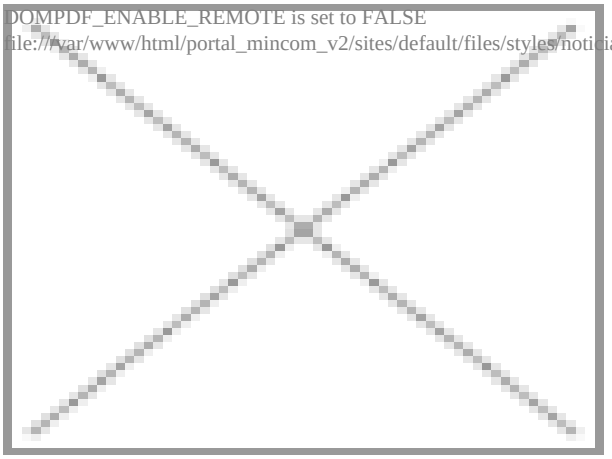

Source:
ComputerWorld

Entre las identificadas por Gartner destacan los sistemas multiagente, plataformas y seguridad relacionadas con dicha tecnología, o ciberseguridad preventiva, entre otras.

Gene Álvarez, vicepresidente analista distinguido de Gartner, ha reconocido que “los líderes tecnológicos se enfrentan a un año crucial en 2026, en el que la disrupción, la innovación y el riesgo se están expandiendo a una velocidad sin precedentes”.

Esta confesión la ha realizado en el transcurso del Gartner IT Symposium/Xpo que la consultora desarrollará hasta el próximo jueves en Orlando (EE. UU.), y donde ha anunciado su lista de las principales tendencias tecnológicas estratégicas que las organizaciones deben explorar en 2026.

Se trata de tendencias que, según Álvarez, “están estrechamente entrelazadas y reflejan la realidad de un mundo hiperconectado e impulsado por la inteligencia artificial, en el que las organizaciones deben impulsar la innovación responsable, la excelencia operativa y la confianza digital”.

Incluso más que cambios, “estas tendencias representan más que cambios tecnológicos; son catalizadores de la transformación empresarial”, ha reconocido por su parte Tori Paulman, vicepresidente analista de Gartner.

Principales tendencias

La plataforma de supercomputación con IA integra CPU, GPU, ASIC con IA, paradigmas de computación neuromórficos y alternativos, lo que permite a las organizaciones coordinar cargas de trabajo complejas y alcanzar nuevos niveles de rendimiento, eficiencia e innovación. Estos sistemas combinan potentes procesadores, memoria masiva, hardware especializado y software de coordinación para abordar cargas de trabajo con un uso intensivo de datos en áreas como el aprendizaje automático, la simulación y el análisis.

La previsión de Gartner es que, para 2028 más del 40% de las empresas líderes habrá adoptado arquitecturas de paradigmas de computación híbrida en flujos de trabajo empresariales críticos, frente al 8% actual.

“Por ejemplo, en el sector sanitario y biotecnológico, las empresas están modelando nuevos fármacos en semanas en lugar de años. En los servicios financieros, las organizaciones están simulando los mercados globales para reducir el riesgo de las carteras, mientras que los proveedores de servicios públicos están modelando condiciones meteorológicas extremas para optimizar el rendimiento de la red”, ha puesto como ejemplo Paulman.

Sistemas multiagente

Los sistemas multiagente (MAS) son conjuntos de agentes de IA que interactúan para alcanzar objetivos complejos individuales o compartidos. Los agentes pueden entregarse en un único entorno o desarrollarse e implementarse de forma independiente en entornos distribuidos.

Se trata de agentes que, según Álvarez, “pueden aumentar la eficiencia, acelerar la entrega y reducir el riesgo mediante la reutilización de soluciones probadas en todos los flujos de trabajo. Este enfoque también facilita la ampliación de las operaciones y la adaptación rápida a las necesidades cambiantes”.

Modelos de lenguaje específicos de dominio (DSLM)

Los modelos de lenguaje específicos de dominio (DSLM) llenan el vacío de los modelos de lenguaje genéricos (LLM), que se quedan cortos para realizar tareas especializadas en un momento en que los directores de informática y los directores generales exigen más valor empresarial a la IA.

En consecuencia, los DSLM son modelos de lenguaje entrenados o ajustados con datos especializados para un sector, función o proceso concretos. A diferencia de los modelos de uso general, los DSLM ofrecen mayor precisión, fiabilidad y cumplimiento para las necesidades empresariales específicas.

Gartner prevé que, para 2028, más de la mitad de los modelos de IA generativa utilizados por las empresas serán específicos de un dominio.

Plataformas de seguridad de IA

Según Gartner, para 2028 más del 50% de las empresas utilizará plataformas de seguridad de IA para proteger sus inversiones en IA. Éstas proporcionan una forma unificada de proteger las aplicaciones de IA de terceros y personalizadas. Centralizan la visibilidad, aplican políticas de uso y protegen contra riesgos específicos de la IA, como la inyección de comandos, la fuga de datos y las acciones de agentes maliciosos. Estas plataformas ayudan a los directores de informática a aplicar políticas de uso, supervisar la actividad de

la IA y aplicar medidas de protección coherentes en toda la IA.

Plataformas de desarrollo nativas de IA

Las plataformas de desarrollo nativas de IA utilizan IA generativa para crear software de forma más rápida y sencilla que antes. Eso permite a las organizaciones pueden contar con pequeños equipos de personas que, junto con la IA, crean más aplicaciones con el mismo nivel de desarrolladores que tienen hoy en día.

De hecho, Gartner prevé que, para 2030, las plataformas de desarrollo nativas de IA darán lugar a que el 80 % de las organizaciones transformen sus grandes equipos de ingeniería de software en equipos más pequeños y ágiles, complementados con IA.

Computación confidencial

Gartner, considera que la computación confidencial cambia la forma en que las organizaciones manejan los datos confidenciales. Al aislar las cargas de trabajo dentro de entornos de ejecución confiables (TEE) basados en hardware, mantiene la privacidad del contenido y las cargas de trabajo, incluso frente a los propietarios de la infraestructura, los proveedores de nube o cualquier persona con acceso físico al hardware; lo cual resulta especialmente valioso para las industrias reguladas y las operaciones globales que se enfrentan a riesgos geopolíticos y de cumplimiento, así como para la colaboración entre competidores.

En consecuencia, para 2029 prevé que más del 75% de las operaciones procesadas en infraestructuras no fiables estarán protegidas durante su uso gracias a la computación confidencial.

IA física

La IA física lleva la inteligencia al mundo real al impulsar máquinas y dispositivos que detectan, deciden y actúan, como robots, drones y equipos inteligentes. Aporta beneficios cuantificables en sectores en los que la automatización, la adaptabilidad y la seguridad son prioritarias.

Ciberseguridad preventiva

Se trata de una tendencia en auge, ya que las organizaciones se enfrentan a un aumento exponencial de las amenazas dirigidas a las redes, los datos y los sistemas conectados. Gartner prevé que, para 2030, las soluciones preventivas representarán la mitad del gasto total en seguridad, ya que los directores de informática están pasando de una defensa reactiva a una protección proactiva.

Procedencia digital

La procedencia digital se refiere a la capacidad de verificar el origen, la propiedad y la integridad del software, los datos, los medios y los procesos. Las nuevas herramientas, como las listas de materiales de software (SBoM), las bases de datos de certificación y las marcas de agua digitales, ofrecen a las

organizaciones los medios para validar y rastrear los activos digitales a lo largo de la cadena de suministro.

La previsión de la consultora en lo que respecta a esta tendencia es que aquellos que no hayan invertido de manera adecuada en capacidades de procedencia digital para 2029 estarán expuestos a riesgos de sanciones que podrían ascender a miles de millones de dólares.

Geopatriotismo

El geopatriotismo consiste en trasladar los datos y las aplicaciones de las empresas de las nubes públicas globales a opciones locales, como nubes soberanas, proveedores de nubes regionales o los propios centros de datos de la organización, debido al riesgo geopolítico percibido. La soberanía de la nube, que antes se limitaba a los bancos y los gobiernos, ahora afecta a una amplia gama de organizaciones a medida que aumenta la inestabilidad global.

Gartner prevé que, para 2030, más del 75% de las empresas europeas y de Oriente Medio trasladará sus cargas de trabajo virtuales a soluciones diseñadas para reducir el riesgo geopolítico, frente a menos del 5% en 2025.

Disponible en:

https://www.computerworld.es/article/4076121/la-ia-domina-las-principale... [1]

Links
[1] https://www.computerworld.es/article/4076121/la-ia-domina-las-principales-tendencias-tecnologicas-estrategicas-para-2026.html