior adesão e confiança ao uso das plataformas e sistemas governamentais.

16.8. Redução de incidentes, retrabalho e custos indiretos

- Menor incidência de falhas associadas à expiração inesperada.
- Reduz necessidade de emissão de múltiplos certificados individuais.
- Minimiza interrupções que causariam prejuízos operacionais e desgaste institucional.

16.8.1. Impacto esperado: eficiência operacional e menor custo total de propriedade (TCO).

16.9. Suporte técnico qualificado e previsibilidade operacional

- A contratação de AC internacional assegura atendimento especializado, documentação robusta e reemissão ilimitada.
- Facilita gestão de incidentes e reduz tempo de resposta em caso de emergências.
- Proporciona previsibilidade ao ciclo de vida do certificado e processo de renovação.

16.9.1. Impacto esperado: maturidade na gestão da infraestrutura criptográfica institucional.

16.10. Conclusão

16.10.1. A adoção do certificado SSL/TLS Wildcard OV com raiz internacional proporciona ganhos diretos e mensuráveis de segurança, eficiência, governança, confiabilidade e adequação normativa. Tratase de solução que fortalece a infraestrutura crítica de TIC, protege dados, garante continuidade de serviços essenciais e sustenta o processo de transformação digital do MME, atendendo plenamente ao interesse público e às exigências dos órgãos de controle.

17. Providências a serem Adotadas

17.1. Por se tratar de objeto padronizado e contratado com recorrência por parte do MME, não há necessidade de adequação no ambiente computacional da Pasta, alteração em processos ou procedimentos, bem como adequações de recursos materiais ou capacitação de servidores para operarem a solução. Assim, não existem providências prévias a serem adotadas.

17.2. No entanto, no que se refere a mecanismo de contingência operacional, para garantir a continuidade da segurança das comunicações mesmo diante de falhas ou indisponibilidade do certificado SSL wildcard principal, será mantido um certificado SSL alternativo do tipo gratuito, previamente emitido e armazenado em repositório seguro,

permitindo sua ativação imediata em caso de revogação, expiração inesperada, comprometimento da chave privada ou falhas na renovação automática. Adicionalmente, será adotado monitoramento contínuo do status do certificado e alertas pró-ativos para prevenir indisponibilidades.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

A viabilidade da contratação da solução proposta fundamenta-se nos seguintes aspectos:

- **Amparo legal** para a contratação do objeto pretendido, em conformidade com a legislação vigente aplicável às contratações públicas.
- **Existência de contratações similares bem-sucedidas** realizadas por diversos órgãos da Administração Pública Federal, o que evidencia a maturidade e a aderência da solução no âmbito governamental.
- **Alinhamento entre as necessidades institucionais do Ministério de Minas e Energia (MME)** e as funcionalidades e características apresentadas pela Solução 1.
- **Disponibilidade de equipe técnica qualificada no MME**, com capacidade para gerenciar e acompanhar a execução da Solução 1, assegurando o alcance dos resultados esperados.
- **Existência de fornecedores no mercado** aptos a atender à demanda do MME, tanto em relação aos requisitos técnicos quanto aos quantitativos previstos, garantindo competitividade no processo de contratação.
- **Disponibilidade de recursos orçamentários e previsão orçamentária** para suportar a contratação pretendida.
- **Compatibilidade da contratação com os instrumentos de planejamento institucional do MME**, assegurando sua aderência às diretrizes estratégicas do órgão.
- **Viabilidade técnica da Solução 1**, considerando os requisitos operacionais e tecnológicos necessários ao atendimento da demanda institucional.
- **Expectativa de obtenção de resultados satisfatórios em termos de economicidade, eficiência e tempestividade**, possibilitando o adequado atendimento das necessidades corporativas do MME.

Diante desses fatores, conclui-se pela **viabilidade técnica, administrativa e econômica da contratação da Solução 1**, como alternativa adequada para atendimento da demanda institucional.

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.

NUBIAN MENDONCA AMORIM

Integrante Requisitante

Assinou eletronicamente em 19/03/2026 às 17:27:01.

CESAR RIBEIRO SARMENTO

Integrante Técnico

Assinou eletronicamente em 19/03/2026 às 17:28:19.

LETICIA CIRQUEIRA DE OLIVEIRA

Integrante Administrativo

Assinou eletronicamente em 20/03/2026 às 10:55:19.

Despacho: Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

MARCIO NAHAS RIBEIRO

Autoridade competente

Assinou eletronicamente em 20/03/2026 às 16:14:00.