

¿Qué es la Soberanía en la Nube?

La Comisión Europea ha definido un marco de soberanía en la nube para asegurarse de que los servicios cloud utilizados en la UE están alineados con sus prioridades legales, estratégicas y de seguridad.

En los pliegos de contratación, este marco se usa para:

- Fijar niveles mínimos de garantía de soberanía que un proveedor debe alcanzar.
- Evaluar la efectividad de cada proveedor en distintos aspectos (datos, operaciones, tecnología, seguridad, etc.).



Evaluación de la Efectividad de la Soberanía

SOV-1 Soberanía estratégica

Mide hasta qué punto los servicios del proveedor están anclados en el ecosistema legal, financiero e industrial de la UE y alineados con sus prioridades.

SOV-3 Soberanía de datos y de IA

Determina si los datos y los sistemas de IA permanecen bajo control exclusivo del cliente y de entidades de la UE, incluyendo almacenamiento, procesamiento, cifrado, auditoría y gobernanza de modelos.

SOV-5 Soberanía de la cadena de suministro

Evaluá el origen y control del hardware, firmware, software y proveedores implicados, asegurando visibilidad completa y minimizando dependencias de componentes o actores no-UE.

SOV-7 Soberanía de seguridad y cumplimiento

Verifica si la seguridad, el cumplimiento normativo y las operaciones críticas (como SOC y respuesta a incidentes) se ejecutan dentro de la UE, bajo su jurisdicción y con controles verificables.

SOV-2 Soberanía legal y jurisdiccional

Analiza qué marco legal rige al proveedor y en qué medida está expuesto a la legislación de terceros países, especialmente leyes extraterritoriales que podrían afectar datos o servicios dentro de la UE.

SOV-4 Soberanía operativa

Mide la capacidad del cliente para operar, mantener y migrar servicios sin depender de proveedores no-UE, garantizando continuidad, autonomía, soporte local y ausencia de vendor lock-in.

SOV-6 Soberanía tecnológica

Examina el grado de transparencia, apertura e interoperabilidad del servicio tecnológico, así como la capacidad de la UE para entenderlo, auditarlo, modificarlo y sostenerlo sin restricciones externas.

SOV-8 Sostenibilidad ambiental

Evaluá si la infraestructura y operaciones cloud del proveedor siguen principios de eficiencia energética, uso de energías limpias y economía circular, con métricas verificables y compromiso a largo plazo.

Marco de Soberanía en la Nube

de la Comisión Europea

isms
FORUM

¿Cómo usar este marco en la práctica?



Define requisitos mínimos de soberanía (SEAL) en sus licitaciones.

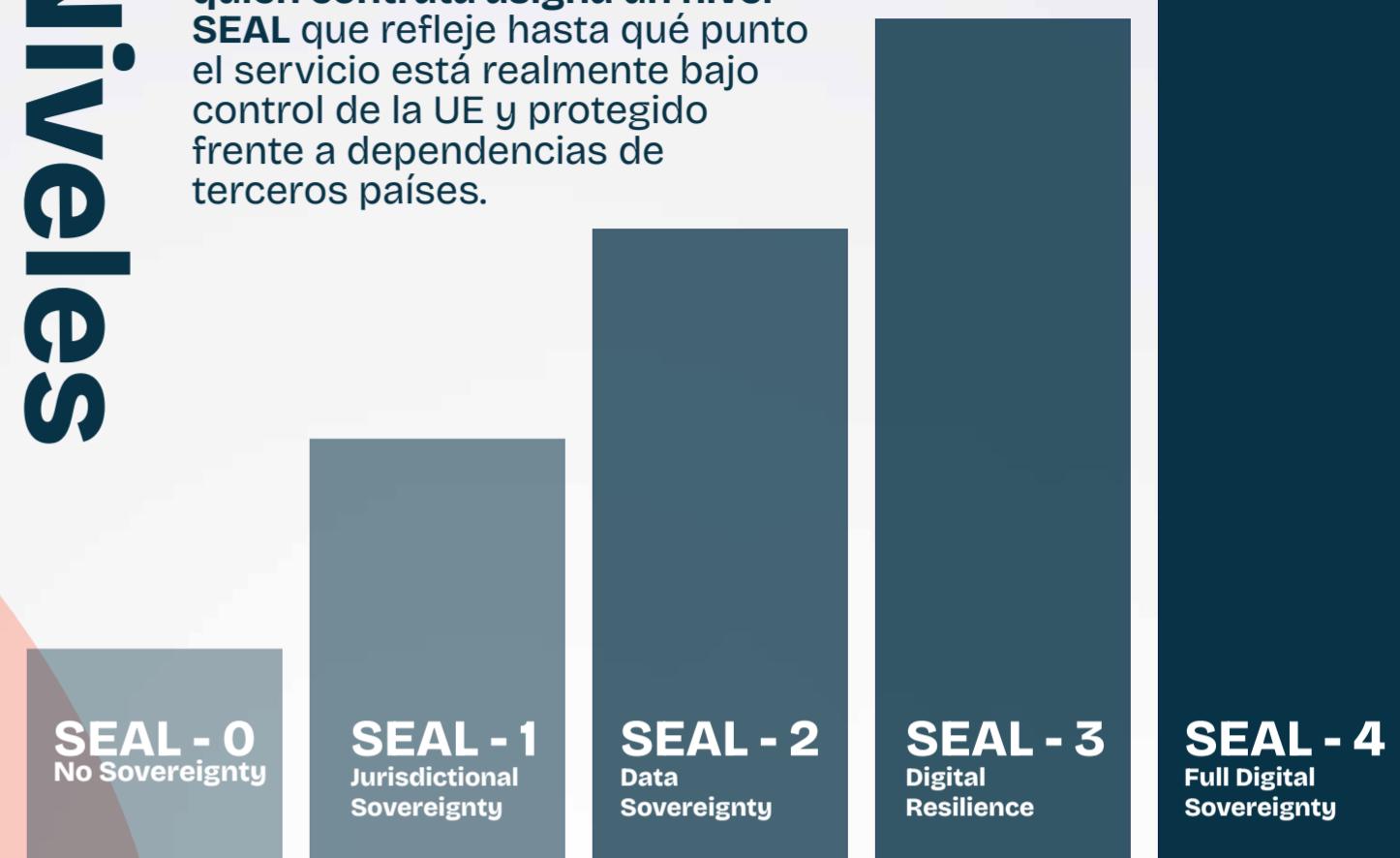


Analiza de forma estructurada riesgos legales, operativos, tecnológicos y de datos asociados a proveedores cloud.

Toma decisiones informadas sobre qué tipo de sistemas o datos pueden desplegarse en cada proveedor, según el nivel de garantía que ofrece.

Niveles

Para cada dimensión de soberanía, quien contrata asigna un nivel SEAL que refleje hasta qué punto el servicio está realmente bajo control de la UE y protegido frente a dependencias de terceros países.



Descripción detallada de los niveles de soberanía:

- SEAL - 0 No Sovereignty:** Servicio, tecnología u operaciones bajo control exclusivo de terceros no-UE, gobernados íntegramente en jurisdicciones no europeas.
- SEAL - 1 Jurisdictional Sovereignty:** El Derecho de la UE se aplica formalmente, pero con limitada capacidad de ejecución práctica.
- SEAL - 2 Data Sovereignty:** El Derecho de la UE es aplicable y ejecutable, pero permanecen dependencias materiales no-UE.
- SEAL - 3 Digital Resilience:** El Derecho de la UE es aplicable y ejecutable, y actores de la UE ejercen una influencia significativa pero no plena.
- SEAL - 4 Full Digital Sovereignty:** Tecnología y operaciones bajo control completo de la UE, sujetas exclusivamente al Derecho de la UE, sin dependencias críticas de terceros no-UE.

isms
FORUM