Plano Nacional de Nuvem Soberana

Uma Infraestrutura Moderna, Soberana e Eficiente

Perguntas Frequentes

Maio 2026

REPÚBLICA PORTUGUESA

XXV GOVERNO CONSTITUCIONAL

Questões e Respostas – Plano Nacional de Nuvem Soberana (PNNS)

1. O que é o Plano Nacional de Nuvem Soberana (PNNS)?
2. Quais são os principais objetivos do PNNS?
3. O que se entende por "cloud"?
4. O que significa "soberania digital"?
5. O que significa "cloud soberana" no contexto da transformação digital do Estado?
6. O PNNS implica a criação de uma cloud única do Estado?
7. Porque é que o Governo decidiu avançar com este plano agora?
8. Quem foi envolvido na definição do PNNS?
9. O PNNS está alinhado com práticas internacionais? Que países foram considerados como referência?
10. Como se articula o PNNS com o Programa do XXV Governo Constitucional e com a Estratégia Digital Nacional?
11. Quem assegura a governação, acompanhamento e monitorização do PNNS?
12. Que impacto terá o PNNS para os cidadãos e para as empresas?
13. Qual é a visão futura do PNNS para o ecossistema digital nacional e fornecedores de cloud nacionais?
14. Como está estruturado o PNNS?
15. O que prevê o Eixo I – Infraestrutura Digital Soberana?
16. Qual é o papel do modelo de qualificação de processos e dados?
17. Que níveis de soberania estão previstos?
18. Que requisitos estão associados a cada nível de soberania?
19. Qual é a distribuição estimada dos dados por níveis de soberania?
20. Quem é responsável por conceber e aplicar a metodologia de qualificação?
21. Qual é o papel do Eixo II – Capacitação de recursos humanos?
22. Em que consiste o Eixo III – Enquadramento Legal e Regulatório?
23. Qual é a despesa atual do Estado em serviços de cloud?
24. Qual é a despesa atual do Estado em centros de dados?
25. Como será financiado o PNNS?
26. Que poupanças o Governo espera obter com a implementação do PNNS?
27. De que forma o PNNS contribui para os objetivos ambientais e de eficiência energética?
28. O Estado irá migrar todos os centros de dados para a cloud?
29. De forma o PNNS articula com o Plano Nacional de Centros de Dados?
30. Como será garantida a segurança e a conformidade regulatória (RGPD, NIS2, etc.)?
31. Qual é a calendarização global de implementação do PNNS?
32. Em termos práticos, o que terão de fazer as entidades da Administração Pública?
33. Como podem as entidades verificar se cumprem os requisitos definidos?
34. Qual será o prazo para a migração das entidades?
35. Qual será o custo da migração para as entidades?
36. Onde se posicionará Portugal em 2030 com a implementação do PNNS?

1. O que é o Plano Nacional de Nuvem Soberana (PNNS)?

O PNNS é o plano do XXV Governo para dotar o Estado de uma infraestrutura digital moderna, assente em soluções *cloud*, que garantam soberania, segurança e controlo sobre os dados e sistemas críticos da Administração Pública. Resulta da Resolução do Conselho de Ministros que o aprova como instrumento central da transformação tecnológica do Estado.

2. Quais são os principais objetivos do PNNS?

Os objetivos centrais são: reforçar a soberania digital e a segurança do Estado; aumentar a eficiência operacional e reduzir custos estruturais de Tecnologias de Informação e Comunicação; modernizar as infraestruturas digitais públicas; acelerar a transformação digital de serviços públicos; e posicionar Portugal como polo de confiança digital e de serviços de dados e IA soberana.

3. O que se entende por "Nuvem" (*Cloud*)?

Cloud Computing é um modelo que permite acesso via rede, de forma conveniente e a pedido (*on demand*), a recursos computacionais partilhados e configuráveis, que podem ser rapidamente provisionados e escalados com mínima gestão e interação com o fornecedor, assegurando flexibilidade, eficiência, elasticidade e otimização de custos.

4. O que significa "Soberania Digital"?

O conceito de "Soberania Digital" traduz-se na capacidade de uma região ou país controlar a sua infraestrutura, dados e tecnologias digitais, tomando decisões autónomas de acordo com os seus objetivos estratégicos, garantindo simultaneamente competitividade económica e segurança para os seus cidadãos, bem como a redução de dependências externas críticas e maior resiliência tecnológica.

5. O que significa "Cloud Soberana" no contexto da transformação digital do Estado?

"Cloud Soberana" corresponde a um modelo de serviços de computação em nuvem que garante ao Estado controlo efetivo sobre os seus dados, sistemas e infraestruturas críticas, de acordo com requisitos de soberania, segurança e resiliência. Na prática, significa assegurar que a localização dos dados, o acesso, a operação, a governação tecnológica e as dependências críticas permanecem sob controlo compatível com o interesse nacional e com o quadro jurídico europeu.

6. O PNNS implica, então, a criação de uma cloud única do Estado?

Não. O PNNS não prevê a criação de uma cloud única e centralizada do Estado. Assenta antes num modelo composto por diferentes soluções de infraestrutura digital, organizadas de forma interoperável e ajustadas aos níveis de soberania exigidos por cada tipo de processo, dados e sistemas. Este modelo permite garantir flexibilidade, eficiência e controlo adequado, evitando uma abordagem única para realidades distintas.

7. Porque é que o Governo decidiu avançar com este plano agora?

Portugal enfrenta uma combinação de desafios: fragmentação de infraestruturas, envelhecimento do parque tecnológico, ameaças crescentes em cibersegurança e forte dependência de fornecedores de fora da Europa. Ao mesmo tempo, a transição digital e a inteligência artificial exigem uma base tecnológica robusta, energéticamente eficiente e soberana, focada em dados, sob pena de o Estado perder capacidade de decisão e competitividade.

8. Quem foi envolvido na definição do PNNS?

A definição do PNNS resultou de um processo alargado de auscultação, coordenado pela Agência para a Reforma Tecnológica do Estado (ARTE, I.P.) que envolveu mais de 100 entidades públicas e privadas. Foram realizadas mais de 25 sessões de trabalho com fornecedores de serviços de *cloud*, associações do setor TIC, entidades da Administração Pública (central e local) no Centro, Norte e Sul do Continente e com representantes de setores críticos, assegurando uma abordagem colaborativa e alinhada com as necessidades reais dos serviços públicos digitais do Estado.

9. O PNNS está alinhado com práticas internacionais? Que países foram considerados como referência?

Sim, o PNNS está alinhado com as práticas internacionais de Cloud Soberana e soberania digital. A sua definição teve por base a auscultação direta e análise comparativa de 11 países com diferentes níveis de maturidade nesta área. Destacam-se países como Alemanha, França, Itália e Reino Unido, que apresentam modelos mais consolidados e estruturados em temáticas de Soberania Digital, bem como Estónia, enquanto referência na modernização e transformação digital do setor público. A análise foi complementada por outros países, como Espanha, Países Baixos, Dinamarca, Ucrânia, Israel e Singapura, permitindo uma visão abrangente e comparável de diferentes abordagens e contextos específicos de cada país. As boas práticas identificadas foram adaptadas ao contexto nacional e constituem a base do modelo definido n**o PNNS.**

10. Como se articula o PNNS com o Programa do XXV Governo Constitucional e com a Estratégia Digital Nacional?

O PNNS operacionaliza a prioridade política de posicionar Portugal entre os países digitalmente mais avançados da Europa, prevista no Programa do XXV Governo. Está integrado no Plano de Ação da Estratégia Digital Nacional 2026-2027, que inclui medidas de centralização/racionalização em cloud, qualificação de dados e desenvolvimento de cloud soberana.

11. Quem assegura a governação, acompanhamento e monitorização do PNNS?

Nos termos do diploma aprovado pelo Governo que estabelece o novo modelo de governação para a transformação digital do Estado, a coordenação estratégica do PNNS insere-se na estrutura criada para assegurar uma direção integrada das políticas digitais e do investimento público tecnológico. Nesse quadro, a Rede de Simplificação e Tecnologias do Estado assegura o acompanhamento e monitorização transversal das medidas do plano, promovendo a articulação entre entidades públicas e a execução coordenada das iniciativas estratégicas.

Em complemento, o Centro Nacional de Cibersegurança (CNCS) e a ARTE, I.P., assumem responsabilidades técnicas na definição de referenciais, na qualificação e na acreditação de soluções, em articulação com as áreas setoriais e entidades operacionais.

12. Que impacto terá o PNNS para os cidadãos e para as empresas?

O PNNS traduz-se em serviços públicos digitais mais simples e melhor integrados (mais disponíveis, com menos falhas, com tempos de resposta mais rápidos e através de maior confiança na proteção dos dados). Ao modernizar a infraestrutura tecnológica do Estado e reduzir a fragmentação existente, o plano permitirá libertar recursos atualmente afetos à manutenção de sistemas dispersos, canalizando-os para a inovação e melhoria contínua dos serviços públicos. Para cidadãos e empresas, isso significará uma Administração Pública mais ágil, eficiente e preparada para responder com maior rapidez às necessidades sociais e económicas do país.

13. Qual é a visão futura do PNNS para o ecossistema digital nacional e fornecedores de Cloud nacionais?

Prevê-se que, no futuro, possam ser credenciadas soluções de cloud tanto do mercado como da própria Administração Pública, desde que cumpram requisitos a serem definidos. Esta abordagem promove um ecossistema aberto e competitivo, estimulando o desenvolvimento do mercado de cloud nacional, reforçando a autonomia tecnológica e criando oportunidades para o crescimento de capacidades digitais no país.

14. Como está estruturado o PNNS?

O plano está organizado em três eixos de ação: (I) Infraestrutura Digital Soberana, (II) Capacitação de recursos humanos, e (III) Alterações Legislativas. Cada eixo agrega um conjunto de iniciativas concretas, com objetivos, responsabilidades e calendário definidos.

15. O que prevê o Eixo I – Infraestrutura Digital Soberana?

O Eixo I inclui: um modelo uniforme de qualificação de processos de negócio e respetivos dados/sistemas; o desenvolvimento de uma oferta nacional de cloud soberana, incluindo capacidades de IA; um plano de adoção faseado para a Administração Pública; a criação de um catálogo unificado de serviços *cloud* e melhores processos de contratação de serviços *cloud*.

16. Qual é o papel do modelo de qualificação de processos e dados?

O modelo de qualificação é o "cérebro/pilar" da estratégia de soberania: permite qualificar processos e dados da Administração Pública segundo o seu impacto em pessoas, estabilidade do Estado e exposição de informação. A partir daí, atribui-se um nível de soberania (0 a 3) que determina os requisitos mínimos de segurança, resiliência e controlo a cumprir pelas infraestruturas e serviços cloud utilizados.

17. Que níveis de soberania estão previstos?

Existem quatro categorias: Neutro (nível 0, sem requisitos específicos de soberania), Corrente (nível 1, requisitos base), Crítico (nível 2, exigência acrescida de soberania de dados e operacional) e

Estratégico (níveis 3.a e 3.b, com requisitos máximos de soberania, incluindo soberania de software e, quando justificado, soberania de software de âmbito nacional).

18. Que requisitos estão associados a cada nível?

Os requisitos de soberania e segurança variam consoante o nível de qualificação atribuído a cada processo, aumentando progressivamente em exigência à medida que sobe o nível de soberania. De forma geral, incluem dimensões como controlo de localização e jurisdição dos dados, encriptação, gestão de acessos e identidades, segurança de redes e operações, conformidade regulatória, bem como requisitos associados à interoperabilidade, portabilidade e controlo sobre software e infraestruturas.

19. Qual é a distribuição estimada dos dados por níveis de soberania?

Com base na experiência internacional, estima-se que a maioria dos dados da Administração Pública se concentre nos níveis mais baixos de soberania: cerca de 70% no nível neutro (nível 0), 20% no nível corrente (nível 1) e aproximadamente 7,5% no nível crítico (nível 2). Apenas uma pequena fração, cerca de 2,5%, deverá ser qualificada como estratégica (níveis 3.a e 3.b), exigindo os requisitos mais elevados de soberania, segurança e controlo.
Estas percentagens têm caráter indicativo, servindo para ilustrar a lógica do modelo, sendo a distribuição efetiva determinada no âmbito do processo de qualificação.

20. Quem é responsável por conceber e aplicar esta metodologia de qualificação?

A metodologia é desenvolvida pelo Centro Nacional de Cibersegurança (CNCS) e pela ARTE, I.P., que definem o procedimento de pontuação, produzem uma tabela de pré-qualificação baseada no catálogo de processos da Administração Pública e estabelecem os requisitos de soberania e segurança associados a cada nível.

21. Qual é o papel do Eixo II – Capacitação de recursos humanos?

O Eixo II responde ao défice de competências tecnológicas na Administração Pública. Prevê uma matriz de competências específica para cloud soberana, programas de formação para técnicos e dirigentes, estágios e ações de capacitação em soberania digital, com metas claras de percentagem de especialistas formados e número de dirigentes capacitados até 2030.

22. Em que consiste o Eixo III – Alterações Legislativas?

O Eixo III trata de "desbloquear" a adoção de cloud do ponto de vista jurídico e financeiro: simplifica o processo de contratação de serviços cloud, alinha o Código dos Contratos Públicos com as necessidades de centralização e escala, e clarifica o enquadramento contabilístico e a elegibilidade dos serviços cloud e de IA soberana em termos de financiamento público e europeu.

23. Qual é a despesa atual do Estado em serviços de cloud?

Não existe ainda uma visão da despesa pública em serviços de cloud para o conjunto da Administração Pública. Contudo, com base no levantamento relativo ao Relatório de Adoção de

Cloud da Administração Pública em 2025 levado a cabo pela ARTE, I.P., identificou-se que a despesa anual em 262 organismos da AP Central e Local é de 35M€.

24. Qual é a despesa atual do Estado em centros de dados?

Com base na informação orçamental disponível, estima-se que a despesa anual do Estado com componentes de infraestrutura digital ronde atualmente os 70M€. Este valor corresponde a uma estimativa dos custos TIC associados a infraestrutura tecnológica, excluindo componentes como energia, instalações, recursos humanos, software e custos operacionais de cloud. Adicionalmente, estima-se que só a componente energética dos centros de dados da Administração Pública represente cerca de 6M€/ano, o que evidencia o potencial de eficiência associado à modernização e consolidação destas infraestruturas. Trata-se de uma estimativa indicativa, excluindo investimentos extraordinários financiados por PRR.

25. Como será financiado o PNNS?

O investimento global estimado ronda os 217M€ no período 2026-2030, combinando recursos do Orçamento do Estado e investimento de parceiros privados. Do lado do Orçamento do Estado, estimam-se cerca de 117M€, distribuídos entre infraestrutura, migração/adoção de cloud e ações de capacitação e governação, privilegiando o recurso a fundos europeus sempre que possível.

26. Que poupanças o Governo espera obter com a implementação do PNNS?

Estimam-se poupanças diretas de cerca de 28M€/ano, sobretudo pela consolidação de centros de dados e pela melhoria da eficiência energética. A estas somam-se poupanças indiretas na ordem de 165M€/ano, resultantes de poupanças indireta derivado de economias de escala, modernização tecnológica, automatização e redução de duplicação entre organismos.

27. De que forma o PNNS contribui para os objetivos ambientais e de eficiência energética?

A consolidação de milhares de pequenas salas técnicas e data centers dispersos em infraestruturas de *cloud* modernas permite reduzir significativamente o consumo de energia por unidade de computação (melhoria do PUE – *Power Usage Effectiveness*). Isto traduz-se numa menor pegada ambiental, maior previsibilidade de custos energéticos e melhor alinhamento com os objetivos de sustentabilidade / ESG assumidos pelo Estado.

28. O Estado irá migrar todos os centros de dados para a *Cloud*?

Não. O PNNS não prevê a migração integral de todos os centros de dados para a *cloud*. O modelo assenta numa abordagem em que a adoção de soluções *cloud* depende do nível de soberania associado a cada processo. Em alguns casos, poderão manter-se soluções *on-premises* ou híbridas, quando tal se justifique em termos de segurança, controlo ou eficiência. O objetivo é promover a consolidação e modernização das infraestruturas, e não uma migração indiscriminada.

29. De forma o PNNS articula com o Plano Nacional de Centros de Dados?

O PNNS articula-se diretamente com o Plano Nacional de Centros de Dados, complementando-o numa lógica integrada de modernização da infraestrutura digital do Estado. Enquanto o Plano

Nacional de Centros de Dados promove a racionalização, consolidação e eficiência física das infraestruturas existentes, o PNNS acrescenta uma camada estratégica de soberania digital, qualificação de processos e adoção de soluções cloud adequadas a cada necessidade. Os centros de dados que cumpram os requisitos de *cloud* soberana poderão ser utilizados para albergar as cargas do Estado.

30. Como será garantida a segurança e a conformidade regulatória (RGPD, NIS2, etc.)?

Os requisitos de soberania e segurança definidos para cada nível de qualificação aplicam-se em paralelo com as obrigações decorrentes de diplomas como o RGPD, a Diretiva NIS2, a legislação de cibersegurança e outros regulamentos setoriais. As soluções qualificadas terão de demonstrar cumprimento sistemático dos requisitos de soberania, com mecanismos de auditoria, certificação e supervisão contínua.

31. Qual é a calendarização global de implementação do PNNS?

Entre 2026 e 2027 serão definidos o modelo de qualificação, a framework de requisitos e o enquadramento legal, e realizado o levantamento e qualificação de processos de negócio da Administração Pública. A partir de 2027 arranca a elaboração dos planos de adoção setoriais, a consolidação de infraestruturas e a expansão da oferta de cloud soberana. Ainda em 2026/27 iniciam-se os trabalhos para garantir que existe uma oferta completa de serviços de cloud soberana no mercado, incluindo a criação de capacidade própria do Estado para um conjunto de necessidades que exigem controlo nacional. Até 2030, o objetivo é ter as principais plataformas comuns da Administração Pública disponíveis em cloud e um nível significativo de capacitação interna em soberania digital.

32. Em termos práticos, o que terão de fazer as entidades da Administração Pública?

As entidades terão de inventariar os seus processos de negócio, sistemas e infraestruturas, aplicar o modelo de qualificação (usando a pré-qualificação ou pontuando os seus processos) e, com base nisso, robustecer as soluções atuais ou planear a migração e adoção para soluções em cloud adequadas ao nível de soberania exigido para cada processo.

33. Como podem as entidades verificar se cumprem os requisitos definidos?

O cumprimento será assegurado através da aplicação do modelo de qualificação de processos e dos referenciais técnicos definidos pelo Centro Nacional de Cibersegurança (CNCS) e pela ARTE, I.P. As entidades deverão qualificar as necessidades de soberania dos seus processos recorrendo a uma tabela de pré-qualificação elaborada pela ARTE e o CNCS. A cada nível de soberania estão associados requisitos de segurança e controlo definidos pela ARTE e CNCS.

34. Qual será o prazo para a migração das entidades?

A migração será faseada e alinhada com os planos de adoção setoriais, a desenvolver a partir de 2026, com implementação progressiva até 2030 com base nas prioridades que se identifiquem na

fase de levantamento. Este modelo permite uma transição controlada, ajustada às prioridades e maturidade de cada entidade.

35. Qual será o custo da migração para as entidades?

Os custos de migração irão variar consoante o ponto de partida e as necessidades específicas de cada entidade. Contudo, o PNNS prevê uma abordagem coordenada e financiada a nível do Estado, reduzindo a necessidade de cada organismo suportar isoladamente os investimentos necessários. financiamento nacional e europeu, permitirá distribuir o esforço ao longo do tempo e gerar ganhos de eficiência e redução de custos operacionais para a Administração Pública.

36. Onde se posicionará Portugal em 2030 com a implementação do PNNS?

Até 2030, Portugal deverá dispor de uma infraestrutura digital moderna, segura e resiliente, com as principais plataformas da Administração Pública suportadas em soluções de cloud alinhadas com os níveis de soberania definidos.

O Estado terá maior controlo sobre os seus dados e sistemas críticos, maior eficiência na gestão de recursos tecnológicos e maior capacidade para inovar e desenvolver serviços públicos digitais mais simples, integrados e centrados no cidadão.

Simultaneamente, o PNNS contribuirá para posicionar Portugal como um polo de confiança digital na Europa, potenciando o desenvolvimento do ecossistema tecnológico nacional, incluindo serviços de cloud, dados e inteligência artificial.

REPÚBLICA
PORTUGUESA