EL MERCURIO Inversiones

Martes, 18 de marzo de 2025 | 12:54

El riesgo invisible en Chile de la inteligencia artificial fuera de control

Tres de cada cuatro trabajadores en Chile utilizan IA para tareas cotidianas y el 80% lo hace sin la autorización explícita de sus empresas. La IA está penetrando silenciosamente, generando vulnerabilidades que podrían llevar a daños financieros y reputacionales.

Eduardo Sboccia

Abogado y asesor de empresas

La inteligencia artificial no es solo una tecnología innovadora; es una poderosa herramienta estratégica que, sin la adecuada anticipación, prevención y diligencia, puede transformarse en una amenaza invisible para las empresas. El futuro está aquí, y quienes no sepan anticiparse podrían verse enfrentados a riesgos que aún ni siquiera imaginan. ¿Están preparados?

Actualmente, tres de cada cuatro trabajadores en Chile utilizan inteligencia artificial para ejecutar tareas cotidianas. Un dato revelador, pero más preocupante aún es saber que el 80% lo hace sin la autorización explícita de sus empresas. Este fenómeno se denomina "Shadow AI" o "IA en las sombras": empleados que recurren a herramientas tecnológicas avanzadas por iniciativa propia, fuera del control o supervisión organizacional. En otras palabras, la inteligencia artificial está penetrando silenciosamente en las empresas, generando vulnerabilidades que podrían traducirse en daños financieros y reputacionales irreversibles.

Este escenario no es hipotético. Empresas globales, incluyendo gigantes tecnológicos, ya lo han vivido. Recordemos brevemente el caso de Samsung: en noviembre de 2022, tras el lanzamiento mundial de ChatGPT, empleados entusiasmados de la unidad de negocios de semiconductores empezaron a introducir datos estratégicos y confidenciales en esta herramienta. La compañía reaccionó prohibiendo el uso inmediato de esta tecnología, pero el daño ya estaba hecho. La información estratégica había quedado expuesta, demostrando una vez más que la reacción es siempre menos efectiva que la prevención.

A mi juicio, prohibir la inteligencia artificial tampoco es la solución; sería como haber prohibido el uso de internet hace dos décadas. Tal enfoque no solo es inefectivo, sino contraproducente, pues provoca la fuga de talentos hacia organizaciones que sí aprovechan estos avances. Por lo tanto, la verdadera solución

pasa por algo que insistentemente vengo sosteniendo en diversas columnas: anticiparse con políticas claras, protocolos rigurosos y un modelo sólido de entrenamiento corporativo.

Sin embargo, la realidad en nuestro país muestra que estamos lejos de esa anticipación. Según expertos locales, solo una minoría de empresas chilenas cuenta con modelos de gobernanza de inteligencia artificial. La mayoría opera en dos extremos peligrosos: o permite la libertad absoluta sin ningún control, o adopta la prohibición total. Ambas decisiones implican riesgos enormes, desde pérdidas millonarias por brechas de ciberseguridad, hasta decisiones operativas basadas en información errónea o contaminada por sesgos.

Esto, sin mencionar las sanciones legales asociadas a incumplimientos regulatorios, particularmente desde la perspectiva de la Ley de Delitos Económicos y de Ley de Protección de Datos Personales, que podrían representar multas significativas e incluso cárcel. En una reciente nota en DF, el director ejecutivo de Agentica Systems, Fernando Roa, advierte que las organizaciones empiezan a preocuparse por este tema solo cuando ya tienen "el incendio encima". Es decir, nuevamente llegan tarde, cuando el daño ya es profundo y visible.

Conviene entonces preguntarse: ¿Está su empresa preparada para identificar y prevenir estos riesgos? ¿Tiene políticas claras para el uso de inteligencia artificial? ¿Se están entrenando activamente en caso de incidentes por mal uso?

La solución, insisto, es apostar por la anticipación estratégica: invertir en conocimiento, establecer protocolos claros, promover una cultura interna orientada a la prevención y, sobre todas las cosas, fortalecer el pensamiento crítico tanto para hacer lo correcto, como para evitar decisiones basadas en información sesgada o errónea.

Esta última parte es crucial, pues ese fortalecimiento implica precisamente imaginar escenarios de crisis o conflictos derivados del mal uso de la inteligencia artificial, bajándolos desde la teoría hasta situaciones prácticas y realistas. Visualizar estos escenarios —desde daños económicos significativos, interrupciones operacionales, hasta responsabilidades penales personales— permite entrenar a los equipos para evitar estas situaciones o para que, si ocurren, las enfrenten de manera rápida y eficiente, minimizando daños, protegiendo la reputación corporativa, y evitando la responsabilidad penal extendida a empresa y ejecutivos.

El uso de inteligencia artificial exige una preparación rigurosa y consciente. Aquellas organizaciones que entiendan esto y lo adopten como filosofía interna serán las que indudablemente liderarán los mercados del futuro.