LT LATERCERA PULSO

Fecha: 03/05/2026 Audiencia: 271.020 Sección: CONTRAPORTADA
Vpe: $2.064.451 Tirada: 76.017 Frecuencia: 0
Vpe pág: $9.570.938 Difusión: 76.017
Vpe portada: $9.570.938 Ocupación: 21,57%

Cuando la IA deja de ser herramienta... y se vuelve amenaza estratégica

Por ***Anil Sadarangani***
Director de Innovación, Universidad de los Andes

Durante años, la inteligencia artificial fue vista principalmente como una herramienta para mejorar la productividad y abrir nuevas oportunidades. Sin embargo, estamos entrando en una nueva fase. Un ejemplo es Mythos, el nuevo modelo de Anthropic, que ha demostrado capacidades avanzadas para identificar y explotar vulnerabilidades en software crítico. Según se ha reportado, el sistema logró detectar fallas en los principales sistemas operativos y navegadores, incluyendo vulnerabilidades que llevaban décadas sin ser descubiertas.

Esto marca un punto de inflexión. Ya no se trata solo de automatizar tareas o generar contenido, sino de una tecnología capaz de intervenir en la infraestructura digital sobre la cual operan empresas, gobiernos y sociedades enteras. La ciberseguridad deja de ser un problema técnico para convertirse en un tema de seguridad nacional.

Las implicancias son profundas. Primero, se abre una carrera entre IA defensiva y ofensiva que ningún actor puede ignorar. Segundo, las empresas deberán auditar sus sistemas antes de liberarlos al mercado, bajo pena de quedar expuestas en tiempo real. Tercero, los Estados enfrentarán desafíos para los cuales sus marcos legales y capacidades institucionales simplemente no fueron diseñados.

Para dimensionar el riesgo: según el Foro Económico Mundial, los ataques cibernéticos cuestan anualmente más de US$8 billones a la economía global, cifra que superará los US$10,5 billones en 2025. Y eso fue calculado antes de que la IA ofensiva alcanzara este nivel de sofisticación. Es como haber construido todos nuestros candados pensando en ladrones humanos y descubrir que ahora el intruso puede leer y copiar cualquier llave en segundos.

Chile no está al margen de este escenario. Somos el país más digitalizado de América Latina, con alta penetración bancaria, infraestructura crítica conectada y un Estado que avanza hacia la tramitación digital. Sin embargo, nuestra inversión en ciberseguridad representa una fracción marginal del gasto público y no contamos con una Agencia Nacional de Ciberseguridad con dientes reales ni con una masa crítica de talento especializado en IA defensiva. Seguimos pensando el problema en términos del siglo XX.

La respuesta no puede ser solo tecnológica. Requiere decisiones políticas: definir qué infraestructura es estratégica e intocable, establecer estándares de certificación para sistemas que incorporen IA, y –crucialmente– invertir en formación de capital humano capaz de operar en este nuevo tablero. Sin eso, corremos el riesgo de convertirnos en espectadores del conflicto digital que se avecina, en lugar de actores con agencia propia.

En este contexto, la pregunta clave ya no es si la IA es peligrosa. Lo es. La pregunta es quién la controla, bajo qué reglas y con qué capacidad de respuesta. Porque cuando la tecnología alcanza este nivel, deja de ser solo una herramienta: se convierte en poder. Y el poder, históricamente, no espera a quienes llegan tarde.