

Qué es Mythos, el modelo de inteligencia artificial que preocupa a gobiernos por su capacidad de “superar a los humanos”

22/04/2026



El desarrollo de la **inteligencia artificial** suma un nuevo capítulo con la aparición de **Mythos**, un modelo creado por **Anthropic** que generó preocupación a nivel global por su capacidad para **detectar y explotar vulnerabilidades en sistemas informáticos**.

Este avance, integrado en la plataforma **Claude**, coloca a la compañía en competencia directa con gigantes tecnológicos como **OpenAI** y **Google**. Sin embargo, más allá de la carrera tecnológica, el foco está puesto en los posibles riesgos asociados a su uso.



Mythos es un modelo de IA diseñado para detectar fallas en sistemas informáticos, incluso en códigos antiguos. Foto: LinkedIn.

*“Mythos Preview ya ha encontrado miles de vulnerabilidades de alta gravedad, incluidas algunas en todos los principales sistemas operativos y navegadores web”, afirmó la empresa. Además, advirtió: **“Dado el ritmo de progreso de la IA, no pasará mucho tiempo antes de que dichas capacidades proliferen, potencialmente más allá de los actores comprometidos con su despliegue seguro”.***

¿Qué es Mythos y cómo funciona?

Mythos es un modelo de **inteligencia artificial** especializado en ciberseguridad, diseñado para analizar código, detectar fallas y proponer soluciones, o incluso formas de explotación, con un **nivel de precisión superior** al de herramientas tradicionales.

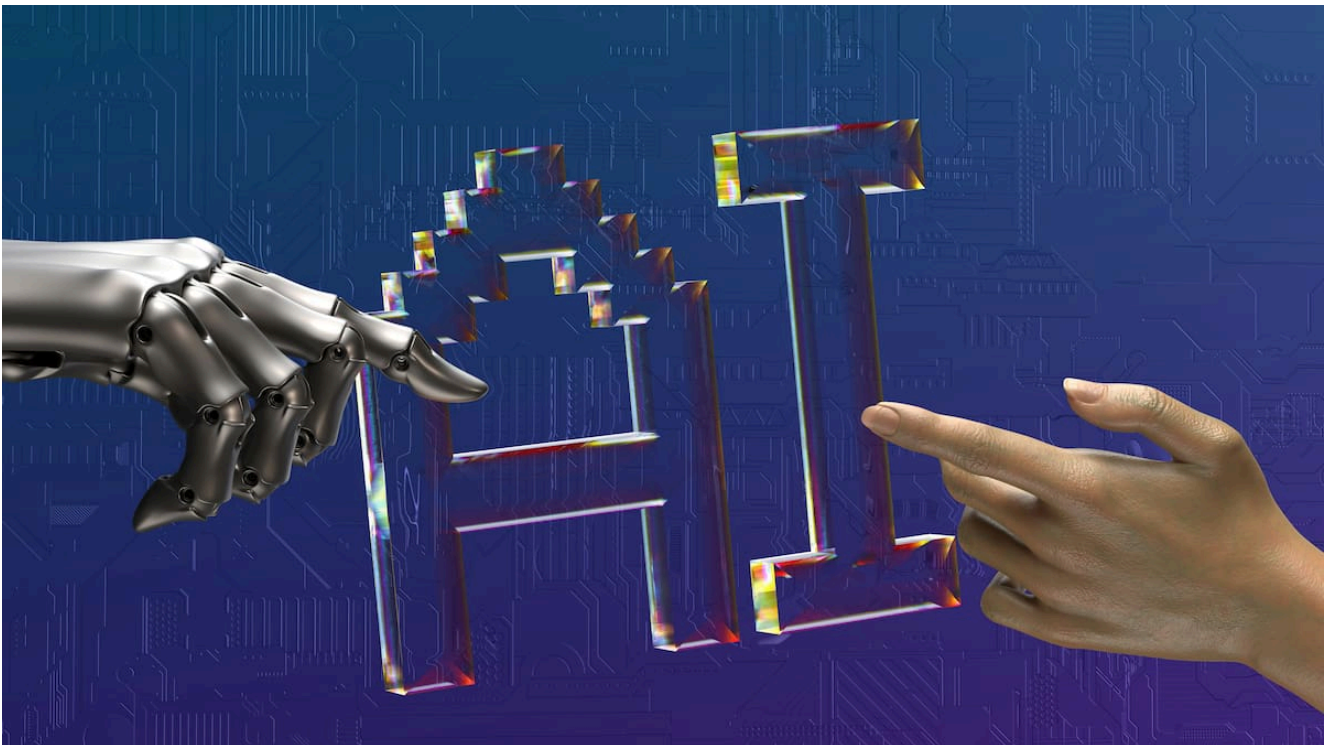
Durante las pruebas, logró identificar errores en sistemas antiguos sin necesidad de supervisión intensiva, lo que encendió alarmas en sectores clave. Para mitigar riesgos, **Anthropic decidió limitar su acceso a través del**

Proyecto Glasswing, una iniciativa que involucra a empresas como **Amazon Web Services**, **Microsoft** y **Nvidia**.

¿Por qué preocupa a gobiernos y organismos internacionales?

El potencial de Mythos para identificar vulnerabilidades críticas despertó inquietud en el ámbito político y financiero. El ministro **François-Philippe Champagne** afirmó: *“Sin duda, es un asunto lo suficientemente serio como para merecer la atención de todos los ministros de finanzas”*, mientras que **Andrew Bailey** advirtió: *“Ahora tenemos que analizar con mucha atención qué podría significar este último avance en inteligencia artificial para el riesgo de ciberdelincuencia”*.

A pesar de las advertencias, especialistas como **Ciaran Martin** piden cautela. *“Para algunos esto es un acontecimiento apocalíptico, para otros parece ser mucha exageración”*, señaló.



Más allá de los temores, expertos coinciden en que herramientas como Mythos también podrían utilizarse para

reforzar la seguridad digital. Foto: Unsplash.

Informes independientes sostienen que el mayor riesgo se concentra en **sistemas con baja protección**, lo que refuerza la importancia de mantener estándares básicos de ciberseguridad.

Riesgos y oportunidades de la inteligencia artificial

El caso Mythos refleja un dilema central: la misma tecnología que puede facilitar ataques también puede fortalecer la defensa digital. En ese sentido, expertos coinciden en que la clave estará en el **uso responsable**, la regulación y la inversión en infraestructura segura.

A medida que la inteligencia artificial continúa evolucionando, el desafío será **equilibrar innovación y control** para evitar que herramientas avanzadas se conviertan en una amenaza para la estabilidad digital global.

Fuente: Canal 26