● Whitepaper

El imperativo de la soberanía de la IA

De la dependencia digital al control organizativo

eraneos

Contenido

Resumen ejecutivo

Durante la última década, los importantes avances en IA han permitido automatizar tareas que antes requerían mano de obra humana. Los sistemas de IA ahora pueden conducir automóviles, leer libros, escribir artículos, hablar, escuchar, programar y hacer descubrimientos científicos. Incluso están empezando a pensar. Las organizaciones utilizan ahora la IA en sus múltiples formas en sus prácticas empresariales básicas para aumentar la eficiencia, reducir los costes y mejorar la calidad de sus productos y servicios. Prevemos que esta tendencia continuará y que las organizaciones que no utilicen estas nuevas tecnologías se encontrarán en desventaja competitiva.

Si bien la dependencia de proveedores de servicios en la nube extranjeros, principalmente de Estados Unidos (USCSP, por sus siglas en inglés), para los datos y la infraestructura básicos es un reto conocido, ha surgido una nueva dependencia igualmente crítica: los servicios de inteligencia artificial (IA).

El rápido progreso de la IA, en particular de los modelos de lenguaje grandes (LLM, por sus siglas en inglés), está cambiando la forma en que operan las organizaciones, lo que convierte a los LLM en un factor importante para la competitividad. Sin embargo, la mayor parte de la innovación y la comercialización en este campo está impulsada por unas pocas empresas extranjeras, lo que introduce profundos riesgos para la soberanía. Cuando delegamos el pensamiento y la toma de decisiones fundamentales a máquinas controladas por entidades extranjeras, surge una pregunta clave: **¿Cómo podemos garantizar que la IA opere en interés de nuestra organización y no en el de terceros? ¿cómo podemos acceder a estas capacidades cruciales que nos ayudarán cada vez más a gestionar nuestro negocio?**

En esta era de externalización de la IA, la soberanía digital (la capacidad de controlar y gobernar la infraestructura digital, los datos y las tecnologías de cada uno) es una contramedida necesaria. En este artículo, definimos la soberanía digital utilizando cuatro principios clave: Soberanía de propósito, Inspección, Adaptación y Elección de proveedores.

La dependencia de modelos cerrados y patentados de IA cómo paquetes de servicio, también introduce cinco riesgos graves: Riesgo de alineamiento (en el que el comportamiento del modelo puede sesgar sutilmente las decisiones para servir a intereses extranjeros); Riesgos de confidencialidad y privacidad (ya que todos los datos de entrada y salida se transfieren y almacenan en el extranjero, lo que puede infringir leyes de cumplimiento como el RGPD); Riesgo de disponibilidad (en el que operaciones críticas pueden quedar paralizadas por la denegación del servicio); Riesgo de integridad (en el que los proveedores pueden implementar un modelo secretamente limitado o censurado); y Riesgo de cumplimiento (que se ve agravado por la legislación extranjera en materia de vigilancia, como la CLOUD Act de EE. UU.).

Aunque la tecnología se ha desarrollado rápidamente, el debate sobre la soberanía de la IA ha obstaculizado significativamente su adopción en Europa. Las organizaciones europeas, especialmente en el sector público, se han mostrado reacias a adoptar nuevas tecnologías debido a las preocupaciones sobre la autonomía tecnológica. Como resultado, la adopción de la IA se ha estancado, lo que ha puesto a Europa en una situación de desventaja competitiva.

Surge un dilema fundamental, ya que los LLM más capaces en la actualidad plantean el mayor riesgo para la soberanía debido a su naturaleza cerrada. Para mitigar esto, las organizaciones deben alejarse del enfoque de "confiar y no verificar" y adoptar un conjunto de estrategias claras. La vía más eficaz para alcanzar una mayor soberanía es la IA autohospedada y Open-weight, que permite a las organizaciones ejecutar modelos verificados en una infraestructura soberana, mitigando por completo los riesgos relacionados con la disponibilidad, la confidencialidad y la integridad. Otras estrategias clave son la implementación de arquitecturas independientes de los proveedores de IA para permitir cambios fluidos y dar prioridad a los proveedores de servicios de IA nativos de la UE para asegurar el cumplimiento normativo.

En Eraneos, entendemos que las regulaciones tienen un alcance limitado. Por ello, nos centramos en la necesidad estratégica de lograr la soberanía digital para los servicios de IA, guiando a las empresas para que saquen el máximo partido a sus soluciones de IA sin comprometer el control. En este documento, exploramos los riesgos únicos que plantea la dependencia de la IA extranjera y proporcionamos estrategias concretas para que las organizaciones mitiguen estas amenazas y avancen hacia una postura de IA independiente y soberana.

Comprender la soberanía de la IA

La mayoría de los servicios de IA de vanguardia, en particular los LLM avanzados, son prestados por un pequeño grupo de proveedores con sede en el extranjero y altamente capitalizados, predominantemente de Estados Unidos (como OpenAI, Google, xAI y Anthropic). Estos servicios de IA, y los datos de su organización —tanto los datos introducidos en los modelos como los resultados que generan— solo están disponibles con el consentimiento y el apoyo del proveedor. En última instancia, el control lo tiene el fabricante de la solución de IA. Por eso es importante comprender qué significa la soberanía de la IA, su importancia estratégica y su relevancia en el contexto más amplio de la soberanía digital.

La importancia estratégica de la soberanía de la IA

¿Confía plenamente en estos terceros, especialmente ahora que los sistemas de IA impulsan cada vez más la estrategia y las operaciones? Las organizaciones deben plantearse algunas preguntas importantes sobre estos proveedores:

- ¿**Seguirán prestando sus servicios de forma fiable** incluso ante presiones políticas? (Riesgo de disponibilidad)
- ¿**Mantienen la confidencialidad de los datos** y las formas de entrenamiento de modelos frente a intereses de terceros, incluso agencias de inteligencia? (Riesgos de confidencialidad y privacidad)
- ¿**Se puede manipular** o censurar **el comportamiento del modelo de IA** sin su conocimiento? (Riesgos de integridad y alineación)
- ¿**Puede su organización cumplir con las leyes y normativas** que rigen sus datos y la toma de decisiones? (Riesgo de cumplimiento)

Tanto las recientes tensiones geopolíticas entre la UE y los EE. UU. como el cada vez más férreo control de los segundos sobre los proveedores de IA han alterado profundamente los equilibrios de confianza, no solo para los estados miembros de la UE, sino para todas las organizaciones de la UE. Esto exige una reevaluación crítica de la relación de dependencia que nuestra sociedad y sus organizaciones tienen con estos proveedores de servicios de IA extranjeros dominantes.

En este artículo, hemos esbozado una definición de soberanía digital en el contexto de los servicios de IA. También hemos identificado oportunidades para lograr un mayor control, una mayor agilidad, una mejor resiliencia y una ventaja estratégica a largo plazo mediante estrategias de IA soberanas.

Definición de soberanía digital en la era de la IA

La soberanía digital es la capacidad de una organización para controlar y gobernar su propia infraestructura digital, sus datos y sus tecnologías. En el contexto de la IA, esto significa garantizar que las soluciones complejas de IA que impulsan cada vez más la estrategia y las operaciones de una organización se ajusten a los intereses, valores y requisitos jurisdiccionales únicos de la organización.

En el caso de los servicios de IA, la soberanía digital se manifiesta a través de cuatro principios clave:

1. Soberanía de propósito
La organización debe poder elegir libremente cómo y con qué finalidad utilizar los sistemas de la IA sin temor a la coacción o la interferencia de terceros (por ejemplo, el proveedor de IA o el Estado que lo regula). Esto garantiza que los sistemas de IA sirvan en última instancia a los objetivos de la organización.

2. Soberanía de inspección
La organización debe tener la capacidad de comprender, inspeccionar y auditar el sistema de IA. Esto es crucial para verificar el alineamiento, evitar la introducción de sesgos y garantizar que el modelo no sirva a intereses ocultos adversos.

3. Soberanía de la adaptación
La organización debe ser capaz de adaptar los sistemas de IA a sus necesidades cambiantes y a su contexto único. La dependencia de un modelo cerrado y externo restringe gravemente esta capacidad, lo que hace que la organización sea inflexible.

4. Soberanía del proveedor
Una organización debe poder elegir y cambiar libremente entre proveedores de servicios de IA, evitando la dependencia y el bloqueo de un único proveedor poderoso. Esto mitiga el poder de fijación de precios del proveedor, el riesgo de disponibilidad y permite una estrategia de salida cuando cambia la evaluación de riesgos de un proveedor o los objetivos estratégicos de la compañía.

Evaluación de la soberanía: niveles de preparación y riesgos

Riesgos de la dependencia digital impulsada por la IA

La dependencia de los servicios de IA extranjeros introduce riesgos específicos y graves que se derivan de la naturaleza inherente de los modelos de IA, sus inmensos costes de entrenamiento y la consiguiente concentración de poder entre unos pocos proveedores con sede en Estados Unidos. Identificamos cinco riesgos fundamentales para la soberanía en torno a las tecnologías de IA:

1. Riesgo de alineamiento
Este es posiblemente el riesgo más insidioso. Los LLM y otros sistemas avanzados de IA se entrenan y perfeccionan para mostrar o inhibir ciertos comportamientos. Un proveedor de IA puede, sin su conocimiento, guiar sutilmente su toma de decisiones, ocultar información sobre ciertos temas o introducir sesgos que se alineen con las prioridades del proveedor o de su gobierno. Si externalizamos nuestro pensamiento y nuestra toma de decisiones, debemos asegurarnos de que los "intereses" de la máquina estén alineados con los nuestros. La naturaleza opaca y de "caja negra" de los modelos propietarios cerrados hace imposible verificar el verdadero alineamiento.

2. Riesgo de confidencialidad y privacidad (fuga de datos)
Cuando una organización utiliza un modelo LLM-as-a-Service, todos los datos enviados al modelo (entrada) y todos los datos generados por él (salida) son recibidos y almacenados por el proveedor. Estos datos sensibles podrían utilizarse, sin su consentimiento explícito, para seguir formando a la IA, para investigación, para su reventa o incluso para ofrecerse a servicios de inteligencia extranjeros y corredores de datos, tal y como permite la legislación estadounidense CLOUD Act. Incluso las promesas de "no uso" son imposibles de verificar.

El uso de servicios de IA, en particular los que manejan datos sensibles de clientes o empleados, debe cumplir con normativas estrictas como el RGPD de la UE. Depender de proveedores extranjeros cuyas prácticas en materia de datos están sujetas a jurisdicciones no pertenecientes a la UE (por ejemplo, la Ley de Vigilancia Extranjera de EE. UU.) hace que sea extremadamente difícil, si no imposible, garantizar el cumplimiento y proteger los derechos de privacidad de los ciudadanos, lo que expone a la organización a un riesgo legal y financiero significativo.

3. Riesgo de disponibilidad (denegación de servicio)
A medida que los servicios de IA se convierten en una parte fundamental de los flujos de trabajo de las organizaciones, aumenta la dependencia de su funcionamiento continuo. Un proveedor extranjero de servicios de IA, al igual que un proveedor de servicios en la nube, puede denegar el servicio por motivos políticos, relacionados con sanciones o accidentales. Esto podría paralizar instantáneamente procesos empresariales críticos, aumentando la dependencia y disminuyendo la soberanía.

4. Riesgo de integridad (manipulación del modelo)
Los proveedores extranjeros de IA mantienen el control sobre los pesos y la configuración del modelo. Pueden decidir, sin su conocimiento o sin que usted pueda darse cuenta, implementar un modelo deficiente o censurado en función de su identidad, lugar de trabajo o ubicación geográfica. Esta violación de la integridad significa que los resultados de la IA podrían verse sutilmente alterados o incompletos de formas que vayan en contra de sus intereses, lo que daría lugar a malos resultados operativos o estratégicos. Dado que el proveedor opera fuera de la jurisdicción de su organización, es imposible detectar o diagnosticar dicha manipulación sin su ayuda activa.

Niveles de preparación para la soberanía digital en materia de IA

Para pasar de la dependencia digital a la soberanía digital plena al utilizar servicios de IA, una organización debe determinar primero con precisión su posición actual en el espectro de dependencia-soberanía. Esta evaluación es crucial para definir las ambiciones de soberanía específicas y trabajar activamente para alcanzarlas.

Dividimos el grado de la soberanía de la IA en cuatro niveles de preparación:

Nivel	Descripción	**Implicaciones para la soberanía de la IA**
0	**Dependiente** 	La organización utiliza modelos cerrados y patentados de IA como servicio de proveedores extranjeros (por ejemplo, con sede en EE. UU.). Los riesgos para la soberanía son desconocidos o no se han analizado. La dependencia se basa únicamente en la confianza, sin que se hayan adoptado medidas para mitigar los riesgos de de alineamiento, confidencialidad, disponibilidad, integridad o privacidad.
1	**Preparada** 	La organización depende de proveedores de servicios de IA extranjeros, pero ha identificado y analizado sus principales riesgos para la soberanía. Se han tomado medidas para reducir los riesgos actuales para la soberanía y la organización está preparada para avanzar hacia el nivel 2 (independiente) en el futuro con una interrupción mínima. Se conocen los riesgos para la confidencialidad, la integridad y la alineación de los datos, pero por ahora siguen basándose en una confianza no verificada.
2	**Independiente** 	La organización solo depende parcialmente de proveedores extranjeros de IA. Los riesgos para la soberanía se mitigan de forma activa (por ejemplo, utilizando proveedores de servicios de IA nativos de la UE o flujos de trabajo altamente protegidos y cifrados de extremo a extremo). Se garantiza la continuidad del negocio. Los datos críticos y sensibles en materia de privacidad que se envían a la IA están protegidos, y la integridad del proceso es verificable hasta cierto punto.
3	**Soberana** 	La organización es casi independiente de los proveedores de servicios de IA extranjeros para su funcionamiento continuo (por ejemplo, utilizando IA Open-Weight autohospedada en infraestructura soberana). Los riesgos para la soberanía se supervisan continuamente y se gestionan de forma activa. La organización tiene control sobre los pesos del modelo de IA, el proceso de inferencia, el hardware, el software y los conocimientos técnicos internos, lo que mitiga eficazmente los cinco riesgos fundamentales.

En las siguientes secciones, describiremos estrategias específicas para aumentar su nivel de preparación para la soberanía digital de la IA.

Estrategias de servicios de IA soberanos

El uso de tecnologías de IA se está convirtiendo rápidamente en algo imprescindible para las organizaciones de todo el mundo. La mayor parte de la innovación y la comercialización de las tecnologías y servicios de IA está impulsada por empresas extranjeras de Estados Unidos y China. Esto introduce un riesgo de soberanía muy real: si externalizamos nuestro pensamiento y nuestra toma de decisiones a las máquinas, y estas máquinas están bajo el control de empresas y gobiernos extranjeros, ¿cómo podemos garantizar que las máquinas trabajen en nuestro interés y no en el suyo?

Los cinco riesgos fundamentales para la soberanía en relación con las tecnologías de IA son:

- **Disponibilidad:** ¿Cuál es el riesgo de que el proveedor de servicios de IA deje de prestar sus servicios?
- **Confidencialidad:** ¿Son confidenciales los datos enviados al modelo de IA y generados por este?
- **Integridad:** ¿Pueden modificarse sin su conocimiento los datos procesados por el modelo de IA, el propio modelo o las aplicaciones de IA?
- **Privacidad:** ¿puede cumplir con las normas de privacidad cuando utiliza la IA?
- **Alineamiento:** ¿El modelo de IA funcionará en su interés o en el de otra persona?

Los avances recientes han situado a los LLM como la punta de lanza de la disrupción tecnológica que impulsa estos riesgos. Dado que los modelos más capaces suelen ofrecerse como un servicio gestionado, los datos más sensibles y los procesos de toma de decisiones de una organización están continuamente expuestos a estos riesgos. Concretamente, la naturaleza de la forma en que se crean y despliegan los LLM se traduce directamente en un mayor riesgo de alineamiento, confidencialidad e integridad, lo que hace que sea esencial realizar un análisis centrado en sus características para desarrollar una estrategia de soberanía sólida.

Soberanía de la IA para los modelos de lenguaje grandes

Antes de poder protegerse realmente contra los riesgos de los LLM, las organizaciones deben comprender plenamente qué es exactamente un LLM.

Un LLM es un sofisticado sistema de IA diseñado para procesar, comprender y generar textos complejos similares a los humanos a partir de enormes volúmenes de datos lingüísticos. Estos modelos se entrenan con diversas fuentes, que abarcan libros, artículos y un vasto contenido web, lo que les permite dominar los patrones lingüísticos, la gramática, los conocimientos fácticos y las complejas capacidades de razonamiento. El resultado es la capacidad de comprender las indicaciones del usuario y ofrecer respuestas muy coherentes y adecuadas al contexto. Es importante destacar que los LLM modernos están ampliando rápidamente su utilidad gracias a sus capacidades multimodales, que les permiten interpretar y generar documentos, imágenes, audio, vídeo y código de programación.

En esencia, los LLM funcionan mediante deep learning, un enfoque de aprendizaje automático que aprovecha las simulaciones de redes neuronales. Una red neuronal procesa la información pasando la entrada a través de múltiples capas de neuronas simuladas interconectadas. Cada conexión posee un valor numérico conocido como peso (o ponderación).

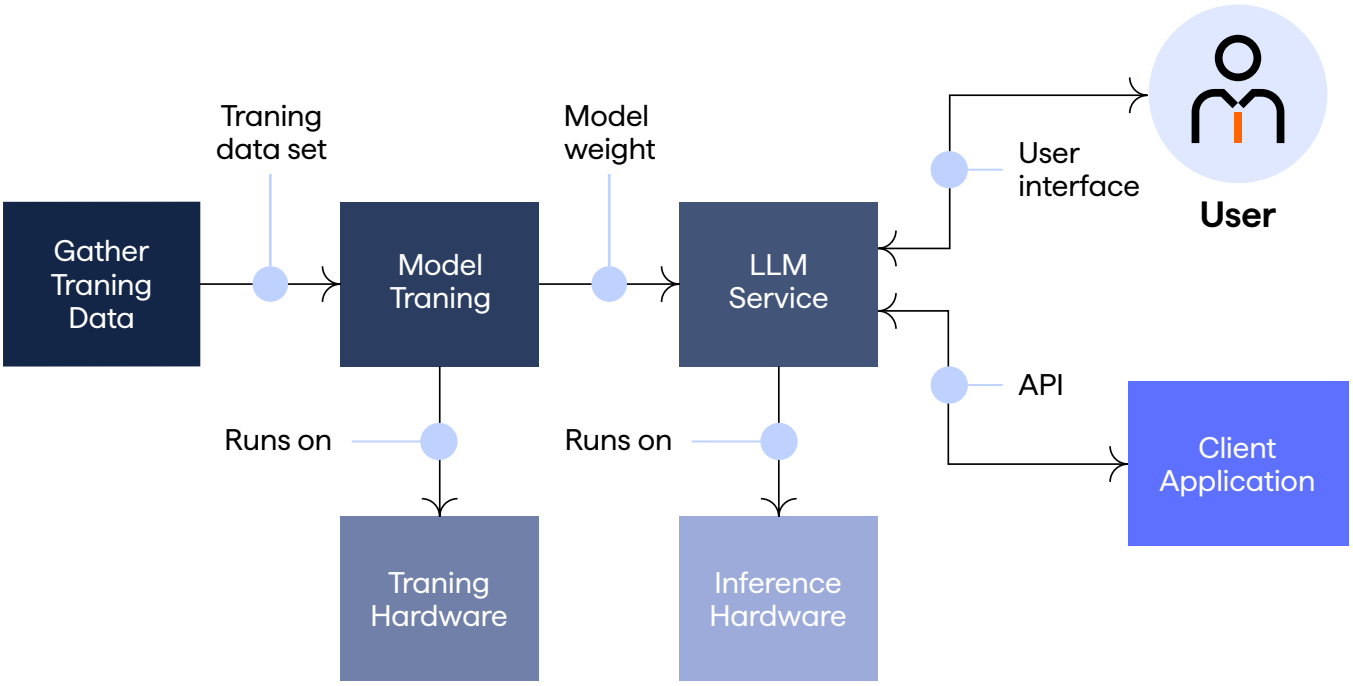
Durante la fase de entrenamiento, estos pesos se calibran automáticamente en función de los datos de entrada proporcionados y la salida deseada. Cuando la red se ejecuta posteriormente (un proceso conocido como inferencia), estos pesos aprendidos se cargan en la memoria y la nueva entrada se procesa a través de la estructura para producir la salida final.

Cómo se crean los modelos de lenguaje grandes

El ciclo de vida de un LLM es un esfuerzo de ingeniería de varias etapas. Comienza con el paso crítico de recopilar un conjunto de datos grande y de alta calidad: los datos de entrenamiento designados. Estos datos sirven de base para las fases posteriores: el diseño de una arquitectura de modelo robusta y la creación de un sofisticado sistema de entrenamiento de modelos.

El núcleo del proceso consiste en entrenar el modelo en este sistema utilizando los datos de entrenamiento acumulados, seguido del refinamiento del modelo mediante diversas técnicas posteriores al entrenamiento (por ejemplo, protocolos de alineamiento y seguridad).

La utilidad del LLM en la producción requiere dos pasos críticos adicionales: ejecutar el LLM (inferencia) y facilitar de manera eficiente el modelo a los usuarios finales o a las aplicaciones cliente a través de una interfaz de servicio LLM dedicada. Todo este proceso requiere un capital significativo y conocimientos especializados.



Los requisitos de capital y computación necesarios para entrenar y mantener un LLM de última generación son enormes, lo que hace que esta tarea sea inviable para casi todas las organizaciones globales, excepto las que cuentan con un gran capital. En consecuencia, los recursos para desarrollar y comercializar los modelos más avanzados se concentran en gran medida en un pequeño número de proveedores, predominantemente con sede en Estados Unidos.

Esta dinámica del mercado dicta el modelo de disponibilidad: los LLM con mejor rendimiento son modelos patentados y muy protegidos. El acceso se ofrece casi exclusivamente a través de un modelo LLM como servicio basado en el consumo, ejemplificado por plataformas como ChatGPT (OpenAI), Claude (Anthropic), Gemini (Google) y Grok (xAI). Esta dependencia de servicios externos cerrados amplifica inherentemente la dependencia digital y los riesgos de soberanía asociados.

Clasificación de los LLM de IA: Un espectro de apertura

Para evaluar y mitigar eficazmente los riesgos de soberanía, debemos clasificar los modelos de lenguaje grandes (LLM) en función de su grado de apertura. Esta clasificación se correlaciona directamente con el control que una organización puede ejercer sobre la tecnología.

- **Datos abiertos (Open-data):** todo el conjunto de datos utilizado para entrenar el modelo está disponible de forma gratuita y pública. Esto permite una verificación completa de la procedencia y reduce el riesgo de sesgo, lo que representa el nivel más alto de soberanía.
- **Entrenamiento abierto (Open-training):** el código y la metodología utilizados para entrenar el modelo son de acceso público. Esto permite una inspección más profunda y la reproducibilidad total del proceso de entrenamiento.
- **Peso abierto (Open-weights):** los "pesos" cruciales del modelo (el resultado del proceso de entrenamiento) están disponibles para su descarga y uso de forma gratuita. Esta es la condición necesaria para el alojamiento propio y la validación completa de la integridad, lo que mitiga significativamente el riesgo.

Por el contrario, los modelos de peso cerrado mantienen estos pesos privados, accesibles solo a través de una API de servicio gestionado o una interfaz propietaria. Este enfoque de modelo como servicio crea la mayor dependencia.

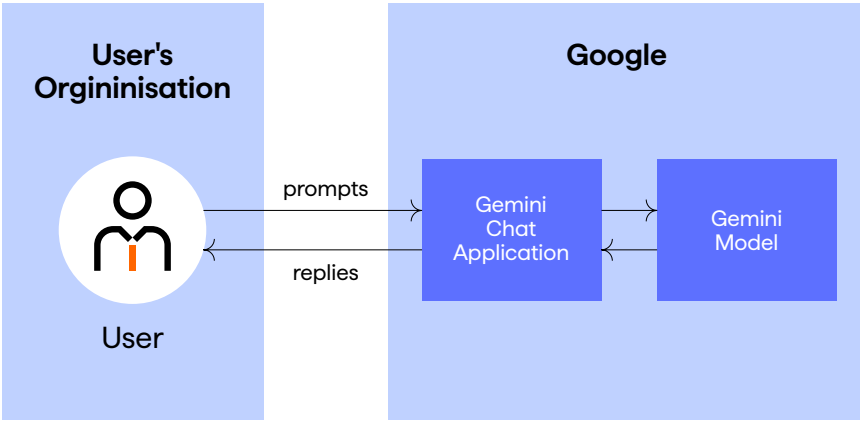
La realidad actual del mercado es que los LLM más capaces y avanzados (los que las organizaciones buscan para obtener una ventaja competitiva) se ofrecen predominantemente como modelos de peso cerrado. Este enfoque de servicio gestionado y propietario dicta inherentemente una pérdida fundamental de control sobre el funcionamiento del modelo, su comportamiento y los datos que fluyen a través de él. Es precisamente esta dependencia estructural de proveedores externos para los pesos básicos y el proceso de inferencia lo que introduce y amplifica los siguientes riesgos críticos para la soberanía.

Aplicaciones de IA y despliegue

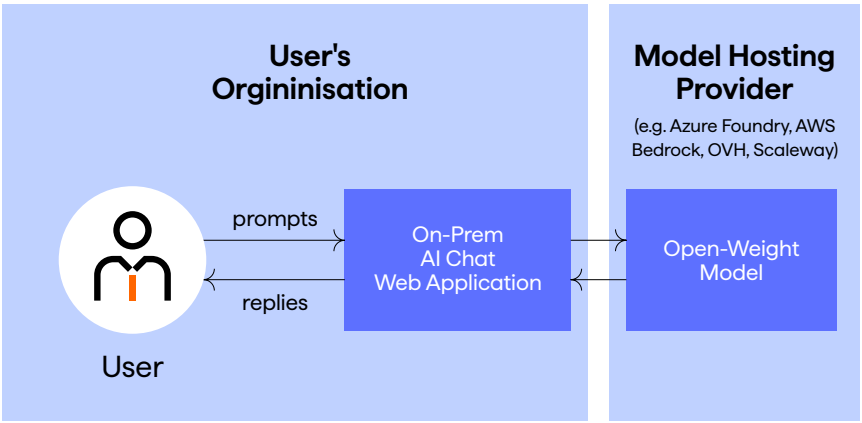
Una vez entrenado un modelo de IA, se despliega en servidores equipados con hardware especializado capaz de ejecutar el modelo. Las comunicaciones con el modelo de IA funcionan a través de una API.

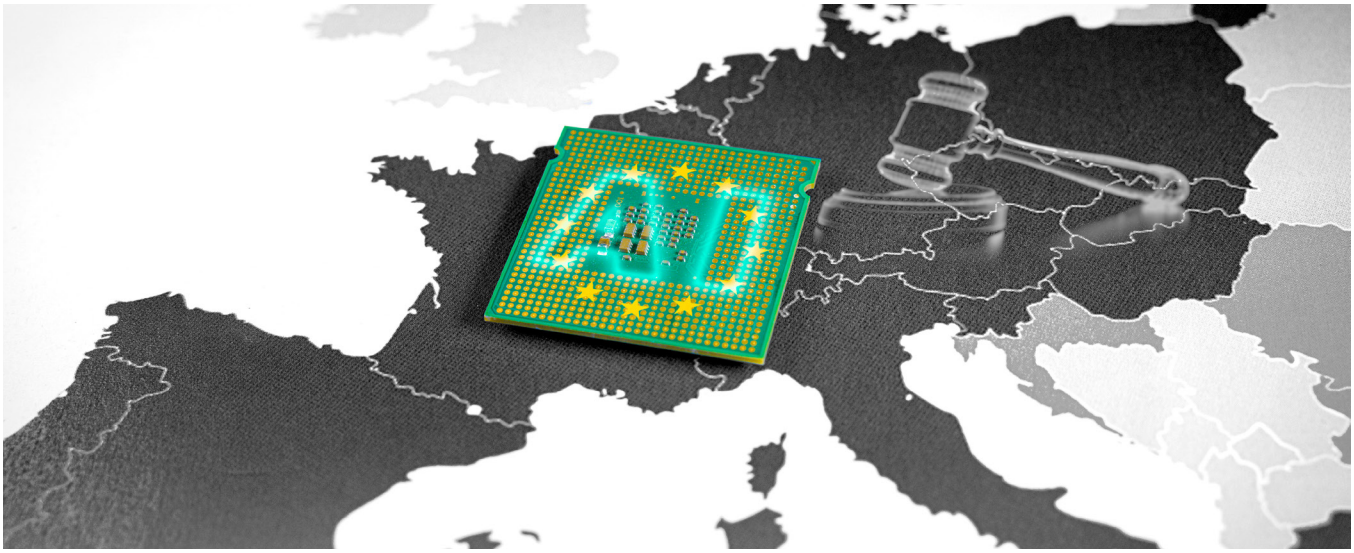
A continuación, este modelo de IA es utilizado por una aplicación de IA, como una interfaz de chat orientada al usuario, un agente autónomo o un software habilitado para IA. La aplicación de IA utiliza el modelo de IA a través de una API.

Muchas aplicaciones de IA orientadas al usuario, como ChatGPT, Gemini y Claude, son una combinación de una aplicación y un modelo alojados y entrenados por el mismo proveedor. Por ejemplo, la interfaz de chat Gemini está desarrollada y alojada por Google, que utiliza modelos de lenguaje grande Gemini entrenados y alojados por Google. En tal escenario, la organización del usuario depende en gran medida de una sola parte: Google.



Pero es importante tener en cuenta que la aplicación, la implementación del modelo y el entrenamiento del modelo pueden separarse. La aplicación podría ser creada y alojada por una parte, mientras que el modelo estaría alojado por otra parte y entrenado por una tercera parte. Por ejemplo, se puede utilizar una aplicación de chat propia o de código abierto alojada en las instalaciones, como un modelo de Open-weights entrenado por un laboratorio de IA alojado en un proveedor de alojamiento de modelos (Model Hosting Provider). En este escenario, la organización es libre de elegir otro proveedor de alojamiento de modelos, desplegar el modelo de peso abierto y hacer el cambio completo con una interrupción mínima para los usuarios y, por lo tanto, para la continuidad del negocio.





Decisiones cruciales en la soberanía de la IA

Hay cuatro decisiones cruciales que afectan a la soberanía de la IA y a la preparación para avanzar hacia una mayor soberanía de la IA en el futuro:

1. La elección del modelo de IA
2. La elección del proveedor de alojamiento de modelos de IA
3. La elección de la aplicación de IA
4. La elección del proveedor de alojamiento de la aplicación de IA

La elección del modelo de IA

Los modelos de IA de open-weights permiten elegir libremente el proveedor de alojamiento del modelo, lo que facilita una salida segura, permite la diversificación de proveedores, reduce la dependencia de un único proveedor y su poder de fijación de precios, y disminuye el riesgo de disponibilidad. Además, la capacidad de controlar la versión del modelo evita actualizaciones subrepticias que reduzcan la integridad y el riesgo de desalineamiento. La capacidad de ajustar el modelo permite adaptar su rendimiento a las necesidades de su organización.

Los modelos de IA de datos abiertos y entrenamiento abierto reducen la dependencia del desarrollador del modelo de IA. Dado que los datos y el método de entrenamiento son abiertos, otras organizaciones pueden volver a formar el modelo. Además, es posible validar el método de entrenamiento y los datos para tener confianza en la adecuación del modelo.

La jurisdicción de la empresa desarrolladora del modelo y las entidades de control también son motivo de preocupación. Los desarrolladores de modelos en otras jurisdicciones (por ejemplo, Estados Unidos) pueden verse influenciados por los intereses de su empresa, su empresa matriz o su Estado, y es posible que estos intereses no coincidan con los suyos. El desarrollador del modelo de IA podría, por fuerza, amenaza o elección, entrenar el modelo para que muestre un determinado comportamiento. Por ejemplo, muchos modelos de IA entrenados por laboratorios chinos se niegan a discutir temas políticamente sensibles. También es posible entrenar modelos para que alerten a las autoridades cuando se detecta un determinado comportamiento.

Elegir un modelo entrenado por un desarrollador de modelos que se encuentre en una jurisdicción aliada, por ejemplo, dentro de la UE, reduce los riesgos asociados a la influencia de actores extranjeros en su IA.

La elección del proveedor de alojamiento del modelo de IA

La ubicación **del alojamiento del modelo** es un factor que influye en la localización de los datos. Los datos de entrada y salida se envían desde y hacia la ubicación de alojamiento del modelo.

La jurisdicción de la entidad proveedora de alojamiento de modelos influye en qué partes y gobiernos pueden influir en el proveedor de alojamiento de modelos, por ejemplo, para cerrar los servicios a empresas, países u organizaciones específicos. ¿La entidad controladora tiene su sede en el país, en la UE, en los EE. UU. o en otro lugar?

La elección de la aplicación de IA

Las aplicaciones de IA propietarias, por ejemplo, las plataformas de chat o las aplicaciones habilitadas para IA, son de código cerrado. Esto significa que hay que confiar en que el software no afecta a la integridad o la confidencialidad de los datos, pero no se puede verificar. Además, usted depende del proveedor de software para la continuidad del uso. Los proveedores sujetos a una jurisdicción extranjera podrían verse obligados por sus gobiernos, mediante sanciones (o la amenaza de las mismas), a interrumpir el suministro, el servicio y el mantenimiento. También pueden verse obligados en secreto a compartir datos o instalar puertas traseras por parte de los servicios de inteligencia extranjeros.

Las aplicaciones de IA gratuitas y de código abierto (FOSS) (por ejemplo, interfaces web de chat, agentes o aplicaciones habilitadas para IA) ofrecen la libertad de implementar, inspeccionar y modificar la aplicación. Esto reduce el riesgo de confidencialidad al permitir verificar que el software no filtra información confidencial ni realiza un seguimiento o supervisión de los usuarios. También reduce el riesgo de disponibilidad, ya que el software es gratuito y de código abierto, por lo que no hay ningún proveedor que pueda denegar o restringir su uso. El riesgo de integridad también se reduce, ya que puede verificar que el software no altere subrepticiamente los datos que van o vienen de los modelos de IA. Además, se puede modificar el software a su gusto o contratar a cualquier otro tercero para que lo haga por usted.

La elección de aplicaciones de IA gratuitas y de código abierto aumenta la soberanía de su stack de IA.

La elección del proveedor de alojamiento de aplicaciones de IA

Cuando una aplicación de IA se aloja fuera de su organización, todos los datos que entran y salen de la aplicación pueden ser interceptados, monitorizados y recopilados por el proveedor de alojamiento o por terceros con acceso privilegiado al proveedor de alojamiento.

Por lo tanto, es importante elegir un proveedor de alojamiento fiable para las aplicaciones de IA, a fin de evitar violaciones de la confidencialidad o la integridad. Elegir una aplicación de IA que pueda alojarse en múltiples proveedores de alojamiento (o en cualquiera) le proporciona una estrategia de salida y libertad para elegir proveedor.

Una estrategia maximalista de soberanía de IA sería, por lo tanto:

1. **Modelo de IA:** modelos de IA de peso abierto, entrenamiento abierto y datos abiertos de un desarrollador de modelos de IA en una jurisdicción de confianza.
2. **Proveedor de alojamiento de modelos de IA:** on-prem o con un proveedor de alojamiento de modelos de IA de confianza dentro de una jurisdicción de confianza con más de un proveedor.
3. **Aplicación de IA:** aplicaciones de IA gratuitas y de código abierto alojadas en un entorno de confianza.
4. **Proveedor de alojamiento de aplicaciones de IA:** on-prem o con un proveedor de alojamiento de confianza.

Mejorando la soberanía de la IA

Gran parte del uso actual de la IA se basa en modelos de IA de peso cerrado, entrenamiento cerrado y datos cerrados entrenados por un laboratorio de IA extranjero, a través de aplicaciones de IA propietarias, ambas alojadas en proveedores de servicios en la nube extranjeros, lo que maximiza los riesgos para la soberanía de la IA.

Pero se trata de una elección por defecto, no de una necesidad práctica.

Durante su transformación de IA, hay opciones reales, prácticas y sin remordimientos que puede tomar ahora para evitar que los riesgos de soberanía de IA le afecten en el futuro:

1. Exija libertad para elegir un proveedor de IA

Al seleccionar, crear o adquirir aplicaciones (habilitadas) para IA, exija que la aplicación pueda funcionar con más de un modelo de IA y más de un proveedor de modelos de IA. Esto le hace independiente del desarrollador y del proveedor del modelo de IA, lo que le permite una estrategia de salida sencilla si cambia la evaluación de riesgos. Priorice las instalaciones propias sobre las nacionales, las de la UE, las de EE. UU. y las de cualquier otro lugar en lo que respecta a la localización de los datos y la jurisdicción de la entidad controladora.

2. Exija libertad para elegir un proveedor de alojamiento de aplicaciones de IA

Al seleccionar, crear o adquirir aplicaciones de IA, exija que la aplicación pueda alojarse en cualquier proveedor de su elección. Esto le permite cambiar de proveedor de alojamiento si el actual deja de estar disponible, no está dispuesto a prestar el servicio o su uso resulta demasiado arriesgado o costoso. En lo que respecta a la ubicación de los datos y la jurisdicción de la entidad, dé preferencia a las instalaciones propias.

3. Priorice aplicaciones que sean gratuitas y de código abierto

A la hora de seleccionar aplicaciones de IA, opte por software gratuito y de código abierto, ya que le permitirá auditar el software y modificarlo o ampliarlo según sus necesidades. Esto también le hará independiente de los desarrolladores, ya que podrá contratar a cualquier persona para mejorar o mantener el software en caso de que sea necesario.

4. Priorice modelos de IA abiertos

Exija que la aplicación de IA pueda funcionar con modelos de peso abierto. Esto le permitirá cambiar de proveedor de alojamiento de modelos de IA sin tener que cambiar el modelo. Prefiera modelos de entrenamiento abierto y datos abiertos.

Seguir estos cuatro principios al elegir sus aplicaciones y modelos de IA le permite alcanzar un equilibrio pragmático: no es independiente, pero tampoco está atrapado en una dependencia. Esto le permite, como mínimo, cambiar de proveedor, modelo y aplicación a su antojo cuando los riesgos futuros se conviertan en crisis agudas.

Implementar una estrategia de IA soberana hoy

Actualmente, lograr la soberanía total en materia de IA no es factible para la mayoría de las organizaciones, pero mejorar la soberanía en materia de IA es posible para todas ellas. Estas tres medidas prácticas pueden cambiar su nivel de soberanía en materia de IA, pasando de dependiente a preparado, y finalmente a independiente. Cada medida puede implementarse de forma individual o conjunta.

Medida 1: Chat independiente del proveedor de IA

Cuando se utiliza un chat web de IA como ChatGPT, Claude o Gemini, la aplicación de IA (ChatGPT), los modelos (GPT) y el proveedor de alojamiento de modelos (OpenAI) son proporcionados por un único proveedor. Esto aumenta los riesgos de soberanía: todos los datos, la disponibilidad y el comportamiento del modelo están controlados por un único proveedor.

Estos riesgos pueden reducirse utilizando una aplicación de chat de IA de terceros que sea independiente del proveedor. De esta manera, la compañía controla la interfaz y puede elegir libremente entre múltiples modelos de IA y proveedores de alojamiento de IA. Además, esta medida le permite controlar los datos, las integraciones, el coste y el presupuesto. Una aplicación de chat de IA independiente del proveedor puede alojarse en un proveedor de alojamiento de su elección, lo que aumenta aún más la libertad de elección y reduce la dependencia de un único proveedor.

Medida 2: Agentes independientes del proveedor de IA

Agentes como Claude Code, Codex y Gemini CLI están estrechamente vinculados a un único proveedor de modelos y a sus modelos propietarios. Seleccionar un agente independiente del proveedor le permite elegir libremente tanto los proveedores de modelos como los modelos.

Medida 3: Pasarelas de IA independientes del proveedor de IA

Una solución más general para garantizar la independencia del proveedor y el control sobre los datos es implementar una pasarela de IA. Se trata de un servicio de software que conecta las aplicaciones de IA a los modelos de IA. Se puede implementar como SaaS o en un proveedor de alojamiento de su elección. Una pasarela de IA sirve como proxy entre sus aplicaciones de IA (como interfaces de chat y agentes) y los proveedores de alojamiento de modelos. Esto garantiza la libre elección del proveedor de modelos y le da control. Por ejemplo, puede asegurarse de que determinadas aplicaciones de IA utilicen solo determinados modelos (que cumplan con la normativa) y proveedores de modelos, obtener información y control sobre los costes y cambiar de proveedor sin problemas si es necesario.

Servicios integrales que generan impacto

Combinando una profunda experiencia en el sector con la excelencia tecnológica, Eraneos ofrece un impacto empresarial medible. Un enfoque pragmático garantiza una adopción sostenible frente a una implementación experimental, mientras que las metodologías probadas y el estatus de líder en IA generativa convierten los retos en ventajas estratégicas, todo ello con plena soberanía y cumplimiento normativo.

Asóciese hoy mismo con Eraneos para implementar las medidas de soberanía de IA que se adapten a su organización y garantizar la continuidad, la confidencialidad y la integridad en la era de la IA.

Author:

Mathijs de Meijer
Senior Consultant – Data & AI
Eraneos

mathijs.de.meijer@eraneos.com

Contáctanos

Claudia Schulze
Partner – Data & AI
Alemania
claudia.schulze@eraneos.com

Dave Kiwi
Practice Lead – Data & AI
Países Bajos
dave.kiwi@eraneos.com

Katharina Fulterer
Partner – Data & AI
Suiza
katharina.fulterer@eraneos.com

Eduardo Martín
Senior Manager – Sourcing & IT Advisory
España
eduardo.martin@eraneos.com