

PARA CISO, DPO Y RESPONSABLES DE CUMPLIMIENTO

La soberanía de los datos es arquitectura, no una cláusula contractual

Sus datos. Su jurisdicción. Su control.

El reto

España se ha convertido en uno de los mercados de soberanía de datos más vigilados de Europa. En febrero de 2026, la Agencia Española de Protección de Datos (AEPD) emitió recomendaciones formales sobre soberanía de datos tras analizar una interrupción global de servicios en la nube ocurrida en octubre de 2025, causada por un fallo técnico originado en Estados Unidos que afectó a servicios en España. La conclusión de la AEPD replanteó el debate de cumplimiento: incluso cuando los datos personales se almacenan dentro de la UE, una organización puede arrastrar un riesgo de cumplimiento pasado por alto si la infraestructura de procesamiento, las funciones de soporte o el plano de control que operan sobre esos datos se encuentran fuera del Espacio Económico Europeo. El regulador traza ahora una línea explícita entre la soberanía de los datos –el control sobre dónde residen los datos y quién puede acceder a ellos– y la soberanía operativa –la capacidad de mantener los servicios en funcionamiento cuando la infraestructura que los sustenta está controlada desde el extranjero–. En la práctica, se está diciendo a las organizaciones españolas que la residencia de los datos en la UE es necesaria, pero no suficiente.

Esta señal regulatoria coincide con la hoja de ruta nacional de soberanía digital de España, «Acelerar la Soberanía Digital en España», aprobada por el Consejo de Ministros el 24 de febrero de 2026, y con el papel activo de España en la consulta pública de la Ley de Desarrollo de la Nube y la IA de la UE (CADA), cerrada en julio de 2026. La hoja de ruta parte de un diagnóstico contundente –más del 80% de los servicios en la nube y el 90% de los datos europeos están controlados por empresas estadounidenses– y respalda explícitamente una «nube soberana europea» para proteger los datos europeos sensibles frente a leyes extraterritoriales extranjeras. Bajo la LOPDGDD y el RGPD, las promesas contractuales y los centros de datos ubicados en el país ya no responden, por sí solos, a la pregunta que los reguladores españoles plantean ahora: ¿puede demostrar, de forma arquitectónica, dónde residen sus datos, qué impide que salgan y quién controla la infraestructura que los procesa?

La solución

Kiteworks ofrece la soberanía de los datos como arquitectura, no como una cláusula contractual, respondiendo directamente a la distinción de soberanía operativa planteada por la AEPD. Despliegue la solución en infraestructura de un solo inquilino (single-tenant), on-premises, en su propia nube o como nube privada alojada por Kiteworks, en España o en la jurisdicción que elija, cifrada con claves que solo usted posee. Dado que Kiteworks nunca conserva sus claves de cifrado ni comparte infraestructura entre clientes, la capa operativa que preocupa a la AEPD –los procesos y funciones de soporte con control de continuidad– permanece bajo su control, y no bajo el de un proveedor con sede en el extranjero.

Gobierne cada envío, cada uso compartido y cada descarga mediante las reglas de geolocalización del Data Policy Engine, aplicadas en tiempo real en todos los canales. Demuéstrelo con un registro de auditoría completo y sin limitaciones, transmitido en vivo a su SIEM, respaldado por opciones de alojamiento evaluadas conforme a FedRAMP e IRAP: evidencia que responde a la AEPD y a la hoja de ruta nacional de España en sus propios términos.

Por qué la soberanía es ahora una cuestión de consejo de administración en España

33%	de las organizaciones sufrieron un incidente de soberanía en el último año.
6.110 M€	en multas acumuladas por incumplimiento del RGPD en toda la UE.
57%	de las pymes europeas no está seguro de si sus datos se almacenan exclusivamente en la UE.
Feb. 2026	La AEPD emite sus primeras recomendaciones formales sobre soberanía de datos, tras una interrupción de servicios en la nube de origen estadounidense que afectó a España.

Cómo Kiteworks ofrece una soberanía que usted puede demostrar

■ Arquitectura de un solo inquilino por diseño

Infraestructura dedicada, sin bases de datos, sistemas de archivos, entornos de ejecución de aplicaciones ni sistemas operativos compartidos. Despliegue on-premises, en su propia nube o como nube privada de un solo inquilino alojada por Kiteworks, en España o en la jurisdicción que elija, abordando la preocupación de soberanía operativa de la AEPD, no solo la residencia de los datos.

■ Claves de cifrado propiedad del cliente

Con integración de HSM, ni Kiteworks ni ninguna parte que obligue a Kiteworks a actuar puede descifrar sus datos, incluida una autoridad extranjera que curse una orden de cumplimiento sobre infraestructura ubicada fuera del EEE.

■ Control de salida por geolocalización (geo-fencing)

El Data Policy Engine bloquea o exige aprobación para envíos y comparticiones, y puede bloquear descargas por completo, según la geolocalización del usuario, países bloqueados y rangos de IP: una respuesta práctica a hacia dónde pueden dirigirse los datos españoles y europeos.

■ Un único plano de control para todos los canales

El correo electrónico, el uso compartido de archivos, SFTP, MFT, las API y los agentes de IA están gobernados por las mismas políticas de salida, de modo que no existen brechas por canal a través de las cuales puedan escapar los datos.

■ Registro de auditoría completo y sin limitaciones

Cada acción de usuarios, administradores y sistemas se registra en tiempo real y se transmite en vivo a su SIEM, sin muestreo ni limitación bajo carga: el registro probatorio que las inspecciones de la AEPD exigen cada vez más.

■ Evaluada conforme a estándares gubernamentales

FedRAMP High en proceso, FedRAMP Moderate autorizado desde 2017, y alojamiento evaluado conforme a IRAP demuestran que la arquitectura cumple con los requisitos de soberanía de nivel gubernamental, a medida que la propia estrategia de nube de la administración pública española evoluciona hacia un modelo de soberanía híbrida.

Dónde la soberanía no es negociable en España



Administración pública y sector gobierno

Datos de la ciudadanía bajo el programa de Infraestructura Digital Pública de España (Cl@ve, DNle, cartera de identidad digital) y mandatos de contratación pública que favorecen un control demostrable dentro de la jurisdicción, a medida que la estrategia nacional de nube avanza hacia un modelo de soberanía híbrida.



Defensa e infraestructuras críticas

Datos técnicos y operativos regidos por las instituciones españolas de ciberseguridad (CCN-CERT, INCIBE) y por las nuevas normas de la UE en el marco de la Ley de Desarrollo de la Nube y la IA (CADA), que está remodelando los requisitos nacionales de contratación pública y alojamiento.



Servicios financieros

Datos de clientes sujetos al Reglamento de Resiliencia Operativa Digital (DORA) de la UE y a la supervisión de la AEPD.



Sanidad y ciencias de la vida

Datos de pacientes protegidos por el RGPD y por la normativa nacional de datos de salud derivada de la LOPDGDD, además de datos de investigación sujetos a condiciones de residencia.

Copyright © 2026 Kiteworks. La misión de Kiteworks es capacitar a las organizaciones para gestionar eficazmente el riesgo en cada envío, compartición, recepción y uso de datos privados. La plataforma Kiteworks ofrece a los clientes un intercambio seguro de datos que proporciona gobernanza, cumplimiento y protección de datos en un plano de control unificado. Kiteworks unifica, rastrea, controla y protege los datos sensibles que se mueven dentro, hacia y fuera de su organización, mejorando de forma significativa la gestión de riesgos y garantizando el cumplimiento normativo en todos los intercambios de datos privados. Con sede en Silicon Valley, Kiteworks protege a más de 100 millones de usuarios finales y a miles de empresas y organismos gubernamentales de todo el mundo.