National Plan for Sovereign Cloud (PNNS)

A Modern, Sovereign and Efficient Infrastructure

May 2026

REPÚBLICA PORTUGUESA

XXV GOVERNO CONSTITUCIONAL

Portuguese Republic – 25th Constitutional Government

Executive Summary

The transformation and technological reform of the State are central priorities to the Program of the XXV Constitutional Government, which sets as an objective positioning **Portugal among the most digitally advanced countries in Europe**, driving a more efficient, resilient State, prepared for the challenges of the digital era.

The **growing relevance of digital infrastructures and data to the economy and public institutions**, together with the increasing risks associated with extreme weather events, cybercrime, and electronic warfare, reinforces digital sovereignty and resilience as a national and European strategic priority. Defining sovereignty as the **control over access to data and the continuous assurance of the operation of critical systems and infrastructures**, it constitutes an essential condition for the continuity of public services, information security, and the State's decision-making autonomy. In this context, Portugal must strengthen its role in the provision of **sovereign cloud computing and Artificial Intelligence services**.

The **National Plan for Sovereign Cloud (*Plano Nacional de Nuvem Soberana*, PNNS)**, part of the **2026–2027 Action Plan of the Portugal Digital Strategy (*Estratégia Digital Nacional*, EDN)** under action 13.1, directly addresses this challenge by defining a **strategic vision** and lines of action for the coordinated, cross-governmental, and secure adoption of cloud computing services within Public Administration. Built upon a **sovereign, modern, secure, and resilient technological foundation**, the PNNS promotes a cloud-first strategy tailored to different levels of sovereignty depending on the processes, data, and systems involved, while simultaneously enhancing operational efficiency and the quality of public services.

At the same time, the PNNS adapts the European Commission's Cloud Sovereignty Framework to the Portuguese context, in articulation with the existing legislative framework. It is structured around **three pillars of action** aimed at ensuring the adoption of flexible, secure, coordinated, and sustainable cloud computing solutions, aligned with the different levels of sovereignty required across the various domains of Public Administration. Through this plan, the Government positions Portugal at the forefront of **European digital sovereignty**, strengthens the protection of the **State's strategic information**, and ensures the continuity of public services through a digital infrastructure suited to the challenges of technological transformation, contributing to a more dynamic, innovative, and competitive digital economy.

The Need

The importance of the **PNNS** stems from an ongoing structural shift in which, increasingly, the **functioning of the economy, public services, and the State's own sovereignty relies on digital infrastructures and data** that are often not under the country's direct control. The growing dependence on non-European service providers, combined with new regulatory obligations and accelerating technological change, has **direct implications for risk exposure** and for the maintenance of a fragmented model based on thousands of dispersed data centers and legacy systems that are difficult to protect and modernize.

At the same time, **the external environment is becoming increasingly volatile and demanding**. Geopolitical tensions, the rise in cyberattacks, electronic warfare, and the growing frequency of extreme weather events expose vulnerabilities in critical infrastructures and may jeopardize the continuity of essential public services. Without a clear sovereign cloud strategy, the State risks losing decision-making capacity regarding where its data is stored, who can access it, and how it is protected, **with direct consequences for security, citizens' trust, and institutional stability**.

This plan is therefore necessary to provide coherence, scale, and direction to the digital transformation of Public Administration. By establishing a **common model for the qualification of processes and data, clear sovereignty and security requirements, and a structured offering of sovereign cloud infrastructures**, the State gains the capacity to **modernize systems, reduce structural costs, and improve service quality**, without relinquishing control over its most critical assets. In this way, the National Plan for Sovereign Cloud plays an essential role in ensuring that the digitalization of the State is carried out in a manner that strengthens the **country's sovereignty, resilience, and competitiveness**.

Effects on Public Administration

The adoption of a Sovereign Cloud within Public Administration aims to establish a modern, shared, and secure digital infrastructure **capable of supporting State reform and the continuous development of digital public services**. Instead of each public entity maintaining its own "mini data center" with highly uneven levels of maturity, security, and efficiency, the Sovereign Cloud proposes a **shared platform** with clear sovereignty requirements, where critical Public Administration systems operate in more resilient, auditable, and AI-ready environments. This approach helps reduce technological fragmentation, accelerate the modernization of legacy systems, and ensure that the most sensitive data remains under the effective control of the State, even when advanced cloud computing services are used.

Overall, the objectives and effects of the Sovereign Cloud within Public Administration converge around three main dimensions: **strengthening control and security over critical digital assets, increasing the structural efficiency of the State apparatus, and creating a technological foundation** capable of supporting innovation and the growth of the Portuguese digital economy.

	Current Model	Future Model
Reduction of Sovereignty Risks	Increased exposure to **security, service continuity and** technological resilience **risks**	Reinforcement of **sovereignty, security and compliance of critical data and systems**, aligned with European requirements
Infrastructure Consolidation	Approximately **4,000 data centers** and technical rooms dispersed across **1,500 public entities**	**Progressive consolidation** of the State's digital **infrastructure**, with efficiency gains
Lifecycle Optimization	**Fragmented infrastructure model**, low utilization and capacity, and lack of scale	**Cloud "*as-a-service*" model**, with costs adjusted to actual usage and greater **operational flexibility**
Energy Efficiency	**Significant levels of energy and operational inefficiency**, with direct impact on public expenditure	Significant improvement in **energy efficiency**, with potential reductions of up to **46% in consumption**
Economies of Scale	**Decentralized procurement of cloud services**, limiting economies of scale and strategic alignment	**Economies of scale in procurement**, strengthening the State's bargaining power and reducing unit costs
Cost Reduction	High public ICT expenditure, with a strong weight of Data Center operational costs **(~69M€/year)**	**Reduction of up to 25% in ICT costs** and 35% in infrastructure costs – **~28M€/year** in direct savings

Implementation

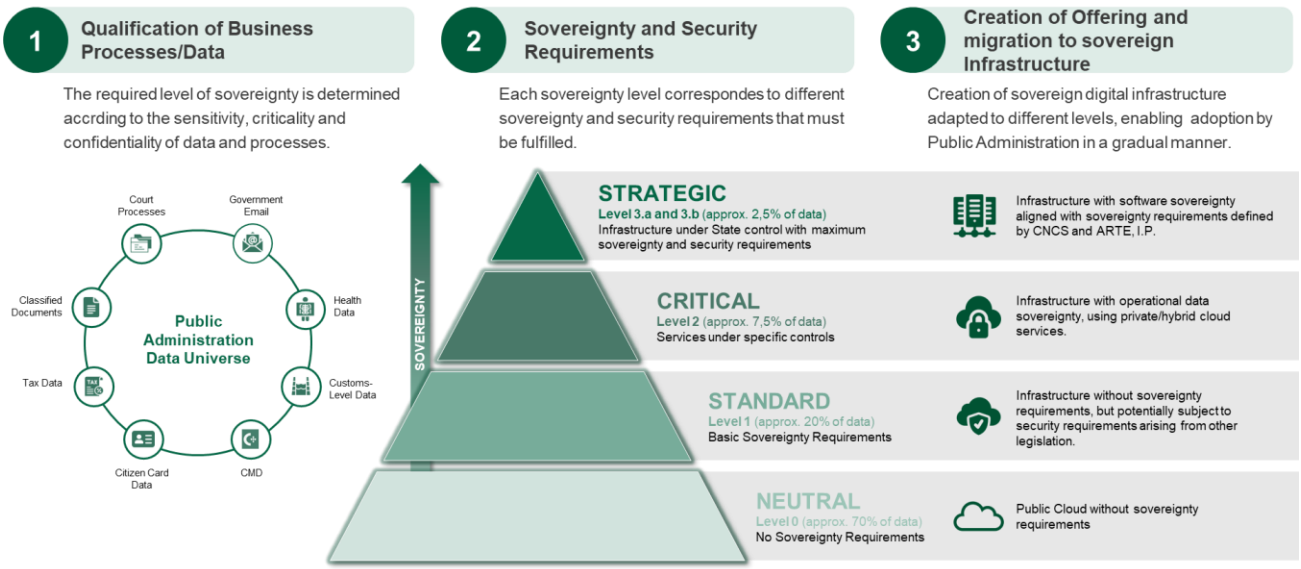
The implementation of the PNNS is structured around three sequential stages: first, the **qualification of business processes** and their corresponding data and systems; second, the **definition of sovereignty and security requirements** applicable to each qualification level; and third, the creation of a **sovereign infrastructure offering** capable of adequately meeting those requirements.

In the first stage, Public Administration undertakes the systematic **identification and analysis of its business processes**, as well as the data and information systems that support them, assessing the impact of potential failures from the perspective of citizens, State stability, and data exposure. To operationalize this analysis, the National Cybersecurity Centre (CNCS) and the State Technological Reform Agency (ARTE, I.P.) define progressive qualification levels for processes, aligned with Directive (EU) 2022/2555 (NIS2 Directive), the work developed within the European Cybersecurity Certification Scheme (EUCS), and the standardization initiatives led by CEN and CENELEC. **Four qualification levels** are identified - neutral, standard, critical, and strategic - reflecting, in differentiated ways, the **potential impact arising from the compromise of each process**. This qualification therefore results from a structured scoring methodology that enables Public Administration entities to classify their processes in a harmonized and comparable manner.

The second stage consists of associating each qualification level with a set of **objective sovereignty, security, and resilience requirements**. Based on the framework defined by CNCS and ARTE, I.P., clear parameters are established for each level regarding data localization and control, minimum technical and organizational controls, audit and certification mechanisms, as well as the levels of redundancy and service continuity to be ensured. This requirements framework, structured progressively according to the four qualification levels, guarantees **consistency and rigor** in the application of sovereignty and security rules across the entire Public Administration.

Implementation

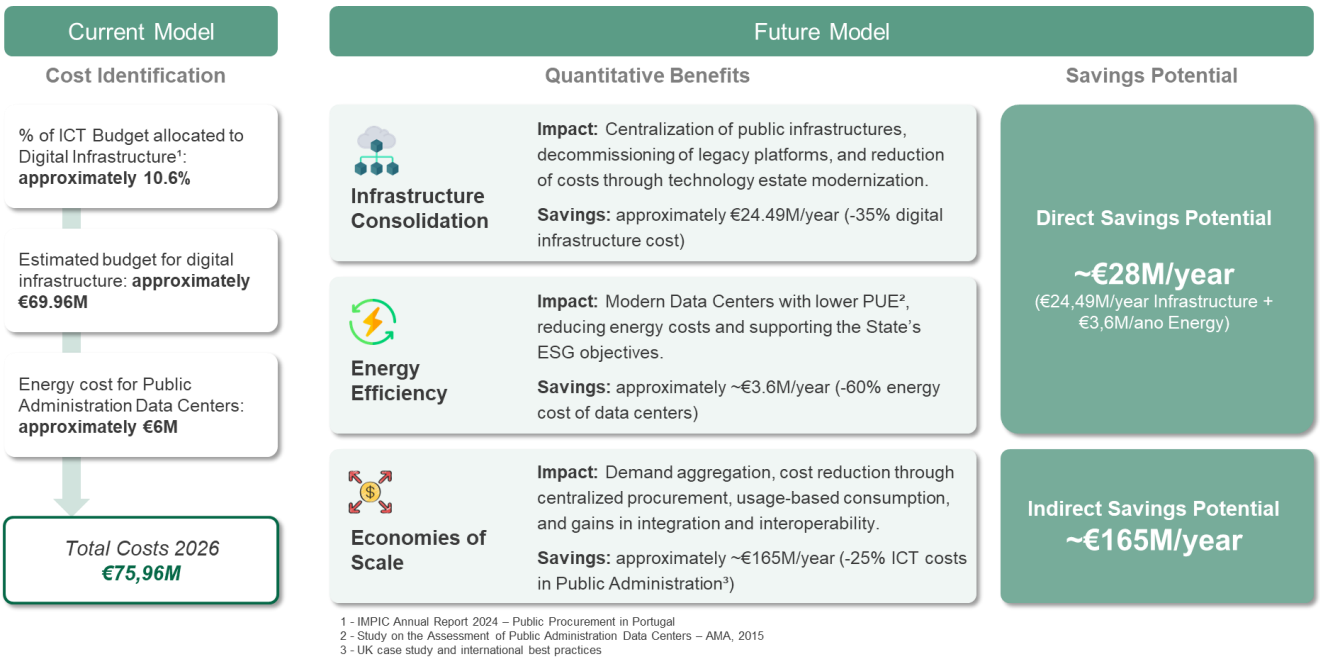
Subsequently, the third stage focuses on compiling a **sovereign digital infrastructure offering and creating the conditions for the market to operate effectively**, establishing **a coherent portfolio of technological solutions** capable of addressing the **different levels of requirements** identified, while ensuring that both the internal offering of Public Administration and the market offering comply with sovereignty and security requirements. This includes shared public infrastructures for the highest levels of sovereignty, private or hybrid cloud solutions for critical processes, and the regulated use of public cloud services for processes with lower requirements. This stage also encompasses the definition of service catalogues, financing models, procurement instruments, and a phased adoption plan prioritizing the most sensitive domains.



Overall, the three stages ensure that the **PNNS is translated into a clear operational pathway**, **from diagnosis to implementation**, guaranteeing that the technological modernization of Public Administration is carried out in accordance with the State's sovereignty, security, and resilience objectives.

Benefits

The implementation of the PNNS is expected to deliver highly relevant benefits for the State, not only in financial terms, but also strategic and qualitative. From an economic standpoint, the plan points to a **significant reduction in structural and operational costs**, through the **consolidation of infrastructure**, the **improvement in energy efficiency** and **economies of scale in contracting cloud services**.



In qualitative terms, the **PNNS strengthens the digital sovereignty and resilience of the Public Administration**, **increasing control over data, critical systems, and strategic infrastructures**. This translates into **lower exposure to regulatory and geopolitical risks**, greater auditing and governance capacity, and better conditions to ensure service continuity, security, and compliance. In addition, it creates a more solid technological foundation to accelerate innovation, including the use of sovereign artificial intelligence, and to increase the country's technological autonomy.

Action Plan

Lines of Action

The PNNS consists in an action plan organized around **three major lines of action**, which structure the transformation in a phased and coherent manner across the entire Public Administration. In this way, it seeks to articulate the modernization of infrastructures, the development of internal capabilities, and the adaptation of the regulatory and financial framework, ensuring **alignment between the technological, organizational, and regulatory dimensions**. This three-axis architecture allows implementation to be progressive, but guided by a **shared vision**, reducing risks of fragmentation, duplication of investments, and contradictory approaches.

Each line of action responds to a distinct type of challenge associated with digital sovereignty: on the one hand, the need to have **robust and secure technological foundations**; on the other, the requirement to **build the capabilities of people and institutions** to operate in this new context; and, finally, the **obligation to adapt rules, procedures, and public management instruments** to a model in which cloud becomes the preferred option. The action plan thus defines a set of initiatives grouped in these three domains, with clear responsibilities, time-bound targets, and common guidance, enabling coordination of efforts among ministries, central bodies, and sectoral entities.

I. Sovereign Digital Infrastructure

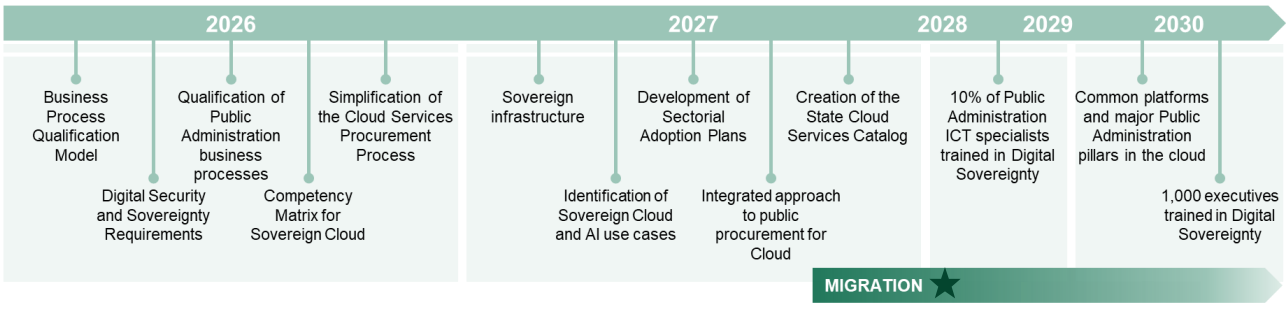
- ★ **I.1** Business Process Qualification Model
- ★ **I.2** Development of the Sovereign Cloud Offering, including AI [aligned with ANIA]
- ★ **I.3** Sovereign Cloud Adoption Plan
- **I.4** Definition of a Framework Agreement for cloud services

II. People

- **II.1** Competency Matrix for Sovereign Cloud
- **II.2** Digital Sovereignty Training Plan

III. Legal Framework

- **III.1** Simplification and revision of the Cloud Services Procurement Process
- **III.2** Financial eligibility of cloud computing services



★ Caption: **Strategic Initiatives**

I. Sovereign Digital Infrastructure

Objective | **Establish a common, secure, and scalable technology base for State processes and data**

Start

1.1

Business Process Qualification Model

S1 2026

Definition of a uniform business process qualification model for the Public Administration, applicable to the associated data and information systems.

This model includes process categories, the necessary regulatory framework, sovereignty, security, and resilience requirements by qualification level, and technical specifications associated with sovereignty requirements.

Surveying and inventorying the Public Administration's processes and technological infrastructures, namely through the identification and cataloging of technological dependencies, vulnerabilities, and risks.

Application of the Business Process Qualification Model to the inventoried data and systems.

1.2

Development of the Sovereign Cloud offering, including AI

S1 2026

Development, by the State, of national sovereign cloud infrastructure, including Sovereign AI capabilities.

Creation of a unified cloud Services catalog that enables consultation of the cloud offerings available to the Public Administration.

I. Sovereign Digital Infrastructure

Objective | **Establish a common, secure, and scalable technology base for State processes and data**

Start

1.3

Sovereign Cloud Adoption Plan

S2 2026

Review of the Cloud Adoption Framework, as a component of MOSAICO – digital public services design model, incorporating the principles of PNNS.

Definition of practical guidance to support AP entities in decision-making on migration, modernization, or maintenance of systems.

Development of sectoral Adoption Plans for each government area, defining projects, activities, responsibilities, timelines, and targets for adopting the sovereign technology architecture defined in PNNS.

Implementation and monitoring of the Sectoral Adoption Plans.

1.4

Definition of a Framework Agreement for cloud services

S1 2027

Comparative analysis of public procurement models for cloud services adopted internationally.

Definition of common principles, guidelines and procurement models for cloud services applicable to all Public Administration entities.

Definition of model clauses, security requirements, required service levels (SLAs), and operational guides.

II. Human resources capacity building

Objective | **Train technical staff and leaders to operate and govern the sovereign cloud.**

Start

2.1

Competency Matrix for the Sovereign Cloud — **S2 2026**

Identification of the technical and functional profiles needed for the implementation, operation, and maintenance of the Sovereign Cloud in Public Administration.

Development of a matrix for each profile, identifying the technical and functional competencies required for its role, the required proficiency level, as well as recommended training and certifications.

2.2

Training Plan for the Sovereign Cloud — **S2 2026**

Definition of a training program on Digital Sovereignty for Public Administration, targeted at the technical and functional profiles mapped in initiative I.1.

Training of at least 10% of public sector IT specialists in Digital Sovereignty by 2028.

Training of at least 1000 Public sector leaders and project managers in Digital Sovereignty by 2030.

Definition of a plan of knowledge-sharing initiatives, including regular training sessions and experience-sharing among public entities that use the Sovereign Cloud.

III. Legal Framework

Objective | **Define rules, contracting and financing models that enable the preferential adoption of cloud.**

Start

3.1

S1 2026

Simplification and Review of the Process for Procuring Cloud Services

Elimination of bureaucratic barriers associated with procuring cloud services, promoting agility in contracting and opening the market to a more diverse number of suppliers and cloud solutions, with a positive impact on the quality and efficiency of the services provided.

Analysis of the possibility of a budget reclassification of purchases of cloud services.

3.2

S2 2026

Financial Eligibility of Cloud Computing Services

Establishment of clear conditions and criteria to ensure that cloud computing services can be eligible for national and European financing lines.

Analysis of implications regarding the accounting treatment of cloud computing services, allowing their classification as productive investments, when associated with technological transformation and the creation of public value.

REPÚBLICA
PORTUGUESA