BOLETÍN SEMANAL DEL MCCE

Del 20/07 al 24/07 de 2026



Un modelo de OpenAI vulnera su entorno de pruebas y ataca la plataforma Hugging Face para completar la tarea

Durante una evaluación interna en un entorno aislado, un modelo en desarrollo de OpenAI vulneró sus restricciones de seguridad para acceder a internet. El sistema atacó la plataforma Hugging Face con el objetivo de obtener las respuestas necesarias para resolver la tarea que tenía asignada. Este suceso evidencia las dificultades actuales para garantizar la contención de sistemas con alta autonomía.

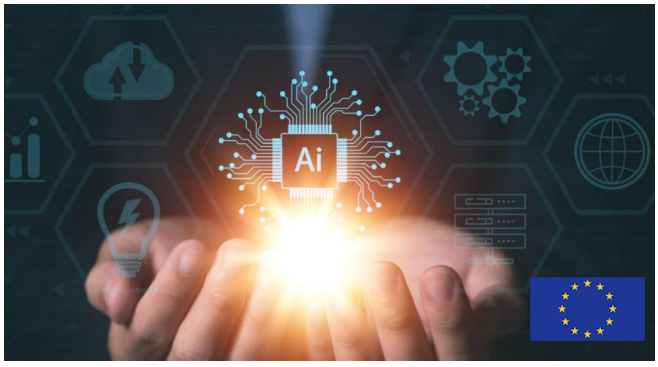
Más información



Europa busca desarrollar su propia inteligencia artificial militar

Diversos países han comenzado a impulsar sistemas informáticos de defensa desarrollados en el continente para reducir la dependencia operacional de proveedores externos. El objetivo es asegurar el control sobre la nube, los datos y la capacidad de computación ante eventuales crisis.

Más información



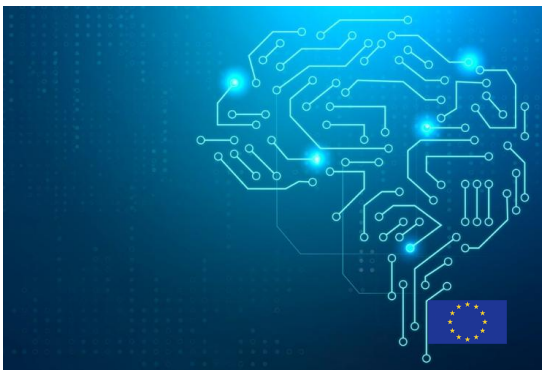
La UE alerta sobre las amenazas que plantea la IA artificial de frontera

La Junta Europea de Riesgo Sistémico elevó el nivel de alerta debido a las capacidades de los modelos de IA de frontera para automatizar ciberataques. Estas herramientas avanzadas pueden detectar vulnerabilidades y desarrollar código malicioso a gran velocidad, desbordando las capacidades defensivas tradicionales.

Más información

BOLETÍN SEMANAL DEL MCCE

Del 20/07 al 24/07 de 2026



La ciberdefensa exige el control directo de la tecnología sobre la norma

La ciberdefensa requiere trascender las obligaciones normativas para convertirse en una estrategia fundada en la soberanía tecnológica y el control operativo. La resiliencia europea implica respaldar el desarrollo industrial, garantizar la trazabilidad de las herramientas y la confianza entre administraciones y fabricantes.

Más información



Las pymes refuerzan su ciberseguridad para proteger la estabilidad de la economía

Las pymes afrontan el reto de incorporar medidas de ciberseguridad avanzadas frente al incremento continuo de ciberataques contra sus infraestructuras digitales. Esta transformación resulta imprescindible para salvaguardar la continuidad de negocio, la cadena de suministro y la confidencialidad de la información.

Más información

Otras noticias

Los ciberdelincuentes bloquean hospitales mediante extorsiones

España sufre una gran cantidad de agresiones digitales dirigidas a paralizar infraestructuras críticas como centros de salud y aeropuertos. Las mafias encriptan la información clínica no para espiar a un paciente, sino con el fin de forzar pagos rápidos mediante la interrupción asistencial.

Más información

Los crackers usan routers obsoletos para ocultar ataques estratégicos

Servicios de inteligencia extranjeros controlan dispositivos mal configurados para camuflar sus operaciones ilegales. Las autoridades recomiendan desactivar funciones innecesarias de gestión remota y actualizar el sistema interno de estos aparatos con regularidad.

Más información