ANÁLISIS | ATHENALAB

Resiliencia o subordinación ante la IA: Desafíos para Chile

Alejandro Amigo
Investigador Senior AthenaLab
9 de junio 2026

En apenas cuarenta y ocho horas, entre el 2 y 3 de junio de la semana pasada, tres hechos reconfiguraron el cambiante escenario de las tecnologías emergentes. Un laboratorio académico de la Universidad de Toronto, Canadá, demostró el riesgo potencial de que modelos de IA basados en códigos de fuentes abiertas podrían transformarse en malwares (gusanos) extremadamente difíciles de contener en el ciberespacio[1]. La Casa Blanca, por su parte, reticente a regular a las empresas desarrolladoras de IA, decidió adoptar medidas tendientes a vigilar las capacidades cibernéticas más peligrosas de los modelos avanzados y a coordinar con la industria la protección de la infraestructura crítica[2]. En cambio, Europa, que a la fecha se había enfocado en legislar sobre la regulación de la IA, ha optado por implementar medidas tendientes a incrementar su soberanía tecnológica[3].

No es que un evento causara los otros, porque tanto la orden estadounidense como el paquete europeo venían gestándose hace meses. Lo relevante es que los tres son síntomas de un mismo cambio estructural. Al analizarlos en conjunto, es posible inferir que la lógica de control sobre la IA en el dominio cibernético se transforma, porque deja de residir en la contención de unos pocos actores y se desplaza hacia la resiliencia y la soberanía como nuevos ámbitos prioritarios. Para un país que es predominantemente usuario de tecnología como Chile, este giro profundiza la necesidad de adoptar decisiones.

EL ACCESO ABIERTO QUE REMECE EL TABLERO

Un equipo de la Universidad de Toronto, liderado por el profesor Nicolas Papernot, construyó un “gusano” informático potenciado por IA capaz de inferir nuevos modos y adaptar distintos ataques según la máquina o sistema objetivo, que además se propaga sin intervención humana. Lo novedoso de esta creación no es el prototipo en sí, sino que sus principales insumos provienen de fuentes abiertas (open source) disponibles en internet.

Como advierte el Dr. Papernot, no existiría un parche único que detenga algo que muta. Sin embargo, el propio estudio reconoce que persiste una brecha considerable entre lo que se logra en un laboratorio y el daño que puede causarse en el mundo real, porque los sistemas de IA todavía son, en parte, impredecibles.

Por otra parte, este experimento confirma que la IA continuará desnivelando la cancha entre atacante y defensor. La capacidad ofensiva suficiente para hacer daño ya se difunde por fuentes abiertas, mientras que la defensiva exige acceso, modelos de IA, talento y recursos que hay que financiar y sostener en el tiempo. A esto se suma que al atacante le basta un solo éxito, mientras que el defensor está obligado a acertar siempre. Desde luego, esta asimetría va más allá de los costos asociados a atacar sistemas adversarios y a defenderlos por parte de las potenciales víctimas, ya que ambos lados de la ecuación exigen capacidades y recursos similares. La desigualdad que se consolida es de otra naturaleza, porque opera sobre el margen de error y sobre la facilidad de acceso a la capacidad ofensiva, más que sobre el costo.

Podría objetarse, como hace el propio paper del profesor Papernot[4], que el "gusano" es neutro, ya que también puede modificarse para proteger a los sistemas y, por tanto, el poder de contar con esos programas depende de lo que se intente hacer con ello. Pero esa neutralidad es teórica, porque en la práctica la versión dañina ya circula al alcance de cualquiera que sepa configurarla, mientras que la que protege todavía hay que construirla. En esta carrera desigual, Chile, que se encuentra consolidando sus capacidades cibernéticas, parte en desventaja.

WASHINGTON, LA REGULACIÓN Y LA EMPRESA PIONERA

Lo notable de la orden ejecutiva firmada por el presidente Trump el pasado 2 de junio[5] no es que regule, sino que la misma administración que se define por haber desmantelado las "obligaciones burocráticas" de su antecesora establece un complejo proceso estatal.

Sus elementos principales, entre otros, son una evaluación clasificada de capacidades a cargo de la National Security Agency para designar “modelos de frontera cubiertos”, un centro de intercambio y coordinación de vulnerabilidades, liderado por el Departamento del Tesoro, y un canal de acceso a modelos avanzados para los operadores de infraestructura crítica. Con esto, la regulación de los modelos de IA se traslada desde el consumidor hacia el Estado, como una función adicional a su rol de principal responsable de la seguridad nacional.

Al respecto, se podría decir que el Estado llegó segundo. Semanas antes, Anthropic había restringido la difusión de su modelo más avanzado por considerarlo demasiado peligroso, entregándolo primero solo a un grupo de organizaciones para que solucionaran sus vulnerabilidades. Esta orden ejecutiva, en lo esencial, sistematiza como política pública un procedimiento que una empresa ya había hecho voluntariamente. Así como en otras áreas de la industria de defensa, en el ámbito de la IA el sector privado no solo es parte de la respuesta, sino que tiene las capacidades para ser pionero en el ámbito de la seguridad.

Estos hechos confirman que hoy los Estados no pueden actuar solos ante el avance de las tecnologías. La orden ejecutiva estadounidense es deliberadamente multiagencia y de colaboración voluntaria con la industria. Un enfoque whole-of-nation, donde gobierno, empresas, academia y operadores de infraestructura actúan coordinados. Es la ratificación de que la capacidad técnica ya no reside en el Estado, sino repartida en un ecosistema. En el caso de Chile, es imperante la articulación entre las necesidades públicas e iniciativas privadas que aporten en esa dirección.

REGULAR LO AJENO Y LA SUBORDINACIÓN EN EL HORIZONTE

La Unión Europea anunció esta semana un paquete de soberanía tecnológica, y los datos que lo motivan son elocuentes. A la fecha, la UE produce menos del 10% de los semiconductores del mundo y depende casi por completo de Estados Unidos y Asia para los chips avanzados que alimentan la IA.

A esa dependencia en el hardware, se añade la de los modelos más potentes, o de frontera, que permanecen cerrados y concentrados en un puñado de laboratorios estadounidenses y chinos. El paquete busca revertir esa situación impulsando la producción propia de semiconductores, expandiendo la capacidad europea de centros de datos e introduciendo requisitos de soberanía para los proveedores de nube e IA en sectores sensibles, como la banca, la energía y la salud. Europa no domina ni el insumo físico que sostiene la IA ni la capacidad de punta que la define, y reducir esa doble carencia es el propósito de fondo de la iniciativa.

Sin embargo, una potencia que depende de otros para los componentes esenciales de su tecnología puede regular cuanto quiera dentro de sus fronteras, pero las decisiones de fondo, tales como quién fabrica los chips, quién entrena los modelos y bajo qué condiciones se accede a ellos, quedan en manos de actores externos. Esto significa depender de quienes no se tiene poder alguno y es exactamente el destino que Europa busca evitar al pasar de solo regular a priorizar también la construcción de capacidad propia.

DEPENDENCIA CONSCIENTE

Los hechos relatados pueden parecer lejanos, propios de grandes potencias y de enormes presupuestos, pero en realidad le impactan a Chile de manera directa. La amenaza que se demostró en la Universidad de Toronto no distingue el tamaño de un país ni su nivel de desarrollo, porque una vez que una herramienta de este tipo circula por internet, alcanza con la misma facilidad a una potencia que a un Estado mediano. La diferencia entre un país y otro no está en si será alcanzado, sino en su capacidad para confrontar el ataque y recuperarse; y en ese escenario Chile estaría en desventaja.

Chile no cuenta con los desarrolladores y laboratorios avanzados que tiene Estados Unidos ni con los recursos que Europa busca destinar a construir soberanía, y eso es esperable en un país que es, ante todo, usuario de

tecnología y no productor. Además, el documento estadounidense menciona que hay tipos de infraestructura que son muy vulnerables y que representan gran parte de lo que sostiene la vida cotidiana en nuestro país.

Frente a este escenario, hay tres decisiones que Chile puede adoptar. La primera es asumir que la seguridad total no existe y que hay que concentrarse en la resiliencia; esto es incorporar inteligencia artificial defensiva en la infraestructura crítica (energía, agua, telecomunicaciones, salud, banca y transporte) como una política de Estado, de modo que el país pueda detectar, contener y recuperarse de previsibles ataques futuros. Si la capacidad ofensiva está disponible para cualquier tipo de actor, la defensa y la recuperación son la variable que está en nuestras manos. La segunda es elegir de quién dependemos de manera consciente, evaluando con criterio a los proveedores de tecnología en lugar de suponer una autonomía con la cual hoy no se cuenta. En esta área, la regulación nacional tiene un papel acotado, porque Chile no producirá los modelos más avanzados que se requieran a futuro y por eso su esfuerzo sería más efectivo en fijar condiciones de acceso, transparencia y seguridad a esos proveedores. Y la tercera es propender a un grado mínimo de soberanía en aquellos puntos donde una interrupción externa del servicio, decidida fuera del país, dejaría a Chile sin capacidad de reacción.

En el fondo, la pregunta que importa es quién controla en última instancia la tecnología de la que todos dependemos, y para un país abierto como el nuestro, esa pregunta es especialmente urgente. Chile todavía está a tiempo de tomar las decisiones que le permitan no quedar a merced de lo que otros resuelvan por él.

---

[1]New York Times. “Scientists Find Way to Supercharge Dangerous Computer ‘Worms’ With A.I.”, 2 de junio de 2026.https://www.nytimes.com/2026/06/02/technology/scientists-find-way-to-supercharge-dangerous-computer-worms-with-ai.html?campaign_id=9&emc=edit_nn_20260603&instance_id=176596&nl=the-morning&regi_id=92547472&segment_id=220885&user_id=97af3860a63d30d069257fbddbdf8ffa

[2]The White House. Executive Order: “Promoting Advanced Artificial Intelligence Innovation and Security”. 2 de Junio de 2026. https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/

[3]European Comission. “Commission proposes tech sovereignty package to strengthen Europe’s digital autonomy and resilience”, 2 de junio de 2026. https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1187

[4]New York Times, ibidem.

[5]The White House, ibidem.