SOCINFO sociedad de la información digital

Evento “Estrategia Nacional de Servicios Públicos en la Nube de las AAPP”

Estrategia de servicios en la nube híbrida para las Administraciones Públicas

Miguel A. Amutio

Director de Planificación y Coordinación de Ciberseguridad

DT 2ª Real Decreto 1118/2024

Agencia Estatal de Administración Digital

26 de febrero de 2025

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

Plan de Recuperación, Transformación y Resiliencia

Financiado por la Unión Europea NextGenerationEU

España | digital 2026

1. Contexto relativo a los servicios en la nube

Esquema Nacional de Interoperabilidad

[RD 4/2010](#)
[PAe Interoperabilidad](#)

Esquema Nacional de Seguridad

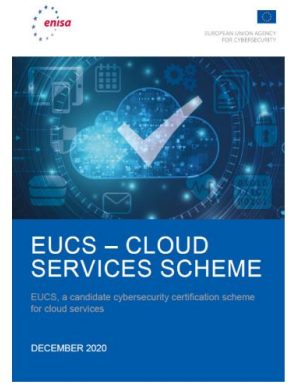
[RD 311/2022](#)
[Portal CCN-CERT: ENS](#)

Convergencia:
- Tecnologías en la nube
- Orientación al dato
- Inteligencia Artificial
- Ciberseguridad

At the core of the common public interest lie two pivotal elements: **cybersecurity** and **digital sovereignty**.

To achieve this goal, the report recommends adopting EU-wide data security policies for **collaboration between EU and non-EU cloud providers**, allowing access to US hyperscalers' latest cloud technologies **while preserving encryption, security and ring-fenced** services for trusted EU providers.

Cloud and edge computing (RP 2024)



Draft EUCS

1. Servicios en la nube para Administraciones Públicas

Los servicios en la nube han permitido a las AAPP prestar **servicios homogéneos y de igual calidad**, con independencia del tamaño de la organización, sus recursos o su localización.

Los Servicios basados en la nube privada facilitan…

- **Cohesión territorial** impulsado la digitalizacion de las entidades locales.
- **100% Servicios públicos electrónicos**, a pesar de ser un país altamente descentralizado.
- **Colaboración privada** que complementa los servicios de la administración.
- **Interoperabilidad garantizada** con el Esquema Nacional de Interoperabilidad (ENI).

…

El uso de estos servicios…

- ✓ Fomenta la **reutilización deaplicaciones**
- ✓ **Reduce costes** de infraestructura
- ✓ Aumenta la **redundancia y la resiliencia** de los servicios públicos
- ✓ **Reduce la huella de carbono** al incrementar la **eficiencia energética y la sostenibilidad** medioambiental.

2. Estrategia de nube híbrida para las Administraciones Públicas

Enero 2023

Medida 7 Plan de Digitalización AAPP

- ✓ Proporciona **dirección estratégica para implementación y control** de soluciones en nube.
- ✓ Nuevo paradigma de prestación de Servicios más flexible, ágil, adaptable.
- ✓ Poder acometer innovaciones impulsadas por el valor de los datos y la inteligencia artificial

OBJETIVO PRINCIPAL: Priorizar la provision de servicios basados en tecnologías en la nube.

DESAFÍOS

Autonomía tecnológica

Soberanía del dato

Redundancia y resiliencia

Interoperabilidad

Protección de datos

Ciberseguridad

OBJETIVOS ESPECÍFICOS

- **Dotar a las AAPP de infrastructuras tecnológicas necesarias** para profundizar en su modernización.
- **Consolidar los CPDs** en menor nº con mejores prestaciones, **para reducir costes operativos** (económicos y medioambientales) y **maximizar la agilidad** de las operaciones TIC.
- **Potenciar unos servicios en la nube seguros**, con mayor autonomía tecnológica, soberanía del dato, ciberseguridad y protección de datos.
- Potenciar la **participación de las infraestructuras en la nube** en inicativas en el marco de la UE.

3. Estrategia de servicios en la nube híbrida para las AAPP

7 Pilares desarrollados mediante **19 iniciativas**:

eni Esquema Nacional de Interoperabilidad

ens Esquema Nacional de Seguridad

Pilar 1 Nube híbrida por diseño — 2

Pilar 2 Catálogo de Servicios creciente — 3

Pilar 3 Política de provision de Servicios en la nube híbrida primero — 2

Pilar 4 Soberanía del Dato — 2

Pilar 5 Orientación al Dato — 2

Pilar 6 Evolucionar los sistemas existentes hacia la nube — 2

Pilar 7 Nube Segura — 6

Pilar 4. Soberanía del Dato

i8 Desarrollar una guía para análisis de riesgos en entornos de Servicios en la nube alineada con ENS que contemple el marco legal español y europeo.

i9 Establecer criterios para contratación Centralizada de Servicios en la nube.

Desafío

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.

Pilar 4

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.

Pilar 7. Nube Segura

i14 Establecer criterios para distribución de cargas en la nube que contemple la seguridad en todos sus aspectos, incluyendo un análisis de riesgos específico para cada proveedor.

i15 Certificación de la conformidad con el ENS

i16 Promover las capacidades de ciberseguridad de AAPP, y mejora de sus capacidades de prevención, detección y respuesta ante incidentes de ciberseguridad.

i17 Promover la extension y evolución del COCS de la AGE 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 de desarrollo del ENS acerca de medidas que deben cumplir los sistemas de servicios en la nube.

NubeSARA certificado **ALTA**


AENOR

Certificado de Conformidad
con el Esquema Nacional de Seguridad

ENS-2024/0106

AENOR, certifica que los sistemas de información reseñados todos ellos de categoría ALTA y los servicios que se relacionan, de:

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

han sido auditados y encontrados conforme con las exigencias del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, según se indica en el correspondiente Informe de Auditoría de 2024-09-13

para las actividades: Los sistemas de información que soportan el servicio Cloud de NubeSARA de acuerdo a la categorización vigente a fecha del certificado

que se realizan en: Pº DE LA CASTELLANA, Nº 162. 28046 - MADRID

Certificación inicial: 2024-11-07 Válida hasta: 2026-11-07

Fecha: En Madrid a 7 de noviembre de 2024

Centro de Operaciones de Ciberseguridad

COCS Centro de Operaciones de Ciberseguridad EELL

Red Nacional de SOC

PNNSC

4. Nube Segura – ENS "Protección de servicios en la nube"

Esquema Nacional de Seguridad

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	
op.exp.7	Gestión de incidentes	Categoría	aplica	+ R1 + R2	+ R
op.exp.8	Registro de la actividad	T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R
op.exp.9	Registro de la gestión de incidentes	Categoría	aplica	aplica	
op.exp.10	Protección de claves criptográficas	Categoría	aplica	+ R1	
op.ext	Recursos externos				
op.ext.1	Contratación y acuerdos de nivel de servicio	Categoría	n.a.	aplica	
op.ext.2	Gestión diaria	Categoría	n.a.	aplica	
op.ext.3	Protección de la cadena de suministro	Categoría	n.a.	n.a.	
op.ext.4	Interconexión de sistemas	Categoría	n.a.	aplica	
op.nub	Servicios en la nube				
op.nub.1	Protección de servicios en la nube	Categoría	aplica	+ R1	
op.cont	Continuidad del servicio				
op.cont.1	Análisis de impacto	D	n.a.	aplica	
op.cont.2	Plan de continuidad	D	n.a.	n.a.	
op.cont.3	Pruebas periódicas	D	n.a.	n.a.	
op.cont.4	Medios alternativos	D	n.a.	n.a.	
op.mon	Monitorización del sistema				
op.mon.1	Detección de intrusión	Categoría	aplica	+ R1	
op.mon.2	Sistema de métricas	Categoría	aplica	+ R1 + R2	
op.mon.3	Vigilancia	Categoría	aplica	+ R1 + R2	+ R1 + R2

4.5 Servicios en la nube [op.nub].

4.5.1 Protección de servicios en la nube [op.nub.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

– [op.nub.1.1] Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten: Software como Servicio (*Software as a Service, SaaS*), Plataforma como Servicio (*Platform as a Service, PaaS*) e Infraestructura como Servicio (*Infrastructure as a Service, IaaS*) definidas en las guías CCN-STIC que sean de aplicación.

– [op.nub.1.2] Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información que los soportan deberán ser conformes con el ENS o cumplir con las medidas desarrolladas en una guía CCN-STIC que incluirá, entre otros, requisitos relativos a:

a) Auditoría de pruebas de penetración (*pentesting*).
b) Transparencia.
c) Cifrado y gestión de claves.
d) Jurisdicción de los datos.

Refuerzo R1- Servicios certificados.

– [op.nub.1.r1.1] Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.

– [op.nub.1.r1.2] Si el servicio en la nube es un servicio de seguridad deberá cumplir con los requisitos establecidos en [op.pl.5].

Refuerzo R2-Guías de Configuración de Seguridad Específicas.

– [op.nub.1.r2.1] La configuración de seguridad de los sistemas que proporcionan estos servicios deberá realizarse según la correspondiente guía CCN-STIC de Configuración de Seguridad Específica, orientadas tanto al usuario como al proveedor.

Aplicación de la medida.

– Categoría BÁSICA: op.nub.1.
– Categoría MEDIA: op.nub.1 + R1.
– Categoría ALTA: op.nub.1+ R1 + R2.

+ Perfiles de Cumplimiento Específicos

Preparado para el futuro **EUCS**

4. Nube Segura – SDA Normas comunes de seguridad - CPSTIC

Pliego de prescripciones técnicas que rige la celebración del Sistema Dinámico de Adquisición para el suministro de software de sistema, de desarrollo y de aplicación (SDA25/2022) 6 lotes, incluyendo Lote 4 – Software de ciberseguridad

NORMAS COMUNES A TODOS LOS LOTES:

CERTIFICACIÓN DE LA FUNCIONALIDAD DE SEGURIDAD DE LOS PROGRAMAS CONDICIONES GENERALES PARA EXIGIR LAS CERTIFICACIONES DE SEGURIDAD

- ✓ Que el sistema se encuentre bajo el alcance del ENS
- ✓ Declaración de Categoría Media o Alta, y de aplicación la medida [op.pl.5]
- ✓ Que la función de seguridad esté relacionada con el objeto de su adquisición, y la exigencia de certificación sea proporcionada a la categoría y el nivel de seguridad.

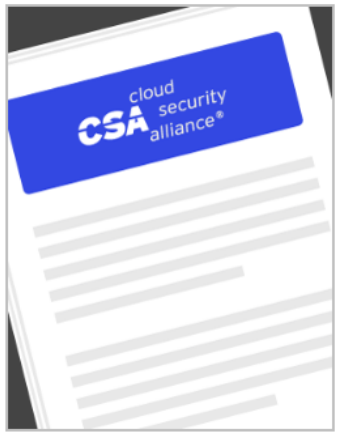
MEDIOS ADMISIBLES PARA ACREDITAR LA SEGURIDAD DE LOS PROGRAMAS EN INFRAESTRUCTURA LOCAL

- ✓ El programa está incluido en el **Catálogo CPSTIC**
- ✓ El programa está incluido en otro catálogo considerado equivalente por el CCN
- ✓ El programa tiene **certificada la funcionalidad de seguridad**, según los criterios y metodologías de evaluación reconocidas por el OC del CCN conforme al artículo 19.2 del ENS
- ✓ El producto tiene **certificada la funcionalidad de seguridad dentro del EUCC** o cualquier otro que sea aprobado por la Comisión Europea en virtud del artículo 49 del Reglamento (UE) 2019/881

III.2.3. MEDIOS ADMISIBLES PARA ACREDITAR LA SEGURIDAD DE LOS PROGRAMAS EN LA NUBE

- ✓ El programa tiene certificada la **conformidad con el ENS** al nivel y categoría del sistema de información
- ✓ El programa está incluido en el **Catálogo CPSTIC**
- ✓ El programa está incluido en otro catálogo considerado equivalente por el CCN
- ✓ El programa y la infraestructura de nube estén certificados de manera conjunta dentro del **EUCS** (European Cybersecurity Certification Scheme for Cloud Services) o cualquier otro que sea aprobado por la Comisión Europea en virtud del artículo 49 del Reglamento (UE) 2019/881.
- ✓ La certificación deberá extenderse al programa y a la infraestructura de nube sobre la que se ejecuta como un todo unitario.

4. Nube Segura – Correspondencia CCM v4.0 <-> ENS



CSA CCM v4.0 Addendum - Spain National Security Framework (ENS)

Release Date: 12/08/2022

This document is an addendum to the CCM V4.0 that contains controls mapping between the CSA CCM and Spain's National Security Framework (ENS).

The document aims to help ENS compliant organizations meet CCM requirements. This is achieved by identifying compliance gaps in ENS in relation to the CCM. This document contains the following information:

- Controls Mapping
- Gap Analysis
- Gap Identification (i.e., Partial, Full or No Gap)

ens Esquema Nacional de Seguridad

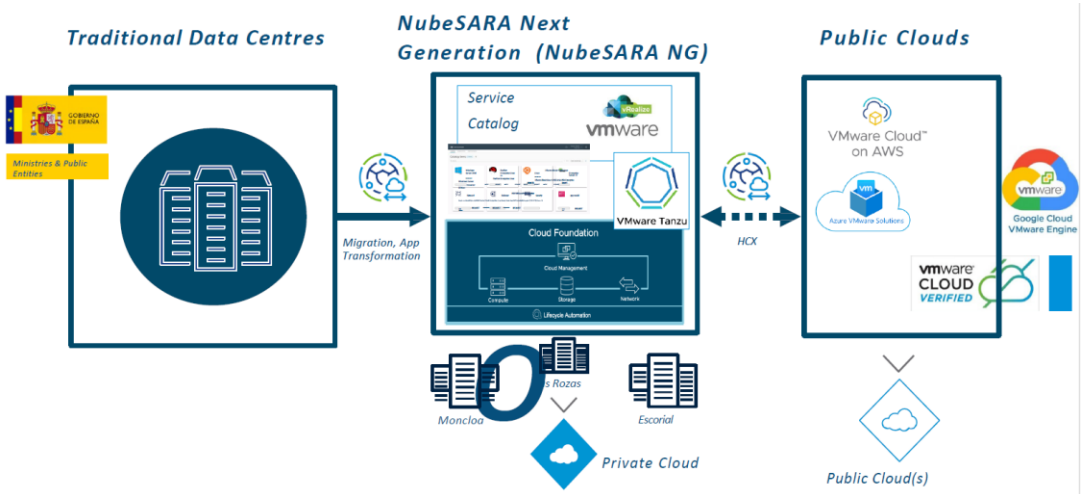
Objetivo: Facilitar el cumplimiento del ENS para los proveedores de Servicios cloud en España.

El capítulo español de la Cloud Security Alliance (CSA) ha creado la tabla de **correspondencia entre la Cloud Control Matrix v4.0 y el Esquema Nacional de Seguridad** para facilitar su aplicación en entornos en la nube.

La Cloud Control Matrix se alinea con las mejores prácticas de la Cloud Security Alliance (CSA) y se considera el estándar de facto para la seguridad en la nube.

5. Hoja de ruta de NubeSARA

NubeSARA Next Generation (NubeSARA NG)



- ✓ **30 centros usuarios de la AGE en 12 ministerios diferentes**, con más de 10.000 máquinas virtuales.
- ✓ **Conectando a los principales proveedores** de servicios en la nube
- ✓ **Movimiento fluido de máquinas virtuales** entre nubes privadas y públicas.
- ✓ **Recursos de nube pública** proporcionados por la AEAD.
- ✓ **Autonomía de la entidad** para utilizar la insfraestructura pública o privada.
- ✓ Datos no confidenciales, entorno de desarrollo, etc., en nube pública, entornos de producción y datos sensibles en nube privada.

SOCINFO sociedad de la información digital

Evento “Estrategia Nacional de Servicios Públicos en la Nube de las AAPP”

Muchas gracias

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU
España | digital 2026