España | digital 2026

Hybrid cloud services strategy for Public Administrations

PLAN FOR THE DIGITALISATION OF PUBLIC ADMINISTRATIONS 2021-2025

Digital transformation of the General State Administration

Cloud Infrastructure Service

December 2022

Funded by the European Union
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
SECRETARÍA GENERAL DE ADMINISTRACIÓN DIGITAL

España | digital 2026

Ministry of Economic Affairs and Digital Transformation
Madrid, December 2022
NIPO: 094-23-077-9

Funded by
the European Union
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
SECRETARÍA GENERAL DE ADMINISTRACIÓN DIGITAL

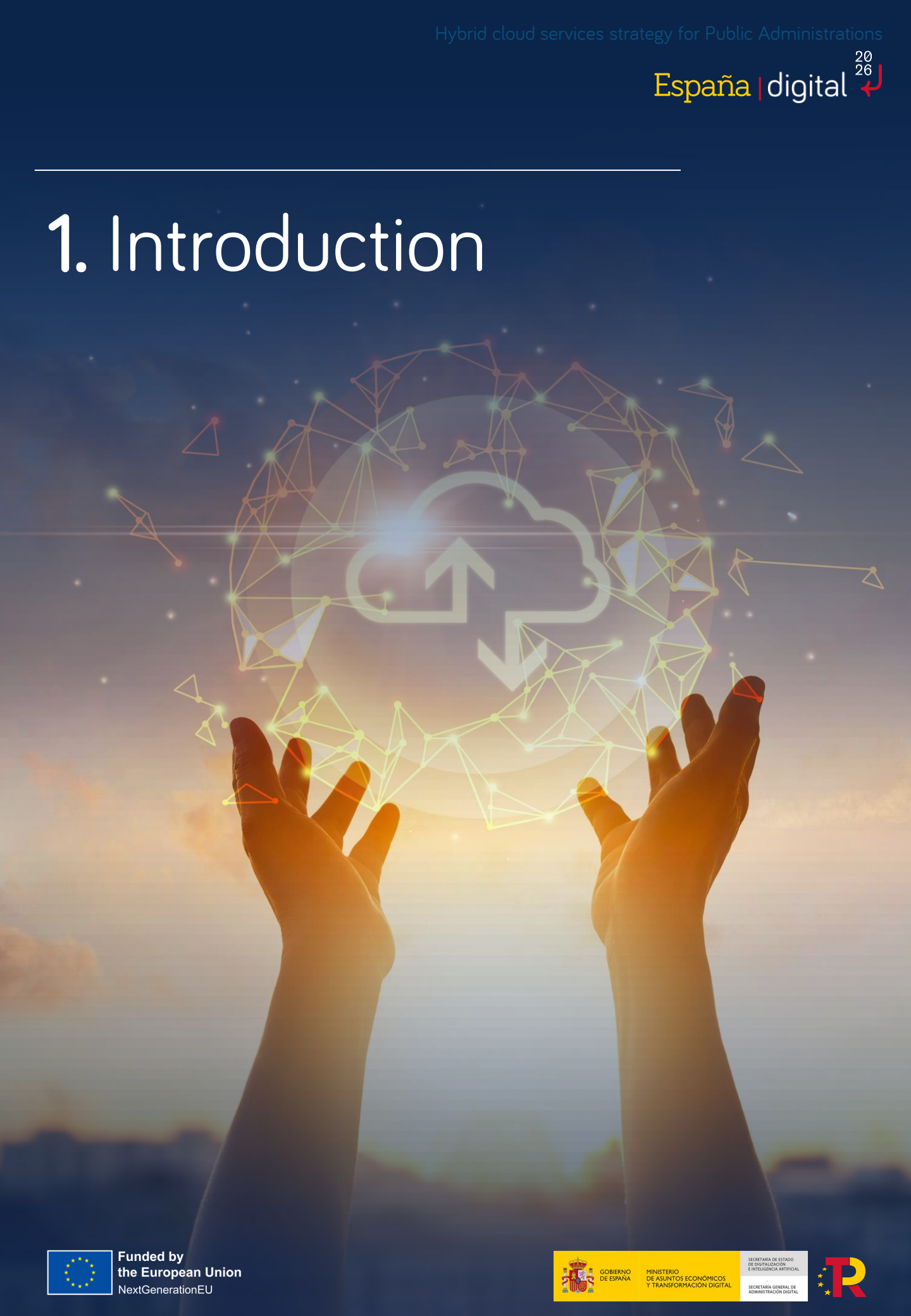
España | digital 2026

CONTENTS

Funded by the European Union NextGenerationEU

España | digital 2026

1. Introduction



Funded by the European Union
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
SECRETARÍA GENERAL DE ADMINISTRACIÓN DIGITAL

The Hybrid Cloud Strategy for Public Administrations aims to provide strategic direction for the implementation and control of cloud solutions by Public Administrations.

The digital transformation of Public Administrations requires a new paradigm in the provision of public services that includes greater flexibility, agility and adaptability demanded by society. It also means being able to **undertake innovations driven by the value of data artificial intelligence and the Internet of Things** and new **5G/6G** networks as highlighted in the declaration "*Towards a new generation Cloud for Europe*" of the 27 EU Member States of 15 October 2020.

Cloud services are based on **automated, on-demand availability** of a computer system's resources, **without direct involvement of the provider**. These cloud services are offered through catalogues which include **service level agreements and associated costs** for each service.

This model is based on technological infrastructures that are dynamically sized, characterised by the virtualisation of resources, a high degree of automation and multi-entity operating capacities, guaranteeing isolation and security in access to the data of the different entities. The wide range of possibilities offered by the cloud services paradigm, together with the different architectures and delivery models, requires a **strategy to ensure the necessary autonomy, security and control of the data and services** provided, as well as **facilitating the implementation of innovations** in the provision of public services.

Indeed, the use of cloud services allows Public Administrations to provide digital services and to have **secure, efficient and reliable technological infrastructures**, while requiring special attention to safeguard guarantees **for the country's strategic autonomy, security and control over data**.

To this end, a number of challenges need to be addressed, including the need for **technological autonomy** to avoid risks arising from unilateral decisions by providers or from the legal framework that may apply to them.

The Strategy, structured in **7 pillars and 19 initiatives**, is part of the **Digitalisation Plan for Public Administrations 2021-2025** specifically under the umbrella of measure 7, linked to the Cloud Infrastructure Service and measure 9, linked to the Cybersecurity Operations Centre.

The **investments** will amount to a total of **854 million euros** earmarked for the **State Administration and the Territorial Administrations** and will be financed by the Recovery, Transformation and Resilience Plan.

Funded by the European Union
NextGenerationEU

España | digital 2026

This paper discusses the **potential of cloud services** for Public Administrations, the **challenges** of adopting such services, the **aims** and the **pillars** of the strategy.

The 7 pillars underpinning the strategy are developed through **19 initiatives**:

Hybrid cloud by design	i1 Extend existing private cloud solutions i2 Promote connectivity and interoperability with different cloud providers
Growing catalogue of services	i3 Create the NubeSARA "shop" i4 Broker the supply of private sector service mode solutions i5 Regularly expand the catalogue of services
Hybrid first service provision policy	i6 Prioritise the use of hybrid cloud services i7 Develop new procurement tools for cloud services
Data sovereignty	i8 Develop a guide for risk analysis in cloud service environments according to the ENS i9 Establish criteria for centralised procurement

Funded by the European Union
NextGenerationEU

Data orientation

- **i10** Integrate the General State Administration's data platform with NubeSARA
- **i11** Provide additional analytical tools

Evolution of systems towards the hybrid cloud

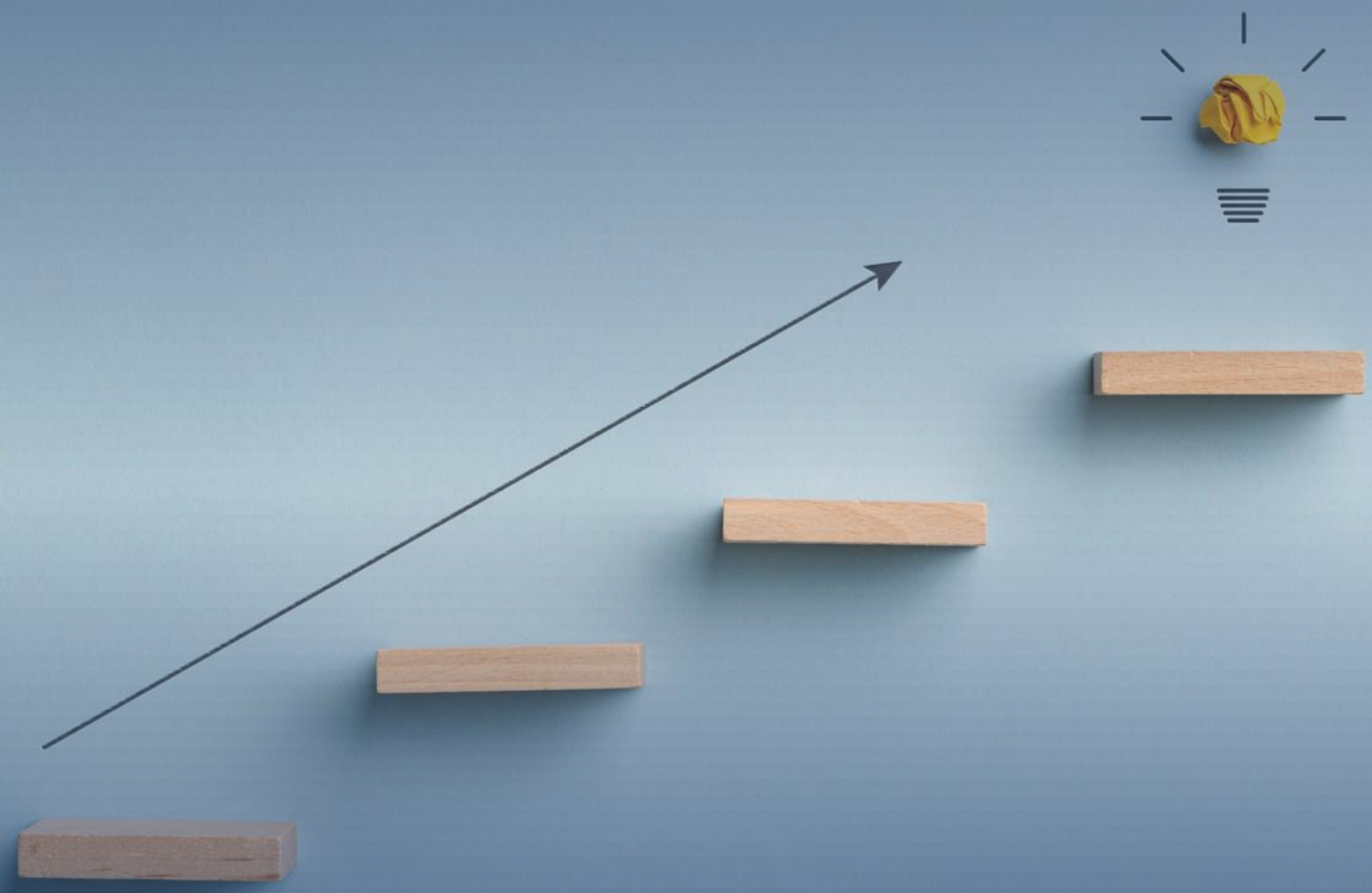
- **i12** Drive the transformation of individual sites to hybrid cloud solutions
- **i13** Consolidate and strengthen the Administration's private cloud services

Secure cloud

- **i14** Establish criteria for load sharing in the cloud
- **i15** Certification of the National Security Scheme compliance of cloud infrastructures
- **i16** Promote cyber-security capabilities in public administrations
- **i17** Promote the extension and evolution of the Cybersecurity Operations Centre of the General State Administration and its Public Bodies
- **i18** Promote the National Network of Cybersecurity Operations Centres, as well as the National Platform for Notification and Monitoring of Cyberincidents
- **i19** Elaborate CCN-STIC Guidelines in the development of the ENS on measures according to the cloud service model

España | digital 2026

2. The potential of cloud services for Public Administrations



Funded by the European Union
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
SECRETARÍA GENERAL DE ADMINISTRACIÓN DIGITAL

Cloud services have provided Spanish Public Administrations with tools to provide homogeneous and equal quality services, regardless of the size of the organisation, its resources or its location.

Positioning in the social and economic development index

The application of the cloud services model to digital administration services has contributed to Spain's outstanding position in indicators such as the Digital Economy and Society Index, DESI.

Digital Administration services that have followed this cloud-oriented model include, by way of illustration, cases such as the registration solution (ORVE/GEISER/SIR), the Data Intermediation Platform (PID), the Identification services (CL@VE) and, notably, electronic invoicing, one of whose **key success factors** was the deployment of **a cloud-based solution for all public administrations**.

The potential of this type of solution facilitates the **strengthening territorial cohesion** insofar as it allows organisations with fewer resources, such as Local Authorities, to achieve an adequate level of digitalisation. This is achieved through the deployment of cloud-based tools such as those mentioned above.

On the other hand, the **regulatory framework in Spain** provides for a **fully electronic operation** which promotes the digital transformation of public administrations, as well as the deployment of first class digital services. The focus on cloud services has facilitated the implementation of this ambitious regulation with a generalised scope, allowing the complexity of a highly decentralised country to be circumvented.

In addition, the possibility has been developed for private providers to offer eGovernment solutions as a service, complementing the services provided by the State Administration.

All these services are interoperable thanks to the fact that Spain has a highly developed regulatory framework in this field, with the regulation of the **National Interoperability Scheme**.

The provision of cloud services is not something new for the Spanish Administration, so the use of these services allows Public Administrations to use them to:

- Encourage the **reuse of applications**,
- **Reduce** infrastructure **costs**,
- **Increase the redundancy and resilience** of public services,
- **Reduce the carbon footprint** by increasing **energy efficiency and environmental sustainability**.

This reduction will depend on the specific technological solution as well as other aspects of the infrastructure and common support such as power supply, but in any case it can be a significant improvement on the previous circumstances.

Along these lines, the present strategy aims to **extend the cloud services modality**, in order to universalise it and use it as a lever to enable a **qualitative leap to be made in the digital transformation of the different Public Administrations**.

Since 2015, it has also strengthened its catalogue of services for **Infrastructure as a Service** (IaaS) and **Platform as a Service** (PaaS) as a tool to reduce the number of State Administration Data Processing Centres, optimising the use of available resources and the quality of service provision.

As a result, a significant percentage of the State Administration's data processing resources currently run on a **private cloud solution called NubeSARA**.

In particular, the General Secretariat for Digital Administration deployed nubeSARA in 2015, which currently partially hosts the computing infrastructure of 22 Agencies and Entities linked to or dependent on 11 different Ministries.

This solution has a **Service Catalogue** with known cost and associated service level agreements. The most important activities in the provision of these services have been automated, obtaining significant benefits in their operation compared to traditional information and communications technology infrastructures.

In a next step, this Service Catalogue **will become the Solutions, Services and Applications Store** (as a Marketplace) **for the different Public Administrations,** with the aim of increasing both the number of Public Bodies and Entities of Public Law that use it and the integration of external suppliers in the portfolio of available products. This aim will be achieved after a process of incorporation of both services and user organisations.

The State Administration's own private cloud (NubeSARA) currently hosts the infrastructure of 22 Public Law Bodies and Entities linked to or dependent on 11 Ministries

España | digital 2026

3. Challenges related to cloud services

Funded by the European Union
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
SECRETARÍA GENERAL DE ADMINISTRACIÓN DIGITAL

Technological autonomy

In relation to cloud services, it is of particular importance to retain the ability to be able to **govern and manage the infrastructure** that supports them and, consequently, the storage and processing of data.

However, it is a fact that European companies' market shares in cloud services represent a very small value (less than 10%) compared to those held by companies outside the European Union. This imbalance in market share is not only limited to digital services and platforms but also to the infrastructures that enable them to function.

Thus, the mass adoption of technology for cloud services by public administrations would be subject to risks such as unilateral changes in service conditions, cost increases, service interruption or data location.

Consequently, having **technological autonomy** in particular with capacities in Spain, has implications, not only in terms of the possibility of having **control over data and services,** but also in terms of **promoting an ecosystem of technologies necessary for digital transformation** (Cloud Services, Artificial Intelligence, Internet of Things, Quantum Computing, Data Spaces, etc.).

Having technological autonomy with capacities in Spain will enable the promotion of the ecosystem of technologies necessary for the digital transformation of public administrations

Data sovereignty

In relation to data sovereignty, it should be borne in mind that it is of interest both **where the data is located**, as well as from **where the infrastructures and services that provide and manage it are managed**. Although the Data Processing Centres that support cloud services are located on Spanish or European Union soil, in some cases they are operated from outside this space by companies subject to other jurisdictions.

This could allow, under certain circumstances **unilateral requests or accesses originating from outside the European Union** to the cloud service provider to provide access to data, which could be of a strategic and/or sensitive nature for the institutions and citizens requests that could eventually be outside the knowledge, control and decision-making capacity of national decision-makers.

This challenge was highlighted in the **Berlin Declaration on the Digital Society and Value-based eGovernment**, signed in December 2020, which identifies issues such as the need to step up efforts to ensure that **data stored by Member States' public administrations to be immune from unwanted interference**s well as the need to **encourage Member States' own key digital capabilities** to develop and deploy digital solutions in secure cloud infrastructures for public services.


Berlin Declaration
on
Digital Society and
Value-Based Digital Government

at the ministerial meeting during the
German Presidency of the Council of the European Union
on 8 December 2020

Redundancy and resilience

Resilience is a fundamental characteristic that critical systems and infrastructures must possess. Cloud infrastructures and services supporting Public Administration applications must adopt adequate **security and redundancy measures**.

The implementation of **security controls according to the requirements of the processed data**, as well as the continuity of service and **disaster recovery measures** should improve resilience in the face of cyber-attacks and other incidents.

Interoperability

Given the importance of the data and services involved, the cloud migration strategy requires taking into account, when selecting providers and technologies, the necessary **competition and future interoperability and portability**, avoiding technologies that generate captivity, so that the **resources** that have been migrated to the cloud are **reversible and can be located in different external providers**, or in the Administration's private cloud, without the need for costly transformation projects, both in time and investment resulting from possible changes of provider.

Data protection

As the **Spanish Data Protection Agency in its "Guide for cloud computing service providers"** states, *"it should not be forgotten that cloud computing services have specific implications for the protection of personal data for which the client contracting the services is responsible. These implications call for an assessment of how best to incorporate the* ***safeguards provided for in data protection regulations, modulating them to adapt*** *them to the specific characteristics of the data".*

Moreover, as set out in the "**Guide for clients** contracting cloud computing services" of the Spanish Data Protection Agency, *"the possibility of processing data outside the national territory, a characteristic of cloud computing, is a particularly relevant element for Public Administrations. In this respect, it should be borne in mind that the* ***regulations*** *for international data movements is* ***applicable both to public and private entities****".*

It should be recalled here that the main implementing regulations are the **General Data Protection Regulation and Organic Law 3/2018, of 5 December, on Data Protection and the Guarantee of Digital Rights**.

The rules governing international data movements apply to both public and private entities

Cybersecurity

Cybersecurity has become a strategic priority, as evidence of increasing exposure to the materialisation of cyberspace threats and cyber-attacks has become evident. There has been a notable increase in these cyber-attacks, both in volume and frequency, as well as in sophistication, with agents and actors with greater technical and operational capabilities; all of this in a context of high dependence on technologies.

An increasing number of public and private entities, their supply chains, citizens and businesses are exposed to these threats, as recognised in the 2019 National Cybersecurity Strategy.

In particular, the **adoption of the cloud services model** introduces new **risks that need to be controlled** in order to meet the requirements of current regulations, such as the National Security Scheme, by means of the corresponding **certification of conformity or application of the specific compliance profile**, or data protection or personal data protection, as well as the security requirements that in each case the organisations establish as necessary in their respective security policies.

The adoption of the cloud services model introduces new risks that need to be controlled, ensuring compliance with the appropriate security requirements in each case

4. Aims

Funded by the European Union
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
SECRETARÍA GENERAL DE ADMINISTRACIÓN DIGITAL

España | digital 2026

The overall aim of this strategy is to:

Prioritise the provision of services based on cloud technologies by Public Administrations,

using first and foremost own resources and complementing them with private sector solutions, achieving synergies that result in **better service delivery**, greater **technological autonomy** while guaranteeing the **security and protection of personal data** at all times.

Funded by the European Union
NextGenerationEU

And its specific aims are to:

Provide Public Administrations with the necessary technological infrastructures to further modernise them in order to ensure availability under any circumstances and to adapt the available capacity to the needs existent at any given time, contributing to the development of digital connectivity, data orientation and artificial intelligence in Administrations.

Consolidate the State Administration's Data Processing Centres into a smaller number of centres with better performance, reducing operating costs (economic and environmental) and maximising the agility of ICT (Information and Communications Technology) operations, adapting more quickly to the demands of society, without being a burden or obstacle to future technological evolution.

Enhance secure cloud service, promoting greater technological autonomy and ensuring data sovereignty requirements, with cybersecurity and data protection, so that the information systems that support them comply with the National Security Scheme and, in the case of cloud services provided by the private sector, are certified under a certification methodology recognised by the Certification Body of the National ICT Security Evaluation and Certification Scheme.

Promote the participation of the State Administration's cloud infrastructures in initiatives within the framework of the European Union, such as the EU Cloud Federation and Gaia-X ; and in particular, facilitate the adoption of the principles, architectures and components from the different European initiatives promoting the European principles of transparency, trust and sovereignty of cloud services

España | digital 2026

5. Hybrid cloud services strategy for Public Administrations

Funded by the European Union
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
SECRETARÍA GENERAL DE ADMINISTRACIÓN DIGITAL

The strategy is based on 7 pillars, which are developed through 19 initiatives:

PILLAR 1

Hybrid cloud by design

The aim is to have **hybrid cloud infrastructure consisting of the State Administration's own cloud**, located in its data processing centres, combined with those of other public administrations and external public cloud service providers.

The State Administration's cloud solution, called NubeSARA, is defined as hybrid, as it is made up of a **combination of several interconnected cloud typologies**. In its design, it includes four elements:

- **The private cloud or the State Administration's** own cloud, based on **two main data processing centres** located at an appropriate distance from each other, and an additional back-up centre. These centres provide cloud services and also hosting as a service in cases where they cannot be migrated to the cloud. This cloud concentrates inter-ministerial services that handle sensitive data or deploy critical government processes.
- **The clouds of other Spanish Public Administrations or of the European Union**.
- **The "outer" cloud of the State Administration** provided by public cloud service companies and consumed from a catalogue of services. The "outer" cloud will mainly host workloads relying on less sensitive data and will be a back-up solution to the proprietary cloud.
- **Edge Computing Capabilities** which, depending on the case, may be combined with the previous elements, analysing the possible advantages of combining them in the face of large volumes of data, depending on the entities and their type of applications/systems.

A fundamental aspect of a hybrid cloud solution is to establish an **adequate interoperability framework between providers**, so that they satisfy a number of conditions, such as compatibility or reversibility of loads. The design of a set of **reusable services or "building blocks"** will also be promoted to allow the aforementioned interoperability for the creation of cloud services.

To enable hybrid cloud by design, the following initiatives will be undertaken:

i1. **Extend existing private cloud solutions**

Additional capacity will be acquired, adding new functionalities to the service catalogue.

i2. **Promote connectivity and interoperability with different cloud providers**

A procedure will be established to make connections with private sector suppliers while maintaining the necessary safeguards.

PILLAR 2

Growing catalogue of services

The aim is to have a **growing catalogue of services with the incorporation of applications that respond to the common needs** of Public Administrations with Software as a Service (SaaS) solutions.

The aim is to continuously enrich this catalogue of services with higher value-added elements in all areas of cloud services, whether as infrastructure, platform or software as a service.

The catalogue will be easily accessible through the NubeSARA "shop", which will allow for easy deployment of services to Public Administrations and will initially draw on the solutions already available and currently provided as a service.

In addition, the incorporation into this catalogue of applications that respond to the common needs of the Administrations will be promoted.

To enable the growing catalogue, the following initiatives will be implemented:

i3. **Create the NubeSARA "shop"**
An interface will be deployed to provide user entities with a simple service consumption model.

i4. **Broker the supply of private sector service mode solutions**
A mechanism will be articulated for the inclusion of private sector service mode solutions that have undergone an approval process.

i5. **Regularly expand the catalogue of services**
In response to user demand, the catalogue will be periodically expanded with solutions that add value to administrations.

PILLAR 3

Hybrid cloud first cloud service provision policy:

The 'hybrid cloud first' principle aims to **prioritising the provision of cloud-based services over traditional solutions**, due to the former's potential to offer a large number of networked services in an agile and flexible manner, with high scalability and minimised deployment times.

To make this possible, the following initiatives will be carried out:

i6. Prioritise the use of cloud services

The use of cloud solutions will be prioritised over infrastructure investment by each of the administrations.

i7. Develop new procurement instruments for cloud services, seeking the simplification and efficiency of the process

The Directorate General for the Rationalisation and Centralisation of Procurement of the Ministry of Finance and Public Administration will be collaborated with in the creation of procurement tools complementary to this strategy.

PILLAR 4

Data sovereignty

The aim is to have **criteria** in relation to the **location and management of data** in a way that guarantees at all times **digital sovereignty, jurisdiction, security and data protection** in accordance with current regulations.

These criteria should address, in the context of European digital sovereignty, issues such as the following:

- That **sensitive government data should not be transferred** outside the outside the European Union.
- That the data handled by **systems** which are of **HIGH category according to the National Security Scheme** may only be handled by companies to which exclusive Community jurisdiction applies.
- That the **authorities of third countries cannot access the data** in an uncontrolled manner.
- That the **availability of infrastructure can be preserved** even in the event of possible geopolitical tensions.

To enable data sovereignty, the following initiatives will be implemented:

i8. Develop a guide for risk analysis in cloud service environments, including, among others, jurisdiction and data sovereignty, taking into account the requirements established by the National Security Scheme

The drafting of a guide will be collaborated on with the National Cryptologic Centre that covers the Spanish and European legal framework in these matters.

i9. Establishing criteria for centralised procurement of cloud services

The Directorate General for the Rationalisation and Centralisation of Procurement of the Ministry of Finance and Public Administration will be collaborated with to set procurement criteria for cloud services.

PILLAR 5

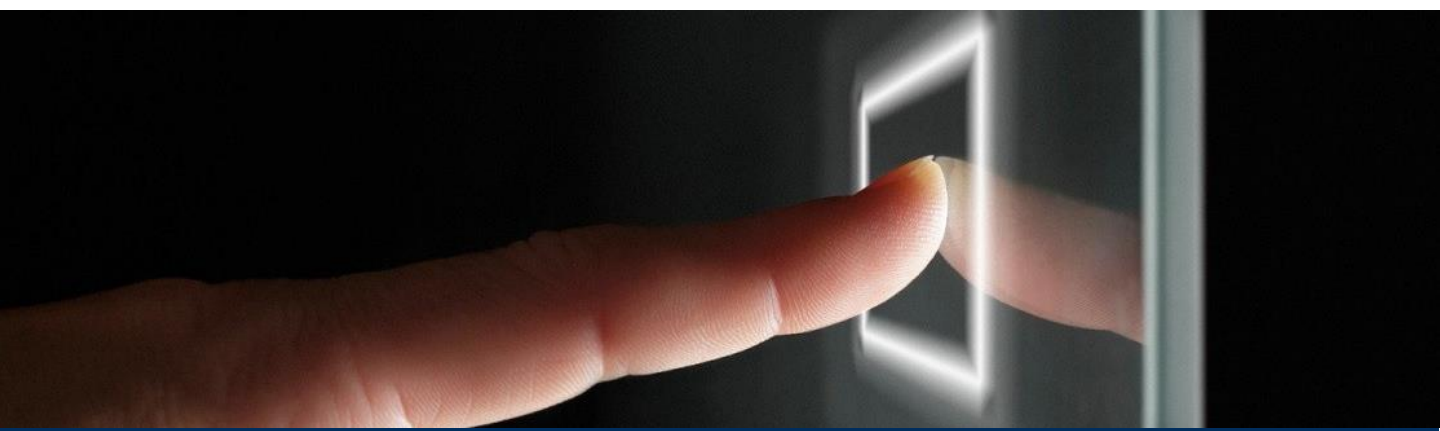
Data orientation

The aim is to focus the **infrastructures on the development of an information architecture that supports the transversal vision of data As-a-Service** and ensuring hyper-connectivity of services and data.

The aim is to **simplify the interoperability of data**, enabling their orderly transfer between silos for better use.

This development contributes to the **data economy** by providing infrastructure services for storing and processing data, a **sharing architecture** between the different actors and a **high-capacity, secure, reliable and resilient connectivity**. At the same time it seeks to simplify the deployment of tools for analytics and data science.

This approach will make it easier for Public Administrations to undertake data value-driven innovations without having to address the deployment of the necessary technological infrastructure themselves on an ad hoc basis.



The following initiatives will be implemented to enable data orientation:

i10. **Integrate the General State Administration's data platform with NubeSARA**

The data platform of the General State Administration will be integrated with NubeSARA.

i11. **Provide additional analytical tools as a service**

Additional analytics tools will be added to the NubeSARA service catalogue.

PILLAR 6 

Evolving existing systems to the cloud

The aim is to **transform existing systems into the cloud model, continuously enriching the service catalogue** with elements of higher added value.

The aim is to ensure the **coherent evolution of existing information systems towards state-of-the-art technologies** using cloud services using cloud services. To this end, as many of the elements already present in the NubeSARA "shop" will be reused as possible.

Special attention will be given to transformation initiatives for each service or application to be migrated, for which it is necessary to:

- Carry out **transformation projects** of the current services, applications and infrastructures of Public Administrations, **to enable their migration** to the cloud.
- Define and execute the **migration plan to NubeSARA**.
- **Consolidate all services** which cannot be migrated to NubeSARA, but need an alternative plan until these services reach their end of life.
- **Enhance Edge Computing capabilities** which, depending on the case, may be combined with the previous elements, analysing the advantages in the face of large volumes of data according to the entities and type of applications/systems.

To enable the evolution to the cloud, the following initiatives will be implemented:

i12. Promote the transformation of the different centres of the State Administration to hybrid cloud solutions

The processes of transformation of the centres of the General State Administration towards the adoption of solutions that include the use of the hybrid cloud will be promoted.

i13. Consolidate and strengthen the Administration's private cloud services

The services of the State Administration's infrastructures that are necessary to be able to carry out the consolidation processes will be strengthened.

PILLAR 7 |  Secure cloud

The aim is to secure cloud services with the **appropriate security measures according to the corresponding cloud service model**, as provided for in the National Security and in the specific compliance profiles, as well as in the applicable CCN-STIC guides.

The **National Security Scheme** includes the new measure "Protection of cloud services" which, in addition to the requirement of compliance with the Scheme, includes the reinforcement that when using cloud services provided by third parties, these must be certified under a methodology recognised by the Certification Body of the National Information Technology Security Evaluation and Certification Scheme, referring to cloud services provided by third parties having the future European EUCS - CLOUD SERVICES SCHEME certification.

The following initiatives will be undertaken to enable the secure cloud:

i14. Establish criteria for load sharing in the cloud

A hybridisation process will be defined that considers security in all its aspects, including a specific risk analysis for each supplier. Likewise, CCN-STIC guides will be used to establish the criteria for the location of charges, taking into account data sovereignty and data protection aspects.

---

i15. Certification of compliance with the National Security Scheme for cloud infrastructures

Certification of compliance with the National Security Scheme will be promoted for all cloud infrastructures that provide services to Public Administrations.

i16. Promote cyber-security capabilities in Public Administrations

The security of digital infrastructures, communications and services provided by public administrations will be promoted, as well as the improvement of their capacities to prevent, detect and respond to cybersecurity incidents. All of this aims to better protect the information processed and the digital services provided, in a context of increasingly intense exposure to the materialisation of threats from cyberspace, to cyber-incidents, which follow a pattern of growth in frequency, sophistication, scope and severity of impact.

---

i17. Promote the extension and evolution of the Cybersecurity Operations Centre of the General State Administration and its Public Bodies

The evolution of the maturity of the Cybersecurity Operations Centre services, the integration of NubeSARA and more entities in the scope of its services, as well as the expansion of services in light of the cybersecurity scenario will be promoted, along with the implementation of new capabilities for resilience, protection, auditing, security testing and code analysis, cybersecurity research, vulnerability disclosure, information sharing, and application of state-of-the-art Artificial Intelligence.

---

i18. Promote the National Network of Cybersecurity Operations Centres, as well as the National Platform for Notification and Monitoring of Cyberincidents

The National Network of Cybersecurity Operations Centres is an instrument for coordinating collaboration and information exchange between the Cybersecurity Operations Centres of the Spanish public sector. All national Cybersecurity Operations Centres of the Spanish public sector and those managed security service providers that offer services to this type of centres, which have requested to be part of the network, are part of this network. The National Platform for Notification and Monitoring of Cyber Incidents is launched by the CCN-CERT in collaboration with INCIBE-CERT and ESPDEF-CERT of the Joint Cyberspace Command to implement the incident notification and management procedure, which will be available all hours of the day and every day of the year.

i19. Draw up CCN-STIC guidelines for the development of the National Security Scheme, on the measures that systems providing a cloud service to public sector bodies must comply with, depending on the cloud service model they provide

Appropriate guidance will be developed for different types of cloud services, to ensure that their design, delivery and configuration are appropriate to the use made of them by different entities.

España | digital 2026

6. Budget

Funded by the European Union
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
SECRETARÍA GENERAL DE ADMINISTRACIÓN DIGITAL

Budget

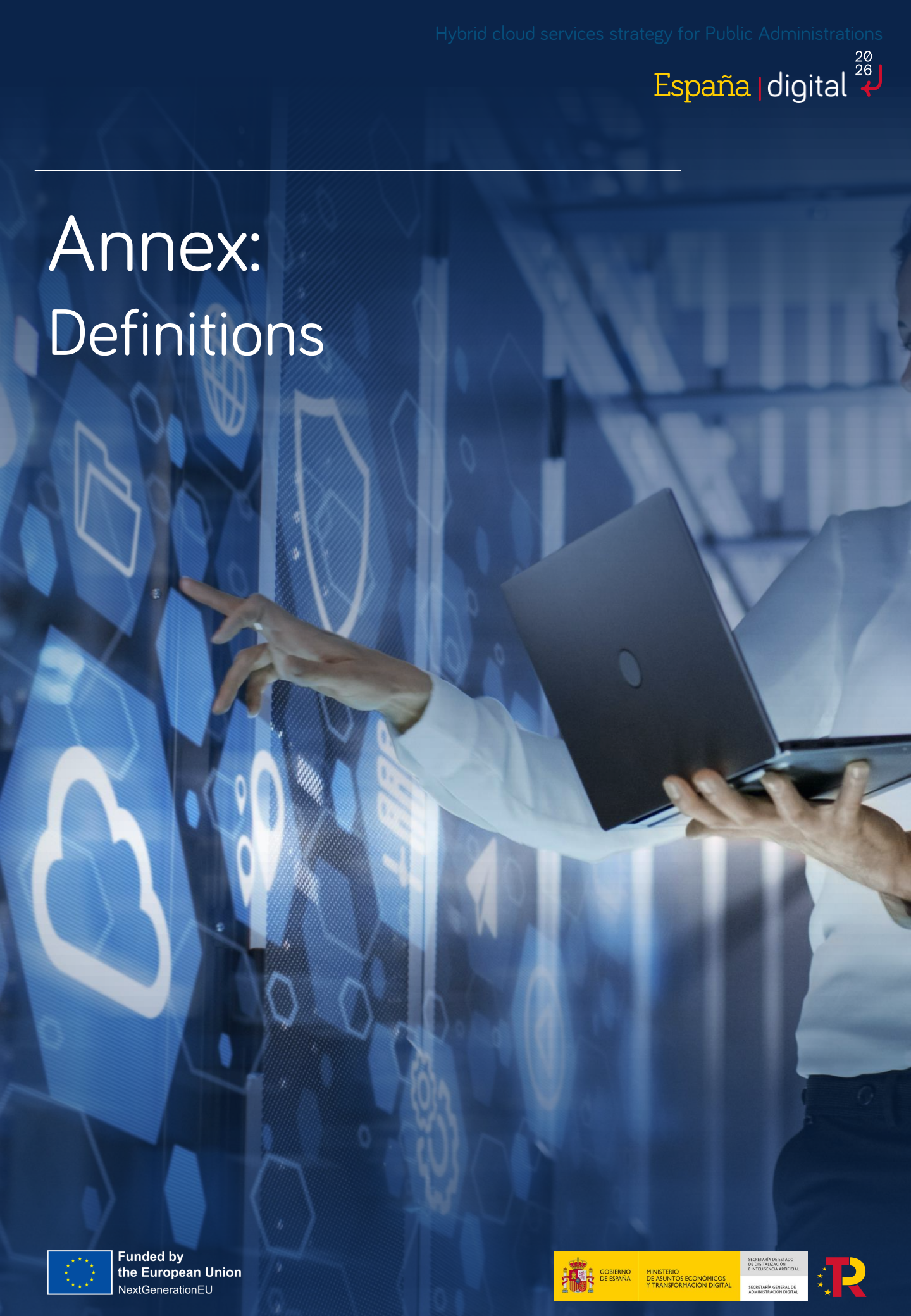
The budget structure of the Cloud Services Strategy for Public Administrations, within the framework of the Public Administrations Digitalisation Plan, is presented below. All items are funded under Component 11 of the Recovery, Transformation and Resilience Plan (PRTR):

Scope	PRTR	Estimated total investment (M€)
State Administration	Component 11. Investment 1	265
Autonomous Community	Component 11. Investment 3	461
Local Entities	Component 11. Investment 3	128
		854

** The amount corresponds to the financing of the projects submitted by the Autonomous Regions for this purpose in the framework of the Agreements of the Sectoral Conference of Public Administration formalising the distribution criteria corresponding to investment 3 of component 11 of the Recovery, Transformation and Resilience Plan for the years 2021, 2022 and 2023, aimed at the digital transformation and modernisation of the Autonomous Regions and the cities of Ceuta and Melilla (Resolutions of 13 December 2021 and 19 September 2022).*

España | digital 2026

Annex: Definitions



Funded by the European Union
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
SECRETARÍA GENERAL DE ADMINISTRACIÓN DIGITAL

Cloud computing

Cloud computing is a model of delivery and consumption of computing resources based on the **automated, on-demand availability of the resources of a computer system, without direct intervention by the provider**. Cloud services are offered through catalogues that include service level agreements and associated costs for each service.

Cloud services can be classified into **three categories according to service models**:

Software as a Service (SaaS)

This offers the use of applications, hosted by a service provider, which are made available to users through the network in an automated way, without the need for any infrastructure. An example could be a logging application, such as GEISER.

Platform as a Service (PaaS)

This offers the use of complete platforms, hosted by a service provider, and made available to users through the network in an automated way. On these platforms, users can build their applications and solutions without requiring any infrastructure. An example could be a database platform, or an Artificial Intelligence solution.

Infrastructure as a Service (IaaS)

This offers the use of full hardware with configurable processing and storage resources, which are made available to users over the network in an automated manner, hosted by a service provider. This equipment is managed by the user. An example of such a service is a virtual PC, hosted in the cloud.

Cloud services can also be categorised according to who provides them:

Public cloud

The infrastructure and on-demand IT services of an external provider are shared between several organisations via the public Internet.

Private cloud

IT infrastructure and resources are dedicated for a set of users. It may be owned, managed and operated by the organisation, a third party or some combination of these, and may exist on or off-site.

Hybrid cloud

Services are offered both publicly and privately. A user owns some parts and shares others, albeit in a controlled manner.

Multi-cloud

When using Public Cloud providers, the aim is to use several providers for the same service so that there is no dependency on one provider for a particular service.

Edge Computing

Services that are provided close to the user, to improve response times and save bandwidth.

The essential characteristics of cloud services are:

Self-service on demand

Once requested, services can be received automatically, without requiring human interaction from the service provider.

Wide and ubiquitous access to the entire network

All capacities are available through the network and are accessed through standard mechanisms and heterogeneous platforms, e.g. mobile phones, tablets, computers etc.

Transparent location and pooling of resources

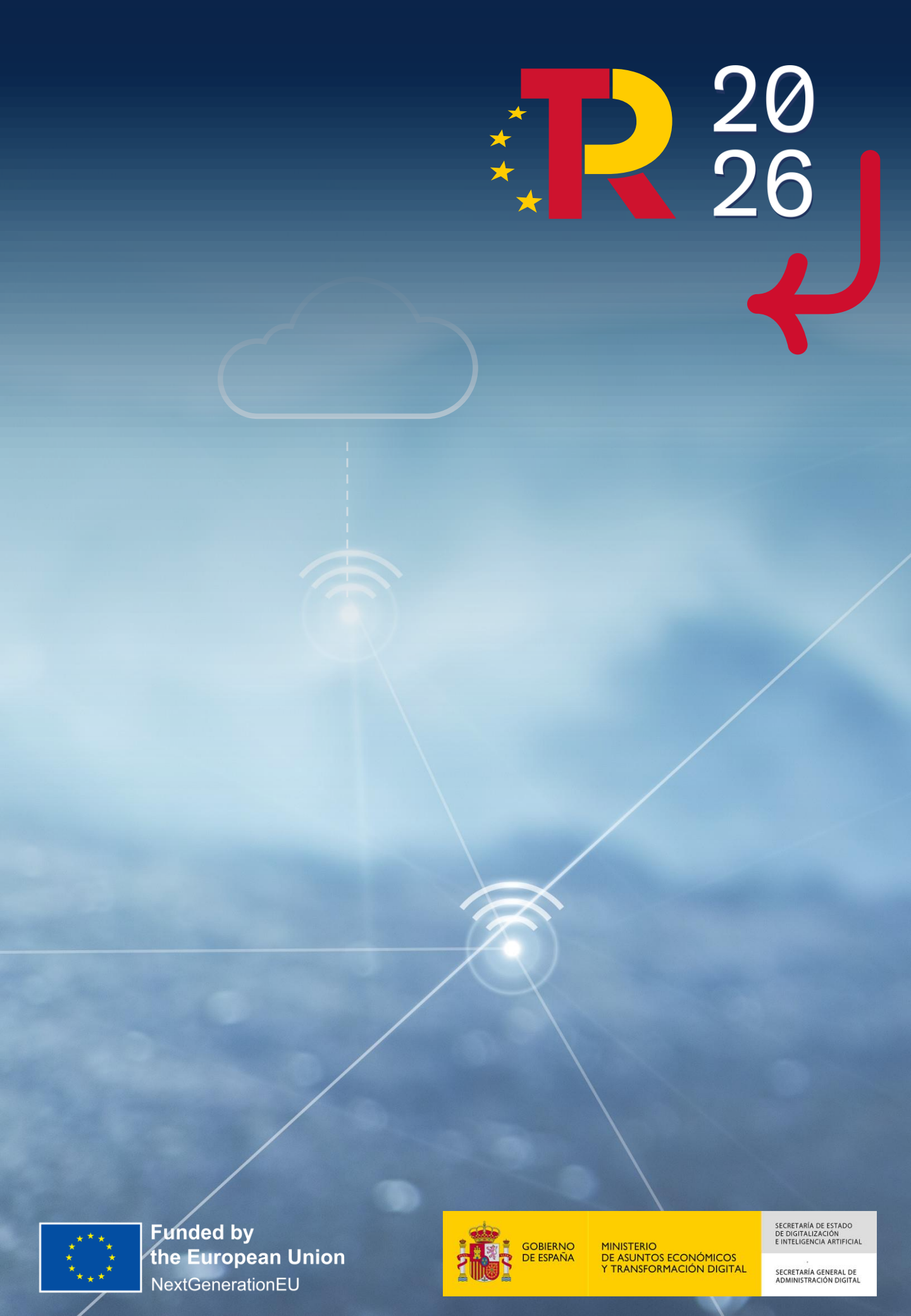
Infrastructure is pooled to serve multiple users, with different virtualised physical resources dynamically allocated and reallocated according to demand.

Rapid elasticity and scalability

Resources can be allocated and released, i.e. increased or decreased, rapidly according to demand. For the consumer, the capacities available for procurement often appear to be unlimited and can be used in any quantity at any time.

Metered service

Infrastructure is pooled to serve multiple users, with different virtualised physical resources dynamically allocated and reallocated according to demand.



Funded by
the European Union
NextGenerationEU

GOBIERNO
DE ESPAÑA

MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL

SECRETARÍA GENERAL DE
ADMINISTRACIÓN DIGITAL