

# Plano Nacional de Nuvem Soberana

**Uma Infraestrutura Moderna, Soberana e Eficiente**

Maio 2026



**REPÚBLICA  
PORTUGUESA**

---

XXV GOVERNO CONSTITUCIONAL

# Sumário Executivo

A **transformação e reforma tecnológica do Estado** constituem prioridades centrais do Programa do XXV Governo Constitucional, que visa posicionar **Portugal entre os países digitalmente mais avançados da Europa**, impulsionando uma Administração Pública mais eficiente, resiliente e preparada para os desafios da era digital.

A **crescente relevância das infraestruturas digitais e dos dados** para a economia e instituições públicas, bem como o aumento dos riscos associados a fenómenos meteorológicos extremos, ao cibercrime e à guerra eletrónica, reforçam a soberania e resiliência digital como prioridade estratégica nacional e europeia. Definindo soberania como o **controlo do acesso aos dados e a garantia permanente de funcionamento de sistemas e infraestruturas críticas**, esta é condição essencial para a continuidade dos serviços públicos, a segurança da informação e a autonomia de decisão do Estado, cabendo-lhe reforçar o papel de Portugal na oferta de serviços de **computação em nuvem e de Inteligência Artificial soberanos**.

O **Plano Nacional de Nuvem Soberana (PNNS)**, parte do **Plano de Ação 2026-2027 da Estratégia Digital Nacional (EDN)** sob a ação 13.1, responde diretamente a este desafio, definindo uma **visão estratégica** e linhas de ação para a adoção coordenada, transversal e segura de serviços de computação em nuvem na Administração Pública. Assente numa **base tecnológica soberana, moderna, segura e resiliente**, o PNNS promove uma estratégia de preferência pela computação em nuvem, ajustada a diferentes níveis de soberania consoante os processos, dados e sistemas, reforçando simultaneamente a eficiência operacional e a qualidade dos serviços públicos.

Simultaneamente, o PNNS adapta o *Cloud Sovereignty Framework* da Comissão Europeia ao contexto português em articulação com o enquadramento legislativo existente, organizando-se em **três eixos de ação** que visam garantir que a adoção de soluções de computação e nuvem flexíveis, seguras, coordenadas e sustentáveis, de forma coerente com os diferentes níveis de soberania exigidos pelos diversos domínios da Administração Pública.

Com este plano, o Governo posiciona Portugal na vanguarda da **soberania digital europeia**, reforça a proteção da **informação estratégica do Estado** e assegura a continuidade dos serviços públicos e uma infraestrutura digital adequada aos desafios da transformação tecnológica, contribuindo para uma economia digital mais dinâmica, inovadora e competitiva.

# A Necessidade

A importância do **PNNS** advém de uma mudança estrutural em curso, em que, e de forma crescente, **o funcionamento da economia, dos serviços públicos e da própria soberania do Estado assenta em infraestruturas digitais e em dados** que, muitas vezes, não estão sob controlo direto do país. A crescente dependência de prestadores de serviços extra-europeus, combinada com novas obrigações regulatórias e com a aceleração tecnológica, tem **implicações diretas no risco** e manutenção de um modelo fragmentado, assente em milhares de centros de dados dispersos e sistemas legados difíceis de proteger e de atualizar.







Ao mesmo tempo, o **contexto externo apresenta-se como tendencialmente mais volátil e exigente**. As tensões geopolíticas, o aumento dos ciberataques, a guerra eletrónica e a frequência de fenómenos meteorológicos extremos expõem vulnerabilidades nas infraestruturas críticas e podem pôr em causa a continuidade de serviços públicos essenciais. Sem uma estratégia clara para a nuvem soberana, o Estado arriscar-se-ia a perder capacidade de decisão sobre onde estão os seus dados, quem lhes pode aceder e como são protegidos, com **impacto direto na segurança, na confiança dos cidadãos e na estabilidade das instituições**.

Este plano é, por isso, necessário para dar coerência, escala e direção à transformação digital da Administração Pública. Ao definir um **modelo comum de qualificação de processos e dados, requisitos claros de soberania e segurança e uma oferta estruturada de infraestruturas de nuvem soberanas**, o Estado ganha capacidade **para modernizar sistemas, reduzir custos estruturais e melhorar a qualidade dos serviços**, sem abdicar do controlo sobre os seus ativos mais críticos. Desta forma, o Plano Nacional de Nuvem Soberana tem um papel essencial na garantia de que a digitalização do Estado é feita em termos que reforçam a **soberania, a resiliência e a competitividade do país**.

# Efeitos na Administração Pública

A adoção de uma Nuvem Soberana na Administração Pública tem como objetivo criar uma infraestrutura digital moderna, comum e segura, **capaz de suportar a reforma do Estado e o desenvolvimento contínuo de serviços públicos digitais**. Em vez de cada organismo manter o seu próprio “mini-data-center” com níveis muito desiguais de maturidade, segurança e eficiência, a Nuvem Soberana propõe uma **plataforma partilhada**, com requisitos claros de soberania, em que os sistemas críticos da Administração passam a operar em ambientes mais resilientes, auditáveis e preparados para a Inteligência Artificial. Isto permite reduzir a fragmentação tecnológica, acelerar a modernização de sistemas legados e garantir que os dados mais sensíveis permanecem sob controlo efetivo do Estado, mesmo quando são utilizados serviços avançados de computação em nuvem.

No conjunto, os objetivos e efeitos da Nuvem Soberana na Administração Pública convergem para três dimensões principais: **reforçar o controlo e a segurança sobre os ativos digitais críticos, aumentar a eficiência estrutural da máquina do Estado e criar uma base tecnológica capaz de sustentar a inovação e o crescimento da economia digital portuguesa.**

	Modelo atual	Modelo futuro
 <b>Redução Riscos de Soberania</b>	Exposição acrescida a <b>riscos de segurança, continuidade de serviço</b> e resiliência tecnológica	Reforço da <b>soberania, segurança e conformidade de dados e sistemas críticos</b> , alinhado com requisitos europeus
 <b>Consolidação de Infraestrutura</b>	Cerca de <b>4.000 data centers e salas técnicas</b> , dispersos em <b>1500 entidades</b> públicas	<b>Consolidação progressiva da infraestrutura</b> digital do Estado, com ganhos de eficiência
 <b>Otimização do Ciclo de Vida</b>	<b>Modelo de infraestrutura fragmentado</b> , baixa utilização e capacidade e ausência de escala	<b>Modelo cloud “as-a-service”</b> , com custos ajustados à utilização real e maior <b>flexibilidade operacional</b>
 <b>Eficiência Energética</b>	Níveis <b>significativos de ineficiência energética e operacional</b> , com impacto direto na despesa pública	Melhoria significativa da <b>eficiência energética</b> , com reduções potenciais até <b>46% no consumo</b>
 <b>Economias de Escala</b>	<b>Contratação de serviços cloud descentralizada</b> , limitando economias de escala e coerência estratégica	<b>Ganhos de escala na contratação</b> , reforçando o poder negocial do Estado e reduzindo custos unitários
 <b>Redução de Custos</b>	Despesa pública em TIC elevada, com forte peso da despesa de operação de Data Centers ( <b>-69M€/ano</b> )	<b>Redução de até 25% nos custos de TIC</b> e 35% custos de infraestrutura - <b>28M€/ano</b> de poupanças diretas

# Implementação

A implementação do PNNS estrutura-se em três etapas sequenciais: em primeiro lugar, a **qualificação dos processos** de negócio e dos respetivos dados e sistemas; em segundo lugar, a **definição dos requisitos de soberania e de segurança aplicáveis** a cada nível de qualificação; e, em terceiro lugar, a criação de **uma oferta de infraestruturas** soberanas que responda de forma adequada a esses requisitos.

Na primeira etapa, a Administração Pública procede ao **levantamento e análise sistemática** dos seus **processos de negócio**, bem como dos dados e sistemas de informação que os suportam, avaliando o impacto de eventuais falhas na perspetiva das pessoas, da estabilidade do Estado e da exposição de dados. Para operacionalizar esta análise, o Centro Nacional de Cibersegurança (CNCS) e a Agência para a Reforma Tecnológica do Estado, I.P. ( ARTE, I.P.) definem níveis graduais de qualificação de processos, alinhados com a Diretiva (UE) 2022/2555 (Diretiva NIS2) e com o trabalho desenvolvido no contexto do sistema europeu de certificação de cibersegurança (EUCS) e das iniciativas de normalização do CEN e do CENELEC. São identificados **quatro níveis de qualificação** – neutro, corrente, crítico e estratégico – que refletem, de forma diferenciada, o **impacto potencial do comprometimento de cada processo**. A classificação resulta, deste modo, de um procedimento de pontuação estruturado, que permite às entidades da Administração Pública qualificar os seus processos de forma harmonizada e comparável.

A segunda etapa consiste em associar a cada um destes níveis de qualificação um conjunto de **requisitos objetivos de soberania, segurança e resiliência**. Com base no enquadramento definido pelo CNCS e pela ARTE, I.P., são estabelecidos, para cada nível, parâmetros claros quanto à localização e ao controlo dos dados, aos controlos técnicos e organizacionais mínimos, aos mecanismos de auditoria e certificação, bem como aos níveis de redundância e continuidade de serviço a assegurar. Este quadro de requisitos, estruturado de forma crescente em função dos quatro níveis de qualificação, garante **consistência e rigor** na aplicação das regras de soberania e segurança em toda a Administração Pública.

# Implementação

Posteriormente, a terceira etapa centra-se na **compilação de uma oferta de infraestruturas digitais soberanas e na criação de condições para que o mercado funcione**, configurando um **portefólio coerente** de soluções tecnológicas que dê resposta aos **diferentes níveis de exigência** identificados, assegurando que a oferta interna da Administração Pública e a oferta do mercado cumprem os requisitos de soberania e segurança. Tal inclui infraestruturas públicas partilhadas para os níveis mais elevados de soberania, soluções de nuvem privada ou híbrida para processos críticos e a utilização enquadrada de nuvem pública para processos com menores requisitos. Esta etapa integra ainda a definição de catálogos de serviços, modelos de financiamento, instrumentos de contratação e um plano faseado de adoção que prioriza os domínios mais sensíveis.

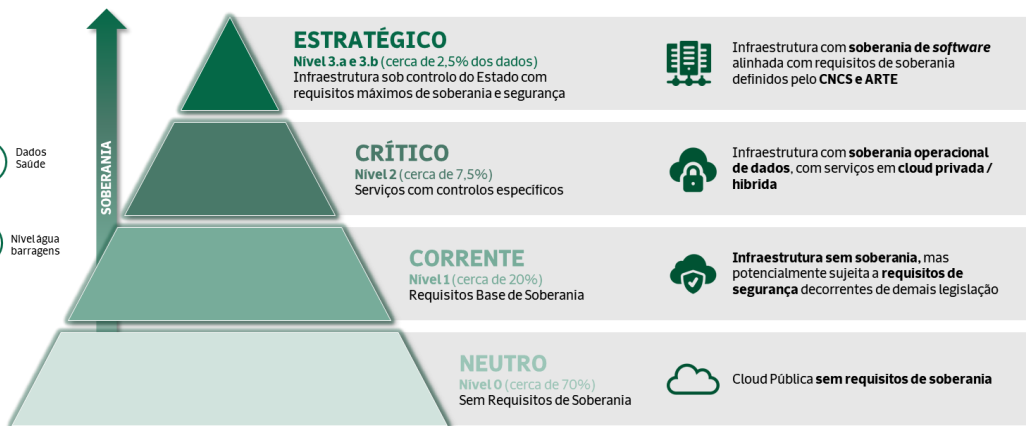
## 1 Qualificação dos Processos de Negócio / Dados

Determina-se o **nível de soberania** necessário em função da **sensibilidade, criticidade e confidencialidade dos dados e processos**



## 2 Requisitos de Soberania e Segurança

A cada **nível de soberania** correspondem diferentes requisitos de soberania e segurança, **que definem as condições** a cumprir



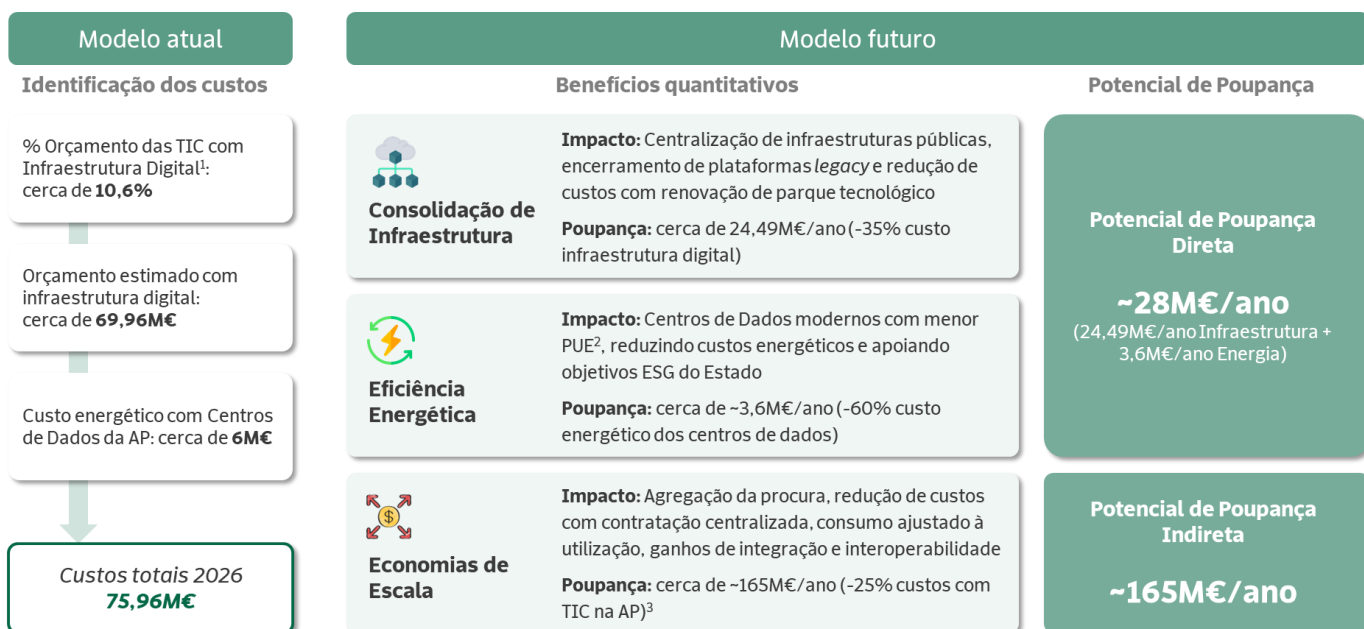
## 3 Criação de Oferta e Migração para Infraestrutura Soberana

Criação de **infraestrutura digital soberana** adequada aos diferentes níveis e **migração e adoção pela AP** de forma gradual

No seu conjunto, as três etapas permitem que o **PNNS se traduza num percurso operacional claro, do diagnóstico à implementação**, garantindo que a modernização tecnológica da Administração Pública é realizada em conformidade com os objetivos de soberania, segurança e resiliência do Estado.

# Benefícios

A implementação do PNNS deverá trazer benefícios muito relevantes para o Estado, não só em termos financeiros, mas também estratégicos e qualitativos. Do ponto de vista económico, o plano aponta para uma **redução significativa de custos estruturais e operacionais**, através da **consolidação de infraestruturas**, da **melhoria da eficiência energética** e das **economias de escala na contratação de serviços de computação em nuvem**.



1 - IMPIC Relatório anual de 2024 - Contratação Pública em Portugal  
2 - Estudo do Levantamento dos Data Centers da AP - AMA 2015  
3 - Estudo de caso do UK e melhores práticas internacionais

Em termos qualitativos, o **PNNS reforça a soberania e a resiliência digital da Administração Pública, aumentando o controlo sobre dados, sistemas críticos e infraestruturas estratégicas**. Isso traduz-se numa **menor exposição a riscos regulatórios e geopolíticos**, maior capacidade de auditoria e governação, e melhores condições para assegurar continuidade de serviço, segurança e conformidade. Além disso, cria uma base tecnológica mais sólida para acelerar a inovação, incluindo o uso de Inteligência Artificial soberana, e para aumentar a autonomia tecnológica do país.

# Plano de Ação

# Eixos de Ação

O PNNS assenta num plano de ação organizado em **três grandes eixos**, que estruturam a transformação de forma faseada e coerente em toda a Administração Pública. Deste modo, procura-se a articulação da modernização das infraestruturas, o desenvolvimento de capacidades internas e a adaptação do enquadramento normativo e financeiro, garantindo **alinhamento entre a dimensão tecnológica, organizacional e regulatória**. Esta arquitetura em três eixos permite que a implementação seja progressiva, mas orientada por uma **visão comum**, reduzindo riscos de fragmentação, duplicação de investimentos e abordagens contraditórias.

Cada eixo responde a um tipo distinto de desafio associado à soberania digital: por um lado, a necessidade de dispor de **bases tecnológicas robustas e seguras**; por outro, a exigência de **qualificar pessoas e instituições** para operar nesse novo contexto; e, finalmente, a **obrigação de adequar regras, procedimentos e instrumentos de gestão pública** a um modelo em que a nuvem se torna a opção preferencial. O plano de ação define, assim, um conjunto de iniciativas agrupadas nestes três domínios, com responsabilidades claras, metas temporais e orientações comuns, permitindo coordenar esforços entre ministérios, organismos centrais e entidades setoriais.

## I. Infraestrutura Digital Soberana

- ★ I.1 Modelo de Qualificação de Processos de Negócio
- ★ I.2 Desenvolvimento da Oferta de Cloud Soberana Incluindo IA [alinhada com ANIA]
- ★ I.3 Plano de Adoção da Cloud Soberana
- I.4 Definição de Acordo-Quadro para serviços cloud

## II. Capacitação de recursos humanos

- II.1 Matriz de Competências para a Cloud Soberana
- II.2 Plano de Capacitação em Soberania Digital

## III. Alterações Legislativas

- III.1 Simplificação e revisão do Processo de Aquisição de Serviços Cloud
- III.2 Elegibilidade financeira dos serviços de computação em nuvem



★ Legenda: **Iniciativas Estratégicas**

# I. Infraestrutura Digital Soberana

Objetivo | **Estabelecer uma base tecnológica comum, segura e escalável para processos e dados do Estado**

Início

## Modelo de Qualificação dos Processos de Negócio

S1 2026

Definição de um modelo uniforme de qualificação dos processos de negócio da Administração Pública, aplicável aos dados e sistemas de informação associados.

Inclui categorias de processos, o respetivo enquadramento normativo, requisitos de soberania, segurança e resiliência por nível de qualificação e, ainda, especificações técnicas associadas a tais requisitos de soberania.

1.1

Levantamento e inventariação dos processos e infraestruturas tecnológicas da Administração Pública, nomeadamente através da identificação e catalogação das dependências tecnológicas, vulnerabilidades e riscos.

Aplicação do Modelo de Qualificação dos Processos de Negócio aos dados e sistemas inventariados.

## Desenvolvimento da Oferta de Nuvem Soberana incluindo IA

S1 2026

Desenvolvimento, pelo Estado, de infraestrutura nacional soberana de nuvem, incluindo capacidades de IA Soberana.

1.2

Criação de catálogo unificado de serviços de nuvem que permita a consulta das ofertas de nuvem disponíveis para a AP.

# I. Infraestrutura Digital Soberana

Objetivo | **Estabelecer uma base tecnológica comum, segura e escalável para processos e dados do Estado**

Início

## Plano de Adoção da Nuvem Soberana

S2 2026

Revisão do Framework de Adoção na Nuvem, enquanto componente do MOSAICO, incorporando os princípios do PNNS.

1.3

Definição de orientações práticas para apoiar as entidades da Administração Pública na tomada de decisão sobre migração, modernização ou manutenção de sistemas.

Elaboração de Planos de Adoção Setoriais para cada área governativa, estabelecendo projetos, atividades, responsabilidades, calendarização e metas para a adoção da arquitetura tecnológica de soberania definida no PNNS.

Execução e acompanhamento dos Planos de Adoção Setoriais.

## Definição de um Acordo-Quadro para serviços de nuvem

S1 2027

Análise comparativa aos modelos de contratação pública para serviços de nuvem adotados a nível internacional.

1.4

Definição de princípios, diretrizes e modelos de aquisição comuns para serviços de nuvem aplicáveis a todas as entidades da Administração Pública.

Definição de cláusulas-tipo, requisitos de segurança, níveis de serviço exigidos (SLAs) e guias operacionais.

## II. Capacitação de recursos humanos

Objetivo | **Capacitar técnicos e dirigentes para operar e governar a nuvem soberana.**

Início

### Matriz de Competências para a Nuvem Soberana

S2 2026

2.1

Identificação dos perfis técnicos e funcionais necessários para a implementação, operação e manutenção da Nuvem Soberana na Administração Pública.

Construção de uma matriz para cada perfil, que identifique as competências técnicas e funcionais necessárias à sua função, nível de proficiência exigido, bem como formações e certificações recomendadas.

### Plano de Capacitação em Soberania Digital

S2 2026

2.2

Definição de um programa de formação em Soberania Digital para a Administração Pública, dirigido aos perfis técnicos e funcionais mapeados na iniciativa I.1.

Formação de, pelo menos, 10% dos especialistas de informática da Administração Pública em Soberania Digital até 2028.

Formação de, pelo menos, 1000 dirigentes e gestores de projeto da Administração Pública em Soberania Digital até 2030.

Definição de um plano de iniciativas de partilha de conhecimento, incluindo sessões regulares de capacitação e troca de experiências entre entidades públicas que utilizem a Nuvem Soberana.

## III. Alterações Legislativas

Objetivo | **Definir regras, modelos de contratação e financiamento que viabilizam a adoção preferencial de nuvem.**

Início

### **Simplificação e revisão do Processo de Aquisição de Serviços Nuvem**

S1 2026

3.1

Eliminação de barreiras burocráticas associadas à aquisição de serviços Nuvem, promovendo a agilidade na contratação e a abertura do mercado a fornecedores mais diversificados e a soluções de nuvem, com impacto positivo na qualidade e eficiência dos serviços prestados.

Análise da possibilidade de reenquadramento orçamental das compras de serviços de nuvem.

### **Elegibilidade financeira dos serviços de computação em nuvem**

S2 2026

3.2

Estabelecimento de condições e critérios claros para garantir que serviços de computação em nuvem possam ser elegíveis para linhas de financiamento nacionais e europeias.

Análise de implicações em matéria de tratamento contabilístico dos serviços de computação em nuvem, permitindo a sua classificação como investimentos produtivos, quando associados à transformação tecnológica e à criação de valor público.



**REPÚBLICA  
PORTUGUESA**