Gartner

Las principales tendencias tecnológicas estratégicas para 2026

Cómo orientarse en un mundo hiperconectado, impulsado por la IA

Los responsables de tecnología se enfrentan a un año decisivo en 2026, con unos niveles de disrupción, innovación y riesgo acelerándose a una velocidad sin precedentes. Las 10 principales tendencias tecnológicas estratégicas de Gartner para 2026 son algo más que cambios tecnológicos, son catalizadores de la transformación del negocio y exigen una respuesta por parte de la alta dirección.

Las tendencias de este año reflejan la realidad de un mundo hiperconectado e impulsado por la IA, en el que tener una capacidad única ya no es suficiente. Se han organizado en tres perfiles estratégicos que definen de qué forma las principales organizaciones van a innovar, competir y proteger su valor:

El arquitecto

Crea unas bases digitales seguras, escalables y adaptativas con plataformas de desarrollo nativas de IA, supercomputación de IA y computación confidencial.

El sintetizador

Orquesta diferentes tecnologías, desde sistemas multiagente hasta modelos de lenguaje específicos de dominio e inteligencia artificial física, para encontrar nuevas fuentes de valor.

El vanguardista

Potencia la confianza, la gobernanza y la seguridad mediante la ciberseguridad preventiva, la procedencia digital, las plataformas de seguridad de IA y la geopatriación.

Al examinar estas tendencias, pregúntate si están alineadas con las ambiciones estratégicas de tu organización y cómo puedes integrarlas en tus planificación para conseguir un crecimiento sostenible y ventaja competitiva.

Gene Alvarez
Distinguido vicepresidente, Business and Technology Insights, Gartner

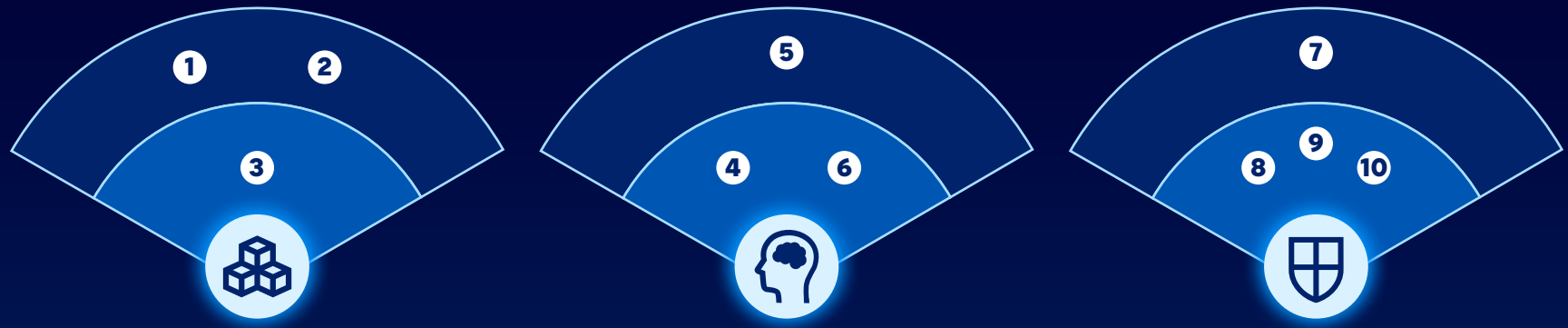
Las principales tendencias tecnológicas estratégicas de Gartner para 2026

Gartner ha seleccionado meticulosamente estas 10 tendencias por el potencial que ofrecen de impulsar la innovación, reforzar la resiliencia y mejorar la confianza en un mundo hiperconectado e impulsado por la IA.

Se trata de prioridades estratégicas que requieren reflexión y una acción decisiva por parte de los responsables de tecnología.

Ahora
De 1 a 3 años

Futuro próximo
De 3 a 5 años



El arquitecto

1. Plataformas de desarrollo nativas de IA
2. Plataformas de supercomputación de IA
3. Computación confidencial

El sintetizador

4. Sistemas multiagente
5. Modelos de lenguaje específicos de dominio
6. IA física

El vanguardista

7. Ciberseguridad preventiva
8. Procedencia digital
9. Plataformas de seguridad de IA
10. Geopatriación

El arquitecto

Crea unas bases digitales seguras, escalables y adaptativas.

Para acelerar la innovación y la resiliencia, los responsables de tecnología deben modernizar las plataformas y la infraestructura. Las tendencias del perfil de arquitecto se centran en crear las bases de IA que permitan ganar velocidad, seguridad y escalabilidad, unas características esenciales para prosperar en un mundo hiperconectado e impulsado por la IA.

1

Plataformas de desarrollo nativas de IA

¿Qué es?
Las plataformas de desarrollo nativas de IA consiguen crear software de forma más rápida y fácil que nunca, usando la IA generativa. Entre estas plataformas se encuentran desde herramientas únicas que generan software con una sola instrucción, hasta herramientas de programación en lenguaje natural ("vibe-coding") que permiten desarrollarlo sin grandes conocimientos técnicos, e incluso agentes de IA orquestados para crear software.

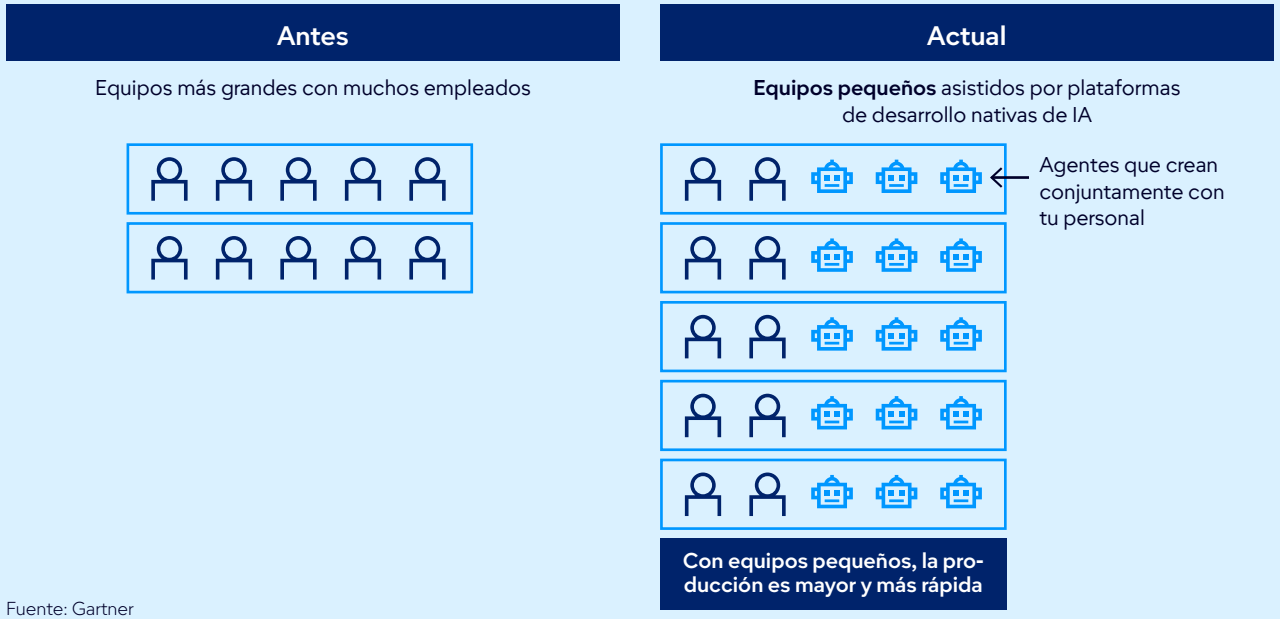
¿Por qué es tendencia?
La mayor rapidez en la entrega de software y las ganancias de productividad entusiasman a los CIO, mientras que el potencial de ahorro de costes es de interés para los CEO y los CFO. Las plataformas de desarrollo nativas de IA capacitan a los "equipos pequeños" para crear más aplicaciones con los mismos recursos; por ejemplo, cinco equipos de dos personas para entregar cinco aplicaciones a la vez. Esta tendencia permite a los CIO abordar los retrasos por acumulación y resolver el dilema entre "crear o comprar" a favor de crear.

El futuro inmediato

El **80 %** de las organizaciones transformarán los grandes equipos de ingeniería de software en equipos más pequeños, asistidos por IA, para 2030.

El **40 %** de las carteras de aplicaciones de las empresas incluirán aplicaciones personalizadas, creadas con plataformas nativas de IA, para 2030 (partiendo del 2 % en 2025).

Equipos pequeños



Fuente: Gartner

1

Consigue resultados con las plataformas de desarrollo nativas de IA

Plan de acción para potenciar la rapidez, ahorrar costes e incentivar la innovación

Pasos	1 Establece un equipo de plataforma	2 Implementa barreras de protección de la seguridad	3 Ensaya el desarrollo nativo de IA	4 Adopta la mentalidad de dar prioridad a la IA	5 Mejora las habilidades y capacidades de tus equipos
Resultado esperado	Supervisión centralizada que asegura la coherencia de los estándares y la gobernanza.	Reducción de los riesgos de código inseguro o no conforme.	"Quick wins" que demuestran valor y generan confianza.	Aceleración de la entrega y mejora de la capacidad de innovación.	Adopción más generalizada y colaboración eficaz.
Acción	Crea un equipo especializado para gestionar las plataformas nativas de IA y seleccionar los modelos de IA.	Integra las plataformas de gobernanza de la IA para la revisión y la verificación del cumplimiento del código.	Empieza con proyectos de bajo riesgo para validar las ganancias de productividad.	Prioriza las herramientas nativas de IA en las iniciativas de nuevo desarrollo.	Forma a desarrolladores y socios comerciales en materia de ingeniería de instrucciones y gobernanza.

Roles esenciales para apoyar el éxito de la implementación

CIO

Como socios: definen la estrategia basada en IA y el marco de gobernanza.

Como colaboradores: alinean las capacidades de la plataforma con las prioridades de la empresa.

Como directores: garantizan el cumplimiento y las barreras de protección de la seguridad en el desarrollo nativo de IA.

Socios de TI

Ingeniería de plataformas: gestionan las herramientas nativas de IA, sus integraciones y su rendimiento.

Seguridad: implementan la gobernanza de la IA para la revisión del código y la gestión del riesgo.

Aprovisionamiento: evalúan y seleccionan los proveedores y servicios de plataforma nativa de IA.

Socios empresariales

Responsables de producto: aportan experiencia en el dominio y validan las soluciones impulsadas por IA.

Finanzas: alinean los modelos de financiación para apoyar las iniciativas de desarrollo nativo de IA.

2

Plataformas de supercomputación de IA

¿Qué es?
Las plataformas de supercomputación de IA proporcionan la potencia de procesamiento masiva que se necesita para entrenar y ejecutar los modelos de IA avanzados. Estos sistemas combinan computación de alto rendimiento (HPC), procesadores especializados y arquitecturas escalables para manejar cargas de trabajo con uso intensivo de datos.

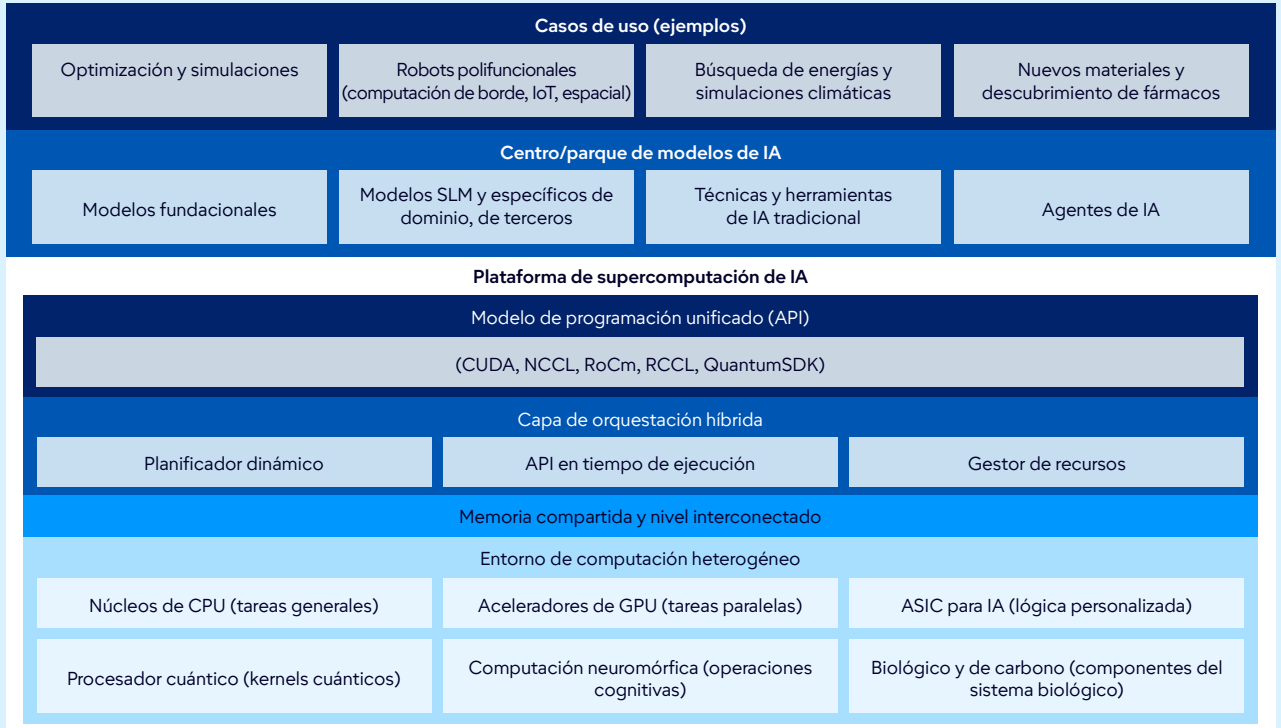
¿Por qué es tendencia?
La demanda de supercomputación de IA aumenta a medida que las organizaciones desarrollan modelos de mayor tamaño y complejidad que sobrepasan los límites de la infraestructura tradicional.

El futuro inmediato

El **40 %** de las empresas adoptarán arquitecturas de computación híbridas para 2028 (partiendo del 8 %).

+ de 20 proveedores ofrecerán plataformas para desarrolladores unificadas que aprovecharán los entornos de supercomputación, para 2028.

Plataforma de supercomputación de IA



Fuente: Gartner

2

Consigue resultados con las plataformas de supercomputación de IA

Plan de acción para activar potencia de procesamiento masiva

Pasos	1 Identifica cargas de trabajo de alto impacto	2 Invierte en pilas de software unificadas	3 Desarrolla una estrategia de integración por fases	4 Simplifica el desarrollo en los diversos entornos	5 Planifica para la gobernanza y el cumplimiento
Resultado esperado	Demostración del valor y creación de especialización interna.	Integración simplificada y asignación flexible de la carga de trabajo.	Infraestructura y fuerza laboral preparadas para el futuro.	Aceleración de la entrega y reducción de fricciones.	Reducción de riesgos y mejora de la supervisión.
Acción	Ensaya proyectos piloto usando la orquestación híbrida.	Adopta estándares abiertos en los sistemas tradicionales y emergentes.	Introduce gradualmente nuevos paradigmas computacionales y forma al personal de TI.	Anima a los equipos a adoptar las plataformas híbridas y las arquitecturas componibles.	Diseña las estrategias de seguridad y de cumplimiento a nivel del sistema.

Roles esenciales para apoyar el éxito de la implementación

CIO

Definen una estrategia de orquestación híbrida, alineada con las prioridades de la empresa.

Aseguran la gobernanza en la asignación de la carga de trabajo, la seguridad y el cumplimiento.

Se asocian con los directivos empresariales para priorizar las cargas de trabajo de alto impacto.

Socios de TI

Infraestructura y operaciones: integran los aceleradores emergentes en los sistemas heredados.

Seguridad: implementan la gobernanza en entornos de múltiples arquitecturas.

DevOps: adoptan pilas de software unificadas y herramientas de orquestación.

Socios empresariales

Producto: identifican casos de uso de computación híbrida (como simulaciones o aplicaciones basadas en IA, entre otros).

Finanzas: alinean la financiación de la integración por fases y los objetivos de sostenibilidad.

Operaciones: preparan para los flujos de trabajo basados en IA durante los procesos esenciales.

3

Computación confidencial

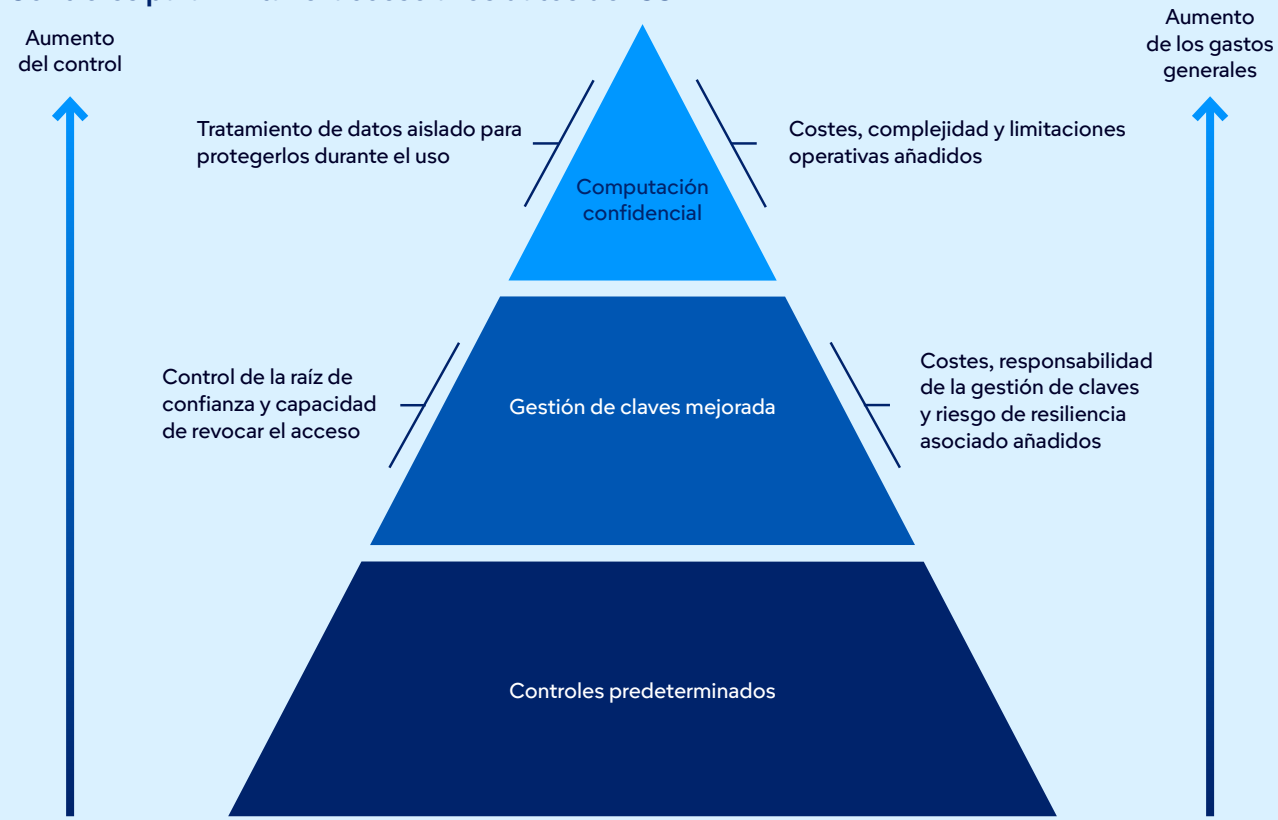
¿Qué es?
La computación confidencial consiste en usar entornos de ejecución de confianza (TEE) basados en hardware para proteger los datos durante su tratamiento, lo que previene el acceso no autorizado, incluso de los proveedores de la nube.

¿Por qué es tendencia?
Unas leyes de privacidad más estrictas, las reglas de localización de datos y la adopción de IA hacen esencial la protección durante el uso. La computación confidencial posibilita el cumplimiento y unas estrategias de nube seguras para las cargas de trabajo sensibles.

El futuro inmediato

El **75 %** del procesamiento en infraestructuras no fiables se protegerá mediante computación confidencial para 2029.

Controles para limitar el acceso a los datos del CSP



Fuente: Gartner

3

Consigue resultados con la computación confidencial

Plan de acción para garantizar un tratamiento de datos seguro y conforme a la normativa en cualquier lugar

Pasos	1 Audita las cargas de trabajo sensibles	2 Ensaya algunos TEE para los modelos de IA	3 Facilita la colaboración segura	4 Establece una gestión de claves independiente	5 Prepárate para los retos de la integración
Resultado esperado	Identificación del momento en que se requiere protección durante el uso.	Refuerzo de la confidencialidad y la protección IP.	Divulgación de conocimientos sin exponer datos en bruto.	Pleno control del acceso a los datos.	Implementación sin obstáculos en varios entornos.
Acción	Asigna las cargas de trabajo sujetas a reglas de privacidad o de localización.	Prueba los TEE con modelos de IA propios y de código abierto.	Usa la computación confidencial para análisis y proyectos de inteligencia empresarial.	Implementa sistemas de claves criptográficas propios de la organización.	Planifica la orquestación con múltiples chipsets y proveedores.

Roles esenciales para apoyar el éxito de la implementación

CIO

Definen una estrategia de computación confidencial alineada con los objetivos de privacidad, cumplimiento y nube.

Se asocian con los equipos legal y de cumplimiento para cumplir con los requisitos de localización y soberanía de datos.

Supervisan la gobernanza de los TEE y aseguran la integración en los marcos de seguridad existentes.

Socios de TI

Infraestructura y operaciones: implementan TEE en entornos híbridos y multinube.

Seguridad: incorporan procesos de atestación y gestión de claves criptográficas.

DevOps y plataforma: adaptan las cargas de trabajo para la computación confidencial y supervisan el rendimiento.

Socios empresariales

Cumplimiento: validan el respeto de los mandatos reglamentarios y la preparación para la auditoría.

Finanzas: alinean la financiación para adoptar la computación confidencial y reducir el riesgo.

Responsables de los datos: identifican las cargas de trabajo sensibles para su protección durante el uso y priorizan los proyectos.

El sintetizador

Orquesta diversas tecnologías para generar nuevo valor.

Con el fin de activar nuevas fuentes de diferenciación, los responsables de tecnología deben integrar modelos especializados, sistemas multiagente e inteligencia artificial física para soluciones específicas de dominio. Las tendencias del perfil sintetizador se centran en la orquestación de diferentes tecnologías con el objetivo de crear ecosistemas inteligentes y adaptativos que impulsen la innovación en flujos de trabajo, productos y experiencias.

4 Sistemas multiagente

¿Qué es?
Los sistemas multiagente (MAS) usan grupos de agentes de IA especializados que colaboran para llevar a cabo flujos de trabajo complejos. Cada agente se ocupa de una tarea específica, lo que mejora la eficiencia y la escalabilidad, en comparación con las soluciones de IA monolíticas.

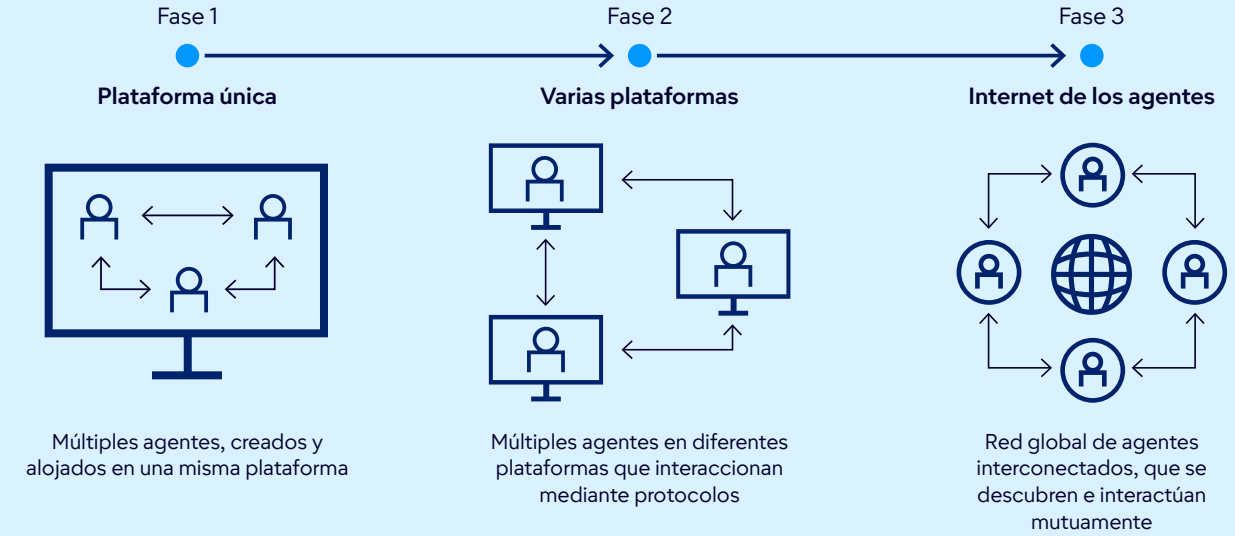
¿Por qué es tendencia?
Mientras que la IA de agente único tiene dificultades con los procesos de varios pasos, los MAS permiten la automatización modular y la integración entre varias plataformas. Hemos registrado un incremento del 1,445 % en las consultas sobre MAS entre el 1T de 2024 y el 1T de 2025, lo que demuestra el creciente interés de las empresas.

El futuro inmediato

El **70 %** de los MAS usarán agentes muy especializados para 2027, lo que mejorará la precisión, pero dificultará la coordinación.

El **60 %** de los MAS permitirán la interoperabilidad de varios proveedores para 2028, lo que impulsará la innovación y la flexibilidad.

Evolución de los sistemas multiagente



Fuente: Gartner

4

Consigue resultados con los sistemas multiagente

Plan de acción para impulsar la automatización modular y la integración sin obstáculos

Pasos	1 Identifica casos de uso de alto valor	2 Diseña agentes modulares	3 Implementa gobernanza y observabilidad	4 Adopta estándares de interoperabilidad	5 Mejora las habilidades de los equipos
Resultado esperado	Impacto medible y adopción más rápida.	Mejora de la fiabilidad y la escalabilidad.	Reducción del riesgo y optimización del control.	Inversiones en MAS preparados para el futuro.	Implementación eficaz y reducción del riesgo.
Acción	Empieza definiendo bien los flujos de trabajo para los ensayos de MAS.	Crea agentes especializados en lugar de soluciones monolíticas.	Aplica herramientas de gobernanza y de supervisión de API sólidas.	Usa los protocolos emergentes para la colaboración entre agentes de múltiples proveedores.	Forma al personal en los marcos de los MAS y la gestión del cambio.

Roles esenciales para apoyar el éxito de la implementación

CIO

Definen la estrategia de MAS para unos flujos de trabajo de alto valor y la alinean con las prioridades de la empresa.

Establecen la gobernanza para la interoperabilidad, la seguridad y el cumplimiento de los agentes.

Comunican los planes de gestión del cambio para abordar las preocupaciones de la fuerza laboral.

Socios de TI

Plataforma y DevOps: diseñan los agentes modulares y gestionan las herramientas de orquestación.

Seguridad: implementan la gobernanza de las API y supervisan las interacciones de los agentes.

Equipos de integración: adoptan estándares de interoperabilidad y observabilidad.

Socios empresariales

Responsables de proceso: identifican flujos de trabajo para los ensayos de MAS y validan los resultados.

Finanzas: gestionan los costes imprevistos y financian las herramientas de observabilidad.

Operaciones: apoyan la colaboración humano-agente y las iniciativas de formación.

5

Modelos de lenguaje específicos de dominio

¿Qué es?
Los modelos de lenguaje específicos de dominio (DSLM) son modelos de IA entrenados con conjuntos de datos especializados para determinados sectores o departamentos de empresa, lo que garantiza su mayor nivel de precisión y cumplimiento, comparados con los grandes modelos de lenguaje (LLM).

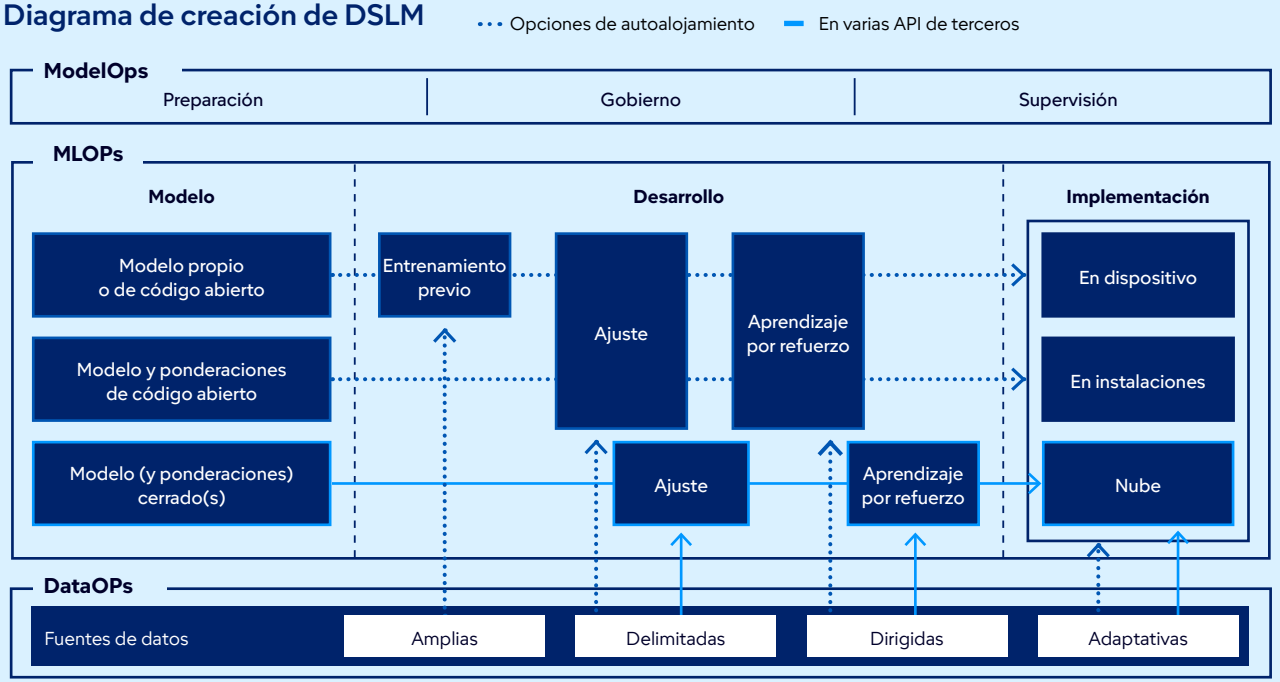
¿Por qué es tendencia?
Los CIO necesitan obtener valor empresarial medible de la IA. Los DSLM reducen los errores, aceleran la implementación y recortan costes en flujos de trabajo esenciales como los de finanzas, sanidad y RR. HH.

El futuro inmediato

+ del 60 % de los modelos de IA generativa serán específicos de dominio para 2028.

El 30 % de las cargas de trabajo de IA generativa ejecutarán DSLM en las instalaciones o en dispositivos, para 2028.

Diagrama de creación de DSLM



Fuente: Gartner

5

Consigue resultados con los DSLM

Plan de acción para ofrecer un cumplimiento preciso y específico según sector

Pasos	1 Identifica casos de uso de alto impacto	2 Refuerza la gobernanza de datos	3 Ensaya los DSLM en dominios esenciales	4 Crea equipos interdisciplinarios	5 Supervisa y optimiza
Resultado esperado	ROI más rápido y mejora de la precisión.	Resultados del DSLM fiables y conformes con la normativa.	Demostración de valor empresarial medible.	Integración y adopción sin obstáculos.	Rendimiento sostenible y control de costes.
Acción	Fíjate como objetivo los flujos de trabajo en que los LLM genéricos no estén ofreciendo un buen rendimiento.	Implementa controles de privacidad y de calidad robustos.	Empieza con los procesos de finanzas, sanidad o RR. HH.	Incluye TI, expertos en la materia y cumplimiento en los proyectos con DSLM.	Aplica marcos de explicabilidad y cumplimiento.

Roles esenciales para apoyar el éxito de la implementación

CIO

Definen la estrategia de los DSLM para los dominios regulados y de alto valor.

Aseguran la gobernanza para la precisión, el cumplimiento y la explicabilidad.

Alinean la adopción de los DSLM con los objetivos de ROI y de gestión del riesgo.

Socios de TI

Análisis de datos: preparan los conjuntos de datos específicos de dominio y mantienen su calidad.

ModelOps: gestionan el ajuste, la supervisión y la gobernanza del ciclo de vida.

Seguridad: velan por el respeto de la privacidad y el cumplimiento en las implementaciones de los DSLM.

Socios empresariales

Expertos en la materia: validan la precisión y la pertinencia de los resultados de los DSLM.

Finanzas: elaboran el presupuesto de la adopción de los DSLM y optimizan los costes.

Cumplimiento: aseguran el respeto de las normas legales.

6

IA física

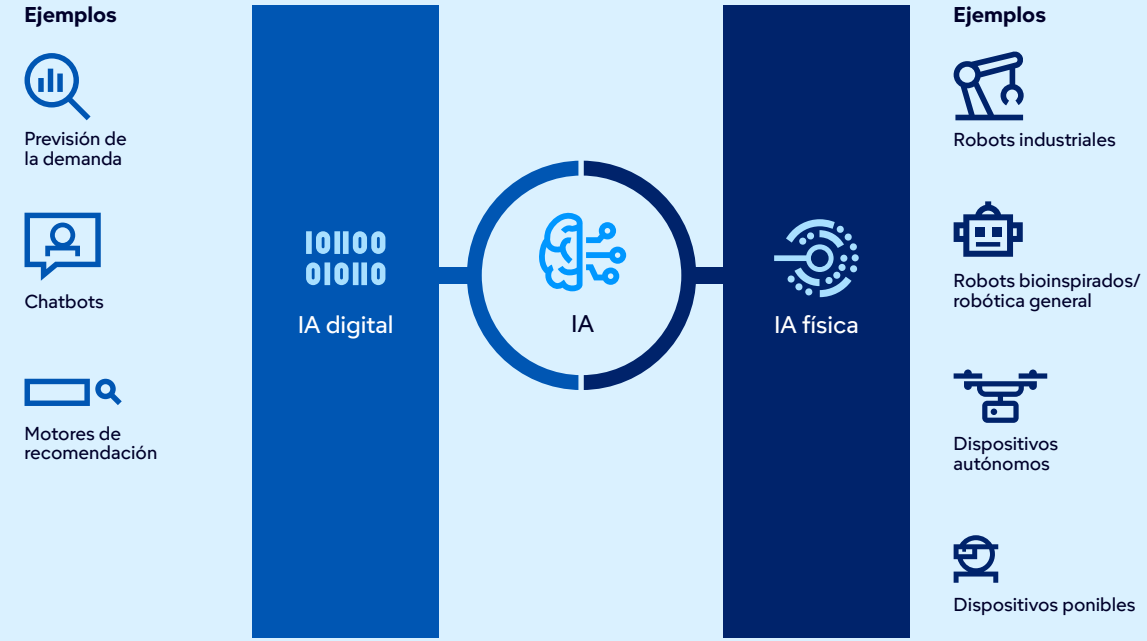
¿Qué es?
La IA física aporta información al mundo físico mediante robots, drones, vehículos y dispositivos inteligentes con capacidad para detectar, decidir y actuar. Estos sistemas combinan sensores, actuadores y modelos de IA para automatizar tareas físicas.

¿Por qué es tendencia?
Las organizaciones buscan la productividad de la IA digital aplicada a entornos físicos. Para 2028, cinco de los diez principales proveedores de IA ofrecerán productos de IA física.

El futuro inmediato

El **80 %** de los almacenes funcionarán con robótica o automatización para 2028.

Categorización de la IA



Fuente: Gartner

6

Consigue resultados con la IA física

Plan de acción para automatizar tareas del mundo físico e impulsar la productividad general

Pasos	1 Audita los dominios operativos	2 Ensaya los sistemas de IA física	3 Crea equipos interdisciplinarios	4 Instruye a las partes interesadas	5 Planifica la coordinación multiagente
Resultado esperado	Identificación de áreas susceptibles de automatización y ahorro de costes.	Validación del rendimiento y del ROI.	Eficacia de la gobernanza y la integración.	Eliminación de las confusiones y los desajustes de inversión.	Implementaciones preparadas para el futuro.
Acción	Dirígete a los flujos de trabajo de logística, mantenimiento y seguridad.	Usa simulaciones y gemelos digitales antes de implementar en producción.	Incluye TI, operaciones e ingeniería en la planificación.	Deja clara la distinción entre IA física, IA integrada e IA en el perímetro.	Investiga plataformas de orquestación de flotas de dispositivos.

Roles esenciales para apoyar el éxito de la implementación

CIO

Definen una estrategia de IA física alineada con los objetivos operativos.

Aseguran la gobernanza de la seguridad, la fiabilidad y la explicabilidad.

Se asocian con operaciones e ingeniería para la integración y la gestión del riesgo.

Socios de TI

Infraestructura y operaciones: integran la IA física en los sistemas heredados y el Internet de las cosas (IoT).

Seguridad: implementan protecciones para los sistemas autónomos.

Análisis de datos: respaldan las simulaciones y las pruebas de gemelos digitales.

Socios empresariales

Operaciones: identifican casos de uso de alto valor y validan el rendimiento.

Finanzas: elaboran el presupuesto de las inversiones en robótica y automatización.

Cumplimiento: aseguran el respeto de las normas legales y de seguridad.

El vanguardista

Potencia la confianza, la gobernanza y la seguridad.

Cuando el riesgo y el escrutinio reglamentario se intensifican, la confianza es innegociable. Las tendencias del perfil vanguardista ponen el énfasis en la seguridad proactiva, la gobernanza transparente y la integridad digital con el fin de ayudar a las organizaciones a proteger su reputación, garantizar el cumplimiento y preservar la confianza de las partes interesadas, al mismo tiempo que escalan la IA y la transformación digital.

7

Ciberseguridad preventiva

¿Qué es?
La ciberseguridad preventiva (PCS) usa técnicas avanzadas basadas en IA con el fin de prever, interceptar y neutralizar los ciberataques antes de que se produzcan, lo que supone un avance respecto a los métodos tradicionales de detección y respuesta.

¿Por qué es tendencia?
Impulsadas por la IA, las amenazas contra redes, aplicaciones y sistemas del IoT están creciendo exponencialmente. Para 2029, los productos tecnológicos que no adopten la ciberseguridad preventiva perderán relevancia en el mercado, ante la adopción de la defensa proactiva como requisito universal.

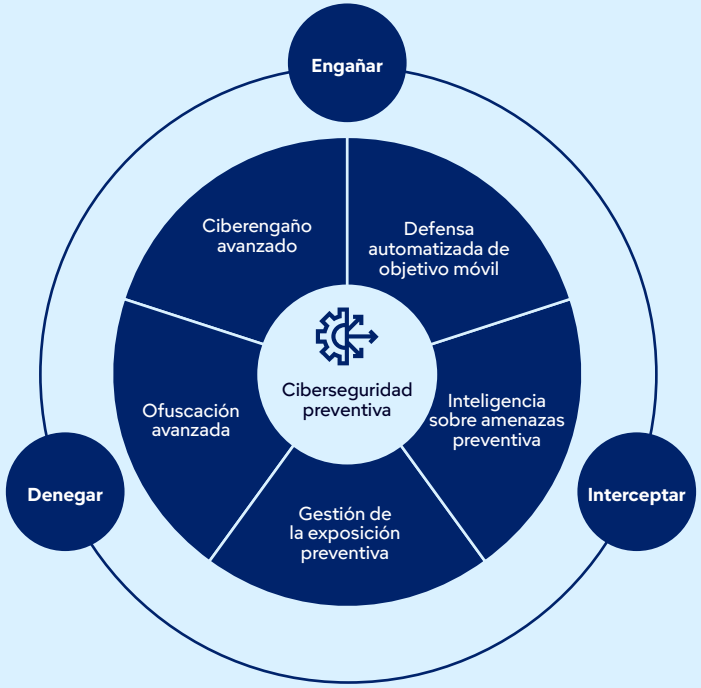
¿Necesitas análisis adaptados para organizaciones proveedoras de tecnología y de servicios? Lee nuestro artículo sobre ciberseguridad preventiva para proveedores **No demores la adopción de soluciones de ciberseguridad preventiva.**

El futuro inmediato

El **50 %** del gasto en software de seguridad se destinará a soluciones preventivas para 2030.

1M de vulnerabilidades documentadas anualmente, o incluso más, para 2030, según las previsiones.

Los tres vértices de la ciberseguridad preventiva



Fuente: Gartner

7

Consigue resultados con la ciberseguridad preventiva

Plan de acción para proteger los activos antes de que surjan las amenazas

Pasos	1 Evalúa la arquitectura de seguridad actual	2 Ensaya la PCS en áreas de alto riesgo	3 Define los criterios de selección de proveedores	4 Socializa la estrategia de PCS	5 Integra la PCS en las herramientas existentes
Resultado esperado	Identificación de carencias y priorización de las inversiones en PCS.	Demostración de una reducción medible del riesgo.	Garantía de adopción de una PCS preparada para el futuro.	Obtención del apoyo de los ejecutivos y la junta directiva.	Maximización del ROI y aceleración de la adopción.
Acción	Lleva a cabo análisis del riesgo y revisiones de la preparación.	Implementa la prevención de amenazas predictiva y el engaño.	Solicita hojas de ruta detalladas de las capacidades preventivas.	Comunica el impacto empresarial y el ROI de la PCS.	Combina la PCS con los procesos de seguridad y de cumplimiento existentes.

Roles esenciales para apoyar el éxito de la implementación

CIO

Defienden el paso de estrategias de seguridad reactivas a preventivas.

Definen los criterios de compra de capacidades de PCS e instruyen a los demás ejecutivos.

Supervisan la gobernanza, en caso de medidas de defensa agresivas, y el cumplimiento.

Socios de TI

Seguridad: implementan tecnologías de prevención de amenazas predictiva y de engaño.

Infraestructura y operaciones: integran la PCS en los sistemas de nube, de tecnología operativa (TO) y ciberfísicos.

Riesgo y cumplimiento: aseguran el respeto de las normas legales y de privacidad.

Socios empresariales

Finanzas: asignan presupuestos a los ensayos de PCS para su adopción a largo plazo.

Operaciones: respaldan las iniciativas de transformación digital segura.

Producto: integran la seguridad preventiva en las ofertas, para diferenciarse en el mercado.

8

Procedencia digital

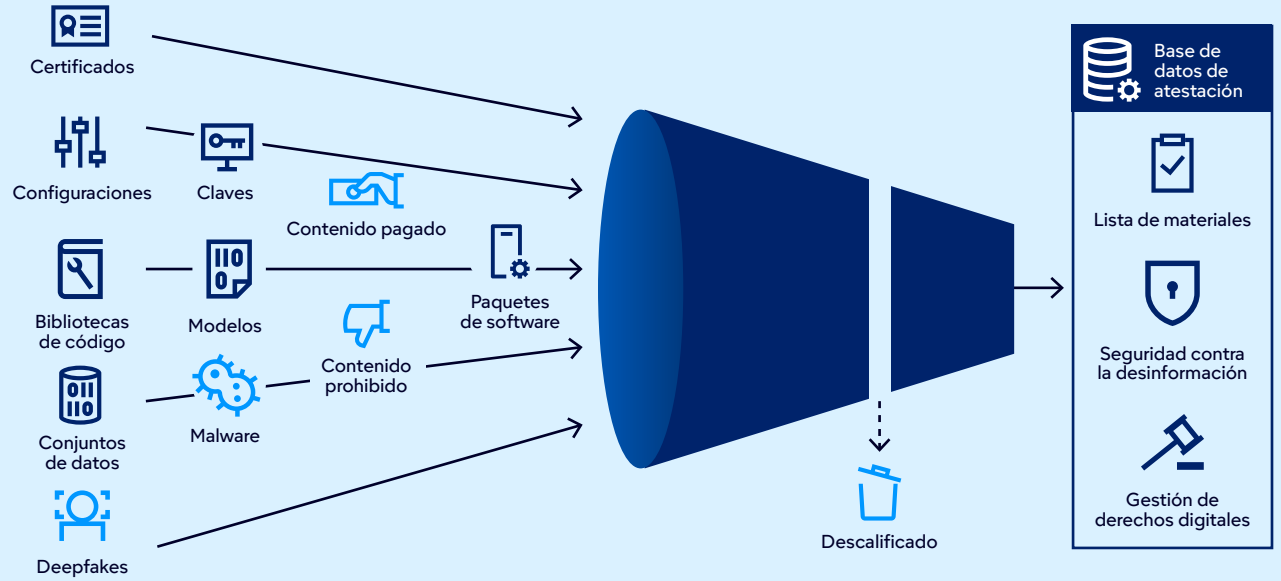
¿Qué es?
La procedencia digital verifica el origen y la integridad del software, los datos y los medios, usando herramientas como las listas de materiales (BOM), las bases de datos de atestación y las marcas de agua. Garantiza la transparencia y la fiabilidad de los sistemas creados con componentes de terceros y del contenido generado con IA.

¿Por qué es tendencia?
Las organizaciones se enfrentan a crecientes riesgos derivados de la manipulación de código, los proyectos de código abierto que quedan abandonados y la desinformación impulsada por deepfakes.

El futuro inmediato

Un creciente número de mandatos reglamentarios (como la Ley de IA de la Unión Europea) exigen incorporar marcas de agua en el contenido generado con IA y permitir la trazabilidad de su procedencia.

Filtros basados en la procedencia digital



Fuente: Gartner

8

Consigue resultados con la procedencia digital

Plan de acción para reforzar la confianza mediante verificación de la autenticidad de los datos y del contenido

Pasos	1 Implementa las BOM	2 Incorpora bases de datos de atestación	3 Adopta herramientas de seguridad contra la desinformación	4 Aplica marcas de agua digitales	5 Refuerza la gobernanza
Resultado esperado	Transparencia, seguridad y conocimiento de la procedencia del software.	Registros de procedencia centralizados y fiables.	Protección contra la suplantación de identidad y el fraude.	Cumplimiento de las regulaciones sobre el contenido de IA.	Reducción del riesgo legal y reputacional.
Acción	Implementa las BOM de software (SBOM) en el software y las BOM de machine learning (MLBOM) en los modelos de IA.	Almacena pruebas de origen con firma criptográfica.	Integra la detección de identidad sintética en la detección de amenazas de identidad y los planes de respuesta.	Marca los medios generados por IA en formatos legibles por máquina.	Colabora con los equipos de TI, cumplimiento y marketing.

Roles esenciales para apoyar el éxito de la implementación

CIO

Definen una estrategia de procedencia digital alineada con la gestión del riesgo y del cumplimiento.

Supervisan la implementación de las BOM y de las bases de datos de atestación.

Colaboran con el CISO y el CMO para responder a la desinformación y proteger la reputación.

Socios de TI

DevOps: integran las SBOM y las MLBOM en los flujos de procesamiento de la entrega.

Seguridad: implementan las herramientas de seguridad contra la desinformación y la gestión de derechos digitales (DRM).

Datos: documentan el linaje de los datos de entrenamiento de los modelos de IA.

Socios empresariales

Cumplimiento: garantizan el respeto de las regulaciones emergentes.

Área legal: validan el cumplimiento del copyright y de las licencias.

Marketing: gestionan los riesgos reputacionales asociados con los deepfakes y el contenido sintético.

9

Plataformas de seguridad de IA

¿Qué es?
Las plataformas de seguridad de IA (AISP) consolidan los controles destinados a proteger tanto los servicios de IA de terceros como las aplicaciones de IA personalizadas. Abordan los riesgos inherentes a la IA, como la inyección de instrucciones, las acciones de agentes deshonestos y la filtración de datos.

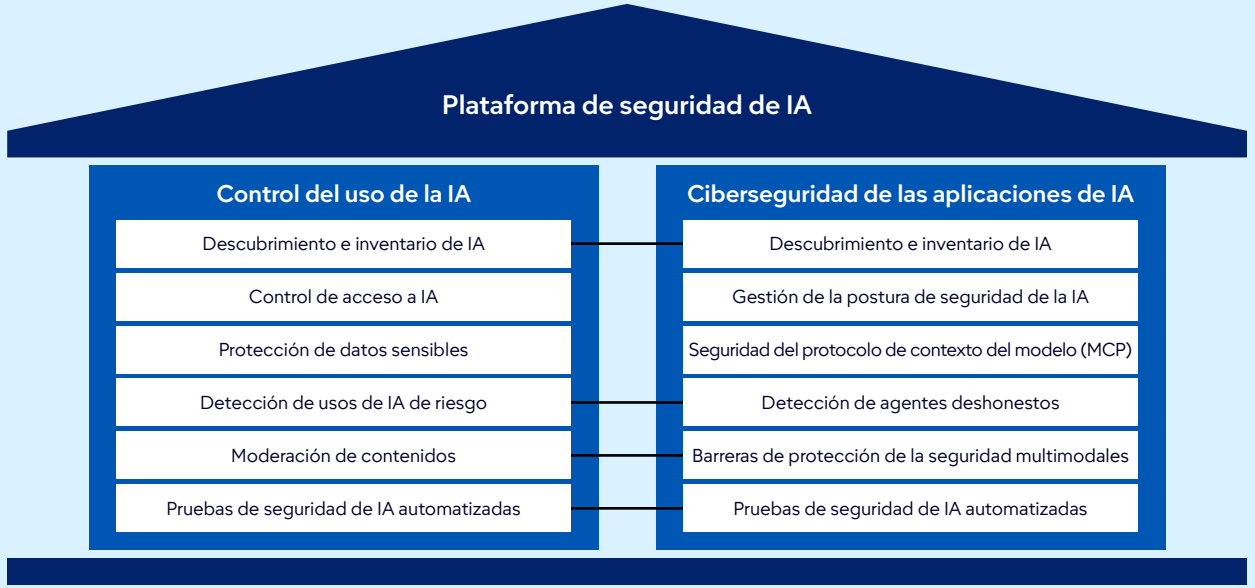
¿Por qué es tendencia?
La adopción acelerada de la IA provoca que las herramientas de seguridad tradicionales ya no sirvan para proteger los nuevos flujos de trabajo.

El futuro inmediato

+ del 50 % de las empresas adoptarán AISP para 2028.

El 80 % de las transacciones de IA no autorizadas derivarán de infracciones de las políticas internas, no de ataques externos.

Atribución de capacidades de las plataformas de seguridad de IA



Fuente: Gartner

9

Consigue resultados con las plataformas de seguridad de IA

Plan de acción para proteger las operaciones empresariales que evolucionan con la IA

Pasos	1 Evalúa el panorama del riesgo de la IA	2 Ensaya soluciones de AISP	3 Favorece las plataformas unificadas	4 Integra pruebas de seguridad	5 Supervisa la innovación de los proveedores
Resultado esperado	Identifica carencias en la pila de seguridad existente.	Valida la eficacia y el ROI.	Simplifica la gestión y reduce la complejidad.	Mejora la resiliencia contra la inyección de instrucciones.	Anticípate a las amenazas emergentes.
Acción	Atribuye los riesgos inherentes de la IA a los diferentes flujos de trabajo.	Empieza con los servicios de IA de alto riesgo y las aplicaciones personalizadas.	Elige AISP que ofrezcan control de uso de la IA y también seguridad de las aplicaciones.	Añade pruebas de seguridad de IA automatizadas en los flujos de procesamiento.	Sigue la información de las startups y los operadores tradicionales para estar al corriente de características avanzadas.

Roles esenciales para apoyar el éxito de la implementación

CIO

Definen una estrategia de seguridad de la IA que incluye tanto las aplicaciones de IA de terceros como las personalizadas.

Seleccionan los proveedores que ofrecen control de uso de IA unificado y seguridad de aplicaciones.

Comunican la postura del riesgo de IA y los requisitos de cumplimiento a la junta directiva.

Socios de TI

Seguridad: implementan barreras de protección contra la inyección de instrucciones, así como detección de agentes deshonestos.

DevOps: integran pruebas de seguridad de la IA en los flujos de procesamiento del desarrollo.

Infraestructura y operaciones: aseguran la compatibilidad con los entornos de nube y en las instalaciones.

Socios empresariales

Cumplimiento: alinean las AISP con los marcos reglamentarios (como la Ley de IA de la Unión Europea).

Finanzas: elaboran el presupuesto de la adopción de plataformas y la reducción del riesgo.

Producto: integran características de seguridad en las ofertas basadas en IA.

10 Geopatriación

¿Qué es?
La geopatriación es la reubicación de las cargas de trabajo, de las nubes a hiperescala globales a entornos soberanos o locales, para reducir el riesgo geopolítico. Incluye estrategias como la reimplementación en regiones de nube soberana o la repatriación de cargas de trabajo a las instalaciones locales.

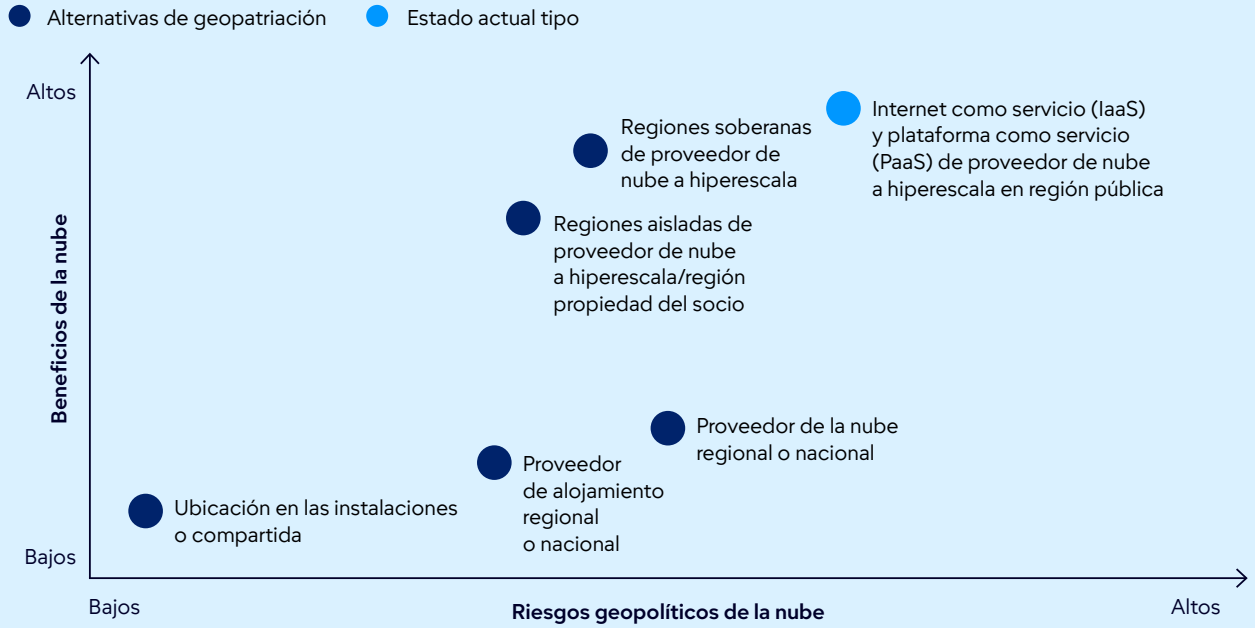
¿Por qué es tendencia?
La inestabilidad geopolítica y los mandatos reglamentarios están llevando a las organizaciones a reevaluar sus dependencias de la nube.

El futuro inmediato

El **75 %** de las empresas optarán por la geopatriación de sus cargas de trabajo para 2030.

Los proveedores de hiperescala y locales están expandiendo rápidamente sus ofertas de nube soberana.

Los beneficios y los riesgos geopolíticos de la nube



Fuente: Gartner

10

Consigue resultados con la geopatriación

Plan de acción para reducir el riesgo mediante la localización de las cargas de trabajos digitales esenciales

Pasos	1 Evalúa la esencialidad de la carga de trabajo	2 Examina las opciones soberanas	3 Planifica estrategias híbridas	4 Implementa controles de gobernanza	5 Supervisa las tendencias geopolíticas
Resultado esperado	Geopatriación como opción prioritaria para los activos de alto riesgo.	Equilibrio entre agilidad y soberanía.	Mantenimiento de la resiliencia y del rendimiento.	Reducción del riesgo de cumplimiento y de seguridad.	Adaptación proactiva de la estrategia.
Acción	Puntúa las cargas de trabajo en función de la sensibilidad y la exposición geopolítica.	Compara las ofertas de los proveedores de nube soberana a hiperescala y de los proveedores locales.	Combina la ubicación en la nube soberana con la ubicación en las instalaciones o compartida.	Adopta marcos de atestación y de soberanía.	Actualiza la colocación de la carga de trabajo a medida que evolucionen los riesgos.

Roles esenciales para apoyar el éxito de la implementación

CIO

Definen la estrategia de geopatriación buscando el equilibrio entre soberanía, agilidad y resiliencia.

Evalúan las contrapartidas entre las opciones de los proveedores locales y los de nube soberana a hiperescala.

Supervisan la puntuación del riesgo de las cargas de trabajo esenciales y la alineación con el cumplimiento.

Socios de TI

Infraestructura y operaciones: planifican las rutas de migración y la integración en los sistemas heredados.

Seguridad: validan los controles de soberanía y aseguran el cumplimiento.

Arquitectos de nube: optimizan la colocación de la carga de trabajo, en beneficio del rendimiento y la resiliencia.

Socios empresariales

Cumplimiento: supervisan los cambios reglamentarios y los mandatos de soberanía.

Finanzas: elaboran el presupuesto de los costes de la migración y las inversiones en reducción del riesgo.

Operaciones: aseguran la continuidad durante la reubicación de la carga de trabajo.

Insights prácticos y objetivos

Explora estos recursos y herramientas gratuitas adicionales para responsables de TI:

Plantilla

Elabora un plan estratégico de TI

Convierte la estrategia en acción con esta plantilla de planificación de una página.

Accede a la plantilla

Herramienta

Diagnósticos y análisis comparativos de Gartner

Descubre los análisis comparativos que impulsan decisiones de TI más acertadas.

Más información

Insights

El Hype Cycle™ de Gartner de 2025

El Hype Cycle para la IA de 2025 va más allá de la IA generativa.

Descúbrelo ahora

Insights

Preguntas de actualidad sobre IA y tecnologías emergentes

Los expertos de Gartner comparten respuestas rápidas a las preguntas que sus clientes les han hecho recientemente sobre las tecnologías emergentes.

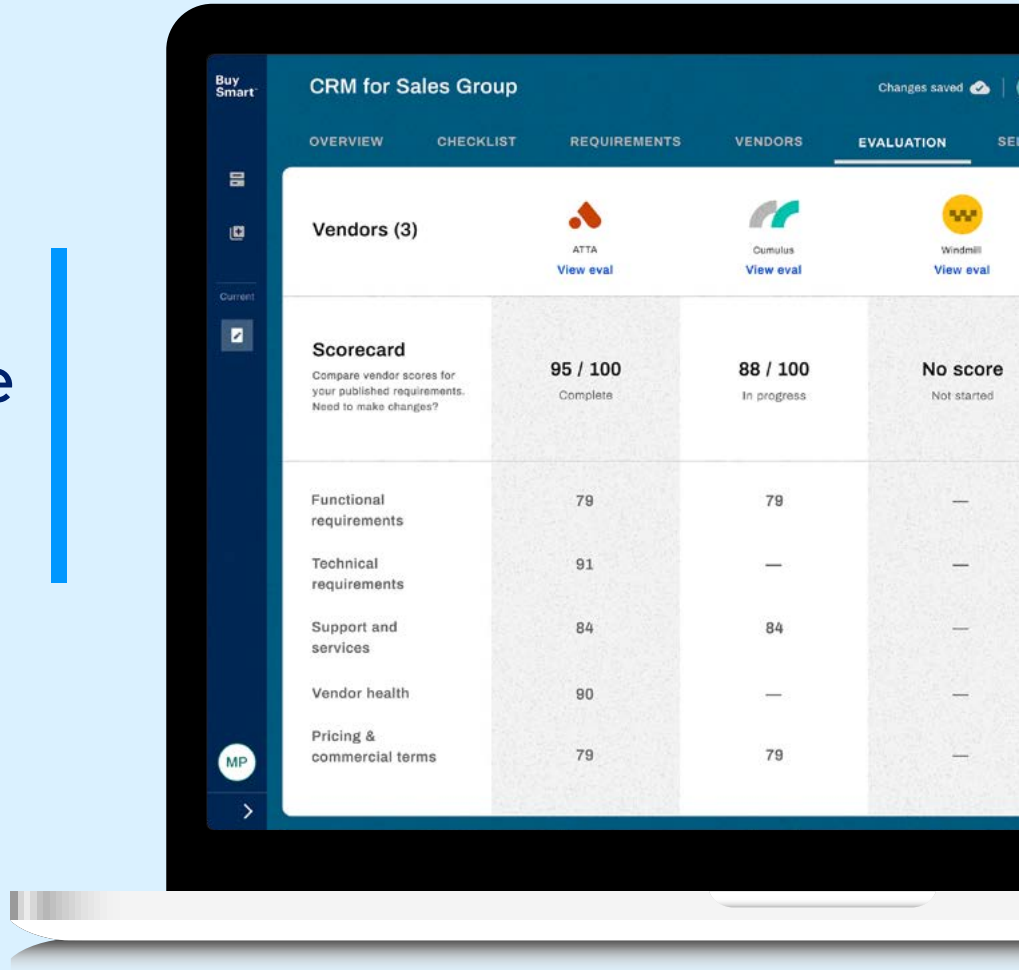
Consulta las respuestas

¿Ya eres cliente?
Obtén acceso a más recursos en tu portal de cliente. **Inicia sesión ↗**

Gartner®

Gartner BuySmart™

Facilita el proceso de toma de decisiones de tu equipo para unas compras tecnológicas más acertadas



Qué obtendrás:

- Acceso a más de 100 plantillas que abarcan los principales mercados tecnológicos
- Listas de verificación y requisitos predefinidos, totalmente personalizables
- Funciones de colaboración para respaldar el flujo de trabajo de tu equipo, todo en un mismo lugar
- Puntuación estandarizada para generar confianza en tu selección de proveedores

Más información ↗

Investiga | Preselecciona | Evalúa | Negocia

Conecta con nosotros

Obtén conocimientos prácticos y objetivos sobre empresa y tecnología para una toma de decisiones más acertada y un mejor rendimiento al abordar las principales prioridades estratégicas.

EE. UU.: +1 855 811 7593

Internacional: +44 (0) 3330 607 044

Habla con un especialista

Obtén más información sobre Gartner para CIO y ejecutivos de TI

gartner.com/en/chief-information-officer

Recibe las últimas novedades

Acude a una conferencia de Gartner

Ver conferencias

Gartner®