



Connect

Genesis Agent Platform

La plataforma agéntica soberana

Juan Pablo Lázaró

Head of Cloud Discipline Spain

Sopra Steria España

Yoann Yvon

Head of Emerging Technologies,
Simulation and AI

Sopra Steria España

sopra  steria



IA en la empresa 2026: los grandes retos

Dos ejes clave para una adopción responsable y sostenible

01 Soberanía

Dependencia tecnológica: la mayoría de los modelos y la infraestructura crítica siguen en manos de un puñado de proveedores extranjeros (EE. UU., China).

Soberanía del dato: ¿dónde se alojan y procesan los datos sensibles? Existe riesgo de exposición a legislaciones extraterritoriales como el Cloud Act.

Marco regulatorio europeo: cumplir el AI Act y el RGPD es una condición de confianza, no un freno.

Alternativas soberanas: el auge de actores europeos impulsa la independencia estratégica.

02 Control (y especialmente el TCO)

Coste total de propiedad (TCO): licencias, cómputo (GPU e inferencia), integración, mantenimiento y formación forman un presupuesto a menudo subestimado.

Shadow AI: uso no autorizado de herramientas de IA por los equipos, fuera del control de seguridad y gobernanza.

Gobernanza y trazabilidad: definir quién accede a qué modelo, con qué datos y con qué nivel de supervisión.

Medición del ROI: pasar de la experimentación a un valor de negocio demostrable y controlado.

¿Qué es una plataforma agéntica?

No es un chatbot. Es el sustrato que ejecuta agentes con mando humano

Soberana

Corre en tu Kubernetes, sin lock-in. El dato y el modelo no tienen que salir para obtener una respuesta.

Human-in-command

Ninguna escritura con consecuencias sin un humano nominado. El debate produce datos, nunca una acción.

Un solo plano de salida

Modelos, herramientas MCP y pares se alcanzan solo por el gateway, autorizados llamada a llamada.

Cumplimiento como propiedad

Identidad, política y evidencia WORM van con cada paso, no en una diapositiva aparte.

Abierta y operable

Open source, GitOps, GPU NVIDIA en el continente y confidential computing cuando la carga lo exige.

Agent First sin plataforma

Seis modos de fallo que aparecen al pasar de piloto a producción. Ninguno es hipotético.

01

Agentes en la sombra

Construidos fuera de cualquier inventario. Nadie puede listar qué está actuando sobre el negocio hoy.

02

Acciones sin mando

Un agente escribe, paga o divulga sin una puerta de aprobación humana en el camino.

03

Prompt injection y fuga

Herramientas y modelos expuestos a entradas no confiables, sin un gateway que inspeccione lo que sale.

04

Lock-in de modelo

Un proveedor cableado en cada agente: coste, disponibilidad y jurisdicción de un solo contrato.

05

Sin evidencia

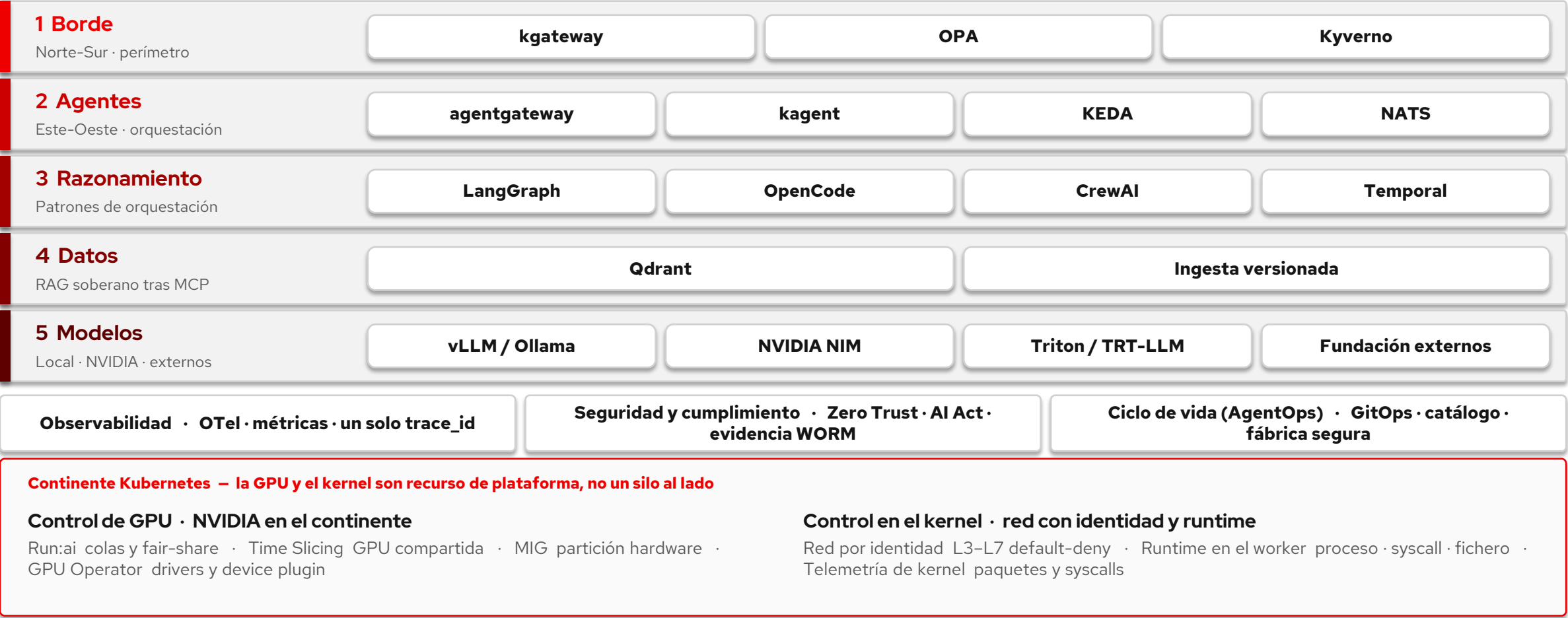
No hay registro inmutable de qué hizo un agente y por qué. La auditoría empieza de cero.

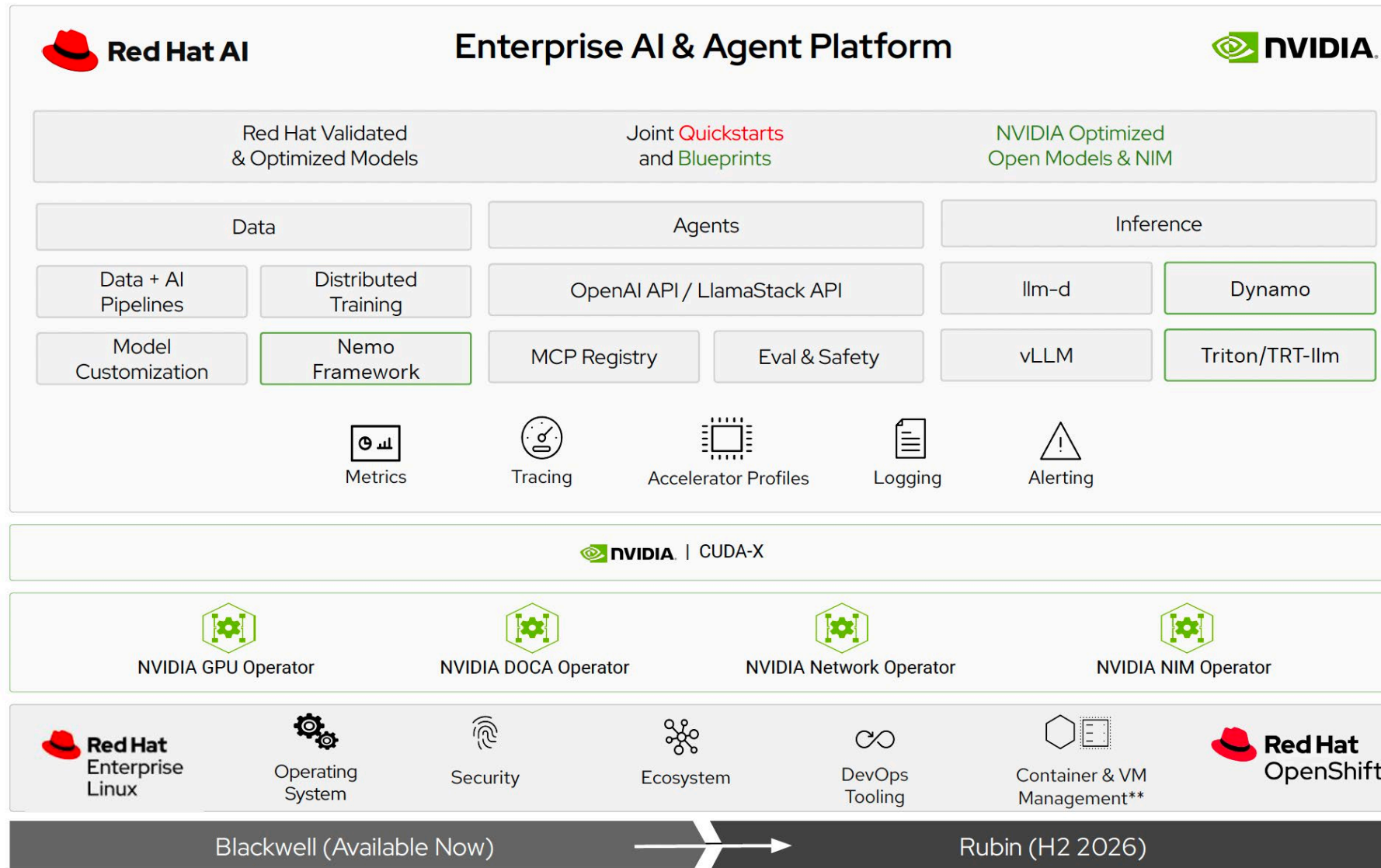
06

Deriva regulatoria

AI Act, DORA y NIS2 se mueven; el gobierno interno no. El cumplimiento se vuelve una reconstrucción.

Por capas, sobre un continente Kubernetes





La prueba, no la promesa

Cuatro mecanismos que corren en cada llamada, la mire o no una persona.

01

Registro y ciclo de vida

Ningún agente corre sin contrato en AgentRegistry. kagent lo provisiona; si no está registrado, no existe.

02

Política por llamada

OPA deniega modelos no aprobados, herramientas fuera de alcance, pares A2A no autorizados y escrituras sin aprobación.

03

Human-in-Command

Las acciones con consecuencias exigen un token de aprobación humana. El debate produce datos; nunca una acción.

04

Evidencia inmutable

Cada decisión –tomada o denegada– se escribe en un registro WORM. No se puede reescribir la historia.

IA confidencial de extremo a extremo

Protección verificable de datos, modelos y cargas desde el datacenter hasta el edge.

ARQUITECTURA HIGH-LEVEL



CASOS DE USO PRIORITARIOS

- 01 IA y propiedad intelectual**
Protección de pesos, algoritmos, prompts y RAG sensible.
 - 02 Edge y OT no confiables**
Ejecución segura en fábricas, sedes remotas y equipos expuestos.
 - 03 Colaboración con terceros**
Procesamiento de datos sensibles sobre infraestructura compartida.
 - 04 Cargas reguladas o clasificadas**
Aislamiento reforzado y evidencia criptográfica para auditoría.
- Mensaje clave · El TEE protege la ejecución. En Genesis se suma a identidad, supply chain, policy-as-code y control en el kernel – seguridad completa, no un recinto aislado.

El control no se delega

Tres fuerzas convergen en 2026. La soberanía deja de ser ideología y pasa a ser requisito.

CLOUD Act

Una ley extraterritorial alcanza datos alojados en Europa. El país del datacenter no es el control del dato.

AI Act

El «confía en nosotros» se convierte en obligación documental y de control. Hay que demostrarlo, no afirmarlo.

Contratación pública

La UE empieza a puntuar quién controla la plataforma y el dato, no quién vende la licencia.

La soberanía deja de ser una postura y pasa a ser un requisito de contratación y auditoría. Genesis pone GPU, modelo y TEE en el mismo continente Kubernetes – el control no se delega.

De los retos a la respuesta: la soberanía se demuestra, no se promete

Genesis Agent Platform convierte cada reto de 2026 en una propiedad operativa de la plataforma, no en un esfuerzo adicional.

01 SOBERANÍA – RETO → RESPUESTA

Dependencia tecnológica → Corre en tu Kubernetes, sin lock-in: modelos, GPU NVIDIA y datos permanecen en el mismo continente.

Soberanía del dato → El dato y el modelo no tienen que salir para obtener una respuesta; IA confidencial (TEE) de extremo a extremo cuando la carga lo exige.

Marco regulatorio (AI Act, RGPD) → Cumplimiento como propiedad: identidad, política y evidencia WORM viajan con cada paso, no en una diapositiva aparte.

Alternativas soberanas → Plataforma abierta y operable (open source, GitOps), sin depender de un único proveedor extranjero.

02 CONTROL Y TCO – RETO → RESPUESTA

Shadow AI → AgentRegistry: ningún agente corre sin contrato. Si no está registrado, no existe.

Gobernanza y trazabilidad → Human-in-Command: ninguna escritura con consecuencias sin aprobación humana nominada; el debate produce datos, nunca una acción directa.

TCO subestimado → Control de GPU (Run:ai, time slicing, MIG) y un solo plano de salida: el coste se dimensiona desde el diseño, no se descubre después.

Medición del ROI → Evidencia inmutable de cada decisión: la auditoría no empieza de cero, empieza con la prueba.

La plataforma, en el corazón de la estrategia empresarial.

El alineamiento regulatorio y sectorial, en su ADN.

El control, el TCO optimizado y una visión clara del valor de la IA como driver de diseño: una plataforma adaptable al cambio.

CONTINUAMOS EN EL STAND – Podemos contrastar juntos qué reto pesa más en tu caso de negocio y el enfoque de implantación más adecuado.



Connect

Muchas gracias

Te esperamos en nuestro stand



linkedin.com/company/red-hat



facebook.com/redhatinc



youtube.com/user/RedHatVideos



x.com/RedHat

sopra  steria



Red Hat