España | digital 2026

Estrategia de servicios en la nube híbrida para las Administraciones Públicas

PLAN DE DIGITALIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS 2021-2025

Transformación digital de la Administración General del Estado

Servicio de Infraestructuras Cloud

Diciembre 2022

Financiado por la Unión Europea
NextGenerationEU

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

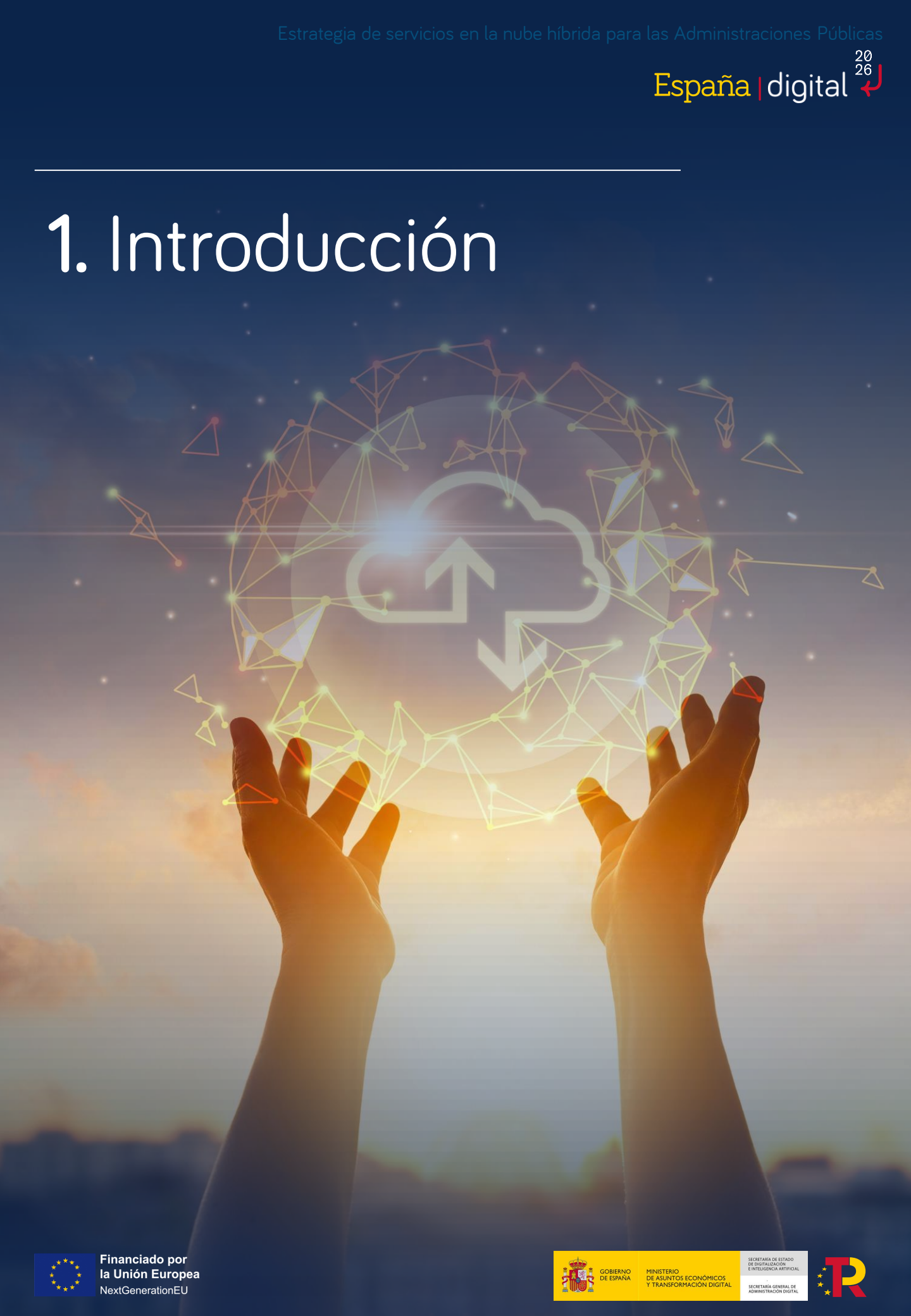
Ministerio de Asuntos Económicos y Transformación Digital
Madrid, diciembre 2022
NIPO: 094-23-011-5

Financiado por la Unión Europea
NextGenerationEU

ÍNDICE

España | digital 2026

1. Introducción



Financiado por la Unión Europea
NextGenerationEU

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

La Estrategia de cloud híbrida para las Administraciones Públicas persigue proporcionar una dirección estratégica para la implementación y control de las soluciones en la nube por parte de las Administraciones Públicas.

La transformación digital de las Administraciones Públicas requiere un nuevo paradigma en la prestación de servicios públicos que contemple mayor flexibilidad, agilidad y adaptabilidad que demanda la sociedad. Además, implica poder **acometer innovaciones impulsadas por el valor de los datos**, la **inteligencia artificial**, el **Internet de las cosas** o las nuevas redes **5G/6G**, tal como se destaca en la declaración «*Towards a new generation Cloud for Europe*» de los 27 Estados miembros de la UE del 15 de octubre de 2020.

Los **servicios en la nube** o *cloud* se basan en la **disponibilidad automatizada, bajo demanda**, de los recursos de un sistema informático, **sin intervención directa por parte del proveedor**. Estos servicios en la nube se ofrecen mediante catálogos que incluyen **acuerdos de nivel de servicio y costes asociados** para cada servicio.

Este modelo se apoya en infraestructuras tecnológicas que se dimensionan de manera dinámica, caracterizadas por la virtualización de recursos, un alto grado de automatización y capacidades de funcionamiento multi-entidad, garantizando aislamiento y seguridad en el acceso a los datos de las distintas entidades. La amplia gama de posibilidades que ofrece el paradigma de servicios en la nube, junto con las distintas arquitecturas y modelos de prestación, requiere disponer de una **estrategia que permita garantizar la necesaria autonomía, la seguridad y el control de los datos y servicios** prestados, así como **facilitar la aplicación de innovaciones** en la prestación de los servicios públicos.

Efectivamente, el uso de los servicios en la nube permite a las Administraciones Públicas prestar servicios digitales y disponer de **infraestructuras tecnológicas seguras, eficientes y fiables,** a la vez que exige especial atención a salvaguardar las garantías **para la autonomía estratégica del país, la seguridad y el control sobre los datos**.

Para ello, se plantea la necesidad de hacer frente a una serie de desafíos, incluyendo el disponer de **autonomía tecnológica**, que evite los riesgos derivados de decisiones unilaterales por parte de los proveedores o del marco jurídico que les pueda resultar de aplicación.

La Estrategia, estructurada en **7 pilares y 19 iniciativas**, se enmarca en el **Plan de Digitalización de las Administraciones Públicas 2021-2025**, concretamente bajo el paraguas de la medida 7, vinculada al Servicio de Infraestructuras Cloud y la medida 9, vinculada al Centro de Operaciones de Ciberseguridad.

Las **inversiones** supondrán un importe total de **854 M€** destinado a la **Administración del Estado y las Administraciones Territoriales**, y se financiarán con cargo al Plan de Recuperación, Transformación y Resiliencia.

España | digital 2026

Este documento trata el **potencial de los servicios en la nube** para las Administraciones Públicas, los **desafíos** que plantea la adopción de dichos servicios, los **objetivos** perseguidos y los **pilares** de la estrategia.

Los **7 pilares** que sustentan la estrategia se desarrollan mediante **19 iniciativas**:

Nube híbrida por diseño	**i1** Ampliar la solución de nube privada existente **i2** Promover la conexión e interoperabilidad con diferentes proveedores de nube
Catálogo de servicios creciente	**i3** Crear la "tienda" de NubeSARA **i4** Intermediar la oferta de soluciones en modo servicio del sector privado **i5** Ampliar periódicamente el catálogo de servicios
Política de provisión de servicios en la nube híbrida primero: *hibrid first*	**i6** Priorizar la utilización de servicios en la nube híbrida **i7** Elaborar nuevos instrumentos de contratación para los servicios en la nube
Soberanía del dato	**i8** Elaborar una guía para análisis de riesgos en entornos de servicios en la nube según el ENS **i9** Establecer criterios para la contratación centralizada

Orientación al dato

i10 Integrar la plataforma del dato de la Administración General del Estado con NubeSARA

i11 Proporcionar herramientas de analítica adicionales

Evolución de sistemas hacia la nube híbrida

i12 Impulsar la transformación de los distintos centros a soluciones en la nube híbrida

i13 Consolidar y reforzar los servicios de la nube privada de la Administración

Nube segura

i14 Establecer criterios para distribución de cargas en la nube

i15 Certificación de la conformidad con el Esquema Nacional de Seguridad de las infraestructuras de la nube

i16 Promover las capacidades de ciberseguridad en las Administraciones Públicas

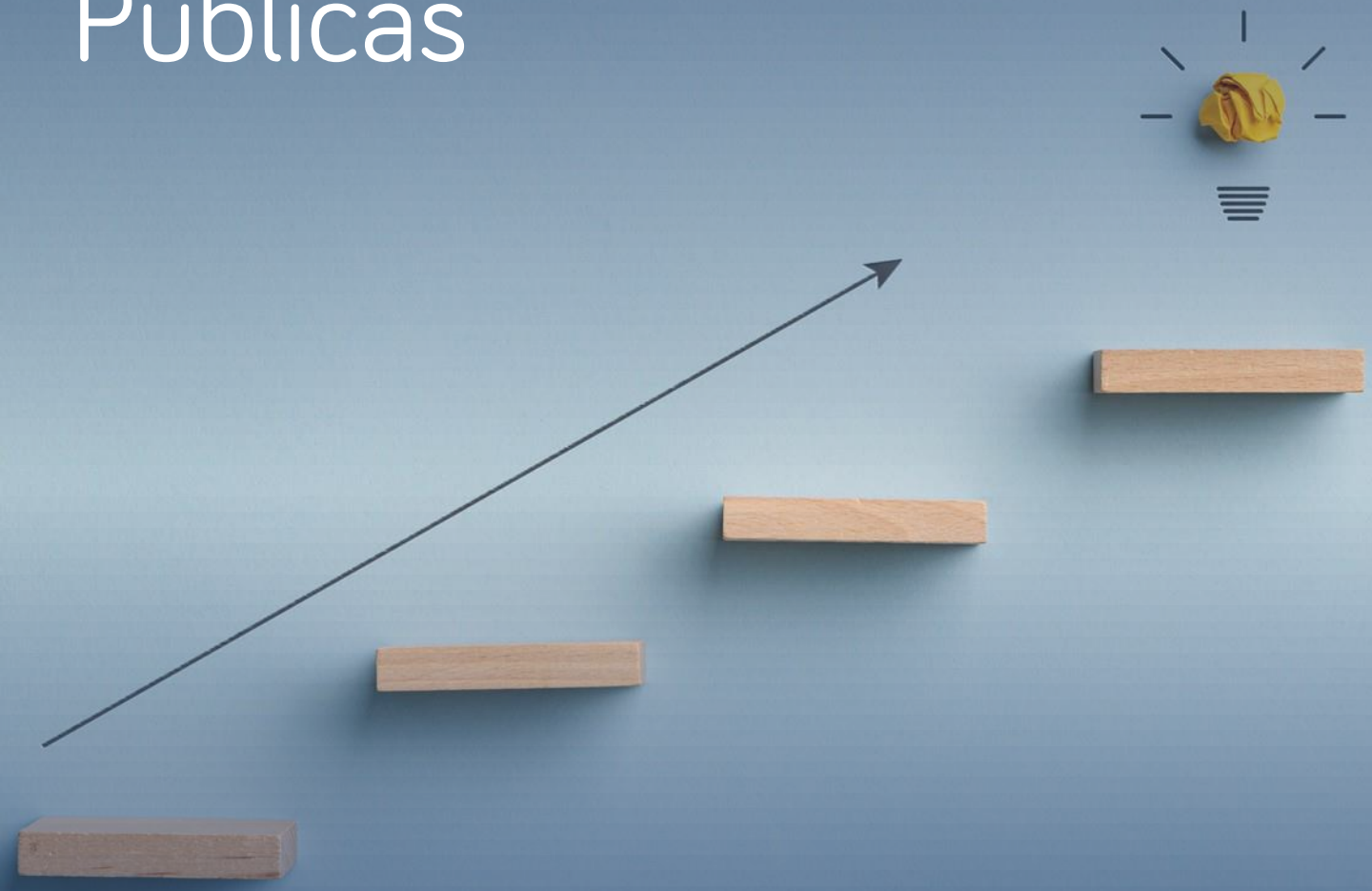
i17 Promover la extensión y evolución del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos

i18 Promover la Red Nacional de Centros de Operaciones de Ciberseguridad, así como la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes

i19 Elaborar Guías CCN-STIC en el desarrollo del ENS sobre medidas según el modelo de servicio en la nube

España | digital 2026

2. Potencial de los servicios en la nube para las Administraciones Públicas



Financiado por la Unión Europea
NextGenerationEU

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

Los servicios en la nube han permitido a las Administraciones Públicas españolas contar con herramientas para prestar servicios homogéneos y de igual calidad, con independencia del tamaño de la organización, sus recursos o su localización.

Posicionamiento en el índice de desarrollo social y económico

La aplicación del modelo de los servicios en la nube proyectado a los servicios de Administración digital es un hecho que ha contribuido a un posicionamiento destacado de España en indicadores como el Índice de Desarrollo Social y Económico, DESI.

Entre los servicios de Administración digital que han seguido este modelo orientado a la nube figuran, a título ilustrativo, casos como la solución de registro (ORVE/GEISER/SIR), la Plataforma de Intermediación de Datos (PID), los servicios de Identificación (CL@VE) y, de forma notable, la factura electrónica, uno de cuyos **factores fundamentales de éxito** fue el despliegue de una **solución en modalidad en la nube para todas las Administraciones Públicas**.

La potencia de este tipo de soluciones facilita el **refuerzo de la cohesión territorial** en la medida en la que permite a organizaciones con menos recursos como las Entidades Locales alcanzar un nivel de digitalización adecuado. Esto se consigue gracias al despliegue de herramientas en la nube como las mencionadas.

Por otra parte, el **marco normativo español** contempla un **funcionamiento íntegramente electrónico** que promueve la transformación digital de las Administraciones Públicas, así como el despliegue de servicios digitales de primera calidad. La orientación de servicios en la nube ha facilitado la aplicación de esta ambiciosa normativa con un alcance generalizado, permitiendo eludir la complejidad de un país altamente descentralizado.

Además, se ha desarrollado la posibilidad de que proveedores privados ofrezcan soluciones de Administración digital como servicio, que complementan los servicios facilitados por la Administración del Estado.

Todos estos servicios son interoperables gracias a que España cuenta con un marco normativo muy desarrollado en este ámbito con la regulación del **Esquema Nacional de Interoperabilidad**.

La provisión de servicios en la nube no es algo novedoso para la Administración española, de forma que para las Administraciones Públicas el uso de estos servicios permite:

- Fomentar la **reutilización de aplicaciones,**
- **Reducir costes** de infraestructura,
- **Aumentar la redundancia y resiliencia** de los servicios públicos,
- **Reducir la huella de carbono** al incrementar la **eficiencia energética** y la **sostenibilidad medioambiental**.

Esta reducción dependerá de la solución tecnológica concreta así como de otros aspectos de las infraestructuras y de soporte común como el suministro eléctrico, pero en todo caso puede suponer un importante avance frente a la situación previa.

En esta línea, la presente estrategia persigue **extender la modalidad de servicios en la nube,** para **universalizarla** y utilizarla como palanca permitiendo **dar un salto cualitativo en la transformación digital de las distintas Administraciones Públicas.**

Desde 2015, también se ha reforzado el catálogo de servicios de **Infraestructura como Servicio** (IaaS) y **Plataforma como Servicio** (PaaS) como herramienta para reducir el número de Centros de Proceso de Datos de la Administración del Estado, optimizando el uso de los recursos disponibles y la calidad de la prestación.

Como resultado de esto, actualmente un porcentaje significativo de los recursos de proceso de datos de la Administración del Estado se ejecutan sobre una **solución de nube privada denominada NubeSARA.**

En concreto, la Secretaría General de Administración Digital desplegó en 2015 la NubeSARA, que alberga actualmente de forma parcial la infraestructura de cómputo de 22 Organismos y Entidades vinculados o dependientes de 11 Ministerios diferentes.

Dicha solución dispone de un **Catálogo de Servicios**, con coste conocido y acuerdos de nivel de servicio asociados. Las actividades más relevantes en la provisión de estos servicios han sido automatizadas, obteniendo importantes beneficios en su operación frente a las infraestructuras de tecnologías de la información y comunicaciones tradicionales.

En un siguiente paso, este Catálogo de Servicios **se convertirá en la Tienda de Soluciones, Servicios y Aplicaciones** (a modo de Marketplace) **para las distintas Administraciones Públicas,** con la vocación de incrementar tanto el número de Organismos y Entidades de Derecho Público que lo usen como la integración de proveedores externos en la cartera de productos disponibles. A este objetivo se llegará después de un proceso de incorporación tanto de servicios como de organizaciones usuarias de los mismos.

La nube privada o propia de la Administración del Estado (NubeSARA) alberga actualmente la infraestructura de 22 Organismos y Entidades de Derecho Público vinculados o dependientes de 11 Ministerios

España | digital 2026

3. Desafíos relativos a los servicios en la nube

Financiado por la Unión Europea
NextGenerationEU

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

Autonomía tecnológica

En relación con los servicios en la nube, es de especial importancia retener la capacidad de poder **gobernar y gestionar la infraestructura** que los soporta y, en consecuencia, el almacenamiento y procesamiento de datos.

No obstante, es un hecho que las cuotas de mercado de las empresas europeas en servicios en la nube representan un valor muy pequeño (inferior al 10%) en comparación con las que poseen las empresas de fuera de la Unión Europea. Este desequilibrio en la cuota de mercado no solo se limita a los servicios y plataformas digitales sino, también, a las infraestructuras que les permiten funcionar.

Así, la adopción masiva de tecnología para servicios en la nube por las Administraciones Públicas estaría sujeta a riesgos tales como cambios unilaterales en las condiciones de los servicios, aumento de costes, interrupción del servicio o ubicación de los datos.

En consecuencia, disponer de **autonomía tecnológica**, en particular, con capacidades en España, tiene implicaciones, no solo en cuanto a la posibilidad de poder **ejercer un control directo sobre los datos y los servicios,** sino también en cuanto a **promover un ecosistema de tecnologías necesarias para la transformación digital** (Servicios en la nube, Inteligencia Artificial, Internet de las cosas, Computación Cuántica, Espacios de datos, etc.).

Disponer de autonomía tecnológica con capacidades en España permitirá promover el ecosistema de tecnologías necesarias para la transformación digital de las Administraciones

Soberanía del dato

En relación con la soberanía del dato hay que tener presente que interesa tanto **dónde se encuentra ubicado el dato**, como desde **dónde se gestionan las infraestructuras y servicios** que lo proveen y administran. Aunque los Centros de Proceso de Datos que soportan servicios en la nube estén ubicados en suelo español o de la Unión Europea, en algunos casos se encuentran operados desde fuera de este espacio por empresas sujetas a otras jurisdicciones.

Este hecho podría permitir, en determinadas circunstancias, **solicitudes o accesos unilaterales con origen de fuera de la Unión Europea** al proveedor de servicios en la nube para que proporcionase acceso a los datos, que podrían ser de carácter estratégico y/o sensible para las instituciones y los ciudadanos, solicitudes que, eventualmente, podrían quedar fuera del conocimiento, control y capacidad de decisión de los responsables nacionales.

Este desafío se puso de manifiesto en la **Declaración de Berlín sobre la sociedad digital y la Administración digital basada en valores**, firmada en diciembre de 2020, en la que se apuntan cuestiones tales como la necesidad de intensificar los esfuerzos para que **los datos almacenados por las Administraciones Públicas de los Estados miembros sean inmunes a cualquier interferencia no deseada**; así como de **fomentar las propias capacidades digitales claves** para desarrollar y desplegar soluciones digitales en infraestructuras de nube segura para los servicios públicos.


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

Redundancia y resiliencia

La resiliencia es una característica fundamental que deben poseer los sistemas e infraestructuras críticas. Las infraestructuras y los servicios en la nube que soporten las aplicaciones de las Administraciones Públicas deben adoptar **medidas de seguridad y redundancia** adecuadas.

La aplicación de **controles de seguridad según los requisitos de los datos tratados**, así como la continuidad del servicio y las **medidas de recuperación ante desastres** han de mejorar la resiliencia frente a ciberataques y otros incidentes.

Interoperabilidad

Dada la importancia de los datos y servicios involucrados, la estrategia de migración a la nube requiere tener en cuenta, a la hora de seleccionar proveedores y tecnologías, la necesaria **competencia y la futura interoperabilidad y portabilidad,** evitando tecnologías que generen cautividad, de manera que los **recursos** que se migren a la nube sean **reversibles y puedan ubicarse en diferentes proveedores externos**, o bien en la nube privada de la Administración, sin necesidad de realizar costosos proyectos de transformación, tanto en tiempo como en inversión, derivados de eventuales cambios de proveedor.

Protección de datos

Como expone la **Agencia Española de Protección de Datos en su "Guía para prestadores de servicios** de cloud computing", *«no cabe olvidar que los servicios de cloud computing tienen implicaciones específicas para la protección de los datos personales de los que es responsable el cliente que contrata los servicios. Esas implicaciones exigen una valoración del mejor modo de incorporar las* ***garantías contempladas en la normativa de protección de datos, modulándolas para adaptarlas*** *a* las *características específicas de los mismos».*

Además, como expone la "**Guía para clientes** que contraten servicios de cloud computing" de la Agencia Española de Protección de Datos, *«la posibilidad de tratamiento de los datos fuera del territorio nacional, característica del cloud computing, constituye un elemento de especial relevancia en el caso de las Administraciones Públicas. En este sentido, debe tenerse en cuenta que la* ***normativa*** *que regula los movimientos internacionales de datos es* ***aplicable tanto a entidades públicas como privadas»***. Cabe recordar aquí que las principales normas de aplicación son el **Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales.**

> La normativa que regula los movimientos internacionales de datos es aplicable tanto a entidades públicas como privadas

Ciberseguridad

La ciberseguridad se ha convertido en una prioridad estratégica, pues se ha evidenciado la exposición de forma cada vez más intensa a la materialización de las amenazas del ciberespacio y a los ciberataques. Se viene produciendo un notable incremento de estos ciberataques, tanto en volumen y frecuencia, como en sofisticación, con agentes y actores con mayores capacidades técnicas y operativas; todo ello en un contexto de alta dependencia de las tecnologías.

A estas amenazas se ven expuestas un número cada vez mayor de entidades públicas y privadas, sus cadenas de suministro, y la ciudadanía y las empresas, tal como se reconoce en la Estrategia Nacional de Ciberseguridad de 2019.

En particular, la **adopción del modelo de servicios en la nube** introduce nuevos **riesgos que es necesario controlar** para poder satisfacer los requisitos exigibles por la normativa vigente, como la relativa al Esquema Nacional de Seguridad, mediante la correspondiente **certificación de la conformidad o aplicación del perfil de cumplimiento** específico, o a la protección de datos personales, así como por los requisitos de seguridad que en cada caso las organizaciones establezcan como necesarios en sus respectivas políticas de seguridad.

La adopción del modelo de servicios en la nube introduce nuevos riesgos que es necesario controlar, asegurando el cumplimiento de los requisitos de seguridad que correspondan en cada caso

España | digital 2026

4. Objetivos

Financiado por la Unión Europea
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

Esta estrategia tiene como objetivo general:

Priorizar el aprovisionamiento de servicios basado en tecnologías en la nube por las Administraciones Públicas,

empleando en primer término los recursos propios y complementándolos con soluciones del sector privado, consiguiendo sinergias que redunden en una **mejor prestación de los servicios**, una mayor **autonomía tecnológica**, a la vez que garantizando en todo momento la **seguridad y la protección de los datos personales.**

Y como objetivos específicos:

Dotar a las Administraciones Públicas de las infraestructuras tecnológicas necesarias para profundizar en su modernización, con el fin de asegurar la disponibilidad en cualquier circunstancia y de adaptar la capacidad disponible a las necesidades existentes en cada momento, contribuyendo a desarrollar la conectividad digital, la orientación al dato y la inteligencia artificial en las Administraciones.

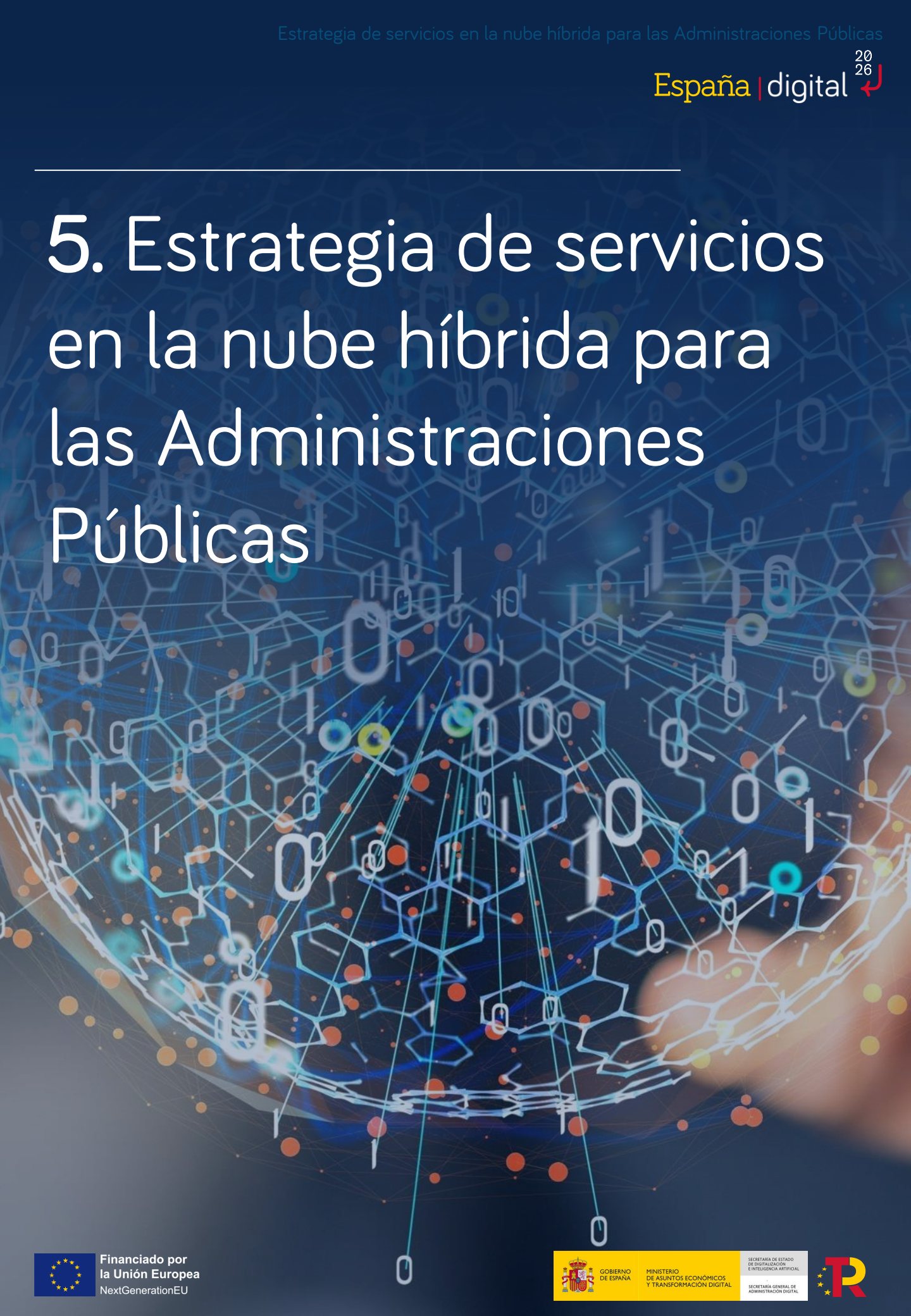
Consolidar los Centros de Proceso de Datos de la Administración del Estado en un número menor de centros con mejores prestaciones, reduciendo costes operativos (económicos y medioambientales) y maximizando la agilidad de las operaciones TIC (Tecnologías de la Información y Comunicaciones), adaptándose más rápidamente a las demandas de la sociedad, sin que suponga un lastre u obstáculo futuro a la evolución tecnológica.

Potenciar unos servicios en la nube seguros, promoviendo una mayor autonomía tecnológica y asegurando los requisitos de soberanía del dato, con ciberseguridad y protección de datos, de forma que los sistemas de información que los soporten sean conformes con el Esquema Nacional de Seguridad y, en el caso, de los servicios en la nube prestados por el sector privado que se encuentren certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las TIC.

Potenciar la participación de las infraestructuras en la nube de la Administración del Estado en iniciativas en el marco de la Unión Europea, como la «EU Cloud Federation» y Gaia-X; y en particular, facilitar la adopción de los principios, arquitecturas y componentes procedentes de las diferentes iniciativas europeas impulsoras de los principios europeos de transparencia, confianza y soberanía de los servicios en nube

España | digital 2026

5. Estrategia de servicios en la nube híbrida para las Administraciones Públicas



Financiado por la Unión Europea
NextGenerationEU

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

La estrategia se sustenta en 7 pilares que se desarrollan mediante 19 iniciativas:

PILAR 1 | Nube híbrida por diseño

El objetivo es disponer de **infraestructura de nube híbrida compuesta por una nube propia de la Administración del Estado**, ubicada en sus centros de proceso de datos, combinada con las de otras Administraciones Públicas y con proveedores externos de servicios de nube pública.

La solución de nube de la Administración del Estado, denominada NubeSARA, se define como híbrida, al estar formada por la **combinación de varias tipologías de nube interconectadas entre sí.** En su diseño, contempla cuatro elementos:

- **La nube privada o propia de la Administración del Estado**, basada en **dos centros de proceso de datos** principales, ubicados a una distancia adecuada uno de otro, y un centro de respaldo adicional. Estos centros proveen los servicios en la nube y adicionalmente alojamiento como servicio para los casos en que no puedan migrarse a la nube. Esta nube concentra los servicios interministeriales que manejan datos sensibles o despliegan procesos críticos de la Administración.
- **Las nubes de otras Administraciones Públicas españolas o de la Unión Europea**.
- **La nube «exterior» de la Administración del Estado**, proporcionada por empresas de servicios en nube pública y consumida a partir de un catálogo de servicios. La nube «exterior» acogerá, principalmente, cargas de trabajo que se apoyen en datos poco sensibles y constituirá una solución de apoyo a la Nube propia.
- **Capacidades de Edge Computing** que, según el caso, podrá ser combinado con los elementos anteriores, analizando las posibles ventajas de la conjunción de ellos, ante grandes volúmenes de datos, según las entidades y su tipología de aplicaciones/sistemas.

Un aspecto fundamental en una solución de nube híbrida es establecer un **adecuado marco de interoperabilidad entre los proveedores**, de forma que satisfagan una serie de condiciones, como la compatibilidad o reversibilidad de las cargas. Asimismo, se potenciará el diseño de un conjunto de **servicios reusables o «building blocks»** que permitirá la citada interoperabilidad para la creación de los servicios cloud.

Para posibilitar la nube híbrida por diseño se llevarán a cabo las siguientes iniciativas:

i1. Ampliar la solución de nube privada existente

Se adquirirá capacidad adicional, añadiendo nuevas funcionalidades al catálogo de servicios.

i2. Promover la conexión e interoperabilidad con diferentes proveedores de nube

Se establecerá un procedimiento para realizar conexiones con proveedores del sector privado manteniendo las garantías necesarias.

PILAR 2

Catálogo de servicios creciente

Se trata de disponer de un **catálogo de servicios creciente con la incorporación de aplicaciones que den respuesta a las necesidades comunes** de las Administraciones Públicas con soluciones del tipo Software como Servicio (SaaS).

Se persigue enriquecer de manera continua este catálogo de servicios con elementos de mayor valor añadido, en todos los ámbitos de los servicios en la nube, sean como infraestructura, plataforma o software como servicio.

El catálogo será accesible de forma sencilla a través de la «tienda» de NubeSARA, que permitirá desplegar servicios con facilidad a las Administraciones Públicas y que inicialmente se nutrirá de las soluciones ya disponibles y que se facilitan en la actualidad como servicio.

Adicionalmente, se promoverá la incorporación a este catálogo de las aplicaciones que den respuesta a las necesidades comunes de las Administraciones.

Para posibilitar el catálogo creciente se llevarán a cabo las siguientes iniciativas:

i3. Crear la «tienda» de NubeSARA

Se desplegará una interfaz que facilite a las entidades usuarias un modelo sencillo de consumo de los servicios.

i4. Intermediar la oferta de soluciones en modo servicio del sector privado

Se articulará un mecanismo para la inclusión de soluciones en modo servicio del sector privado que hayan pasado un proceso de homologación.

i5. Ampliar periódicamente el catálogo de servicios

Respondiendo a las demandas de los usuarios, se ampliará el catálogo periódicamente con soluciones que aporten valor a las Administraciones.

PILAR 3

Política de provisión de servicios en la nube híbrida primero: hibrid first

El principio «en la nube híbrida primero» persigue **priorizar el aprovisionamiento de servicios basados en la nube frente a las soluciones tradicionales**, por razón de la capacidad de los primeros para ofrecer una gran cantidad de servicios en red de forma ágil y flexible, con grandes posibilidades de escalabilidad y reduciendo al mínimo los tiempos de despliegue.

Para hacerla posible se llevarán a cabo las siguientes iniciativas:

i6. Priorizar la utilización de servicios en la nube

Se priorizará el uso de soluciones en la nube frente a la inversión en infraestructuras por parte de cada una de las administraciones.

i7. Elaborar nuevos instrumentos de contratación para los servicios en la nube, buscando la simplificación y eficiencia del proceso

Se colaborará con la Dirección General de Racionalización y Centralización de la Contratación del Ministerio de Hacienda y Función Pública en la definición de herramientas de contratación complementarias a esta estrategia.

PILAR 4

Soberanía del dato

Se trata de disponer de **criterios** en relación con la **ubicación y gestión de los datos** de forma que se garantice en todo momento la **soberanía digital, la jurisdicción, la seguridad y su protección** dentro de la normativa vigente.

Los citados criterios habrán de contemplar, en el contexto de la soberanía digital europea, cuestiones tales como los siguientes:

- Que los **datos sensibles de la Administración no se transfieran** fuera de la Unión Europea.
- Que los datos manejados por **sistemas** que sean de **categoría ALTA según el Esquema Nacional de Seguridad** solo puedan ser manejados por empresas a las que les aplique de manera exclusiva la jurisdicción comunitaria.
- Que las **autoridades de terceros países no puedan acceder** a los datos de manera incontrolada.
- Que la **disponibilidad de las infraestructuras se pueda preservar**, incluso en el caso de posibles tensiones geopolíticas.

Para posibilitar la soberanía del dato se llevarán a cabo las siguientes iniciativas:

i8. Elaborar una guía para análisis de riesgos en entornos de servicios en la nube, incluyendo entre otros, jurisdicción y soberanía del dato, teniendo en cuenta los requisitos al respecto establecidos por el Esquema Nacional de Seguridad

Se colaborará en la redacción de una guía con el Centro Criptológico Nacional que contemple el marco legal español y europeo en estas materias.

i9. Establecer criterios para la contratación centralizada de servicios en la nube

Se colaborará con la Dirección General de Racionalización y Centralización de la Contratación del Ministerio de Hacienda y Función Pública en la definición de criterios para las contrataciones de servicios en la nube.

PILAR 5

Orientación al dato

Se persigue enfocar las infraestructuras hacia el desarrollo de una **arquitectura de información que soporte la visión transversal de los datos "como servicio" ("As-a-Service")** y que garantice la hiperconectividad de servicios y datos.

Se trata de **simplificar la interoperabilidad de los datos**, posibilitando su trasvase ordenado entre silos para su mejor aprovechamiento.

Este desarrollo contribuye a la **economía del dato** aportando servicios de infraestructura para almacenar y procesar datos, una **arquitectura de compartición** entre los diferentes actores y una **conectividad de alta capacidad, segura, fiable y resiliente.** Al mismo tiempo se busca simplificar el despliegue de herramientas para análisis y ciencia de datos.

Este enfoque facilitará a las Administraciones Públicas acometer innovaciones impulsadas por el valor de los datos, sin necesidad de abordar ad hoc por sí mismas el despliegue de la infraestructura tecnológica necesaria.

Para posibilitar la orientación al dato se llevarán a cabo las siguientes iniciativas:

i10. Integrar la plataforma del dato de la Administración General del Estado con NubeSARA

Se integrará la plataforma del dato de la Administración General del Estado con NubeSARA.

i11. Proporcionar herramientas de analítica adicionales como servicio

Se añadirán herramientas de analítica adicionales al catalogo de servicios de NubeSARA.

PILAR 6 | 

Evolucionar los sistemas existentes hacia la nube

Se trata de **transformar los sistemas existentes al modelo en la nube y enriquecer de manera continua el catálogo de servicios** con elementos de mayor valor añadido.

Se persigue garantizar la **evolución coherente de los sistemas de información existentes hacia tecnologías de vanguardia** empleando para ello servicios en la nube. Para ello, se reutilizará el máximo posible de los elementos ya presentes en la «tienda» de NubeSARA.

Se prestará especial atención a las iniciativas de transformación para lo cual es necesario, para cada servicio o aplicación a migrar:

- Realizar **proyectos de transformación** de los servicios, aplicaciones e infraestructuras actuales de las Administraciones Públicas, **para habilitar su migración** a la nube.
- Definir y ejecutar el **plan de migración a NubeSARA.**
- **Consolidar todos aquellos servicios** que no sean susceptibles de ser migrados a NubeSARA, pero necesiten de un plan alternativo hasta que dichos servicios alcancen su fin de vida.
- **Potenciar las capacidades de Edge Computing** que, según el caso, podrán ser combinadas con los elementos anteriores, analizando las ventajas ante grandes volúmenes de datos según las entidades y tipología de aplicaciones/sistemas.

Para posibilitar la evolución a la nube se llevarán a cabo las siguientes iniciativas:

i12. Impulsar la transformación de los distintos centros de la Administración del Estado a soluciones en la nube híbrida

Se promoverán los procesos de transformación de los centros de la Administración General del Estado hacia la adopción de soluciones que contemplen el uso de la nube híbrida.

i13. Consolidar y reforzar los servicios de la nube privada de la Administración

Se reforzarán los servicios de las infraestructuras de la Administración del Estado que sean necesarios para poder llevar a cabo los procesos de consolidación.

PILAR 7 | 

Nube segura

Se trata de proteger los servicios en la nube con las **medidas de seguridad apropiadas en función del modelo de servicio en la nube** correspondiente, según lo previsto en el Esquema Nacional de Seguridad y en los perfiles de cumplimiento específico, así como en las guías CCN-STIC que sean de aplicación.

El **Esquema Nacional de Seguridad** recoge la nueva medida «Protección de servicios en la nube» que, además del requisito de conformidad con el Esquema, contempla el refuerzo de que cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar certificados bajo una metodología reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información, en alusión a que los servicios en la nube suministrados por terceros cuenten con la futura certificación europea EUCS – CLOUD SERVICES SCHEME.

Para posibilitar la nube segura se llevarán a cabo las siguientes iniciativas:

i14. Establecer criterios para distribución de cargas en la nube

Se definirá un proceso de hibridación que contemple la seguridad en todos sus aspectos, incluyendo un análisis de riesgos específico para cada proveedor. Asimismo, se establecerán, mediante guías CCN-STIC que contemplen el marco legal español y europeo en estas materias, los criterios para la ubicación de las cargas, teniendo en cuenta los aspectos de soberanía del dato y protección de datos.

i15. Certificación de la conformidad con el Esquema Nacional de Seguridad de las infraestructuras de la nube

Se promoverá la certificación de la conformidad con el Esquema Nacional de Seguridad de todas las infraestructuras de la nube que presten servicio a las Administraciones Públicas.

i16. Promover las capacidades de ciberseguridad en las Administraciones Públicas

Se promoverá la seguridad de las infraestructuras, comunicaciones y servicios digitales prestados por las administraciones públicas, así como la mejora de sus capacidades de prevención, detección y respuesta ante incidentes de ciberseguridad. Todo ello con el objetivo de lograr una mejor protección de la información tratada y de los servicios digitales prestados, en un contexto de exposición cada vez más intensa a la materialización de amenazas del ciberespacio, a los ciberincidentes, que siguen una pauta de crecimiento en frecuencia, sofisticación, alcance y severidad del impacto.

---

i17. Promover la extensión y evolución del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos

Se promoverá la evolución de la madurez de los servicios del Centro de Operaciones de Ciberseguridad, la integración de NubeSARA y de más entidades en el alcance de sus servicios, así como la ampliación de los servicios a la luz del escenario de ciberseguridad, junto con la implantación de nuevas capacidades de resiliencia, protección, auditoría, pruebas de seguridad y análisis de código, investigación de ciberseguridad, revelación de vulnerabilidades, compartición de información, y aplicación del estado del arte de Inteligencia Artificial.

---

i18. Promover la Red Nacional de Centros de Operaciones de Ciberseguridad, así como la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes

La Red Nacional de Centros de Operaciones de Ciberseguridad es un instrumento para coordinar la colaboración y el intercambio de información entre los Centros de Operaciones de Ciberseguridad del sector público español. Forman parte de esta Red todos los Centros de Operaciones de Ciberseguridad nacionales del sector público español y aquellas empresas proveedoras de servicio de seguridad gestionada que ofrezcan servicios a este tipo de centros, que hayan solicitado formar parte de la red. La Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes se pone en marcha por el CCN-CERT en colaboración con el INCIBE-CERT y el ESPDEF-CERT del Mando Conjunto del Ciberespacio para implementar el procedimiento de notificación y gestión de incidentes, que estará disponible durante todas las horas del día y todos los días del año.

i19. Elaborar Guías CCN-STIC en desarrollo del Esquema Nacional de Seguridad, acerca de medidas que deberán cumplir los sistemas que suministran un servicio en la nube a organismos del sector público en función del modelo de servicio en la nube que presten

Se elaborarán guías adecuadas a los distintos tipos de servicios en la nube, para garantizar que su diseño, prestación y configuración se adecúan al uso que hagan las distintas entidades de ellos.

España | digital 2026

6. Presupuesto

Financiado por la Unión Europea
NextGenerationEU

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

Presupuesto

A continuación, se presenta la estructura presupuestaria de la Estrategia de servicios en la nube para las Administraciones Públicas, en el marco del Plan de Digitalización de las Administraciones Públicas. Todas las partidas se financian con cargo al Componente 11 del Plan de Recuperación, Transformación y Resiliencia (PRTR):

Ámbito	PRTR	Inversión total estimada (M€)
Administración del Estado	Componente 11. Inversión 1	**265**
Comunidades Autónomas*	Componente 11. Inversión 3	**461**
Entidades Locales	Componente 11. Inversión 3	**128**
		854

** El importe corresponde a la financiación de los proyectos presentados por las CCAA para esta finalidad en el marco de los Acuerdos de la Conferencia Sectorial de Administración Pública por los que se formaliza el criterio de distribución correspondiente a la inversión 3 del componente 11 del Plan de Recuperación, Transformación y Resiliencia para los ejercicios 2021, 2022 y 2023, destinada a la transformación digital y modernización de las comunidades autónomas y de las ciudades de Ceuta y Melilla (Resoluciones de 13 de diciembre de 2021 y 19 de septiembre de 2022).*

España | digital 2026

Anexo
Definiciones

Financiado por la Unión Europea
NextGenerationEU

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

Computación en la nube

La computación en la nube o Cloud Computing es un modelo de entrega y consumo de recursos informáticos basado en la **disponibilidad automatizada, bajo demanda, de los recursos de un sistema informático, sin intervención directa del proveedor**. Los servicios en la nube se ofrecen mediante catálogos que incluyen acuerdos de nivel de servicio y costes asociados para cada servicio.

Los servicios en la nube se pueden clasificar en **tres categorías en función de los modelos de servicio:**

Software como Servicio (SaaS)

Ofrece el uso de aplicaciones, alojadas por un proveedor de servicio, que son puestas a disposición de los usuarios a través de la red de manera automatizada, sin que estos necesiten ninguna infraestructura. Un ejemplo puede ser una aplicación de registro, como GEISER.

Plataforma como Servicio (PaaS)

Ofrece el uso de plataformas completas, alojadas por un proveedor de servicio, y son puestas a disposición de los usuarios a través de la red de manera automatizada. Sobre estas plataformas los usuarios pueden construir sus aplicaciones y soluciones sin que se necesite ninguna infraestructura. Un ejemplo puede ser una plataforma de base de datos, o una solución de Inteligencia Artificial.

Infraestructura como Servicio (IaaS)

Ofrece el uso de equipos completos con recursos de procesamiento y almacenamiento configurables, que son puestas a disposición de los usuarios a través de la red de manera automatizada, alojados por un proveedor de servicio. Estos equipos son administrados por el usuario. Un ejemplo de este tipo de servicio es un ordenador PC virtual, alojado en la nube.

Los servicios en la nube pueden clasificarse también en función de **quién los provea:**

Nube pública

La infraestructura y los servicios informáticos a la carta de un proveedor externo se comparten entre varias organizaciones a través de la red pública de Internet.

Nube privada

La infraestructura y recursos informáticos son dedicados para un conjunto de usuarios. Puede ser propiedad, ser administrado y operado por la organización, un tercero o alguna combinación de ellos, y puede existir dentro o fuera de las instalaciones.

Nube híbrida

Los servicios se ofrecen de forma pública y privada. Un usuario es propietario de unas partes y comparte otras, aunque de una manera controlada.

Multi-cloud

Al emplear proveedores de Nube Pública, se busca emplear varios para un mismo servicio de manera que no exista dependencia de un proveedor para un servicio concreto.

Edge Computing

Servicios que se proveen de manera cercana al usuario, para mejorar los tiempos de respuesta y ahorrar ancho de banda.

Las características esenciales de los servicios en la nube son:

Autoservicio bajo demanda

Una vez solicitados, los servicios pueden recibirse de manera automática, sin requerir la interacción humana del proveedor de servicios.

Acceso amplio y ubicuo a toda la red

Todas las capacidades están disponibles a través de la red y se accede a ellas a través de mecanismos estándares y plataformas heterogéneas como, por ejemplo: teléfonos móviles, tabletas, ordenadores, etc.

Ubicación transparente y agrupación de recursos

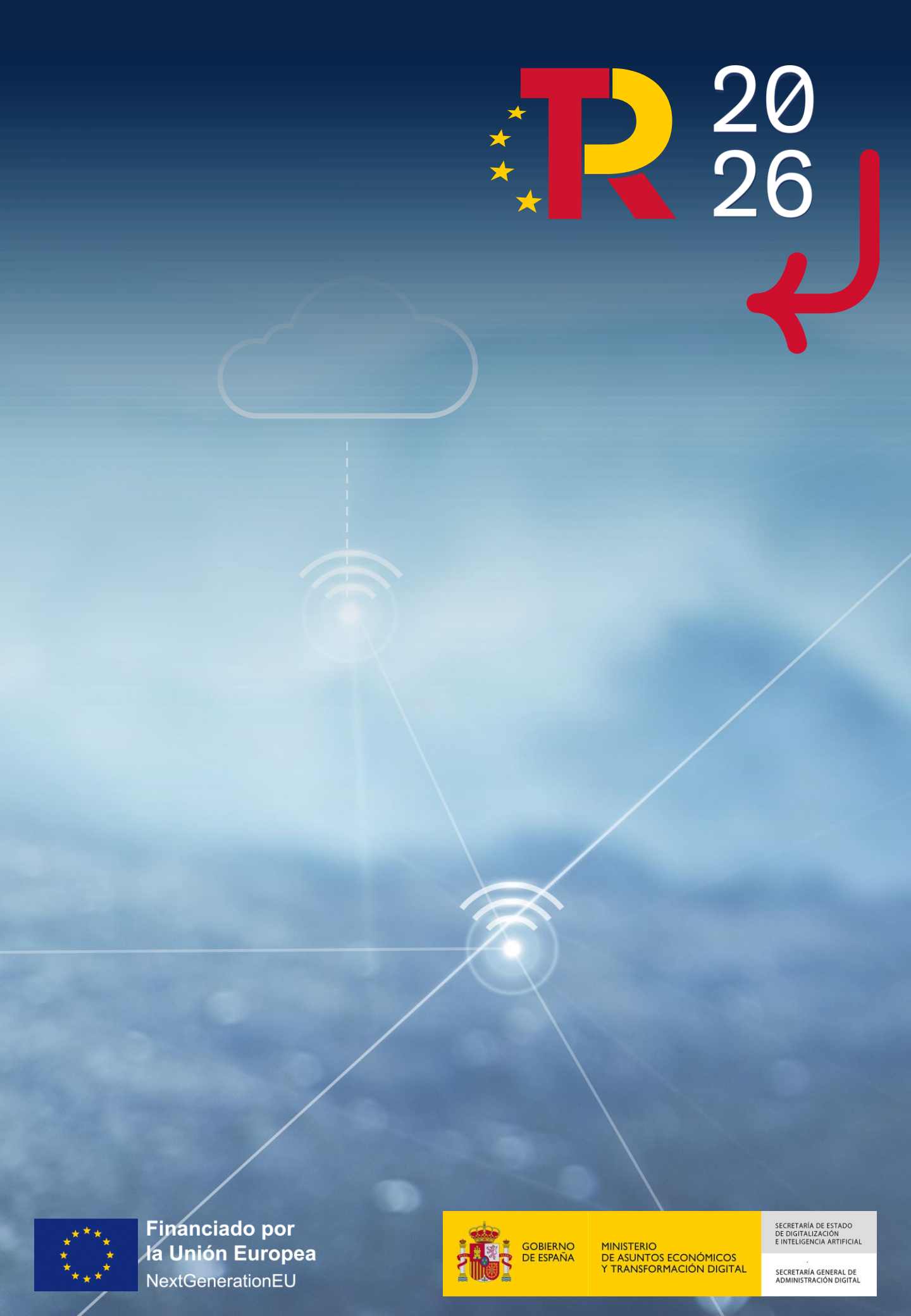
La infraestructura se agrupa para prestar servicio a múltiples usuarios, con diferentes recursos físicos virtualizados que se asignan y reasignan dinámicamente de acuerdo con la demanda.

Rápida elasticidad y escalabilidad

Los recursos se pueden asignar y liberar, es decir, aumentar o disminuir, rápidamente según la demanda. Para el consumidor, las capacidades disponibles para el aprovisionamiento a menudo parecen ser ilimitadas y pueden ser utilizables en cualquier cantidad en cualquier momento.

Servicio medido

La infraestructura se agrupa para prestar servicio a múltiples usuarios, con diferentes recursos físicos virtualizados que se asignan y reasignan dinámicamente de acuerdo con la demanda.



Financiado por la Unión Europea
NextGenerationEU

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