PERGUNTAS E RESPOSTAS AGRUPADAS

ESCUTA DE MERCADO: NUVEM BRASILEIRA

OUTUBRO DE 2026

ABDI
Agência Brasileira de Desenvolvimento Industrial

1. Qual é o objeto da Nuvem Brasileira e como será tratado o hardware, quanto a aquisição, fornecimento, fronteira de responsabilidade e eventual chamamento específico? *(perguntas 27, 61, 62, 69, 75, 76, 86, 93 e 96)*

A Nuvem Brasileira é uma modalidade de computação em nuvem que atende a requisitos elevados de soberania. Seu objeto central, nesta etapa, é o software da própria plataforma, isto é, o desenvolvimento, a manutenção e a evolução contínua da plataforma de nuvem, incluído o P&D relacionado. Ficam fora do escopo, nesse momento, três coisas: a aquisição de ativos de infraestrutura de TIC ou de rede, a contratação de hosting, co-location ou housing e o desenvolvimento de sistemas finalísticos dos órgãos usuários.

Quando entrar em produção, a plataforma será instalada em infraestrutura de propriedade pública no território nacional, operada por empresa pública, e poderá ser oferecida também ao setor privado. Os itens listados no caderno (portal, identidade, IaaS, containers, PaaS, dados, IA, segurança, observabilidade, automação, alta disponibilidade e billing) descrevem, em alto nível, o que será avaliado nas plataformas já disponíveis no mercado nacional. Uma oferta limitada a IaaS é considerada insuficiente para as demandas do governo.

A plataforma dependerá de hardware, mas o tema foi reservado para uma segunda etapa, pela maior complexidade de desenvolvimento nacional nesse pilar. Ainda não está definido se o equipamento será disponibilizado pelo Serpro ou especificado integralmente pelo parceiro, nem se virá junto com a plataforma ou em arranjo separado. Também está em aberto a fronteira de responsabilidade (borda de internet, top of rack, rede ou armazenamento). Em qualquer hipótese, caberá ao parceiro toda a camada de software, do provisionamento da infraestrutura ao portal. Não há, por ora, previsão de chamamento nem de escuta específica de hardware.

2. Como a soberania é tratada nas camadas fora do software da plataforma (HSM, firmware, cadeia de suprimentos e rede), e espera-se P&D conjunto do chip à plataforma? *(perguntas 3, 4, 38, 74 e 89)*

O caderno trata essas camadas pelo ângulo do controle e da substituibilidade, com quatro exigências:

- as chaves de dados de alta criticidade ficam em HSM fisicamente instalado no território nacional, sob gestão e controle exclusivos da operadora pública, vedados o gerenciamento, a custódia e o acesso por fornecedores estrangeiros;
- o hypervisor deve ser de código aberto;
- a cadeia de software é acompanhada por SBOM e assinatura de artefatos;
- a arquitetura deve suportar equipamentos de múltiplos fornecedores, para garantir resiliência diante de interrupções de fornecimento por razões geopolíticas ou comerciais, aspecto medido pelo critério de diversificação da cadeia de suprimentos.

O modelo e o fabricante do HSM não foram definidos. O critério de chaves mede o controle sobre elas; a origem do equipamento, seu firmware e sua cadeia de atualização ficam a cargo do critério de cadeia de suprimentos.

A Administração reconhece que seria irrealista, no contexto atual, pretender o domínio nacional de toda a cadeia de hardware e software. Por isso o P&D esperado se concentra na plataforma, e a camada de hardware tende a ter, por ora, grau de soberania abaixo do desejável. A próxima

versão do Gradiente terá índices separados de soberania tecnológica de software e de hardware. O índice de hardware medirá quão substituíveis são os componentes de rede, computação, armazenamento, GPU e NPU, e indicará onde o país precisaria investir. Nesse sentido, a independência na camada de rede (sistemas operacionais abertos de switch, por exemplo) não é exigida nesta etapa e tende a ser avaliada nesse índice. A mitigação para a eventual descontinuidade de um fabricante é justamente a compatibilidade com múltiplos fornecedores.

3. Como se define soberania em inteligência artificial, dada a dependência de GPUs e de software Nvidia, e há parâmetros para hospedagem, abertura e local de treinamento dos modelos usados pelo governo?
(perguntas 2, 25 e 30)

O caderno exige que a plataforma ofereça portfólio nativo de IA e aprendizado de máquina. Isso inclui suporte a IA generativa e a LLMs (ajuste fino, implantação e escalabilidade), ambientes gerenciados de desenvolvimento interativo e mecanismos de linhagem de dados e registro de métricas, que asseguram a governança e a auditabilidade dos modelos usados no setor público. A prova de conceito deverá demonstrar inferência e treinamento nos níveis de serviço exigidos para aplicações críticas. Não há, contudo, definição específica sobre hospedagem, abertura ou local de treinamento dos modelos.

Quanto aos aceleradores, a avaliação considerará, além do hardware, toda a pilha de software associada a ele (drivers e demais componentes). Serão verificados o grau de dependência, a agnosticidade da arquitetura e a existência de acoplamento direto a CUDA. O hardware propriamente dito será tratado em etapa posterior, com GPU e NPU incluídas no futuro índice de hardware do Gradiente. Ou seja, nesta etapa a soberania em IA corresponde ao controle sobre a plataforma, os dados e a operação, e a dependência de hardware é mapeada e graduada. Pelo Gradiente, hospedagem e processamento no país pontuam nos critérios de localização e de processamento de dados, e o uso de modelos abertos pontua no critério de tecnologia aberta.

4. O que se entende por soberania na Nuvem Brasileira, como se distinguem tecnologia estrangeira, instituição nacional e dependência operacional relevante, como se trata a dependência tecnológica sem efeito operacional e quais critérios objetivos caracterizam a solução?
(perguntas 23, 33, 50 e 56)

As nuvens de governo atuais tratam sobretudo da soberania de dados, com residência no território nacional, jurisdição brasileira e operação por empresas públicas. A Nuvem Brasileira vai além. Ela exige que as próprias tecnologias, especialmente de software, possam ser desenvolvidas, mantidas e evoluídas por instituições e equipes nacionais, sem depender amplamente de tecnologias estrangeiras nem de autorização ou cooperação de fornecedores estrangeiros.

Dois atributos a caracterizam: a interoperabilidade (padrões e formatos abertos, hardware de múltiplos fornecedores) e a capacidade nacional (domínio técnico efetivo no país). Ambos são aferidos pelo Gradiente de Soberania Serpro, atualmente na versão 3.0, com pesos de 30% para dados, 40% para operação e 30% para tecnologia. O Gradiente é complementado por gates, Matriz de Soberania, Declaração de Dependências Externas e Teste de Desconexão, sempre com a regra de que nenhuma nota positiva pode se apoiar em marketing ou presunção. Os termos tecnologia estrangeira, instituição nacional e dependência operacional relevante não têm, até o momento, definição formal.

O Gradiente tem como premissa que a soberania é gradual e se associa à capacidade de escolha e de decisão do Estado, à compreensão do que se controla na cadeia e à mitigação dos riscos de dependência, sem pretensão de isolamento ou de autossuficiência. O peso maior do pilar operacional reflete a importância da execução continuada sob controle do Serpro.

Acontece, pois, que uma dependência tecnológica sem efeito operacional pontua bem no pilar operacional e menos no tecnológico. É justamente esse pilar tecnológico que a Nuvem Brasileira pretende elevar, como Estados Unidos, União Europeia e China fazem com tecnologias produzidas e mantidas no próprio território. Na prática, a distinção entre dependências críticas e dependências próprias dos ecossistemas globais será feita pela combinação do Gradiente, da Declaração de Dependências e do Teste de Desconexão.

5. Como será aferida a capacidade nacional quando a solução se apoia em open source estrangeiro ou em plataforma desenvolvida no exterior, como se trata o conhecimento gerado no Brasil sobre essa base e como se avalia a dependência de comunidades e mantenedores estrangeiros?
(perguntas 21, 22, 24 e 54)

O caderno define a capacidade nacional como a condição de a plataforma ser desenvolvida, mantida e evoluída por pessoas residentes no país e por instituições nacionais. O direito de acesso ao código-fonte não basta; exige-se domínio técnico efetivo sobre os sistemas críticos. O P&D deve ser realizado por técnicos residentes no Brasil. As próprias referências tecnológicas do caderno (OpenStack, Kubernetes, Ceph, Keycloak, entre outras) são, em grande parte, projetos abertos de origem estrangeira, o que indica que essa origem, por si, não impede a soberania. A Matriz de Soberania indicará, para cada componente, o uso de código aberto e a substituibilidade. A Declaração de Dependências Externas incluirá mecanismos de atualização, repositórios e registries.

O modelo ideal consiste em partir de tecnologias abertas e evoluí-las no país, sem desenvolver tudo do zero. O uso de bases como OpenStack ou CloudStack é bem visto, e admite-se que parte da evolução venha da comunidade, desde que a equipe nacional tenha domínio mínimo da tecnologia. Ainda não há métrica objetiva, como percentual de código desenvolvido no Brasil ou número de profissionais. O domínio de uma plataforma originalmente estrangeira será examinado caso a caso, sempre com o princípio de que a capacidade de manter e evoluir o software deve estar no país. O conhecimento gerado sobre essa base segue o regime de propriedade intelectual do bloco 7. O risco residual de dependência de comunidades estrangeiras recai sobre o critério de continuidade e soberania estratégica.

6. O código aberto é requisito eliminatório? Admite-se combinação com componentes proprietários e, nesse caso, o código-fonte deverá ser entregue ao Serpro? Como ficam licenciamento, NDA e licenças copyleft?
(perguntas 12, 19, 20, 36, 37, 63, 65, 85, 94, 97 e 98)

As tecnologias citadas no caderno são referências de maturidade de mercado, sem obrigação de adoção, com uma exceção: a virtualização deve usar hypervisor de código aberto, e a orquestração de máquinas virtuais, plataforma de nuvem de código aberto, requisito classificado como imprescindível. O Kubernetes deve ser compatível com a API padrão e com os padrões OCI. Como só avança à etapa seguinte quem atende a todos os imprescindíveis, o código aberto

funciona como condição eliminatória nessa camada. Nas demais camadas, o caráter aberto ou proprietário conta pontos no pilar tecnológico.

De todo modo, o software deverá ser licenciado às empresas públicas, e o contrato deverá assegurar à Administração acesso irrevogável ao código-fonte. Assim, o Estado poderá operar, manter e evoluir a plataforma mesmo se a parceria for dissolvida.

O modelo ideal é uma plataforma nacional construída sobre tecnologias abertas, e a escolha do OpenStack como base foi considerada adequada, com atenção ao multi-tenancy nativo, à segurança e à observabilidade. Admite-se que parte da tecnologia seja desenvolvida no exterior, desde que o código seja integralmente aberto. O tratamento das licenças copyleft ainda não foi aprofundado.

Ou seja, entregas parcialmente abertas são admitidas fora da camada de virtualização e orquestração, com nota menor nos critérios de tecnologia aberta e de independência de licenciamento. Componentes proprietários de terceiros (balanceadores de carga, por exemplo) deverão ser declarados na Matriz e na Declaração de Dependências.

7. Como serão separadas a propriedade intelectual pré-existente, a desenvolvida no projeto, o open source e os componentes de terceiros?
(pergunta 35)

A propriedade intelectual gerada na parceria será compartilhada entre as partes. Não será aceito modelo em que a totalidade dos direitos sobre o software pertença exclusivamente ao parceiro privado. A propriedade pré-existente será respeitada, nos termos da legislação vigente, e os desenvolvimentos que o parceiro já tiver feito serão valorados e remunerados no arranjo a ser definido. Sobre o desenvolvimento conjunto, o Estado terá, no mínimo, direito de uso gratuito, e os demais termos serão negociados conforme o instrumento escolhido, dada a complexidade do tema. Componentes open source e de terceiros deverão constar da Matriz de Soberania e da Declaração de Dependências Externas, com o respectivo licenciamento, o que permitirá delimitar, componente a componente, o que pertence a cada parte.

8. Como foram definidos os gates e os habilitadores, por que o corte é nota 2, por que o pilar tecnológico não tem nível mínimo, houve calibragem por referencial externo e avaliou-se o impacto dessas exigências sobre as empresas nacionais?
(perguntas 5, 10, 11 e 29)

O caderno recomenda ao edital gates mínimos para os serviços e workloads críticos: nota igual ou superior a 2 em chaves criptográficas, acesso administrativo, processamento de dados, conectividade com o provedor, control plane e continuidade estratégica. A razão é que uma média geral alta não pode compensar fragilidade estrutural em critérios essenciais. Cada gate se ancora numa exigência que o próprio caderno já faz: custódia nacional das chaves, vedação de acesso remoto permanente, operação desconectada, capacidade nacional, controle do control plane e reversibilidade. O caderno, portanto, já prevê um mínimo no pilar tecnológico, no critério de continuidade estratégica. A Matriz de Soberania, que é a exigência mais detalhada, só será cobrada na resposta ao edital.

A apresentação acrescenta, para as cargas críticas, um mecanismo de habilitação em que nove dos quinze critérios têm patamar mínimo: nível 3 em cinco critérios de dados e na console, e nível 2 em conectividade, autonomia e patches, sem mínimo tecnológico.

O nível 2 foi adotado nos critérios operacionais porque é o que as stacks em operação alcançam hoje, quando alguma delas atingir o nível 3, esse passará a ser o novo mínimo exigido. O pilar tecnologia está em evolução: a revisão do Gradiente prioriza esse pilar, com publicação prevista para as próximas semanas, porque a Administração prefere conhecer a oferta antes de fixar um patamar inalcançável ou baixo demais. A calibragem se apoia na experiência operacional do Serpro, e o modelo da Gartner serviu apenas de ponto de partida. Não houve avaliação formal de impacto sobre as empresas; essa função é cumprida pela própria escuta de mercado, ao calibrar os requisitos à oferta existente.

9. Como requisitos e gates serão verificados na prática, há percentual mínimo de atendimento, funcionalidades em roadmap contam, admitem-se entregas parciais e em ondas, e como se organizará o trabalho conjunto?
(perguntas 6, 43, 66, 70, 84, 90 e 99)

Pelo caderno, as notas de soberania devem se apoiar em evidência objetiva, apresentada pelo proponente ou verificável em documentação técnica, e registra-se "não evidenciado" quando ela faltar. Estão previstos prova de conceito, testes de homologação técnica e Teste de Desconexão, este aplicável conforme o estágio da parceria. O caderno exige ainda compromisso com roadmap público e entregas periódicas, e admite compatibilidade com tecnologias pré-existentes, desde que sem dependência operacional. Dos 84 requisitos técnicos, 50 são imprescindíveis, e a avaliação passa primeiro por esses requisitos e depois pelo Gradiente.

Na prática, quem atende aos imprescindíveis passa aos desejáveis, que elevam a pontuação de maturidade. A verificação será feita por testes do Serpro, cujo caderno de testes começou com cerca de setenta casos e hoje soma algumas centenas. Depois de uma fase autodeclaratória, uma equipe de cerca de cem especialistas testará a plataforma diretamente no ambiente do proponente. O teste registrará o que já está disponível e o que consta do roadmap, para identificar quem entrega mais depressa um produto mínimo viável. A implantação será priorizada em ondas, conforme as necessidades definidas pelo governo, e não se pretende exigir de imediato o nível máximo em todos os critérios.

Não há, por ora, percentual mínimo de atendimento, porque as escutas servem justamente para calibrar os requisitos. Também não há modelo definido de acompanhamento (squads ou comitês), que dependerá do instrumento. Ou seja, funcionalidades em roadmap contam para a avaliação de maturidade, mas só pontuam no Gradiente depois de comprovadas. Entregas parciais com complementação contratual são admissíveis em princípio, na forma que o instrumento vier a prever.

10. O Teste de Desconexão será exigido de todos os proponentes, qual será o critério de reprovação e como ele distingue resiliência de isolamento?
(perguntas 9 e 34)

A plataforma deverá operar de forma independente, sem conectividade internacional, para execução, administração e evolução do ambiente. Essa capacidade será comprovada pelo Teste de Desconexão, que simulará a interrupção da conectividade externa. Para cada função (execução de workloads, autenticação, autorização, APIs, portal, provisionamento, Kubernetes, armazenamento, bancos de dados, KMS, DNS, monitoramento, backup, restauração, escalonamento e administração), o teste registrará se ela continua integral, parcial ou temporariamente, ou se deixa de funcionar. O proponente se compromete a passar pelo teste

como etapa da homologação técnica. A interoperabilidade com nuvens estrangeiras continua admitida, desde que não gere dependência operacional. O teste será prático, em laboratório, e a referência de aprovação é a continuidade dos serviços essenciais durante o corte. Seria inaceitável, por exemplo, que a console de administração dependesse de conexão externa.

Como se trata de requisito de arquitetura da própria plataforma, o teste deve alcançar todos os proponentes, qualquer que seja a criticidade das cargas, e o critério formal de reprovação ainda será fixado.

11. Qual é a base legal do modelo, como ele se relaciona com a Portaria SGD/MGI nº 5.950 e com a Nuvem de Governo, qual será a plataforma central de gerenciamento, haverá nova regulamentação e o Gradiente passará a ser obrigatório em outras contratações?
(perguntas 8, 44, 57, 58, 59 e 60)

A plataforma será operada por empresa pública, que presta o serviço aos órgãos federais, em infraestrutura de propriedade pública no território nacional, com certificações de segurança e disponibilidade compatíveis com os requisitos da Administração Pública Federal. O Gradiente de Soberania Serpro v3.0 foi adotado como referência formal desta escuta e do eventual edital. A plataforma terá console unificada de gerenciamento, acessível por portal, API e CLI, sob controle nacional. Sem controle nacional do control plane, a soberania operacional seria apenas nominal, e por isso esse critério está entre os gates. As cargas críticas seguem a IN GSI/PR nº 5/2021. A Nuvem de Governo atual é composta por múltiplas stacks de parceiros globais operadas no perímetro do Serpro, e o grau de soberania deve ser medido em cada uma delas.

Nesse momento, não há previsão e nem expectativa de alteração normativa, nem de norma que imponha o Gradiente às demais contratações. A Nuvem Brasileira entra como mais uma opção, operada por empresas públicas como Serpro e Dataprev, em conformidade com a portaria. Na Nuvem de Governo, o Serpro atua como broker que controla, opera e garante a residência dos dados. Na Nuvem Brasileira, o propósito é ter uma solução construída e mantida no Brasil, que integrará o catálogo da Nuvem de Governo com grau de soberania superior. Os gates serão fixados no edital, e o Gradiente, por ser dinâmico, servirá como referência. O MGI reconhece ainda que o texto vigente da portaria não detalha se o controle deve ser integralmente público, ponto que está em estudo.

Ou seja, vale o arcabouço já existente, incluídas a LGPD e a própria portaria. As cargas restritas e os sistemas estruturantes permanecem na Nuvem de Governo durante a transição, sem regra específica até o momento.

12. Quais dados e cargas exigem soberania máxima, como se assegura a proporcionalidade ao risco, quais serão os primeiros workloads e qual a demanda computacional estimada?
(perguntas 32, 52, 53 e 72)

O caderno reserva os gates aos serviços e workloads críticos, e a custódia nacional das chaves aos dados de alta criticidade. A apresentação define como cargas críticas, nos termos da IN GSI/PR nº 5/2021, três grupos:

- os sistemas estruturantes de governo: arrecadação, identidade, pagamentos, justiça e saúde;
- os dados protegidos por sigilo legal: fiscal, bancário, processual e disciplinar;

- as cargas cuja execução e recuperação devem permanecer sob controle do Estado.

Só para essas cargas a stack precisa atender a todos os habilitadores ao mesmo tempo.

A proporcionalidade decorre da própria gradação. Uma solução que atinge determinado grau de soberania pode receber as cargas que exigem até esse grau, e uma solução com pontuação alta que falhe num habilitador continua apta para cargas não críticas. O governo continuará a contratar nuvem pública, e as três modalidades (pública, de governo e brasileira) seguirão em paralelo, com a alocação definida pela classificação dos dados. Os primeiros workloads ainda não foram definidos; serão priorizados com base na experiência do governo e tendem a ser cargas que exigem soberania acima da oferecida pela Nuvem de Governo. A demanda computacional (CPU, GPU, memória e armazenamento) está em levantamento, ainda sem números consolidados.

13. Quantos fornecedores poderão compor a Nuvem Brasileira? Admitem-se ofertas multistack sob gerenciador único, parcerias e consórcios entre empresas, ou uma nuvem descentralizada e cooperativa de provedores menores, com interconexão de redes públicas?
(perguntas 16, 40, 41, 42, 46, 51, 87 e 91)

O caderno busca evitar a dependência de um único fabricante e exige múltiplas zonas de disponibilidade e múltiplas regiões. Cada zona é um domínio de falha independente em energia, rede, computação, armazenamento, control plane e infraestrutura física. Exige também interconexão dedicada à Administração Pública Federal e operação exclusiva pela empresa pública. O projeto parte, portanto, da premissa de evitar o aprisionamento a um ou poucos fornecedores, e a única concentração exigida é a da operação.

A proposta de nuvem descentralizada e cooperativa foi considerada interessante, mas esbarra em limites para cargas críticas em escala federal:

- latência, vazão e necessidade de conectividade física;
- complexidade de administrar um ambiente distribuído, com equipes 24x7 e infraestrutura própria de energia e facilities;
- dificuldade de cumprir tempos de resposta quando várias equipes respondem pelo mesmo serviço.

Quanto às ofertas multistack sob gerenciador único, o objetivo declarado é avançar além da Nuvem de Governo, que já corresponde a esse arranjo. O parceiro deverá prover toda a camada de software, do provisionamento ao portal, e por isso uma oferta assentada em stacks estrangeiras tende a não atender o atributo de capacidade nacional. Ainda não está definido se haverá uma ou mais plataformas. Para cada uma, a orientação inicial é ter um único provedor responsável, porque hoje é pouco desejável dividir, por exemplo, IaaS, bancos de dados e mensageria entre empresas distintas. Consórcios e parcerias com mais de uma empresa privada, contudo, continuam em avaliação. Na Nuvem de Governo, o TCU passou a exigir ao menos dois data centers geograficamente distintos por fornecedor. O número de pontos de presença e o eventual uso de redes públicas neutras serão definidos na modelagem.

14. Como a Nuvem Brasileira trata o Cloud Act e a jurisdição estrangeira, qual o papel das chaves criptográficas, em que difere da Nuvem de Governo e deverá atender ao Acórdão

TCU nº 1.380/2026?
(perguntas 15, 39, 55 e 100)

O Gradiente avalia a jurisdição e o risco extraterritorial como critério próprio do pilar de dados, ao lado do critério de chaves criptográficas. O caderno veda o gerenciamento, a custódia ou o acesso às chaves por fornecedores estrangeiros ou por infraestrutura fora do território nacional. A apresentação registra que o nível de soberania precisa ser medido em cada stack da Nuvem e está entre os habilitadores das cargas críticas. A sujeição do fornecedor ao Cloud Act entra nesse critério de jurisdição. O HSM das cargas críticas deverá ficar dentro da própria plataforma, sob controle exclusivo da operadora pública, e a mesma régua vale para as stacks atuais e para as novas propostas.

A diferença em relação à Nuvem de Governo está no pilar tecnológico: aquela já alcançou níveis satisfatórios de soberania de dados e operacional, e a Nuvem Brasileira busca agora o domínio da tecnologia. O Acórdão TCU nº 1.380/2026, relativo à Nuvem de Governo, fez três determinações: redundância geográfica, revisão do contrato com a AWS para excluir o acesso a dados por ordem de autoridades estrangeiras e adoção de metodologia padronizada de análise de soberania. A principal preocupação declarada da Administração é assegurar jurisdição brasileira. Isto é, a custódia nacional das chaves reduz o risco de acesso aos dados, e o risco jurisdicional do controlador continua avaliado à parte. Como os requisitos da Nuvem Brasileira vão na mesma direção das determinações do TCU, espera-se aderência.

15. Como serão tratados a cibersegurança, a interoperabilidade e o compartilhamento seguro de dados, como a interoperabilidade será medida, que compatibilidades se esperam (S3, SQL Server) e a computação confidencial será exigida?
(perguntas 31, 64, 71, 73 e 88)

Em segurança, o caderno exige:

- gestão de chaves, HSM e PKI sob custódia nacional, e cofre de segredos;
- hardening, gestão de vulnerabilidades, WAF, firewall e IDS/IPS conforme a criticidade;
- SBOM e assinatura de artefatos;
- logs de auditoria centralizados e imutáveis;
- criptografia em trânsito, em repouso, em backup e entre serviços internos;
- isolamento de tenants em doze dimensões.

A interoperabilidade se apoia em padrões e formatos abertos, para que os sistemas possam migrar sem ser reescritos. Na prática, isso significa compatibilidade com a API S3, runtime OCI, API padrão do Kubernetes, CNI e CSI abertos, formatos abertos como Parquet, telemetria aberta e APIs REST documentadas, versionadas e com compatibilidade retroativa. Os motores relacionais de referência são PostgreSQL, MySQL e MariaDB. SQL Server e computação confidencial não constam dos requisitos.

A preocupação com o aprisionamento, inclusive o que poderia surgir da própria solução nacional, está entre as principais preocupações da Administração. O modelo adotado é interoperável e se apoia em padrões de mercado (como o S3, amplamente adotado, ainda que não seja aberto) e em padrões abertos. A Administração reconhece que algum grau residual de aprisionamento é

inevitável e deve ser mitigado. A indicação inicial para bancos gerenciados é o PostgreSQL. A sugestão de incluir computação confidencial será avaliada pelo grupo técnico, e a de definir testes de interoperabilidade por camada tende a ser considerada no detalhamento do caderno de testes.

16. Qual será o papel do Serpro e o do parceiro, quanto a contratação, desenvolvimento, operação (inclusive do DBaaS), acesso administrativo, sustentação e co-desenvolvimento, e por que não desenvolver internamente uma stack própria?
(perguntas 18, 47, 67, 68, 82 e 92)

A operação e a administração do ambiente de produção caberão exclusivamente à empresa pública. Não haverá acesso remoto permanente de fornecedores, e acessos excepcionais de suporte serão previamente autorizados, auditados e registrados. O parceiro se compromete com a evolução contínua da plataforma, com roadmap público e entregas periódicas, e com a capacitação das equipes públicas, segundo marcos para a transição progressiva da autonomia operacional. Também presta suporte em três níveis, sob acordos de serviço compatíveis com infraestruturas críticas. O DBaaS deve funcionar em autosserviço: sem intervenção manual da operadora para criar instâncias e sem intervenção do consumidor para aplicar patches e upgrades.

Ainda não foi definido se o Serpro será contratante ou parceiro de desenvolvimento, e há cenários em avaliação. A orientação inicial é que o parceiro execute o desenvolvimento, com orientação arquitetural do Serpro e intervenção limitada, e admite-se desenvolvimento conjunto com propriedade intelectual compartilhada. O Serpro terá acesso administrativo ativo e total e responderá pelos níveis 1 a 3 de suporte e pelos acordos de serviço perante os clientes. O parceiro atuará no nível 4, de engenharia, desenvolvimento e evolução, sem acesso ao ambiente de produção.

O Serpro tem equipes de desenvolvimento, mas optou pela parceria para fomentar o mercado nacional com o poder de compra do Estado. A internalização da capacidade será assegurada pela transferência de conhecimento, que deve ir além de manuais e documentação, e pelo acesso irrevogável ao código-fonte. Nesse sentido, o parceiro mantém papel continuado ao longo da vida da plataforma, além da entrega do código.

17. Quem poderá participar? Haverá exigência de capital nacional, e admitem-se P&D colaborativo com universidades, ICTs, startups e fabricantes estrangeiros, propostas desenvolvidas com instituições de pesquisa e parcerias internacionais?
(perguntas 7, 17, 26, 49 e 91)

A eventual parceria envolverá empresas do mercado nacional. Havendo P&D, ele deverá ser realizado por técnicos residentes no Brasil, condição para gerar capacitação e adensar o ecossistema tecnológico nacional; o P&D da plataforma, aliás, faz parte do objeto central da parceria. A Administração pretende ampliar o leque de parcerias e fornecedores do Estado. Considera desejável que o software já existente tenha sido desenvolvido no país, por entender que quem desenvolveu é quem domina a tecnologia. A cooperação internacional está entre os instrumentos em avaliação, e admite-se que certos requisitos de soberania exijam esforço próximo da pesquisa, o que alargaria o prazo de entrega.

A intenção é que o parceiro tenha capital majoritariamente brasileiro, com percentual ainda não definido e com salvaguardas contra a compra posterior da empresa por grupos estrangeiros. Admite-se que parte da tecnologia seja desenvolvida no exterior, desde que o código seja integralmente aberto. Ou seja, arranjos com universidades, ICTs, startups e fabricantes globais, e

propostas desenvolvidas com instituições de pesquisa, são compatíveis com o modelo, desde que o P&D ocorra no Brasil e haja transferência efetiva de conhecimento. Os critérios objetivos de elegibilidade serão fixados no edital.

18. Qual é o cronograma, quando a Nuvem Brasileira estará em produção, o projeto independe das eleições, há orçamento aprovado e quantas pessoas e recursos serão necessários para mantê-la?
(perguntas 1, 13 e 14)

O caderno exige custo competitivo em relação às alternativas disponíveis, evolução contínua e transferência de conhecimento. O processo previsto passa pela redução de assimetrias de informação, pelas análises e relatórios, pela definição do instrumento e por sua execução. A escuta coletiva ocorreu em 3 de setembro, e as individuais, entre 8 e 25 de setembro. O projeto é tratado como política de Estado, sem vínculo com o calendário eleitoral. A estimativa é de algo em torno de dois anos até a primeira plataforma em produção. O orçamento depende do formato da parceria e do volume de desenvolvimento necessário, e por isso ainda não pode ser informado.

Concluído o item 1.3 do cronograma do ACT, que contempla a análise integrada das informações coletadas, o diagnóstico da capacidade de oferta do ecossistema nacional e o desenho conceitual da estratégia de execução, inicialmente o cronograma prevê as seguintes etapas: Planejamento (3 meses), Seleção (2 meses), Homologação (1 mês) e Contratação (1 mês), totalizando 7 meses. O BNDES faz parte do acordo de cooperação, inclusive para fins de financiamento, mas isso está em avaliação e irá depender de uma série de análises técnicas que ainda precisam ser feitas. A Administração reconhece que a entrada das empresas depende de o Estado apoiar tanto o financiamento quanto a compra posterior dos serviços. Não se definiu ainda orçamento específico, a entrada em produção deve ocorrer por volta do fim de 2028, e a equipe necessária só poderá ser dimensionada depois da escolha da base tecnológica e do instrumento.

19. Quais são os requisitos específicos de alta disponibilidade, integração com o MAGMA, CI/CD, VPN, expansão evolutiva e registro de contêineres, analytics e IA, e como fica a preservação de dados de guarda permanente?
(perguntas 45, 77, 78, 79, 80, 81 e 83)

O caderno exige, entre outros pontos:

- mecanismos integrados de alta disponibilidade, com tolerância à perda de uma zona, e de recuperação de desastres, com replicação e restauração entre zonas e entre regiões e com RTO e RPO definidos por classe de serviço;
- integração do autosserviço com o catálogo de APIs da Secretaria de Governo Digital (MAGMA), a ser detalhada no termo de referência;
- na camada de plataforma, ferramentas integradas de CI/CD com suporte a GitOps, e VPN Gateway, VPC Peering, NAT, Internet Gateway e CDN sob demanda;
- expansão evolutiva do catálogo de dados, com padrões de interoperabilidade para registros de contêineres e microsserviços.

IA e aprendizado de máquina são obrigatórios. Analytics (data lake, data warehouse ou lakehouse) é desejável e inclui, como evolução, o treinamento e a disponibilização de modelos, servindo de base para as aplicações de IA. Para dados de guarda longa, o caderno prevê classes de

armazenamento diferenciadas por desempenho e backups exportáveis para fora da solução, com restauração independente dos recursos internos da stack, sem plano específico de preservação permanente.

Nas escutas, foram esclarecidos quatro pontos:

- alta disponibilidade e recuperação devem estar disponíveis em autosserviço dentro dos próprios serviços, inclusive bancos de dados e virtualização, e as regiões secundárias devem manter alta disponibilidade;
- o MAGMA corresponde ao catálogo de APIs governamentais integrado ao provisionamento;
- CI/CD e VPN são serviços de catálogo para os clientes, com a VPN oferecida na camada de tenant;
- a expansão evolutiva diz respeito à previsibilidade do ciclo de vida da stack, sobretudo na oferta de containers e microsserviços.

Soluções dedicadas de preservação de longo prazo poderão se integrar por interoperabilidade.

20. Como acessar a gravação e a apresentação, e as associações empresariais serão ouvidas?
(perguntas 28, 48 e 95)

Todas as reuniões foram gravadas, e as transcrições foram juntadas ao processo administrativo. A gravação, a apresentação e as perguntas com as respectivas respostas ficam disponíveis na plataforma do projeto, em www.abdi.com.br/nuvembrasileira. Com o encerramento das escutas individuais de empresas em 25 de setembro, serão enviados convites para reuniões de contribuição com as associações diretamente envolvidas no projeto.