Mayo de 2026

# Informe global de IA 2026: Playbook para la IA privada y soberana

## Cómo las organizaciones están diseñando la IA con foco en la confianza, el control y la resiliencia

Ignite tomorrow today.

# Índice

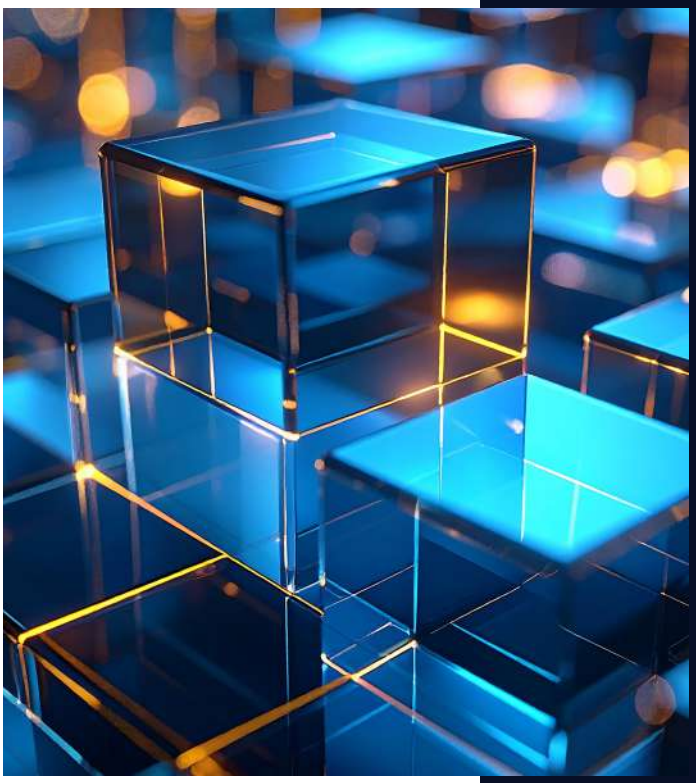
# Resumen ejecutivo

A medida que expanden su uso de la IA, las organizaciones se topan con nuevas limitaciones. Algunas son internas, como el hecho de que la IA deba ejecutarse en **entornos privados** para garantizar el control, la seguridad y el rendimiento. Otras son externas, como el aumento de los **requisitos de soberanía**, que influyen en dónde (y bajo qué condiciones) se alojan y gestionan tanto los datos como los sistemas de IA.

El cambio se observa en prácticamente todas las empresas. De hecho, **el 95% de las organizaciones** considera que la IA privada y soberana son importantes, pero la mayoría reconocen no estar preparadas para implementarlas.

Por lo tanto, se observa una brecha clara. Algunas organizaciones están rediseñando el funcionamiento de su IA: dónde opera, cómo se gobierna y cómo se integran los requisitos de privacidad y soberanía en su arquitectura desde un principio. Otras, en cambio, todavía están tratando de implementar la IA en sistemas que no ofrecen el nivel de control, localización y restricción del flujo de datos que esta tecnología precisa.

Y la diferencia empieza a hacerse evidente.



### ¿Quiénes son los líderes en implementación de la IA?

Las organizaciones del estudio que se han clasificado como líderes en IA[1] son aquellas que, en sus respuestas, han afirmado tener una estrategia de IA bien definida o en progreso; que cuentan con un nivel de adopción maduro o evolucionado, y que han extraído beneficios notablemente mayores de esta tecnología que el resto de los participantes.

El caso de estos líderes en IA es excepcional por el nivel de crecimiento y los márgenes de beneficio de los que disfrutan. Tienen:

- Una probabilidad **2,5 veces** mayor de aumentar sus ingresos en más de un **10%.**
- **Una probabilidad 3,6 veces** mayor de operar con márgenes del **15%** o superiores.

La condición de líder en IA es independiente al tamaño y el nivel de ingresos de la organización. La ventaja competitiva está relacionada con la forma en que estas organizaciones diseñan y operan la IA.

[1] En el *Informe global de IA : Playbook para quienes lideran con IA* de NTT DATA, la primera publicación de esta serie, se describen en detalle las nueve características principales de los líderes en adopción de la IA.

# 1

## La IA está encontrando un límite, y el problema no está en el modelo

Durante años, avanzar en IA significaba contar con mejores modelos, pero las prioridades han cambiado.

Hoy, el principal desafío está en la capa que la sostiene: la infraestructura. De por sí, ejecutar la IA en **entornos privados** exige un mayor control sobre la computación, el acceso a los datos y la seguridad. Los **requisitos de soberanía** añaden una capa extra de complejidad: exigen localización, límites jurisdiccionales y mayores restricciones en la gestión de los datos y las cargas de trabajo.

Una cosa está clara: **la IA obliga a las empresas a replantear su arquitectura y su infraestructura**. Los sistemas diseñados para flujos de datos centralizados y sin fronteras tienen dificultades para dar soporte a una IA que debe ejecutarse en entornos controlados y cada vez más localizados. La mayoría de organizaciones son conscientes de ello. Aproximadamente **el 35% de los responsables de IA** entienden que habilitar la IA privada y soberana es la principal barrera a la hora de adoptar esta tecnología, pues suele requerir cambios significativos en la infraestructura.

La brecha entre lo que la IA requiere hoy y lo que la infraestructura existente puede ofrecer es cada vez mayor.

# 2

## La jurisdicción de los datos se está convirtiendo en una restricción arquitectónica

Uno de los puntos de mayor presión son los datos. La **IA privada** pone el foco en el control de accesos, para garantizar que los datos confidenciales permanezcan dentro de los límites de la empresa. **La IA soberana va un paso más allá**, restringiendo la residencia física de los datos, su movimiento entre regiones y los entornos que pueden procesarlos.

Estas restricciones no son nuevas, ya que los reglamentos para el flujo transfronterizo de datos existen desde hace años. Lo que está cambiando es el papel que desempeñan los datos en la IA. Los sistemas de IA dependen de conjuntos de datos grandes, diversos y, a menudo, distribuidos geográficamente. Necesitan poder acceder continuamente a dichos datos, así como a su movimiento y recombinación, para entrenar sus modelos, realizar ajustes o utilizarlos en tiempo real. En muchos casos, los datos siguen pudiendo transferirse legalmente, pero no con la velocidad, la escala y la fluidez que suelen asumir las arquitecturas de IA. Debido a estos factores, el gobierno de los datos ha pasado de ser una cuestión meramente legal a convertirse en una **limitación fundamental para las arquitecturas**.

La mayoría de líderes en IA, **casi el 60%**, ya citan las restricciones al intercambio transfronterizo de datos como un desafío importante que les obliga a replantearse dónde se alojan los datos, dónde se ejecutan los modelos y cómo se conectan unos y otros. Así pues, **la IA está provocando que se pase de sistemas de escala global a sistemas más fragmentados y con límites regionales**. Como consecuencia, la mayoría de las empresas se enfrentan a disyuntivas totalmente nuevas: ¿se debe priorizar el rendimiento o el cumplimiento?, ¿la eficiencia o el control?

# 3

## Todos ven el cambio, pero pocos actúan

Apenas hay debate acerca de la importancia de la IA privada y soberana, pues casi todas las organizaciones planean implementarlas en algún momento. Pero si analizamos los pasos que se están dando realmente, la cosa cambia. Pese a que la mayoría de las organizaciones son conscientes de la importancia de la IA privada y soberana, **menos de un tercio (29%)** está priorizando la IA soberana a corto plazo y tomando medidas concretas.

Esto sugiere que, aunque las organizaciones entienden la necesidad de ejecutar la IA en entornos controlados y ajustados a la normativa, muchas todavía están en fases iniciales a la hora de traducir esa necesidad en arquitecturas y modelos operativos escalables. Especialmente cuando los requisitos de soberanía añaden complejidad adicional, y llaman especialmente la atención las deficiencias de acción y de confianza. Por ejemplo, **solo el 38% de las organizaciones** afirma sentirse segura de su nivel de seguridad en la nube, un pilar fundamental para la IA privada y soberana.

La meta está clara, pero el camino que se debe seguir suscita dudas.

# 4

## Los líderes están rediseñando desde etapas tempranas y con decisión, lo que abre una brecha competitiva

La razón por la que las empresas líderes en IA cuentan con ventaja no es que se enfrenten a menos restricciones, sino que las gestionan de otra manera. Entienden **la IA privada y soberana como pilares básicos** y **principios de diseño**, y alinean la infraestructura, la gobernanza y los modelos operativos desde el principio. De ahí que consigan pasar rápidamente de proyectos piloto a implementaciones escaladas, incluso en entornos complejos y regulados.

Otras organizaciones adoptan un enfoque más gradual y, a menudo, tratan de seguir utilizando sus configuraciones existentes en contextos soberanos. Lamentablemente, este *modus operandi* está empezando a dar problemas.

Las deficiencias que están surgiendo no son solo tecnológicas, sino estructurales. En muchas organizaciones, la arquitectura y las operaciones no están diseñadas para soportar requisitos de soberanía a escala. Esta diferencia es especialmente evidente en el ámbito de los datos, donde las organizaciones líderes en IA, por lo general, tienen niveles de priorización y preparación **un 10-11% más elevados** que el resto.

# 5

## La IA privada y soberana pueden sonar a independencia, pero se construyen sobre ecosistemas cuidadosamente orquestados

Tanto la IA privada como la soberana aumentan la complejidad, pero de maneras distintas. La **IA privada** concentra la complejidad dentro de la empresa, asegurando los entornos, integrando los sistemas y gestionando los flujos de datos internos. **La IA soberana extiende esa complejidad fuera de los límites de la organización**, y abarca diferentes regiones, proveedores y regímenes normativos. Para ejecutar la IA en estos entornos, es necesario integrar infraestructura, nube, plataformas de datos, modelos y gobernanza. Además, estos servicios suelen depender de múltiples partners

**Más de la mitad de las organizaciones (51%)** citan la complejidad de la integración en entornos híbridos como uno de sus principales desafíos. De hecho, el principal reto para los encuestados.

Esto genera una dinámica menos evidente: **cuanta más presión ejercen las organizaciones para ganar control, más complejos e interdependientes se vuelven sus ecosistemas de IA.** Las organizaciones más avanzadas no trabajan solas. Están construyendo ecosistemas, pero con una orquestación mucho más precisa, mecanismos de rendición de cuentas más claros y una alineación más sólida con sus partners.

No se busca la propiedad de cada componente, sino **que el sistema multiproveedor sea fiable y funcione dentro de unos límites predefinidos.**

Juntas, la IA privada y soberana están cambiando el modo en que se construyen, gobiernan y escalan los sistemas de IA.

Algunas organizaciones ya están rediseñando su infraestructura con esto en mente. Las que no lo hagan tendrán problemas para escalar.

# La IA está encontrando un límite, y el problema no está en el modelo

Las estrategias empresariales de IA, hasta ahora, se centraban en la escala, la velocidad y el rendimiento de los modelos. Se trabajaba con ciertos supuestos: los datos podían moverse libremente, la infraestructura podía ser global y la inteligencia podía centralizarse.

Pero estos supuestos están quedando obsoletos rápidamente. En la actualidad, las estrategias de IA se enfrentan a retos de infraestructura que son tan técnicos como geopolíticos y normativos. ¿Dónde se almacenan los datos? ¿Quién controla la capa de inteligencia? ¿Qué ocurre cuando confluyen distintas jurisdicciones? Y ¿cómo pueden las organizaciones proteger su propiedad intelectual (PI) cuando las tensiones geopolíticas afectan a sus cadenas de suministro tecnológicas?

Pongamos el caso de un banco multinacional que ejecuta modelos de IA en diferentes regiones y, de repente, debe hacer frente a leyes de localización de datos contradictorias o a restricciones al intercambio transfronterizo. O el de una farmacéutica que entrena modelos de IA generativa con datos de sus investigaciones internas y que, ahora, en lugar de preocuparse por la latencia y los costes informáticos, lo que teme es una posible filtración de información confidencial sobre sus ensayos clínicos o sus formulaciones.

En ambos casos, el problema es el mismo: la IA ya no puede desligarse de cuestiones como el control, la jurisdicción o la exposición. En este contexto, el movimiento transfronterizo de los datos supone una vulnerabilidad estratégica. Las empresas precisan de entornos privados que protejan los datos sensibles, por medio no solo de políticas sino de controles de infraestructura aplicables.

**Este playbook de NTT DATA, que forma parte de nuestro Informe global de IA 2026, explora cómo, ante este nuevo paradigma, la IA privada y soberana ya no son opciones arquitectónicas de nicho —o meros obstáculos administrativos—, sino decisiones clave a nivel estratégico.**

## La IA privada y soberana, en el núcleo de la estrategia

Según nuestro estudio, un abrumador **95%** de las empresas ven la IA privada o soberana como un elemento importante de su estrategia de IA. Además, el **96%** de los encuestados está de acuerdo —el **45%**, muy de acuerdo— en que su empresa está planteándose trasladar la infraestructura de IA a puntos geográficos específicos, debido a preocupaciones relacionadas con las presiones geopolíticas o la cadena de suministro en el punto de origen.

Estos planteamientos suelen dividirse en tres categorías generales:

1. **Soberanía obligatoria de la IA,** cuando las restricciones legales o geopolíticas exigen un control interno.
2. **Privacidad regulada,** cuando las organizaciones deben demostrar un control auditable sobre sus datos, modelos y operaciones.
3. **Autonomía estratégica de IA,** en el caso de empresas globales que buscan un mayor control de la PI, los costes y la dependencia de los proveedores.

En la alta dirección, el mensaje es todavía más claro: al **98%** le parece imprescindible contar con un dominio privado que proteja la PI y los datos confidenciales, mediante un modelo de IA generativa no rastreable públicamente.

**El 95%**

de las empresas considera que la IA privada o soberana es importante para su estrategia de IA.

**El 96%**

de los encuestados está de acuerdo (el **45%**, muy de acuerdo) en que su empresa está planteándose trasladar su infraestructuras de IA a puntos geográficos concretos debido a preocupaciones geopolíticas.

**El 98%**

de los directivos de la C-Suite coinciden en que es obligatorio contar con un dominio privado que proteja la PI y los datos internos mediante un modelo de IA generativa no rastreable públicamente.

# La infraestructura, el nuevo foco en materia de IA

En un entorno más controlado y cada vez más localizado, ¿qué diferencia a las organizaciones que saben sacar partido a la IA de aquellas con dificultades?

Construir una IA privada y soberana es un proceso complejo, en el que no basta con trasladar las cargas de trabajo a otra ubicación. Hay que rediseñar el stack completo —infraestructura, datos y modelos—, gestionando las diferencias entre las normativas de las diferentes regiones y sectores. También se necesitan habilidades especializadas, una reestructuración de los contratos y, en ciertos casos, nuevos proveedores. Esto genera urgencia, pero también dudas: las empresas comprenden los riesgos de no hacer nada, pero también la complejidad que entraña este cambio.

**Dentro del stack, la infraestructura se ha convertido en el verdadero cuello de botella.** Lo que obstaculiza el escalado de la IA ya no son los modelos, sino los entornos de los que estos dependen, y aquí surge una brecha clave. Los líderes en IA tienen un **21%** más de posibilidades que las demás organizaciones de diseñar y ejecutar su IA con un enfoque soberano en los próximos años, ya que integran la privacidad y el control en sus infraestructuras desde el principio. Además, alinean cuidadosamente su estrategia de IA con sus decisiones de infraestructura, y modernizan sus entornos al ritmo que demanda su inversión en IA.

**Las fábricas de IA, explicadas**

Las fábricas de IA son entornos de alto rendimiento, diseñados con el propósito específico de entrenar, refinar y desplegar modelos de IA a gran escala. Integran hardware y software especializado, y suelen coordinar distintos agentes de IA para convertir los datos brutos en información aplicable. En el campo de la IA privada y soberana resultan muy relevantes porque ofrecen un sistema específico, automatizado e integral, capaz de operar con los niveles de rendimiento y control necesarios.

# Por qué la infraestructura es determinante para el control

**El control es, fundamentalmente, una cuestión infraestructural. Al hablar de IA empresarial, la arquitectura es tan importante como los algoritmos.** Cuando una organización decide que sus datos deben permanecer dentro de unos límites predefinidos, o que sus modelos han de operar bajo una gobernanza más estricta, la siguiente pregunta es: ¿dónde y cómo deben ejecutarse las cargas de trabajo de la IA?

En particular, esto es importante cuando existe un intercambio transfronterizo de datos, ya que las decisiones de arquitectura influyen directamente en los riesgos de exposición e incumplimiento de la normativa. Así pues, a la hora de escalar las decisiones, surge un nuevo requisito: antes de expandir las implementaciones de IA, las empresas deben demostrar —a nivel arquitectónico y conceptual— que sus controles de soberanía y gobernanza son aplicables.

Las infraestructuras previas se diseñaban para transacciones de aplicaciones y procesamiento por lotes. Esto choca con la IA, que requiere inferencia en tiempo real, movimiento de datos a gran velocidad, procesamiento en el borde y un control más estricto de los datos, modelos y entornos de ejecución. No se puede exigir que una arquitectura desfasada cumpla con estos requisitos.

Aunque prácticamente todas las empresas (**> 99%** ) están estudiando activamente el modo de integrar la IA en sus entornos existentes, el **96%** afirma que su infraestructura actual ralentiza la adopción de la IA. Es más, solo el **49%** está totalmente de acuerdo en que su infraestructura de datos actual permite despliegues de Agentic AI escalables.

## El 96%

de las organizaciones está de acuerdo (el 45%, muy de acuerdo) en que su infraestructura heredada ralentiza la adopción de la IA.

## 23%

Las empresas que adoptan un enfoque soberano en su estrategia de IA tienen un 23% más de probabilidades de confiar plenamente en que su infraestructura de IT responderá a sus necesidades de IA.

## Más del 99%

de las organizaciones está estudiando activamente la manera de integrar la IA en su infraestructura existente.

## N.º 1

La complejidad de la integración en arquitecturas híbridas y multinube es la principal preocupación a la hora de ejecutar cargas de trabajo de IA en entornos privados.

Aunque las empresas que adoptan un enfoque soberano en su estrategia de IA tienen un **23%** más de probabilidades de confiar totalmente en las capacidades de su infraestructura de IT para satisfacer sus demandas, nuestros datos son explícitos al respecto: necesitan ayuda. Aproximadamente 1 de cada 3 directores de IA (**35%**) señala que su principal barrera a la hora de adoptar la IA, por encima de la incertidumbre a nivel normativo, es la dificultad para construir, integrar y gestionar modelos complejos de IA en entornos soberanos. Esto a menudo los obliga a implementar cambios notables en su infraestructura y su manera de gestionar estos entornos.

Y, en medio de todo este desafío infraestructural, los datos se están revelando como una de las limitaciones más inmediatas.

## Aprox. 1 de cada 3

responsables de IA (**35%**) señala la dificultad para construir, integrar y gestionar modelos de IA complejos en entornos privados y soberanos como su principal barrera a la hora de adoptar la IA.

# La jurisdicción de los datos se está convirtiendo en una restricción arquitectónica

Los sistemas de IA dependen de conjuntos de datos grandes, diversos y, a menudo, muy distribuidos. Necesitan poder acceder a esos datos, moverlos y recombinarlos en tiempo real. Sin embargo, incluso en los casos en los que los datos pueden moverse legalmente, cuesta hacerlo con la velocidad, la escala y la flexibilidad que requieren las arquitecturas de IA modernas.

Al mismo tiempo, ahora que la soberanía ha pasado de ser un requisito normativo a una fuente de diferenciación, la búsqueda de privacidad y gobernanza de los datos desempeña un papel protagonista en el diseño de la IA, e influye en las decisiones de arquitectura, los modelos operativos y la composición del ecosistema de partners.

A medida que las arquitecturas de IA dejan atrás los modelos centralizados y evolucionan hacia sistemas más fragmentados y regionalizados, las organizaciones deben diseñar para múltiples jurisdicciones. Cada una cuenta con sus propios requisitos normativos, de datos y de infraestructura.

**Este cambio motivado por los datos introduce nuevas disyuntivas: ¿se debe priorizar más el rendimiento o el cumplimiento?, ¿la eficiencia o el control?** Los modelos ya no pueden entrenarse con todos los datos disponibles a nivel global, y la infraestructura está empezando a variar entre regiones, lo que agrega complejidad a unas operaciones empresariales que ya de por sí eran intrincadas. La mayoría de las organizaciones nunca habían tenido que gestionar estos problemas a escala. Tras pasarse años integrando sistemas aislados, ahora se enfrentan a un desafío diferente: replantearse el diseño, el despliegue y el gobierno de su infraestructura de IA para que sea compatible con la IA privada y soberana.

# Poca confianza en que se cubran las necesidades de soberanía

Globalmente, el **96%** de las organizaciones teme que el uso de la IA y la IA generativa derive en infracciones de privacidad o un mal uso de los datos de los clientes y, aun así, menos de la mitad (**47%**) confía del todo en poder cumplir sus requisitos de soberanía de datos.

Conservar los datos en un entorno local puede parecer sencillo, pero en la práctica requiere capacidad de almacenamiento, potencia de procesamiento y redes resilientes con límites bien definidos. No es una mera decisión política, sino que requiere un importante compromiso operativo y de capital. Menos de la mitad de las organizaciones (**48%**) está completamente de acuerdo en que su inversión en capacidad de almacenamiento y procesamiento de datos sea suficiente para respaldar las cargas de trabajo de la IA generativa.

Al mismo tiempo, la mayoría de los CEO (**57%**) menciona la privacidad de los datos y la soberanía entre regiones y entornos como dos de los riesgos que afrontan sus organizaciones. Estos factores constituyen, de hecho, la principal amenaza de seguridad y cumplimiento a nivel global.

## Al 96%

de las organizaciones le preocupa las infracciones de privacidad y el mal uso de los datos de los clientes que puedan derivar de la IA y la IA generativa.

## N.º 1

La seguridad de los datos (incluida la privacidad) se considera el principal desafío a la hora de adoptar la IA, si excluimos las cuestiones presupuestarias.

Solo el

## 47%

tiene confianza total en poder cumplir con las necesidades de soberanía de datos que demanda la IA.

## N.º 1

Garantizar la privacidad y la soberanía de los datos entre zonas geográficas y nubes es la principal amenaza de seguridad o gobernanza normativa a la que se enfrentan las organizaciones.

# Un enfoque por niveles de la IA soberana

**La soberanía se fundamenta en un diseño deliberado que abarca tres niveles: infraestructura, datos y modelos.** La soberanía de la infraestructura hace referencia a quién controla la computación y las plataformas. La soberanía de los datos determina quién controla los datos, dónde residen y bajo qué marco legal se procesan. Por último, la soberanía del modelo establece quién controla el modo de entrenar, ajustar y distribuir la inteligencia. La verdadera soberanía consiste en mantener estos tres niveles localmente.

La jurisdicción de los datos reside en el centro de esta estructura. Los niveles de infraestructura, datos y modelos están interconectados, pero los datos son a menudo el factor limitante: determinan qué partes deben conservarse a nivel local, qué se puede compartir y dónde puede operar la inteligencia. Una organización puede constreñir sus datos a las fronteras nacionales y mantener un control estricto de su infraestructura; pero, si el modelo se gobierna desde otra parte, el control sobre la capa de inteligencia no será total.

Por esta razón, muchas han empezado a separar deliberadamente los datos de la inteligencia. Conservan sus datos localmente, dentro de unos límites geográficos o normativos claros, pero permiten al mismo tiempo que los modelos, los algoritmos o las capacidades aprendidas se puedan compartir de manera más amplia. Esto implica ajustes regionales, pipelines de datos localizados, aprendizaje federado y controles estrictos de residencia, que se combinan con servicios de IA orquestados globalmente.

# La seguridad de los datos se debe integrar en la arquitectura

**El control jurisdiccional introduce una nueva dinámica en la seguridad de los datos.** Los modelos de IA de gran tamaño dependen de pipelines de datos extensos, integraciones con terceros y ciclos de reentrenamiento continuo, lo que aumenta las posibilidades de que la información se filtre, se utilice mal o se configure erróneamente.

Para abordar estos riesgos, se requiere un gobierno unificado de los datos: clasificación deliberada de los mismos, acceso segmentado mediante principios de zero trust, encriptación en todo el ciclo de vida, linaje, red teaming periódico y gestión centralizada de claves e identidades.

En el caso de la IA privada y soberana, el control solo es real si la forma en que se construye y opera el entorno permite ejercerlo.

# La complejidad de las decisiones sobre la carga de trabajo

Todas estas realidades influyen en las decisiones de infraestructura de IA de las organizaciones. La jurisdicción de los datos ya no es una consideración de última hora para cumplir con la normativa, sino que se ha convertido en una limitación de diseño que afecta desde el principio del proceso.

Las distintas cargas de trabajo de la IA conllevan distintos requisitos de densidad de computación, diseño de red, resiliencia y gravedad de los datos, y el cumplimiento puede hacer que el dónde se ejecuta una carga de trabajo sea igual de importante que el cómo. Muchas organizaciones, en consecuencia, están adoptando arquitecturas híbridas, en las que los entornos controlados se reservan para los datos confidenciales, el rendimiento determinante y la supervisión normativa; y se emplean otros entornos para aquellos datos que comportan un riesgo menor.

Según nuestros datos, el **97%** está de acuerdo en que es mejor alojar las cargas de trabajo críticas en entornos privados o locales, mientras que las tareas no esenciales o menos sensibles pueden gestionarse en otras ubicaciones. La previsibilidad de los costes es otro factor importante que se debe tener en cuenta para estas decisiones.

**La conclusión es muy simple: las empresas que no controlan sus datos y su infraestructura tampoco controlan su IA.**

Los líderes en IA ya están rediseñando su infraestructura teniendo todo esto en cuenta, y nuestro estudio sugiere que su enfoque disciplinado del control se ha convertido en un motor para la mejora del rendimiento.

# Todos ven el cambio, pero pocos actúan

Pocas organizaciones dudan de la importancia de la IA privada y soberana. El problema es que no todas están actuando con la urgencia y la disciplina necesarias.

En el mercado, por ahora, se observan más intenciones que acciones. Nuestros datos revelan que solo el **29%** de las organizaciones está priorizando la IA soberana a corto plazo y con medidas concretas.

Es un desafío muy común: aunque la mayoría de las organizaciones reconocen la necesidad de ejecutar la IA en entornos controlados y ajustados a la normativa, muchas todavía no han logrado traducir esta idea en arquitecturas y modelos operativos escalables, sobre todo por la complejidad extra que aportan los requisitos de privacidad y soberanía. Se observan deficiencias tanto a nivel de ejecución como de confianza.

También encontramos diferencias de actuación entre unas regiones y otras. En la Unión Europea, la inversión en IA soberana está impulsada más explícitamente por la regulación, mientras que en algunas partes de Oriente Medio las consideraciones estratégicas a nivel político y nacional pueden superar a los criterios normativos. Esto significa que las organizaciones no están respondiendo a un mandato único global, sino a todo un muestrario de expectativas locales, presiones sectoriales y requisitos de confianza.

Además, el sector y el caso de uso específico suelen ser tan importantes como las fronteras nacionales. Alinear las decisiones de infraestructura con las expectativas locales es, para las empresas, un modo de ganarse la confianza de los clientes y reforzar su credibilidad dentro de su sector. Pero, a la hora apostar por la IA soberana, no basta con una simple declaración de intenciones. Hacen falta decisiones visibles —una residencia de los datos demostrable, alianzas con partners del propio país y alineación con las estrategias digitales nacionales— para que la soberanía deje de ser una prioridad pretendida y se convierta en un modelo operativo.

# Cómo el sector y el caso de uso específico influyen en el diseño de la infraestructura de IA

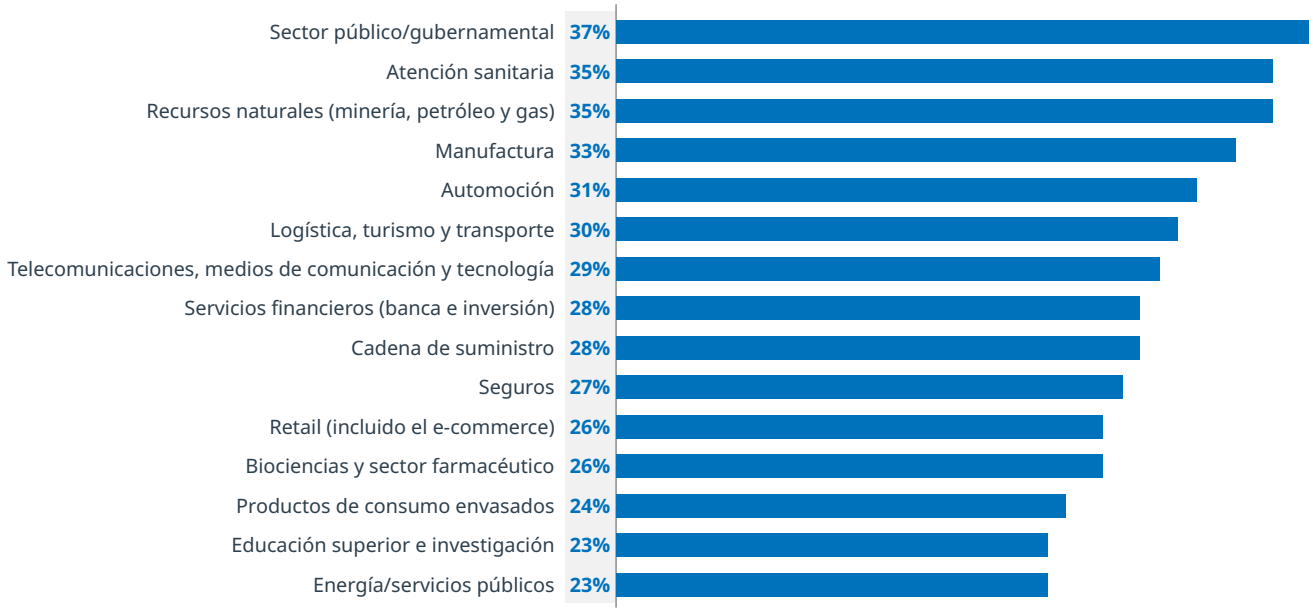
La zona geográfica es un factor fundamental, pero los perfiles de riesgo y los casos de uso concretos de cada sector también determinan en buena medida la influencia que ejerce la soberanía sobre las arquitecturas de IA.

Nuestro estudio revela que, durante los próximos años, la tendencia a adoptar un enfoque soberano en el diseño y el despliegue de soluciones de IA será mayor en unos sectores que en otros. A nivel global, encabezan esta tendencia las organizaciones del sector público con un **37%**; seguidas de las sanitarias y las dedicadas a los recursos naturales (minería, petróleo y gas), ambas con un **35%**; y las manufactureras, con un **33%**.

En estos sectores, un fracaso puede acarrear consecuencias evidentes. En el ámbito público, los sistemas de IA podrían acceder a información de seguridad nacional, datos de los ciudadanos o servicios públicos esenciales. Cualquier brecha o disrupción puede socavar la confianza de la ciudadanía o comprometer la resiliencia de un estado.

En el terreno de la salud, cada vez es más común utilizar la IA en los diagnósticos, la planificación de los tratamientos y la investigación clínica. Que los datos médicos confidenciales puedan circular libremente entre jurisdicciones plantea de inmediato serias dudas éticas y normativas.

**Industrias con más probabilidades de adoptar un enfoque soberano en el diseño y el despliegue de soluciones durante los próximos dos años (a nivel global)**




**¿Qué enfoques es más probable que adopte tu organización para diseñar y desplegar soluciones de IA durante los próximos dos años?**
Base: todos los encuestados, excepto quienes respondieron “No lo sé” (n = 2.567)

## Diferencias regionales

El ranking de los sectores con mayor tendencia a adoptar un enfoque soberano de la IA varía entre regiones y, a menudo más explícitamente, entre países. Por ejemplo, la fabricación ocupa el primer puesto en la región de Asia-Pacífico, el sector público y gubernamental encabeza la lista en Europa y la sanidad hace lo propio en Norteamérica. Esto parece indicar que los factores locales y regionales también influyen en las decisiones estratégicas de implementación de la IA.

# Carencias de seguridad en la nube

En las empresas, los objetivos de IA también avanzan con mayor rapidez que las medidas de seguridad. Solo el **38%** de los encuestados confía mucho en su nivel de seguridad en la nube, y menos de la mitad (**48%**) se considera muy bien preparado para gestionar los riesgos de seguridad de la IA y la nube y cuenta con planes formales para ello.

Muchas organizaciones están avanzando rápidamente en materia de IA, aunque todavía se encuentran en proceso de reforzar las medidas de seguridad que exigen los entornos privados y soberanos. Esto complica la transición, y hace que sea aún más importante contar con partners que aporten disciplina y conocimientos técnicos durante la implementación.

La seguridad en la nube es primordial para la IA privada y soberana, pues garantiza la residencia de los datos, el control de accesos y el cumplimiento de los requisitos normativos y, a la vez, protege los modelos y datos confidenciales frente a accesos no autorizados. Sin una política sólida de seguridad en la nube, las empresas se arriesgan a que sus sistemas de IA queden expuestos a riesgos y errores de gobernanza, lo que les impediría alcanzar la soberanía y la privacidad a la que aspiran.

Solo el

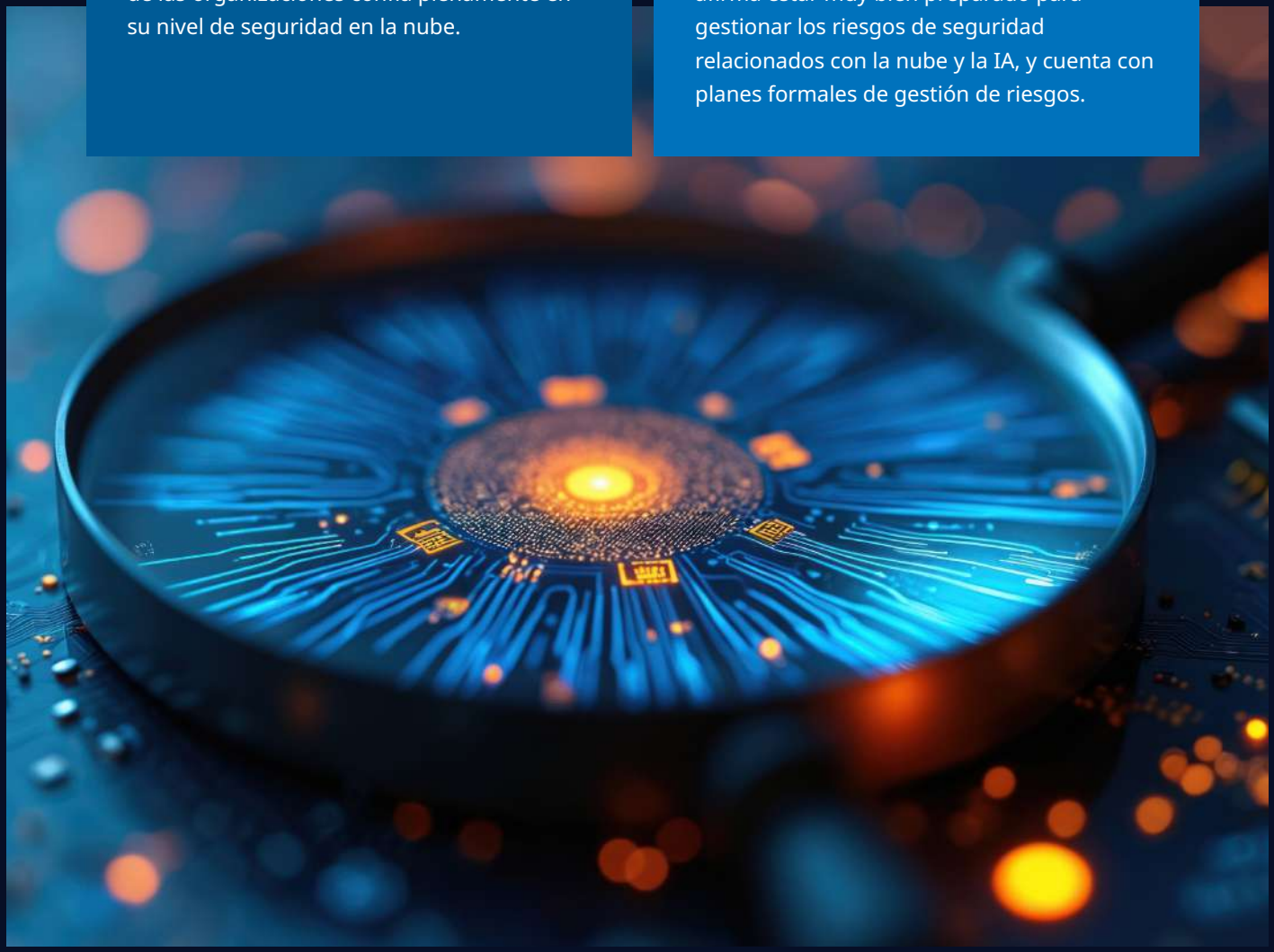
**38%**

de las organizaciones confía plenamente en su nivel de seguridad en la nube.

Y solo el

**48%**

afirma estar muy bien preparado para gestionar los riesgos de seguridad relacionados con la nube y la IA, y cuenta con planes formales de gestión de riesgos.



# Los líderes están rediseñando desde etapas tempranas y con decisión, lo que abre una brecha competitiva

Los líderes en adopción de la IA sitúan la IA privada y soberana en el centro de sus modelos operativos, tratándola como un principio de diseño fundamental. La ven como un motor de ventaja competitiva, que les ofrece mayor poder de negociación y amplía los conocimientos internos, y están alineando sus estrategias empresariales generales en consecuencia.

Avanzan a un ritmo que las empieza a distanciar de la competencia. Se ha abierto una brecha, tanto estructural como tecnológica, entre estos líderes y las organizaciones que están adoptando un enfoque más gradual, tratando de adaptar sus configuraciones preexistentes a las nuevas demandas de privacidad y soberanía. Por lo general, los líderes gozan de ventaja —en algunos casos, de 10 u 11 puntos porcentuales— a nivel de priorización y preparación.

### Porcentaje de empresas que han alineado completamente su infraestructura de IT con su estrategia de IA.


**¿Hasta qué punto está alineada la estrategia de IA de tu organización con tu estrategia de infraestructura de IT?**
Base: todos los encuestados, excepto quienes respondieron "No lo sé" (n = 2.526)

### Porcentaje de organizaciones que afirman que la IA soberana y/o privada es un factor extremadamente importante en su estrategia de IA


**¿Cuánta importancia tienen los siguientes factores en tu estrategia de IA? – IA soberana/privada.**
Base: todos los encuestados, excepto quienes respondieron "No lo sé" (n = 2.567)

### Porcentaje de organizaciones que consideran que la IA soberana aumenta la ventaja competitiva y ofrece mayor poder de negociación y mayores conocimientos


**¿Cuál es el principal motivo de tu organización para invertir en una solución de IA soberana?**
Base: todos los encuestados, excepto quienes respondieron "No lo sé" (n = 2.567)

# Un nuevo enfoque para la gobernanza de la IA

Además de poner el foco en la infraestructura, los líderes en IA también están adoptando un enfoque más estructurado de la gobernanza de esta tecnología, integrándola desde el principio en todas sus iniciativas de IA.

Aunque la confianza en la gobernanza sigue siendo desigual en el mercado, estos líderes son mucho más propensos a optar por una gobernanza centralizada, reconociendo al mismo tiempo la necesidad de modelos operativos federados. La privacidad y la soberanía de los datos están entre sus mayores preocupaciones en materia de gobernanza, y tienen más tendencia que otras organizaciones a formalizar la rendición de cuentas mediante comités que aúnan a partes interesadas de diferentes departamentos (empresarial, legal y de seguridad) y están respaldados por la dirección.

### Porcentaje de organizaciones que ya siguen un modelo de gobernanza de IA centralizado


**¿Qué enfoque describe mejor tu modelo de gobernanza de la IA?**
Base: todos los encuestados, excepto quienes respondieron "No lo sé" (n = 2.567)

### Porcentaje de organizaciones que afirman que la privacidad y la soberanía de los datos que se mueven entre diferentes regiones geográficas es una de sus principales preocupaciones de gobernanza


**Al escalar la IA en tu organización, ¿cuáles de los siguientes riesgos de seguridad o cumplimiento suponen una amenaza mayor?**
Base: todos los encuestados, excepto quienes respondieron "No lo sé" (n = 2.567)

### Porcentaje de organizaciones que cuentan con un comité de gestión de la IA formando por un representante del equipo ejecutivo, líderes de diferentes ámbitos del negocio y miembros de los departamentos legal y de seguridad, entre otros.

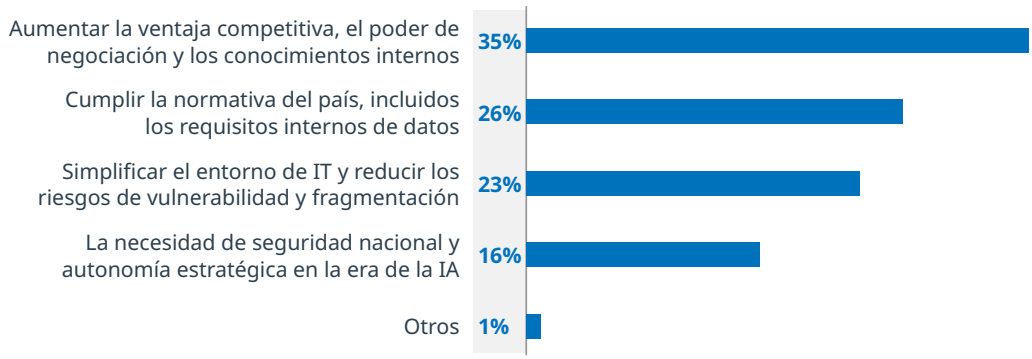

**¿Cuáles de las siguientes opciones se han puesto en marcha como parte de tu modelo de gobernanza de la IA?**
Base: todos los encuestados con un modelo de gobernanza de la IA, excepto quienes respondieron "No lo sé" (n = 2.505)

## La visión del CIO sobre la IA

Para los CIO, una estrategia de IA soberana puede ser también una herramienta defensiva. De acuerdo con los CIO encuestados en nuestro informe global, obtener una ventaja competitiva, ganar poder de negociación y ampliar los conocimientos internos son las razones principales para invertir en IA soberana. Otros motivos son el cumplimiento de la normativa y los requisitos nacionales de datos, la simplificación del entorno de IT, la reducción de la vulnerabilidad y la necesidad de mayor seguridad nacional y autonomía estratégica.

Esto difiere de la visión general de las empresas, para las que simplificar el ecosistema de IT con el fin de reducir los riesgos es el segundo motivo principal para invertir en IA soberana.

**Principales razones para invertir en una solución de IA soberana, según los CIO**




**¿Cuál es el principal motivo de tu organización para invertir en una solución de IA soberana?**
Base: todos CIO encuestados, excepto quienes respondieron “No lo sé” (n = 211)

# La IA privada y soberana pueden sonar a independencia, pero se construyen sobre ecosistemas cuidadosamente orquestados

Aunque la IA privada y la IA soberana se están convirtiendo en necesidades estratégicas, su adopción no se está volviendo más sencilla. **Un nivel mayor de control aumenta la complejidad, ya que los ecosistemas de IA están más interconectados y son más interdependientes.**

Diseñar y ejecutar entornos de IA privada y soberana exige coordinación entre múltiples proveedores, infraestructuras, datos, plataformas y modelos, teniendo en cuenta a su vez la gobernanza, la seguridad y el cumplimiento dentro de unos límites predefinidos. Hasta ahora, la mayoría de las empresas tenían pocos motivos para perseguir este nivel de integración, tal y como muestra nuestro estudio:

- De entre las empresas que están desarrollando estrategias de IA soberana para sus herramientas de IA generativa, el **40%** cita la modernización de la infraestructura como su mayor desafío, seguida de cerca por la dificultad para evaluar e integrar tecnologías complementarias.
- Más de la mitad de las organizaciones (**51%**) cita la complejidad de la integración en entornos híbridos como uno de sus principales desafíos a la hora de ejecutar cargas de trabajo de IA en la nube privada. Es, de hecho, el principal reto para los encuestados.
- Solo el **49%** se muestra totalmente satisfecho con las capacidades de gobernanza y soberanía de datos de sus entornos en la nube actuales. Aquellos que no están del todo satisfechos aluden, en primer lugar, a la falta de colaboración entre empresas y, a continuación, a los desafíos de gestión y a la complejidad arquitectónica. También se menciona el aumento de los costes como una de las causas de este descontento.

Además, la privacidad y la soberanía abarcan las unidades legales, de IT, de riesgos, de adquisiciones y de negocio. El reto con respecto al modelo operativo es, por lo tanto, organizativo y técnico a la vez.

Estos problemas de implementación son un obstáculo determinante para que la IA privada y soberana dejen de ser simples proyectos y se lleven realmente a la práctica.

## Desarrollar un ecosistema de partners

La IA privada y soberana no son capacidades que una empresa pueda ejecutar por sí sola. Puesto que desarrollarlas lleva tiempo, las empresas que antes definan su ecosistema de partners estarán mejor posicionadas para escalar sin disrupción.

Nuestro estudio revela que el **32%** de los responsables de IA —entre las empresas líderes en implementación, el **38%**— considera que la disponibilidad de una solución de IA privada o soberana es un factor clave a la hora de escoger plataformas de IA empresarial. Pero elegir la plataforma es solo el principio. Implementarla de manera efectiva tiene su propia complejidad, ya que en el proceso intervienen la gobernanza, la orquestación, la gestión del ciclo de vida y la integración.

### Aprox. 1 de cada 3

responsables de IA (**32%**) afirma que la disponibilidad de una solución de IA privada o soberana es un factor clave a la hora de escoger una solución de IA empresarial.

**Poder lidiar con esta complejidad depende, cada vez más, de la colaboración con partners que operen en todo el stack** (centros de datos físicos, infraestructura de IA, plataformas, modelos, sistemas de seguridad y servicios de IA de nivel superior) y puedan además conectar estas capacidades con los requisitos específicos de cada sector.

El valor de estos partners radica en su capacidad para, por un lado, proporcionar herramientas tecnológicas y, por otro, traducir los requisitos políticos y de control en entornos listos para la producción que puedan operarse a escala. En lugar de optimizar un solo componente, estos partners orquestan ecosistemas complejos de múltiples proveedores y, además, participan en todo el ciclo de vida: desde la estrategia y el diseño hasta la construcción, la implementación, la operación y la optimización continua. Contar con un ecosistema de partners especializados, arquitecturas de referencia y de eficacia demostrada, relaciones sólidas con los proveedores y playbooks de modernización replicables reduce los plazos y limita las disrupciones.

En el contexto de la IA, la orquestación de ecosistemas adquiere un significado más amplio: no consiste solo en reunir tecnologías, sino en alinear la arquitectura, la gobernanza, la seguridad y las operaciones entre proveedores, regiones y contextos normativos.

> “La IA privada y soberana no son capacidades que una empresa pueda ejecutar por sí sola”.

**Qué hace un partner efectivo:**

- Opera en todo el stack tecnológico, desde la infraestructura hasta los modelos y los flujos de trabajo específicos de cada sector.
- Presta soporte en todo el ciclo de vida, desde la estrategia y el diseño hasta el desarrollo, la operación y la optimización.
- Coordina ecosistemas multiproveedor que engloban distintas empresas, regiones y contextos normativos.
- Aúna escala global, ejecución local y controles que se adaptan a cada jurisdicción.

Estos cambios se perciben también en cómo los líderes en adopción de la IA construyen sus ecosistemas de partners. Es más probable que estas organizaciones tengan en cuenta las capacidades de IA privada y soberana al seleccionar proveedores; exijan mayor flexibilidad en los contratos, y se adapten más rápidamente a los cambios en su relación con proveedores de gran escala. Las organizaciones “maduras en la IA” confían más en aquellos partners que cuentan con capacidades soberanas de eficacia demostrada, sobre todo en lo que respecta a la gobernanza de datos.

**Porcentaje de organizaciones que considera la disponibilidad de una solución de IA privada o soberana como un factor importante al elegir una solución de IA empresarial**


**A la hora de seleccionar una solución de IA empresarial, ¿qué factores tienen mayor importancia en la toma de decisiones?**
Base: todos los encuestados, excepto quienes respondieron “No lo sé” (n = 2.566)

En resumen, a medida que el mercado pasa de experimentar con la IA a operar modelos de IA reales, la estrategia de partners se vuelve en una pieza fundamental dentro de la estrategia de IA. Las organizaciones que escalan con éxito son las que combinan el control con ecosistemas orquestados, y sortean la complejidad gracias a una ejecución fiable. No se busca la propiedad de cada componente, sino **que el sistema multiproveedor sea fiable y funcione dentro de unos límites predefinidos.**

# Empieza un nuevo capítulo en la IA

La IA está adentrándose en una nueva fase, definida no tanto por la innovación en los modelos, sino por las condiciones bajo las que operan dichos modelos.

Las restricciones son cada vez más difíciles de ignorar: la infraestructura está sometida una gran presión, los datos ya no pueden moverse libremente y los requisitos de soberanía y privacidad están empezando a influir en cómo se desarrollan e implementan los sistemas de IA. Aspectos que antes se daban por sentado, como la escala global, la inteligencia centralizada o el flujo ininterrumpido de datos, ahora deben diseñarse, aplicarse y testarse deliberadamente.

Los líderes en IA ya están tomando medidas para ajustarse a este nuevo paradigma. Están alineando su infraestructura y sus estrategias de IA, y rediseñando sus arquitecturas para favorecer el control, la localización y la gobernanza desde un principio. Otras organizaciones avanzan con más cautela, pero la brecha entre unas y otras es cada vez más difícil de cerrar, ya que las exigencias de privacidad y soberanía continúan creciendo.

**Las implicaciones están claras: escalar la IA ya no es una cuestión solo de capacidad, sino también de diseño.** Las organizaciones deben decidir dónde se ejecuta la IA, cómo se gestionan los datos y qué partes de la infraestructura, los modelos y los ecosistemas se pueden controlar.

El próximo capítulo no vendrá definido solo por el acceso. La intencionalidad con la que se desarrolle la IA será igual de importante y, en un mundo donde la privacidad y la soberanía importan más que nunca, las empresas que tomen la iniciativa serán las que estén mejor posicionadas para escalar con confianza.

**Visita la página web de NTT DATA y descubre cómo podemos ayudarte a trazar una hoja de ruta para implementar la IA generativa.**

### Explora los datos del estudio en más detalle

El *Informe global de IA 2026* es una nueva muestra de las capacidades de investigación y el liderazgo intelectual de NTT DATA, y le seguirán nuevos análisis especializados y ejecutivos. Ponte en contacto con nosotros para saber cómo, gracias a nuestros centros de datos globales y a nuestra experiencia en consultoría y servicios, podemos impulsar el éxito de tu organización. Síguenos para no perderte nuestros próximos análisis, investigaciones y publicaciones de liderazgo intelectual.

# Definiciones

## IA privada y soberana

La IA privada y la IA soberana son requisitos para que los países o las organizaciones puedan desarrollar y desplegar soluciones de IA de manera independiente. Se deben aplicar niveles crecientes de privacidad y soberanía, en función de las necesidades específicas de autonomía, la normativa o las limitaciones legales y geopolíticas.

### 4 dimensiones clave de la IA privada y la IA soberana

**01**

**Territorial**
Residencia de los datos y computación

**02**

**Operativa**
Gestión, control y seguridad de los sistemas

**03**

**Tecnológica**
Propiedad del código, los modelos y la PI

**04**

**Legal y normativa**
Jurisdicción sobre el acceso a los datos, el uso y los derechos

**La IA privada** aloja la PI confidencial y los datos sujetos a la normativa en entornos de IA específicos y controlados, con una estricta gestión de identidades y accesos, flujos de datos encriptados y controles del ciclo de vida del modelo.

**La IA soberana** mantiene los datos, la infraestructura, la computación y el control dentro de las fronteras nacionales o regionales, normalmente como respuesta a la realidad geopolítica.

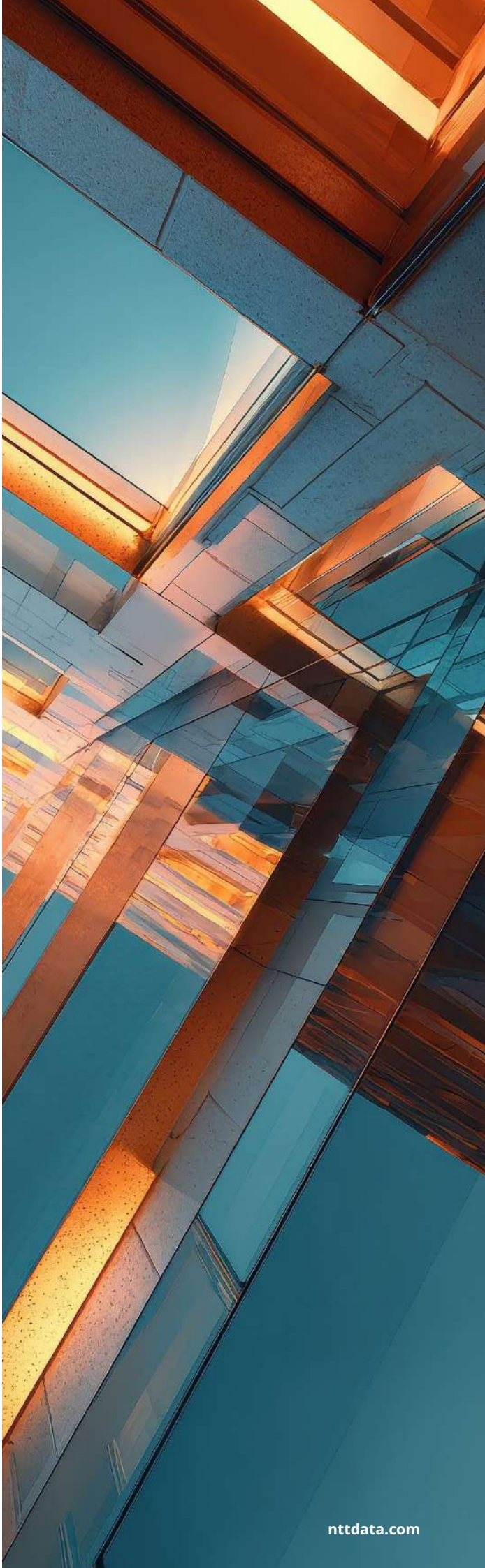
# Madurez en la IA

El *Informe global de IA* de NTT DATA ha identificado tanto empresas líderes en adopción de la IA como organizaciones rezagadas en este ámbito dentro de todos los rangos de ingresos y en todos los sectores. Lo que distingue a los líderes del resto es que cuentan con una estrategia definida de IA y un mayor nivel de madurez en la IA.

### Niveles de madurez en la IA definidos

- **Sin planes:** El uso de la IA aún no se ha explorado en la organización.
- **Exploradoras:** Están barajando diferentes estrategias y planes, pero no han comenzado con la adopción ni cuentan con capacidades concretas todavía.
- **Principiantes:** Acaban de empezar, por lo que tienen experiencia limitada y pocos casos de uso.
- **Avanzadas:** Usos esporádicos y algo aislados, con pilotos de viabilidad y una adopción limitada en unidades de negocio concretas, generalmente para funciones no esenciales.
- **Maduras:** Uso amplio y estratégico en las diferentes unidades y funciones del negocio, con una gobernanza sólida, buenas prácticas y cargas de trabajo escalables.
- **Evolucionadas:** Incorporan la IA en funciones principales y secundarias, así como en la prestación continua de servicios. La innovación impulsada por la IA acelera la transformación del negocio y el logro de los objetivos.

**Leer más:** El **Informe global de IA 2026: Playbook para quienes lideran con IA**, la primera publicación de la serie, presenta nueve características de los líderes en IA para ilustrar cómo operan y por qué ya han empezado a cosechar los beneficios de su inversión en IA.



# Acerca de la investigación

## Metodología del estudio

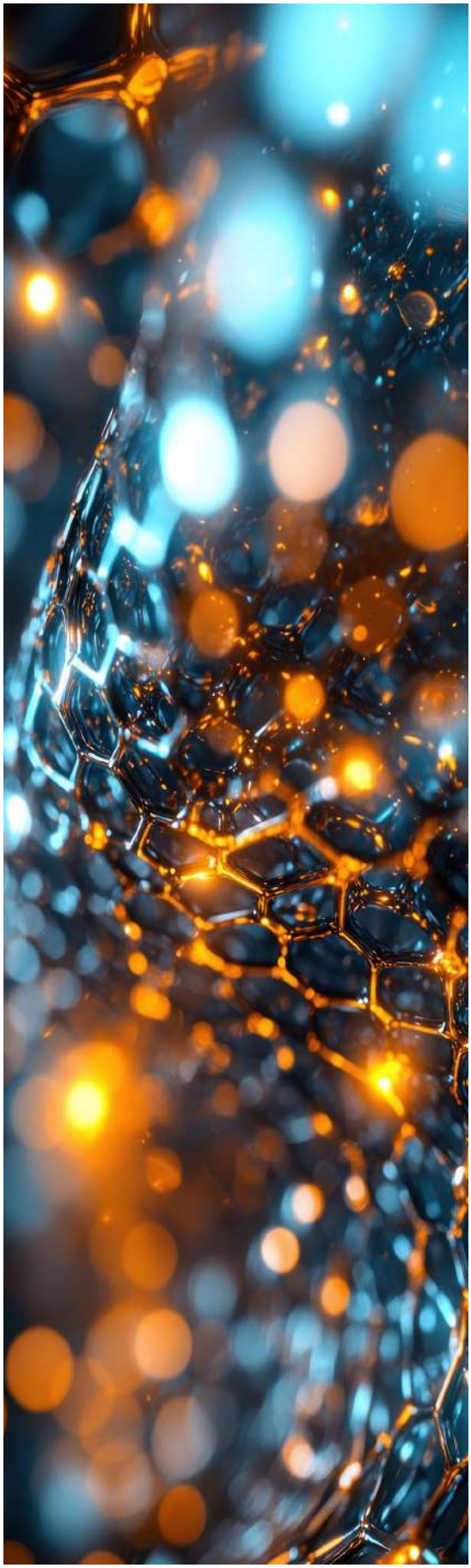
**Todo el contenido de este playbook se basa en datos obtenidos de fuentes independientes.**

STRAT7 Jigsaw, una agencia internacional de análisis estratégico e inteligencia de mercado que cuenta con un equipo compuesto exclusivamente por profesionales de alto nivel, llevó a cabo el trabajo de campo de investigación primaria para NTT DATA.

Los participantes pasaron por un proceso de preselección y después fueron elegidos mediante un muestreo aleatorio, según su capacidad de decisión o su influencia en la estrategia de IA o tecnológica de su organización. Los resultados de la investigación provienen de dos conjuntos de datos diferentes, obtenidos mediante encuestas online realizadas en septiembre y octubre de 2025.

De forma conjunta, STRAT7 Jigsaw y el equipo interno especializado en investigación primaria y evaluación comparativa de NTT DATA llevaron a cabo la integración, la validación y el análisis de los datos. La validación de los datos y los valores atípicos se llevó a cabo en colaboración con STRAT7 Jigsaw, de acuerdo con las reglas, disciplinas y buenas prácticas de uso estándar en trabajos de investigación. Los datos presentan un nivel de confianza del 99%, con un margen de error del 3%.

A nivel global, la investigación abarca más de 30 mercados en cinco regiones, y más de una docena de sectores. La muestra está compuesta de casi 5.000 altos directivos y profesionales con influencia en la toma de decisiones de sus empresas. En la selección de las muestras se ha dado prioridad a organizaciones grandes y altos directivos, con una fuerte representación de la C-suite.



# Cifras del estudio

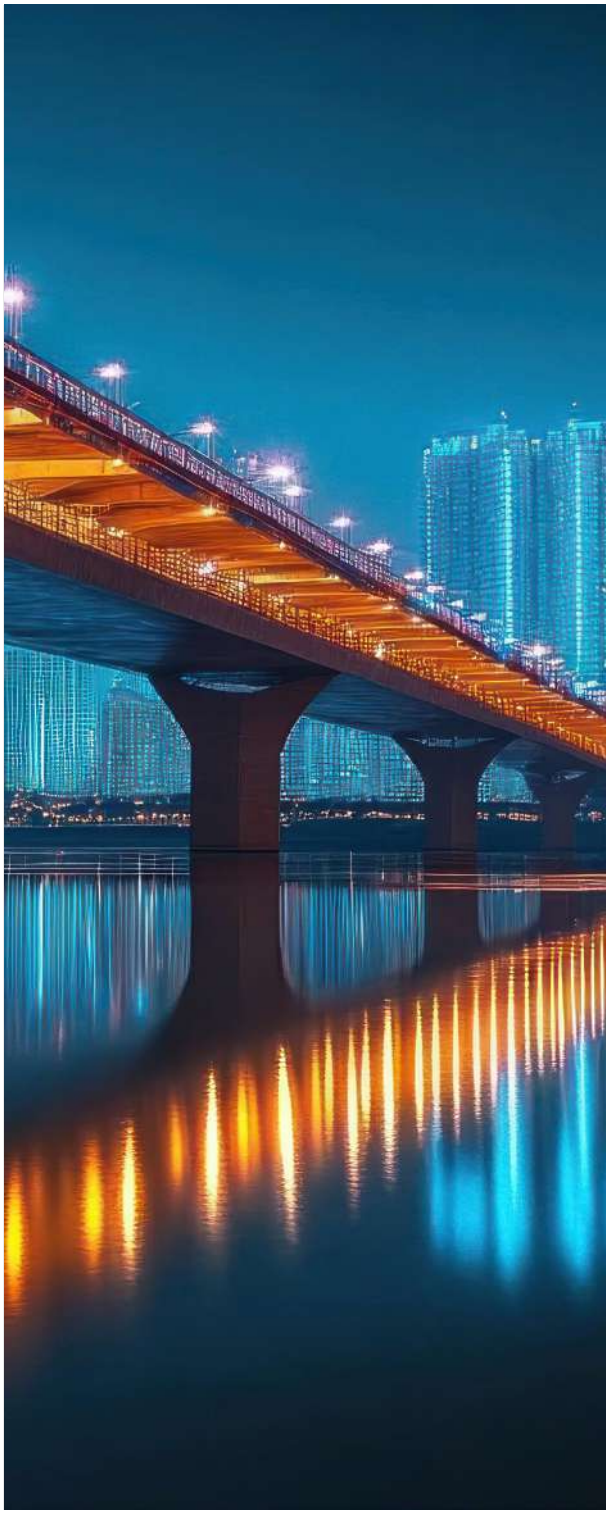
## Informe global de IA 2025

- Una muestra equilibrada de 2.567 responsables de toma de decisiones sobre IA generativa (94%) y otras personas influyentes en este ámbito (6%).
- La selección abarca 35 mercados, 5 regiones y 15 sectores.
- El 84% de los encuestados pertenece a organizaciones grandes con más de 10.000 empleados; el 11%, a organizaciones con entre 5.001 y 10.000 empleados; y el 5%, a organizaciones con entre 2.500 y 5.000 empleados.
- El 79% de los encuestados forma parte de la C-suite; el 15% ocupa cargos de vicepresidente sénior, vicepresidente, jefe de departamento o director; y el 6% restante está formado por gerentes sénior o especialistas.
- El 10% de los encuestados son CEO y el 4% son directores de IA. Además, el 31% proviene de departamentos empresariales de IT (sin contar el área de seguridad); el 11%, de departamentos de seguridad de IT; el 6%, de departamentos de digital; el 21%, de departamentos de operaciones; y el 17%, de departamentos de apoyo al negocio (legal, cumplimiento, riesgos, finanzas, marketing y RR. HH.).

## Investigación sobre arquitectura tecnológica (2025)

- Una muestra equilibrada de 2.335 responsables de toma de decisiones (94%) y otras personas influyentes (6%).
- La selección abarca 33 mercados, 5 regiones y 13 sectores.
- El 83% de los encuestados pertenece a organizaciones grandes con más de 10.000 empleados; el 11%, a organizaciones con entre 5.001 y 10.000 empleados; y el 6%, a organizaciones con entre 2.500 y 5.000 empleados.
- El 73% de los encuestados forma parte de la C-suite; el 21% ocupa cargos de vicepresidente sénior, vicepresidente, jefe de departamento o director; y el 6% restante está formado por gerentes sénior o especialistas.
- El 12% de los encuestados son CEO y el 5% son directores de IA. Además, el 46% proviene de departamentos empresariales de IT (sin contar el área de seguridad); el 9%, de departamentos de seguridad de IT; el 7%, de departamentos de digital; el 12%, de departamentos de operaciones; y el 10%, de departamentos de apoyo al negocio (legal, cumplimiento, riesgos, finanzas, marketing y RR. HH.).[2]

[2] Los porcentajes se redondean a números enteros, por lo que puede que la suma total no sea del 100%.



# Rediseñar y escalar para la nueva realidad de la IA

El 75% de las empresas de la lista Fortune Global 100 confían en NTT DATA para impulsar la transformación y el crecimiento. Ayudamos a las organizaciones a innovar con mayor rapidez y operar de forma más inteligente, gracias a una cartera de servicios integral que incluye consultoría, aplicaciones, datos e IA, lugar de trabajo digital e infraestructura digital segura. En un contexto en el que la demanda de IA privada y soberana crece de manera acelerada, ofrecemos servicios fiables y una infraestructura que permite el control de datos, la alineación normativa y la expansión con seguridad de la IA. NTT DATA forma parte del Grupo NTT, valorado en 90.000 millones de dólares, que invierte anualmente más de 3.000 millones de dólares en I+D para ayudar a las organizaciones a avanzar con confianza y sostenibilidad hacia el futuro digital.

**Visita nttdata.com para saber más.**

NTT DATA es una compañía de servicios empresariales y tecnológicos líder en IA e infraestructuras digitales, con más de 30.000 millones de dólares de facturación anual. Aceleramos el éxito de nuestros clientes y generamos un impacto positivo en la sociedad desde un enfoque de innovación responsable. Somos Global Top Employer y contamos con expertos en más de 70 países. NTT DATA forma parte del Grupo NTT.


NTT DATA