CADERNO DE APOIO DA ESCUTA DE MERCADO SOBRE SOLUÇÃO DE NUVEM BRASILEIRA

MGI/SERPRO/ABDI/BNDES

AGOSTO DE 2026

O Ministério da Gestão e da Inovação em Serviços Públicos (MGI), o Serviço Federal de Processamento de Dados (SERPRO), o Banco Nacional de Desenvolvimento Econômico e Social (BNDES) e a Agência Brasileira de Desenvolvimento Industrial (ABDI), no âmbito das ações previstas em Acordo de Cooperação Técnica, realizarão procedimento de escuta de mercado sobre oferta de solução de computação em nuvem no Brasil.

O objetivo geral dessa escuta é obter contribuições que possam subsidiar a modelagem técnica, jurídica e de negócios para o eventual estabelecimento de parceria para o desenvolvimento de solução nacional de computação em nuvem que atenda a elevados requisitos de soberania (denominada, para fins dessa Escuta de Mercado, Nuvem Brasileira).

Podem participar pessoas físicas, empresas, entidades representativas, instituições de ensino e pesquisa e demais interessados no tema, mediante inscrição na página: www.abdi.com.br/nuvembrasileira. Os dados serão utilizados exclusivamente para controle de acesso à sessão e registro de presença. Os inscritos receberão, no e-mail cadastrado, o link da reunião online que ocorrerá no Microsoft Teams.

1. A Escuta de Mercado

Às 10h da manhã do dia 03 de setembro de 2026 será realizada audiência pública exclusivamente para a apresentação do desafio e o esclarecimento de eventuais dúvidas. Na ocasião, será disponibilizado formulário eletrônico com questionário para que os interessados possam enviar respostas e contribuições ao processo.

Além da audiência pública, a critério dos organizadores, poderão ser realizadas outras reuniões coletivas ou individuais. As reuniões individuais somente serão agendadas após a realização da reunião coletiva e mediante solicitação prévia e formal dos interessados.

O agendamento da reunião individual constitui uma faculdade dos organizadores, que analisarão os pedidos com base em critérios de pertinência, conveniência e oportunidade, não havendo obrigatoriedade de atendimento a todas as solicitações.

As solicitações de Escutas Individuais para a apresentação de potenciais soluções ou para o esclarecimentos de dúvidas remanescentes poderão ser feitas após a Escuta Coletiva pelo e-mail: nuvembrasileira@abdi.com.br.

Todas as reuniões serão gravadas e suas respectivas transcrições, juntadas ao processo administrativo correspondente.

As informações fornecidas pelo MGI, SERPRO, BNDES ou ABDI no âmbito dessa Escuta de Mercado **não possuem caráter vinculante e não configuram qualquer compromisso legal ou obrigacional por parte dessas instituições**. A participação na Escuta de Mercado **não garante o direito de celebração de contrato com o Governo Federal, tampouco gera expectativa legítima de tal contratação**.

2. Definição

A Nuvem Brasileira é uma modalidade de computação em nuvem que atende a requisitos elevados de soberania.

As nuvens de governo atuais endereçam aspectos relacionados com a soberania de dados, garantindo, em muitos casos, a residência de dados críticos em território nacional, sob jurisdição brasileira, operados por órgãos ou empresas públicas e equipes nacionais.

A Nuvem Brasileira vai além, exigindo que as próprias tecnologias, especialmente de software, que compõem o ecossistema para prestação de serviços de computação em nuvem possam ser desenvolvidas, mantidas e evoluídas por instituições e equipes técnicas nacionais, sem depender amplamente de tecnologias estrangeiras ou de autorização e/ou cooperação de fornecedores estrangeiros.

A Nuvem Brasileira é caracterizada por dois atributos:

- **Interoperabilidade:** a plataforma é construída sobre padrões e formatos abertos de modo que os sistemas do governo possam migrar de um ambiente para outro sem precisar ser reescritos. No plano do hardware, a arquitetura deve suportar equipamentos de múltiplos fornecedores, reduzindo a dependência de um único fabricante estrangeiro e garantindo resiliência frente a interrupções de fornecimento por razões geopolíticas ou comerciais.
- **Capacidade nacional:** a plataforma deve ser desenvolvida, mantida e evoluída por pessoas residentes no país e instituições nacionais. Não basta ter o direito de acessar o código-fonte, é preciso que haja, no país, o domínio técnico efetivo sobre os sistemas críticos da nuvem.

Este projeto tem foco em software. Não são objeto da solução buscada neste momento: aquisição de ativos de infraestrutura de TIC ou de rede, ou a contratação de *hosting, co-location ou housing*, nem a contratação de serviços de desenvolvimento e manutenção de software aplicativo finalístico dos órgãos públicos usuários da plataforma. O desenvolvimento, a manutenção e a evolução contínua da própria plataforma de nuvem incluindo eventual P&D relacionado são, por outro lado, objeto central da eventual parceria, conforme detalhado na Seção 5: Exigências Estratégicas.

Ressalta-se que as informações apresentadas a seguir possuem caráter preliminar e têm como principal objetivo subsidiar e orientar o início das discussões sobre o tema.

Nenhuma informação fornecida no âmbito dessa Escuta de Mercado é vinculante e, por isso, pode ser modificada a critério da Administração Pública.

2.1. Definições Arquiteturais

Conceito	Definição
Região	Localidade geográfica onde a plataforma disponibiliza serviços, com identidade, catálogo e conectividade próprios. Diferentes regiões podem oferecer conjuntos distintos de serviços, permitindo crescimento incremental.
Availability Zone (AZ)	Domínio de falha independente dentro de uma região, com independência de energia, rede, compute, storage, control plane e infraestrutura física em relação às demais AZs da mesma região. A perda completa de uma AZ não deve comprometer a disponibilidade de serviços projetados para Alta Disponibilidade.
Cluster	Conjunto de recursos computacionais, de rede e/ou de armazenamento dedicado a uma função específica da plataforma (por exemplo, um cluster Kubernetes, um cluster de banco de dados).
Tenant	Domínio lógico de isolamento entre consumidores da plataforma, com segregação de identidade, recursos, dados, métricas e faturamento em relação a outros tenants.
Projeto / Conta	Subdivisão lógica e administrativa dentro de um tenant, utilizada para organizar recursos, quotas e permissões de forma granular.

2.2. Serviços da Nuvem Brasileira

Os itens a seguir descrevem as CAPACIDADES que a Nuvem Brasileira deverá disponibilizar. Tecnologias específicas mencionadas ao longo desta seção quando houver são citadas apenas como referência de maturidade de mercado, sem caráter de exigência obrigatória de adoção. A lista completa de referências tecnológicas consideradas, sem caráter vinculante, está consolidada na Seção 2.3.

Requisitos de Arquitetura

- Console unificada de gerenciamento, acessível via portal Web, API e CLI.
- Gerenciamento e bilhetagem multi-inquilino (multi-tenant), com isolamento de dados, recursos e faturamento entre tenants.
- A plataforma deverá ser capaz de operar de forma independente (desconectada de provedores externos), sem dependência de conectividade internacional para execução, administração e evolução do ambiente. Essa capacidade deverá ser comprovável por meio de Teste de Desconexão, conforme Seção 3.6.
- A plataforma deverá permitir, quando necessário e a critério da Administração, interoperabilidade com nuvens estrangeiras e compatibilidade com tecnologias pré-existentes, sem que isso implique dependência operacional de tais ambientes.
- A arquitetura deverá suportar nativamente a implantação, distribuição e o gerenciamento de recursos em Múltiplas Zonas de Disponibilidade (Multi-AZ) e Múltiplas Regiões, conforme definições da Seção 2.1. A plataforma deverá fornecer os mecanismos integrados necessários para Alta Disponibilidade (HA) e Recuperação de Desastres (DR), com requisitos mensuráveis conforme Seção 2.2.10.
- A operação e a administração do ambiente de produção são de responsabilidade exclusiva da operadora nacional (empresa pública designada). Não haverá acesso remoto permanente de fornecedores de tecnologia ao ambiente de produção; eventuais acessos excepcionais de suporte deverão ser previamente autorizados, auditados e registrados, conforme Seção 5.

Infraestrutura como Serviço (IaaS)

- Processamento: provisionamento automatizado de máquinas virtuais, incluindo gerenciamento de imagens, templates e flavors (perfis de CPU/memória), suporte a GPU/aceleradores quando aplicável, live migration, autoscaling, políticas de affinity/anti-affinity e quotas por tenant/projeto.
- Armazenamento em bloco, objeto e arquivo, com suporte a snapshots, clones, expansão de volumes, versionamento (objeto), classes de serviço diferenciadas por performance, e compatibilidade com APIs amplamente adotadas pelo mercado (ex.: compatibilidade com a API S3 para armazenamento de objetos).
- Rede: redes virtuais, sub-redes públicas e privadas, DNS, Load Balancer, WAF, grupos de segurança/firewall, NAT, suporte a IPv4 e IPv6, e interconexão dedicada com a Administração Pública Federal (APF).
- Virtualização baseada em hypervisor de código aberto com suporte a live migration e alta disponibilidade, e orquestração de máquinas virtuais por meio de plataforma de nuvem de código aberto.
- Identidade e acesso (IAM): federação corporativa, SSO/SAML/OIDC, controle de acesso baseado em papéis (RBAC) e, quando aplicável, em atributos (ABAC), autenticação multifator (MFA) e gestão de service accounts. Ver detalhamento na Seção 2.2.7.
- Monitoramento e observabilidade nativos da camada de infraestrutura, integrados à observabilidade geral da plataforma (Seção 2.2.8).

- Bancos de dados relacionais gerenciados (DBaaS): ver definição e requisitos detalhados na Seção 2.2.5.
- A solução deverá prever mecanismos para que armazenamento e backups (incluindo Block Storage, Object Storage e bancos de dados) possam ser exportados e mantidos fora do ambiente da solução (off-site/out-of-stack). É requisito técnico fundamental que a restauração desses backups, em caso de sinistro grave, não possua dependência estrita dos recursos de gerenciamento internos da própria stack afetada.
- Controle nacional de consoles administrativos e chaves criptográficas para dados de alta criticidade. A solução deverá suportar a custódia de chaves criptográficas em módulos de hardware especializado (HSM) fisicamente instalados em território nacional, sob gestão e controle exclusivos da operadora nacional. É vedado o gerenciamento, custódia ou acesso a essas chaves por fornecedores estrangeiros ou infraestrutura fora do território nacional.
- A solução deve possuir um cofre de senhas/segredos integrado, permitindo o uso e compartilhamento de secrets de forma segura entre os serviços gerenciados da plataforma.
- Plataforma de provisionamento self-service para órgãos, integrada ao Catálogo de APIs da Secretaria de Governo Digital (SGD): referida no documento original pela sigla “MAGMA”, cuja definição e escopo deverão ser detalhados no Termo de Referência subsequente.

Containers as a Service (CaaS) — Kubernetes

- Runtime de contêineres compatível com padrões abertos (OCI) e orquestração compatível com a API padrão Kubernetes.
- Kubernetes oferecido como serviço gerenciado: criação self-service de clusters, upgrade e lifecycle gerenciados pela plataforma, auto-healing e autoscaling de nós e workloads.
- CNI (rede) e CSI (armazenamento persistente) compatíveis com padrões abertos, load balancer e ingress nativos, integração com IAM da plataforma para autenticação/autorização de clusters.
- Registro de imagens de contêineres integrado, com suporte a scanning de vulnerabilidades e assinatura de imagens.
- Gestão de secrets e políticas (network policies, pod security) integradas à plataforma de segurança.
- Backup e recuperação de estado de clusters (etcd, volumes persistentes, manifests) e suporte a operação multi-cluster.

Plataforma como Serviço (PaaS)

- Service mesh para gerenciamento de tráfego, observabilidade e segurança de comunicação entre serviços, compatível com padrões do ecossistema Kubernetes.
- Plataforma de Function-as-a-Service (FaaS)/serverless para execução de código sob demanda, sem gerenciamento de servidores pelo consumidor.
- Ambientes de execução (runtimes) de aplicação gerenciados pela plataforma, com suporte a múltiplas linguagens/frameworks.
- Middleware de integração e mensageria: ver Seção 2.2.6.
- Ferramentas de desenvolvimento e entrega contínua (CI/CD) integradas, com suporte a GitOps.
- Identidade e autenticação para aplicações, integrada ao IAM da plataforma (Seção 2.2.7).
- VPN Gateway, VPC Peering, NAT/Internet Gateway e CDN como capacidades de rede avançada disponíveis sob demanda.
- Ferramentas de migração automatizada de cargas de trabalho a partir de outras nuvens e ambientes on-premises.

- Expansão evolutiva do catálogo de serviços de dados e adoção de padrões de interoperabilidade para registros de contêineres e microsserviços.

Serviços de Dados e DBaaS

A plataforma deverá oferecer bancos de dados como serviço (DBaaS) para motores relacionais (ex.: PostgreSQL, MySQL e/ou MariaDB) e, quando pertinente, para bancos não relacionais (document, key-value, column, cache distribuído). Um serviço será considerado DBaaS somente quando caracterizado por:

- provisionamento self-service via API/portal, sem intervenção manual da operadora para criação de instâncias;
- alta disponibilidade nativa, com réplicas e failover automatizado;
- backup automatizado com restauração point-in-time (PITR);
- aplicação de patches e upgrades sem intervenção manual do consumidor;
- monitoramento e métricas expostos via a camada de observabilidade da plataforma;
- escalonamento (scaling) de recursos sob demanda;
- criptografia em trânsito e em repouso.

Instalação manual de motor de banco de dados dentro de uma máquina virtual, sem os atributos acima, não caracteriza atendimento ao requisito de DBaaS.

Inteligência Artificial, Machine Learning e IA Generativa (Analytics & AI)

A solução de computação em nuvem deverá obrigatoriamente prover portfólio de serviços voltados à Inteligência Artificial e Machine Learning (IA/ML), contemplando de forma nativa:

- ∉ Suporte a ecossistemas de IA Generativa e Large Language Models (LLMs), permitindo o ajuste fino (fine-tuning), implantação e escalabilidade de modelos de linguagem de grande porte.
- ∉ Ambientes de desenvolvimento interativo gerenciados (ex: Notebooks) pré-integrados com bibliotecas de mercado e com o ecossistema de armazenamento e governança de dados da nuvem.
- ∉ Mecanismos de rastreabilidade de linhagem de dados (data lineage) e registro de métricas para assegurar a governança e a auditabilidade dos modelos de IA utilizados no âmbito do setor público.

Mensageria, Streaming e Change Data Capture (CDC)

- Filas e sistemas de publicação/assinatura (pub/sub) para comunicação assíncrona entre serviços.
- Plataforma de streaming distribuído de eventos, com suporte a partições, retenção configurável, alta disponibilidade e escalabilidade horizontal.
- Capacidade de Change Data Capture (CDC) para replicação de alterações de bancos de dados em tempo real.
- Segurança, observabilidade e suporte a multi-tenancy em todos os componentes de mensageria e streaming.

Analytics e Plataforma de Dados

- A plataforma deverá dispor de estratégia de Analytics, contemplando Data Lake, Data Warehouse e/ou arquitetura Lakehouse, conforme evolução do catálogo.

- Suporte a processamento batch e streaming de dados, motores de consulta SQL distribuída, e pipelines de ETL/ELT.
- Catálogo de dados e uso de formatos abertos de armazenamento e tabela (ex.: Parquet, formatos de tabela transacionais abertos) para garantir portabilidade dos dados analíticos.
- Capacidades de inteligência artificial e machine learning, incluindo treinamento e disponibilização (serving) de modelos, como evolução do catálogo de Analytics.

Identidade e Acesso (IAM)

- Gestão de usuários, grupos, papéis (roles) e políticas, com suporte a controle de acesso baseado em papéis (RBAC) e, quando pertinente, em atributos (ABAC).
- Federação de identidade com mecanismos corporativos existentes (SSO, SAML, OIDC, OAuth2).
- Autenticação multifator (MFA) obrigatória para acessos administrativos e disponível para usuários finais.
- Gestão de service accounts para automação e integração entre sistemas.
- Trilha de auditoria completa de eventos de autenticação, autorização e alteração de permissões.

Segurança

- Gestão de chaves (KMS), módulos de hardware especializado (HSM) e infraestrutura de chave pública (PKI), sob custódia nacional conforme Seção 2.2.2.
- Cofre de segredos (secrets) integrado, hardening de imagens e configurações, e gestão de vulnerabilidades.
- WAF, firewall, e capacidades de detecção/prevenção de intrusão (IDS/IPS) quando pertinente à criticidade do workload.
- Scanning de imagens de contêineres e artefatos, geração de SBOM (Software Bill of Materials) e assinatura de artefatos de software ao longo da cadeia de suprimentos.
- Logs de auditoria centralizados e imutáveis para todas as camadas da plataforma.
- Criptografia em trânsito, em repouso, em backup e entre serviços internos da plataforma.

Observabilidade

- Coleta e exposição de métricas (metrics), logs e traces (rastreamento distribuído), com adoção preferencial de padrões abertos de telemetria.
- Dashboards, alertas e definição de objetivos de nível de serviço (SLOs) por capacidade da plataforma.
- Logs de auditoria acessíveis a cada tenant sobre seus próprios recursos, sem exposição cruzada entre tenants.
- Exportação de dados de observabilidade em formatos abertos, para consumo por ferramentas externas de gestão, quando autorizado.

Automação e Infraestrutura como Código (IaC)

- Suporte a ferramentas de automação declarativa de infraestrutura e a operadores/GitOps para gestão do ciclo de vida de aplicações e clusters.

- Toda operação recorrente da plataforma deverá, preferencialmente, ser automatizável via API, evitando dependência de execução manual por GUI. Funcionalidades disponíveis apenas por interface gráfica deverão ser explicitamente sinalizadas pelo proponente.

Multi-Tenancy e Isolamento

A plataforma deverá isolar tenants nas seguintes dimensões: compute, storage, rede, bancos de dados, clusters Kubernetes, logs, métricas, backups, IAM, KMS/segredos, quotas e billing. Cada proponente deverá declarar, para cada dimensão, o nível de isolamento oferecido, dentre:

Nível	Descrição
Lógico	Isolamento por controle de acesso e segregação de dados dentro de infraestrutura compartilhada.
Projeto	Isolamento adicional por segregação em nível de projeto/conta dentro de um tenant.
Cluster	Recursos dedicados a nível de cluster (ex.: cluster Kubernetes exclusivo do tenant).
Rede	Segregação de rede dedicada (VLAN/VXLAN/VRF) por tenant.
Storage	Volumes, pools ou namespaces de armazenamento dedicados por tenant.
Hardware dedicado	Servidores físicos exclusivos, sem compartilhamento com outros tenants (dedicated hosts).

Metering e Billing

- Medição de consumo por CPU, RAM, GPU/aceleradores, storage, IOPS, tráfego de rede, operações de API, instâncias de banco de dados, containers e demais serviços gerenciados.
- Suporte a metering, billing, showback e chargeback, com centro de custos por tenant/projeto.
- Relatórios de consumo e custo exportáveis, com granularidade suficiente para auditoria e planejamento orçamentário dos órgãos.

Alta Disponibilidade (HA) e Recuperação de Desastres (DR)

A plataforma deverá tratar Alta Disponibilidade (HA) e Recuperação de Desastres (DR) como capacidades distintas e complementares:

- HA: cada classe de serviço crítico deverá ter SLA de disponibilidade definido e mecanismo de failover documentado dentro de uma mesma região, com tolerância à perda de uma Availability Zone (conforme definição da Seção 2.1).
- DR: a plataforma deverá suportar replicação e restauração cross-AZ e cross-região, com RTO (Recovery Time Objective) e RPO (Recovery Point Objective) definidos por classe de serviço e testados periodicamente, viabilizando arquiteturas de resiliência corporativa ativo-ativo e/ou ativo-passivo conforme a criticidade do workload.
- Cada proponente deverá apresentar, para os serviços críticos de sua solução, a matriz de SLA/RTO/RPO correspondente, como parte da demonstração de capacidade técnica.

API-First

- As principais funcionalidades da plataforma deverão ser acessíveis por API REST e/ou declarativa, com documentação, versionamento, política de compatibilidade retroativa (backward compatibility) e mecanismos de autenticação e auditoria.
- Deverão estar disponíveis, adicionalmente, CLI e SDKs para as linguagens de maior adoção pela Administração Pública.
- Toda funcionalidade disponível apenas por interface gráfica (GUI), sem equivalente via API, deverá ser explicitamente sinalizada pelo proponente.

Suporte e Operação

Compreendem também o escopo da Nuvem Brasileira:

- Suporte técnico para software e serviços de computação em nuvem;
- Operação e gerenciamento de recursos em nuvem;
- Migração de recursos para o ambiente de nuvem;
- Integração de serviços de computação em nuvem; e
- Consultoria especializada em software e/ou serviços de computação em nuvem.

Não são objeto deste modelo, neste momento: aquisição de ativos de infraestrutura de TIC ou de rede; contratação de hosting, co-location ou housing; e contratação de serviços de desenvolvimento e manutenção de software aplicativo finalístico dos órgãos públicos usuários da plataforma.

2.3. Referências Tecnológicas (Não Vinculantes)

Capacidade	Exemplos de referência (não vinculantes)
Sistema operacional / Virtualização	Linux, KVM
Orquestração de infraestrutura (IaaS)	OpenStack, Apache CloudStack
Containers e orquestração	Containerd, Podman, OCI, Kubernetes, KubeVirt
Storage distribuído	Ceph, Rook
Rede (SDN)	Cilium, OVN
Identidade	Keycloak
Registro de containers	Harbor
GitOps / Entrega contínua	Argo CD, Flux, Jenkins, GitLab CE
Service mesh	Istio, Linkerd, Consul
Serverless / FaaS	Knative, OpenFaaS, Apache OpenWhisk
Plataforma de aplicação	Cloud Foundry
Bancos de dados relacionais	PostgreSQL, MySQL, MariaDB
Bancos não relacionais / cache	Redis, MongoDB, Memcached
Object storage	MinIO
Mensageria / streaming	Apache Kafka, RabbitMQ, Debezium (CDC)
Analytics / dados	Apache Spark, Trino, Flink, Iceberg, Apache Superset, Metabase, Hadoop
IA / Machine Learning	TensorFlow, PyTorch, Kubeflow
Observabilidade	Prometheus, Grafana, OpenTelemetry, Elastic/OpenSearch
Automação / IaC	OpenTofu (mantido pela Linux Foundation), Ansible, Terraform

3. Critérios de Seleção e Gradiente de Soberania

Para a eventual seleção do parceiro serão empregados critérios de avaliação de experiência prévia e capacidade técnica, e critérios de avaliação do nível de soberania, estes últimos aferidos por meio do Gradiente de Soberania Serpro (versão 3.0), adotado como referência formal desta Escuta de Mercado e do eventual Termo de Referência/Edital subsequente.

3.1. Pilares do Gradiente

Pilar	Peso	Critérios
Soberania de Dados	30%	6 critérios (D1–D6): localização física, metadados, chaves criptográficas, jurisdição e risco extraterritorial, acesso administrativo e privilegiado, processamento de dados.
Soberania Operacional	40%	5 critérios (O1–O5): conectividade com o provedor, autonomia operacional, gestão de patches e upgrades, console de gerenciamento/control plane, independência de licenciamento.
Soberania Tecnológica	30%	4 critérios (T1–T4): tecnologia aberta ou proprietária, arquitetura agnóstica, diversificação da cadeia de suprimentos, continuidade e soberania estratégica.

Cada um dos 15 critérios recebe nota de 0 a 3, conforme as escalas detalhadas do Gradiente de Soberania Serpro v3.0. Os índices são calculados como:

- ISD (Índice de Soberania de Dados) = soma(D1:D6) / 18 × 100
- ISO (Índice de Soberania Operacional) = soma(O1:O5) / 15 × 100
- IST (Índice de Soberania Tecnológica) = soma(T1:T4) / 12 × 100
- ISG (Índice de Soberania Geral) = 0,30 × ISD + 0,40 × ISO + 0,30 × IST

3.2. Classificação do ISG

ISG	Classificação
0–20%	Muito baixa
21–40%	Baixa
41–60%	Moderada
61–80%	Alta
81–100%	Muito alta

A classificação geral do ISG deverá ser sempre apresentada em conjunto com os três índices (ISD, ISO, IST), nunca isoladamente.

3.3. Regra de Evidência

Notas positivas não poderão ser atribuídas com base em marketing, nome comercial, pressupostos, reputação do fornecedor ou afirmações genéricas. A nota deverá ser baseada em evidência objetiva apresentada pelo proponente ou verificável por documentação técnica. Quando não houver evidência suficiente para um critério, o avaliador deverá registrar “NÃO EVIDENCIADO” e apontar a lacuna, em vez de presumir atendimento.

3.4. Gates de Soberania

Uma média geral alta não poderá compensar fragilidade estrutural crítica em critérios essenciais ao objetivo desta Escuta de Mercado. Recomenda-se ao Edital subsequente a adoção dos seguintes gates mínimos de elegibilidade para os serviços e workloads críticos da Nuvem Brasileira, a serem formalmente definidos pela Administração Pública:

Critério	Nota mínima recomendada	Justificativa
D3 — Chaves Criptográficas	≥ 2	Custódia nacional das chaves é condição já afirmada pelo Caderno (Seção 2.2).
D5 — Acesso Administrativo	≥ 2	Coerente com a vedação de acesso remoto permanente de terceiros (Seção 2.2).
D6 — Processamento de Dados	≥ 2	Alinhado à exigência de operação desconectada (Seção 2.2).
O1 — Conectividade com o Provedor	≥ 2	Central ao atributo “capacidade nacional” (Seção 2).
O4 — Control Plane	≥ 2	Sem controle nacional do control plane, a soberania operacional é apenas nominal.
T4 — Continuidade Estratégica	≥ 2	Coerente com a cláusula de reversibilidade já prevista (item 5-h).

Os valores acima são recomendação técnica desta revisão, não parte da metodologia oficial do Gradiente. Os valores mínimos definitivos deverão ser explicitamente fixados pelo Edital.

3.5. Matriz de Soberania da Solução

Cada proponente deverá apresentar, na fase de resposta ao Termo de Referência/Edital subsequente, uma matriz de soberania cobrindo todos os componentes relevantes de sua arquitetura, evitando que qualquer dependência externa relevante permaneça implícita:

Componente	Tecnologia	Open Source	Processamento	Control Plane	Operador	Patches	Licenciamento	Acesso Externo	Telemetria	Substituibilidade

3.6. Teste de Desconexão

Como parte do processo de homologação técnica, deverá ser simulada a interrupção da conectividade externa (internacional) do ambiente, verificando-se a disponibilidade das seguintes funções: execução de workloads, autenticação, autorização, APIs, portal, provisionamento de VMs, Kubernetes, storage, bancos de dados, KMS, DNS, monitoramento, backup, restauração, escalonamento e administração. O resultado deverá registrar, para cada função, se ela continua integralmente, parcialmente, temporariamente ou deixa de funcionar durante a desconexão.

3.7. Declaração de Dependências Externas

Cada proponente deverá declarar formalmente todas as dependências externas de sua solução, incluindo: endpoints, APIs, DNS, mecanismos de autenticação, licenciamento, atualização, repositórios, registries, telemetria, suporte remoto, consoles, serviços SaaS, KMS externo e serviços de certificado.

3.8. Requisitos de validação técnica

Como parte da Prova de Conceito e dos testes de homologação técnica da Nuvem Brasileira, o proponente deverá demonstrar a capacidade de:

- ∉ Provisionar com sucesso ambientes de desenvolvimento interativo e coletar métricas de execução e desempenho computacional.
- ∉ Garantir integração fluida entre o ambiente de IA e os repositórios de dados externos (Data Lakes / Object Storage) para leitura e escrita em larga escala.
- ∉ Comprovar capacidade técnica de interação com a infraestrutura para hospedar e rodar operações de inferência e treinamento com os níveis de SLA exigidos para aplicações críticas de governo.

4. Onde Será Instalada

Quando estiver em produção, a Nuvem Brasileira será instalada em infraestrutura de propriedade pública em território nacional, operada por empresa pública, que conta com certificações de segurança e disponibilidade compatíveis com os requisitos da Administração Pública Federal.

5. Exigências Estratégicas

A eventual parceria com empresas do mercado nacional deverá atender às seguintes exigências:

a) Empresa pública como provedor de nuvem para o governo. A solução desenvolvida na eventual parceria será operada por empresas públicas e disponibilizada aos órgãos e entidades federais por meio de suas estruturas. Não há restrição sobre a provisão da Nuvem Brasileira para o setor privado.

b) Licenciamento do software para o setor público. O software desenvolvido na parceria deverá ser licenciado para empresas públicas, garantindo que o Estado possa operar, manter e evoluir a plataforma independentemente da continuidade da relação com o parceiro privado.

c) Compartilhamento da propriedade intelectual. A propriedade intelectual gerada no âmbito da parceria será compartilhada entre as partes. Não será aceito modelo em que a totalidade dos direitos sobre o software pertença exclusivamente ao parceiro privado.

d) Desenvolvimento contínuo. O parceiro deverá comprometer-se com um plano de evolução tecnológica contínua da plataforma, com roadmap público e entregas periódicas, garantindo que a solução não fique defasada em relação ao estado da arte. Este item refere-se ao desenvolvimento e evolução da própria plataforma de nuvem, objeto central da parceria, e não contraria a exclusão de escopo de desenvolvimento de software aplicativo finalístico prevista na Seção 2.

e) Custo competitivo. A solução deve oferecer custos competitivos em relação às alternativas disponíveis para a Administração Pública Federal, incluindo as nuvens públicas comerciais do catálogo de nuvem de governo.

f) Transferência de conhecimento. O parceiro deve comprometer-se a capacitar equipes técnicas das empresas públicas no domínio das tecnologias desenvolvidas, contribuindo diretamente para o avanço no atributo capacidade nacional, sem isso, a soberania tecnológica plena não se consolida. Recomenda-se que o eventual instrumento contratual estabeleça marcos e prazos objetivos para a transição progressiva de autonomia operacional às equipes nacionais (critério O2 do Gradiente de Soberania).

g) P&D realizado em território nacional. Caso haja P&D, o desenvolvimento do software deve ser realizado por técnicos residentes no Brasil, condição para que o projeto gere os efeitos de capacitação e adensamento do ecossistema tecnológico nacional.

h) Cláusula de saída / reversibilidade. O instrumento contratual deve prever mecanismos que garantam a continuidade operacional da plataforma em caso de dissolução da parceria ou descontinuidade do parceiro privado, incluindo acesso irrevogável ao código-fonte pela Administração Pública.

i) Acordos de Nível de Serviço (SLA). O modelo de prestação de suporte técnico para software e serviços de computação em nuvem deve ser pautado por Acordos de Nível de Serviço (SLA) compatíveis com infraestruturas críticas de governo. Espera-se que os interessados sugiram métricas de SLA realistas e exigíveis, abordando: (i) garantias de disponibilidade (uptime), por classe de serviço, conforme Seção 2.2.10; (ii) tempos máximos de resposta e de resolução para incidentes críticos; e (iii) estrutura de suporte de múltiplos níveis (Tier 1 a 3).

j) Matriz de Soberania e Declaração de Dependências Externas. O proponente deverá apresentar, como parte de sua proposta técnica, a Matriz de Soberania da Solução e a Declaração de Dependências Externas,

conforme Seções 3.5 e 3.7, sob pena de a proposta ser considerada incompleta para fins de avaliação de soberania.

k) Submissão ao Teste de Desconexão. O proponente deverá comprometer-se a submeter sua solução ao Teste de Desconexão descrito na Seção 3.6 como etapa da homologação técnica, quando aplicável ao estágio da parceria.

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 24/08/2026 | Edição: 159 | Seção: 3 | Página: 147

Órgão: Ineditoriais/Agência Brasileira de Desenvolvimento Indústrial

AVISO DE CONSULTA PÚBLICA Nº 1/2026

Objeto: Escuta de mercado sobre oferta de solução nacional de computação em nuvem, no âmbito do Acordo de Cooperação Técnica Nº 134/2026MGI/ABDI/SERPRO/BNDES.

Processo nº: 19974.000976/2026-41 (SEI-MGI)

O primeiro evento da Escuta de Mercado será uma audiência pública, conforme abaixo:

Data da realização: 03/09/2026

Horário: 10:00

Local da realização: A sessão virtual da Escuta de Mercado será realizada através do software Microsoft Teams mediante inscrição na página: www.abdi.com.br/nuvembrasileira.

Documentação: O caderno de apoio com as informações sobre o projeto, o contexto e justificativas estão disponíveis em: www.abdi.com.br/nuvembrasileira.

Envio de Questionamentos e Sugestões: Os interessados poderão enviar suas contribuições para o e-mail: nuvembrasileira@abdi.com.br.

ANDRÉ SANTA RITA PEREIRA
Gerente da Unidade de Licitações, Contratos e Convênios