El Rancagüino
El Diario de la Región de O'Higgins

Fecha: 27/04/2026 Audiencia: 15.000 Sección: ACTUALIDAD
Vpe: $1.441.721 Tirada: 5.000 Frecuencia: DIARIO
Vpe pág: $1.606.745 Difusión: 5.000
Vpe portada: $1.606.745 Ocupación: 89,73%

¿Y QUÉ TANTO CON ESE MYTHOS?

En los últimos días, un nombre ha saltado de los foros especializados en ciberseguridad a los titulares de la prensa económica: Mythos. Se trata del nuevo modelo de frontera de Anthropic que, a diferencia de sus predecesores, fue "confinado" por la propia empresa debido a su capacidad para encontrar vulnerabilidades críticas de forma autónoma. Pero, ¿es realmente una amenaza mágica o estamos ante un cambio de paradigma que no queremos aceptar?

¿De qué se trata realmente? Mythos no es una IA para escribir poemas o resumir reuniones. Es una arquitectura diseñada para el razonamiento técnico profundo. Su particularidad es que puede analizar software complejo (como el núcleo de un sistema operativo o un navegador web) e identificar fallos que han pasado desapercibidos por décadas. No solo "ve" el error, sino que es capaz de redactar el código necesario para explotarlo.

¿POR QUÉ ES PELIGROSO?

El peligro radica en la asimetría y la velocidad. Tradicionalmente, encontrar una vulnerabilidad de "día cero" (aquellas que nadie conoce) requería meses de trabajo de hackers de élite. Mythos puede reducir ese tiempo a minutos. Para instituciones del Estado o la banca, esto significa que sus defensas actuales podrían volverse obsoletas de la noche a la mañana. Si una IA puede generar ataques más rápido de lo que los humanos pueden programar parches, el sistema de seguridad global entra en crisis. Por ejemplo, hay empresas con una frecuencia de ataques cada 15 minutos en promedio, por lo que es usual tener profesionales dedicados permanentemente a resolverlos.

¿QUÉ PUEDEN HACER LAS PERSONAS E INSTITUCIONES?

La respuesta ya no puede ser solo "instalar un antivirus".

- Las instituciones deben migrar a arquitecturas de "Cero Confianza" (Zero Trust), donde se asume que el atacante ya está dentro.
- Las empresas deben auditar su software con herramientas de IA ofensiva propias para cerrar brechas antes de que otros las encuentren.
- Las personas deben extremar la higiene digital: la IA hace que el phishing sea perfecto, sin errores de ortografía y altamente personalizado.

LA VERDADERA LECCIÓN: EL "PIPELINE" SOBRE EL MODELO

Es cierto que Mythos de Anthropic parece ser el vencedor actual en este nicho, rodeado de una potente campaña de marketing que lo posiciona como una entidad casi mitológica. Sin embargo, lo relevante aquí no es la IA específica con nombre comercial.

Lo verdaderamente disruptivo no es el modelo de lenguaje en sí, sino el procedimiento (pipeline). La magia ocurre cuando conectas una IA potente a un ciclo cerrado de ejecución: un agente que propone una hipótesis, la prueba en un entorno real, recibe el error del sistema y corrige su propia lógica hasta que logra entrar.

LA GENERACIÓN "PROMPTIANA"

En el fondo, estamos ante la democratización del ataque complejo. Cada vez es más factible que cualquier joven de la generación "promptiana", con los conocimientos técnicos adecuados y acceso a modelos de código abierto (sin las bulladas restricciones éticas de las grandes corporaciones), pueda desarrollar su propio "Mythos" casero.

La tecnología ya está ahí, distribuida y disponible. El genio salió de la botella: ya no se necesita una corporación multimillonaria para poner en jaque la infraestructura digital; solo se necesita un buen flujo de trabajo y una IA que no tenga miedo a preguntar "¿y si pruebo esto?".

Manuel Reyes
Académico
Facultad de
Ingeniería UNAB