La gobernanza: el paso previo para desbloquear el potencial de la IA

Por José Lagos, Docente UEjecutivos Facultad de Economía y Negocios Universidad de Chile La inteligencia artificial está avanzando rápidamente dentro de las organizaciones.

Herramientas de inteligencia artificial generativa, algoritmos de machine learning y agentes capaces de ejecutar tareas, ofrecen oportunidades para aumentar la productividad, automatizar procesos y mejorar la toma de decisiones. Sin embargo, antes de preguntarse sobre las herramientas que se pueden habilitar, las organizaciones deberían responder otra pregunta: ¿Estamos preparados para gobernar la inteligencia artificial que queremos implementar?

Habilitar una tecnología puede ser relativamente sencillo. Gestionar sus riesgos, establecer responsabilidades, controlar los datos que utiliza y supervisar sus decisiones requiere una estructura de gobierno. Por eso, la gobernanza de inteligencia artificial no debería aparecer después de la adopción. Debe ser una condición previa para ampliar progresivamente las capacidades de inteligencia artificial.

Cuando una organización adopta inteligencia artificial sin reglas claras pueden aparecer rápidamente problemas de privacidad, seguridad, sesgo, confidencialidad, cumplimiento o responsabilidad. Un empleado puede introducir información sensible en una herramienta pública. Un modelo puede apoyar decisiones relevantes sin haber sido validado. Un proveedor puede procesar datos corporativos bajo condiciones que la organización desconoce.

El riesgo aumenta aún más con los agentes de inteligencia artificial. A diferencia de un chatbot que responde preguntas, un agente puede consultar sistemas, recuperar información, utilizar herramientas y ejecutar acciones. Esto obliga a controlar no solamente qué responde la IA, sino también qué puede hacer, con qué permisos y bajo qué supervisión. Cuanto mayor sea la autonomía de una solución, mayor debe ser la madurez de gobernanza necesaria para habilitarla.

Una gobernanza efectiva comienza con visibilidad. La organización debe identificar qué soluciones de inteligencia artificial utiliza, quién es responsable de ellas, qué datos procesan, qué proveedores participan y qué decisiones apoyan o automatizan. Esto incluye modelos desarrollados internamente, soluciones de terceros, funciones de inteligencia artificial integradas en aplicaciones existentes y herramientas utilizadas directamente por empleados. Sin un inventario adecuado, la organización no puede evaluar de manera consistente sus riesgos. No se puede gobernar aquello que no se sabe que existe.

La gobernanza tampoco significa aplicar el mismo proceso a todos los casos de uso. Un asistente utilizado para redactar un correo interno no presenta el mismo riesgo que un algoritmo empleado para evaluar clientes o que un agente capaz de modificar registros y ejecutar transacciones. Por ello, las organizaciones deberían clasificar sus casos de uso, según factores como la sensibilidad de los datos, impacto sobre personas, importancia de las decisiones y nivel de autonomía.

Los casos de bajo riesgo pueden seguir procesos simplificados. Las soluciones de mayor impacto pueden requerir evaluaciones adicionales de seguridad, privacidad, cumplimiento, legal o riesgos. La gobernanza debe ser proporcional al riesgo.

Los agentes de inteligencia artificial elevan significativamente la necesidad de control, porque pueden combinar modelos generativos, acceso a información, herramientas externas y capacidad de actuar. Antes de habilitarlos, la organización debería determinar qué sistemas pueden consultar, qué información pueden modificar, qué acciones están autorizadas y cuáles requieren aprobación humana. También deben aplicarse principios tradicionales de seguridad como mínimo privilegio, segregación de funciones, monitoreo, registro de actividades y mecanismos para detener el agente cuando sea necesario. Un agente no debería recibir acceso simplemente porque técnicamente puede utilizarlo.

La inteligencia artificial depende de información. Por eso, la gobernanza en este ámbito está directamente relacionada con la gobernanza de datos. La organización debe definir qué información puede introducirse en cada solución y bajo qué condiciones, especialmente cuando se trata de datos personales, información confidencial, propiedad intelectual o datos de clientes.

En soluciones externas, también es necesario comprender dónde se almacenan los datos, cuánto tiempo se conservan, si pueden utilizarse para entrenar modelos y qué terceros participan en el servicio. La responsabilidad debe ser compartida

El negocio, la tecnología, la seguridad, la privacidad, el cumplimiento, lo legal, los riesgos y la auditoría tienen responsabilidades diferentes dentro del modelo de gobierno. En ese aspecto, debe quedar claro quién propone un caso de uso, quién evalúa sus riesgos, quién aprueba su implementación, quién monitorea su desempeño y quién puede detenerlo si aparecen problemas.

Antes de desplegar la inteligencia artificial generativa, machine learning avanzado o agentes autónomos, una organización debería poder responder qué sistemas utiliza, para qué, quién es responsable, qué datos procesan, y qué acciones pueden

realizar.