



evolutio

Empowering secure AI

OpenShift

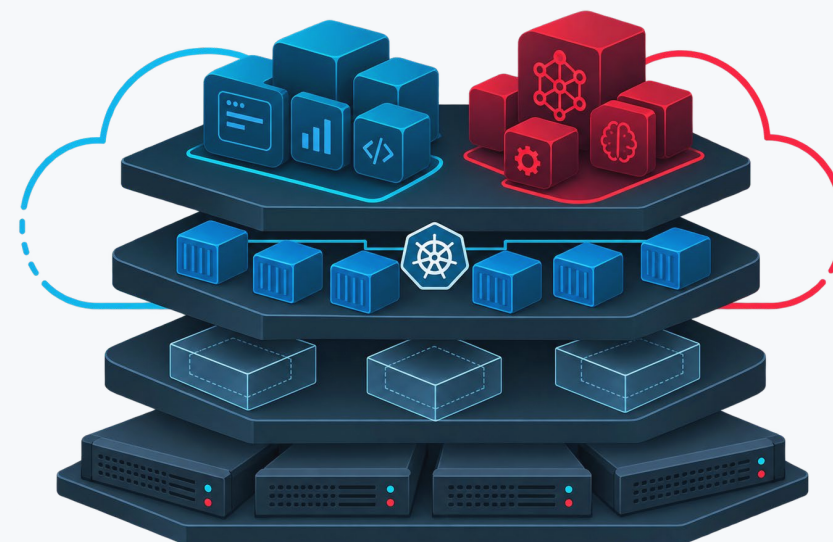
Soberanía e IA
sobre una plataforma abierta

Red Hat Summit 2026 · Madrid

Soberanía e inteligencia artificial sobre una plataforma abierta

Rafael Antonio García Jiménez

Principal Senior Consultant en Soluciones Red Hat
Evolutio Cloud Enabler S.A.U.
rafaelantonio.garcia@evolutio.com



Agenda

Del marco de soberanía a una arquitectura OpenShift para IA

- 01 **Soberanía digital**
Datos, tecnología, operación y garantía.
- 02 **Inteligencia artificial soberana**
Modelos, datos, infraestructura y control económico.
- 03 **Iniciativas de Red Hat**
Portfolio, assessment, regulación, innovación y sostenibilidad.
- 04 **Arquitectura propuesta**
OpenShift Platform Plus, AI, GitOps, Compliance y Zero Trust.
- 05 **Conclusiones**
Soberanía por diseño, desde el metal hasta el agente de IA.



La soberanía digital exige control verificable

No basta con alojar datos dentro de una frontera.

Capacidad de una organización para controlar sus activos digitales, decidir dónde residen sus datos, cómo funcionan sus sistemas y quién tiene acceso a ellos.

Soberanía de los datos

Residencia, localización, gobernanza, protección y privacidad.

Soberanía tecnológica

Evitar la dependencia de un único proveedor y conservar libertad de elección.

Soberanía operativa

Control sobre estándares, normas, diseño, transparencia y auditabilidad.

Garantía de soberanía

Verificar integridad, seguridad y fiabilidad para proteger la continuidad.



Nube soberana: tres capas de control

Residencia, cumplimiento y operación local o regional.

a) Dónde residen y cómo se mueven los datos

Cumplimiento de residencia, localización y movilidad regulada.

b) Qué jurisdicción legal aplica

Normativa, entidad responsable y límites de acceso externo.

c) Quién opera la infraestructura

Personal, procedimientos y control administrativo local/regional.

Las tensiones geopolíticas están impulsando la demanda de servicios de nube soberana. Cada vez más se exigirá proteger datos, infraestructura y cargas críticas del control de jurisdicciones externas y del acceso de gobiernos extranjeros. Gartner predice que más del 50% de las organizaciones multinacionales tendrán estrategias de soberanía digital para 2029.

IA soberana: control sobre datos, modelos e infraestructura

La soberanía entra en todo el ciclo de vida de IA: entrenamiento, ajuste, inferencia y operación.

Trata de poseer o controlar la infraestructura —desde GPU hasta servidores de inferencia— para mantener independencia tecnológica, datos en propiedad y cumplimiento local/regional.

Datos

Datos sensibles de entrenamiento, ajuste fino e inferencia bajo leyes locales.

Modelos

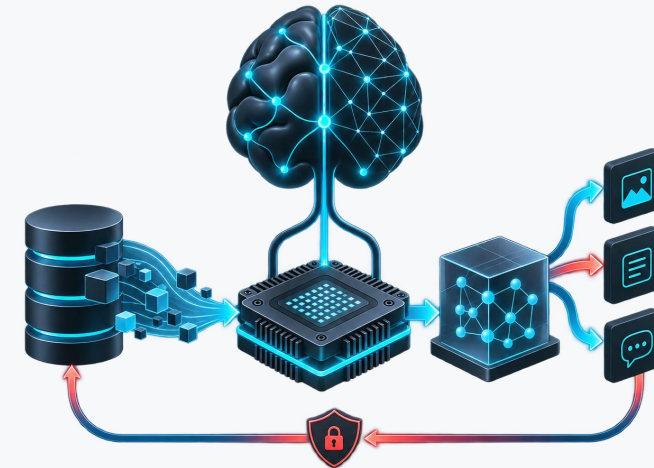
Libertad para construir, entrenar y ajustar modelos según contexto cultural y lingüístico.

Infraestructura

Ejecución local/regional en nube privada, pública, multinube, híbrida o edge.

Operativa y económica

Gestión por personal acreditado y estructura financiera más controlada.



Dos fuerzas empujan la arquitectura hacia el control

Adopción de IA y soberanía digital pasan de discusión a diseño.

a) Aceleración de la adopción de IA

La demanda crece por la presión de pasar de experimentos aislados a operaciones centrales. Los clientes buscan productividad medible y plataformas con control y elección durante todo el ciclo de vida de IA a escala empresarial.

b) Auge de la soberanía digital

La residencia de datos, la autonomía tecnológica y la resiliencia de la cadena de suministro obligan a reevaluar nube, repatriar cargas críticas y priorizar soluciones con control operativo.



De experimentos aislados a producción integrada

Control y capacidad de elección en arquitectura, despliegue, modelos, hardware y nube.



Objetivo estratégico: acelerar la adopción de IA con una plataforma abierta, flexible y portátil para cargas empresariales, evitando la dependencia exclusiva de un proveedor de modelos, hardware o nube.

Red Hat OpenShift + OpenShift AI

Base para crear, desplegar y gestionar modelos de IA y flujos de trabajo basados en agentes.

Red Hat AI Inference Server

Despliegues soberanos y autogestionados con herramientas open source nativas de contenedores, orquestación de GPU y multitenancy.

vLLM, llm-d y Hugging Face

Inferencia distribuida, escalable y eficiente, con acceso integrado a modelos abiertos.

Assessment de soberanía: medir antes de diseñar

Red Hat Digital Sovereignty Readiness Assessment sitúa la madurez por dominios.

● Datos: Control físico y jurisdiccional de los datos durante todo el ciclo de vida.

● Técnica: Composición de la pila de software subyacente.

● Operativa: Capacidad de mantener y recuperar sistemas sin dependencia externa.

● Garantía: Auditar y validar de forma independiente la integridad de los sistemas.

● Código abierto: Innovación impulsada por comunidad para reducir bloqueo de proveedores.

● Supervisión ejecutiva: Alineación de objetivos de soberanía con la gobernanza de liderazgo.

● Servicios gestionados: Flexibilidad de despliegue en regiones y centros de datos específicos.



Regulación, innovación y sostenibilidad

Tres ángulos que condicionan la IA empresarial soberana.

Regulación

Red Hat colabora con responsables de políticas para aportar comentarios y buscar legislación práctica que no perjudique involuntariamente al ecosistema de código abierto.

Innovación

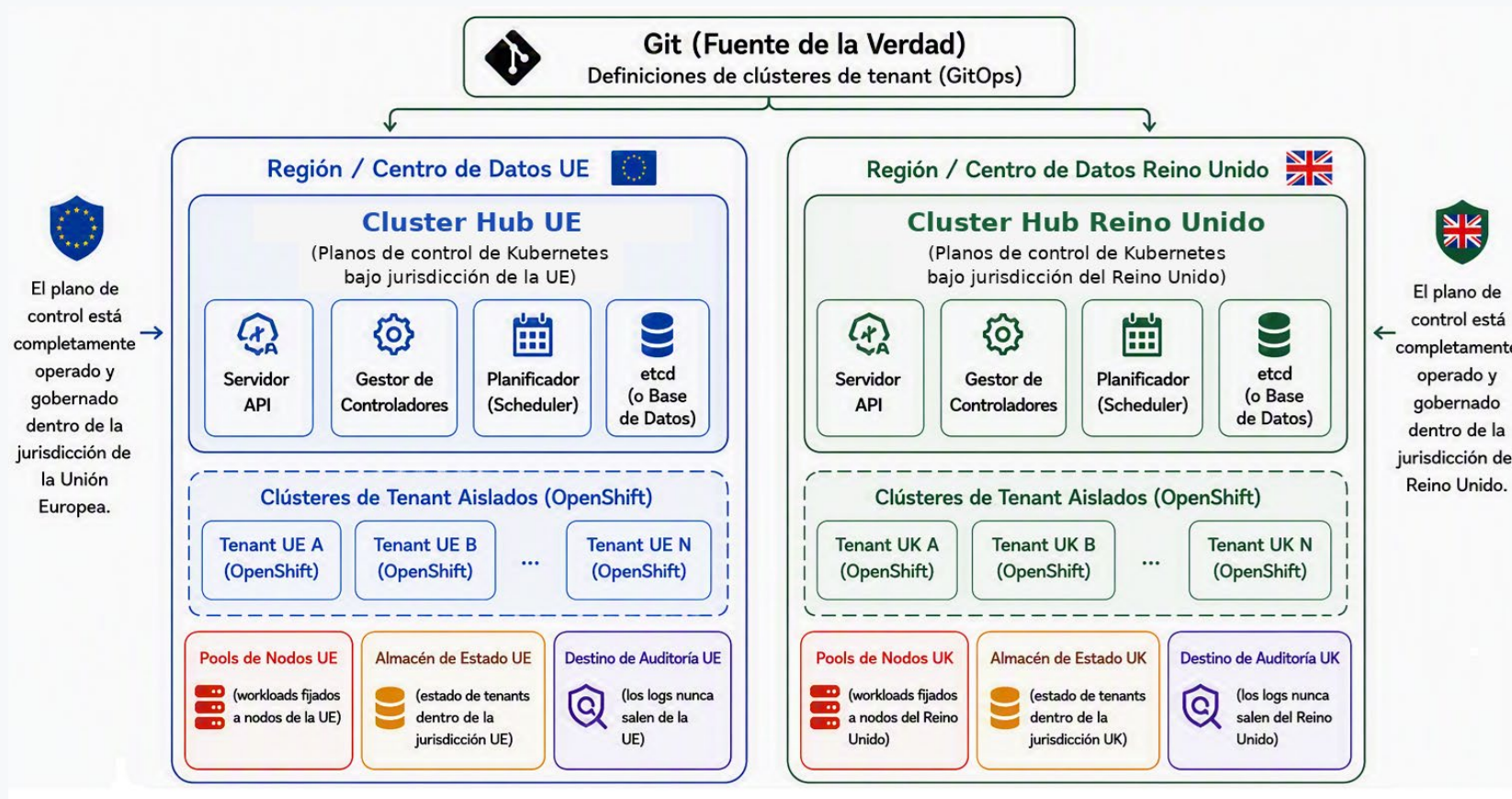
La adquisición de Neural Magic mejora capacidades de aceleración y optimización de inferencia, permitiendo ejecución de modelos más eficiente.

Sostenibilidad

El consumo energético de las GPU impacta licitaciones y costes. Técnicas como cuantización y compresión reducen tamaño de LLM, consumo y coste.

Arquitectura propuesta

Dos dominios soberanos, una fuente de verdad y control independiente por jurisdicción.



Fuente de la verdad: GitOps

Cada región mantiene plano de control, tenants, estado y auditoría dentro de su jurisdicción.

Base de plataforma y control

Componentes usados para desplegar, gestionar y aislar clústeres.

a) Red Hat OpenShift Platform Plus

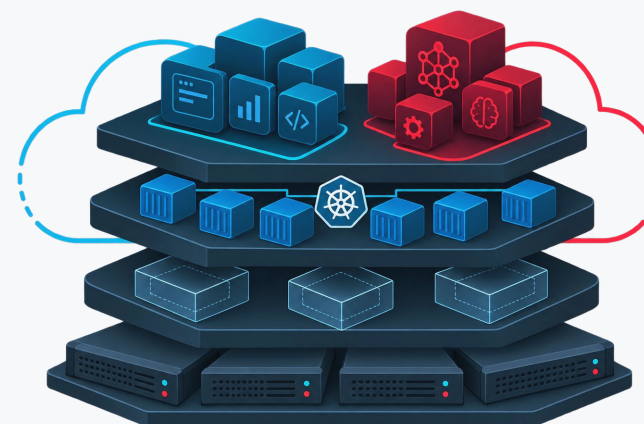
Plataforma para desplegar y gestionar el ciclo de vida de clústeres hub y gestionados, así como el sustrato de cómputo de IA. Incluye RHACM, RHACS y OpenShift Data Foundation en el clúster de gestión.

b) Red Hat OpenShift Virtualization

Proporciona la tecnología de virtualización para nodos.

c) RHACM con Hosted Control Planes

Despliega el clúster hub en cada región UE/UK y aporta aislamiento multi-tenant. Cada tenant recibe un servidor API dedicado de Kubernetes vía HyperShift Hosted Control Planes.



d) RHEL y CoreOS

Base fiable del sistema operativo: módulos criptográficos validados FIPS 140-2/3, SELinux, soporte de hardware y operación empresarial.

Base de plataforma y control

Componentes usados para desplegar, gestionar y aislar clústeres.

e) Red Hat AI Enterprise

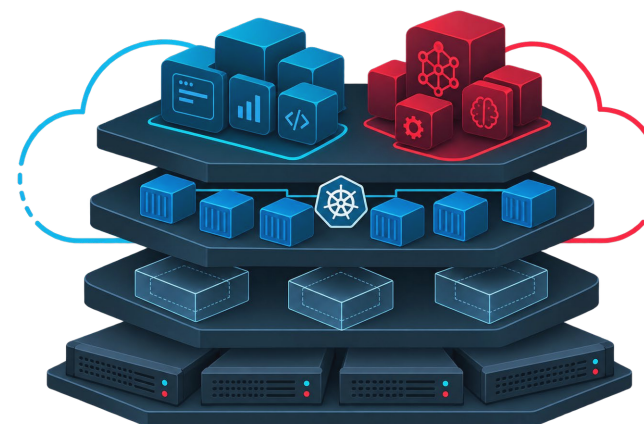
Base para construir, desarrollar y desplegar aplicaciones IA en nube híbrida. Aporta inferencia con vLLM y LLM-d, catálogo/registro de modelos validados y gestión del ciclo de vida del modelo en plataformas GPU.

f) Red Hat OpenShift GitOps 1.19

Despliegue automatizado y gestión de configuración

g) Red Hat Compliance Operator

Escaneo continuo de configuraciones OpenShift con perfiles CIS mapeados a controles regulatorios, generando pruebas de auditoría para auditores.



h) Workload Identity Manager, Trustee y Sandboxed Containers

Características para conceptos de Zero Trust y computación confidencial.

Soberanía por diseño

La decisión arquitectónica afecta a toda la pila, desde el hardware hasta el agente de IA.

- **Control de pila completa**
Hardware, datos, modelos y aplicaciones: quién los posee, quién los opera y quién accede.
- **Diseño, no adaptación**
La soberanía se evalúa desde el principio en datos, operaciones y tecnología.
- **Open source como palanca**
Soluciones abiertas desde el metal hasta el agente de IA ayudan a mantener control y capacidad de elección.
- **Fronteras locales/regionales**
El objetivo arquitectónico es mantener la pila completa dentro de los límites requeridos allí donde se presta el servicio.



Fuentes utilizadas

Anexo con los enlaces completos, manteniendo intactas las slides de contenido

Soberanía digital

- Red Hat — Digital sovereignty
<https://www.redhat.com/en/topics/ai/digital-sovereignty>
- Gartner — Top trends shaping the future of Cloud
<https://www.gartner.com/en/newsroom/press-releases/2025-05-13-gartner-identifies-top-trends-shaping-the-future-of-cloud>

IA soberana

- Red Hat — Sovereign AI
<https://www.redhat.com/en/topics/ai/sovereign-ai>
- Red Hat — Blueprint for sovereign AI
<https://www.redhat.com/en/resources/blueprint-sovereign-ai-ebook>
- Red Hat / IDC — Shaping sovereignty modernization
<https://www.redhat.com/en/engage/idc-shaping-sovereignty-modernization-analyst-material>

Readiness assessment

- Red Hat — Sovereignty Readiness Assessment
<http://redhat.com/sovereigntyassessment>
- Red Hat blog — How sovereign is your strategy
<https://www.redhat.com/en/blog/how-sovereign-your-strategy-introducing-red-hat-sovereignty-readiness-assessment-tool>

Arquitectura y diseño

- CNCF — Architectural patterns for cloud-native platforms
<https://www.cncf.io/blog/2026/06/16/from-data-residency-to-digital-sovereignty-architectural-patterns-for-cloud-native-platforms/>
- Red Hat Architecture — Cloud sovereignty
<https://www.redhat.com/architect/portfolio/detail/131-cloud-sovereignty>
- Red Hat Summit — Sovereign by design lessons
<https://www.redhat.com/en/blog/sovereign-design-lessons-red-hat-summit>





evolutio

Empowering secure AI

Gracias

OpenShift · Soberanía e IA sobre una plataforma abierta