LITORALPRESS

Fecha: 30-03-2026
Medio: Revista Gerencia
Supl. : Revista Gerencia
Tipo: Noticia general
Título: Agentes de IA: ¿El nuevo riesgo interno?

Pág. : 22
Cm2: 471,3

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

Agentes de IA: ¿El nuevo riesgo interno?

El avance de los agentes de inteligencia artificial está redefiniendo la automatización empresarial, pero también introduce un nuevo vector de riesgo. Su autonomía, acceso a sistemas críticos y capacidad de tomar decisiones en tiempo real obligan a las organizaciones a replantear sus estrategias de ciberseguridad y gestión de amenazas internas.

Claudio Ordoñez, Director de Ciberseguridad de PwC Chile.

La adopción acelerada de agentes de inteligencia artificial (IA) está marcando un cambio profundo en las operaciones empresariales a nivel global. De acuerdo con la última encuesta de PwC sobre agentes de IA, el 79% de los altos ejecutivos afirma que sus organizaciones ya están implementando estas tecnologías para optimizar procesos y mejorar la eficiencia.

Por tanto, lo que comenzó como una herramienta para automatizar tareas rutinarias, como la programación de reuniones o la gestión de facturas, hoy evolucionan rápidamente a través de agentes de IA hacia capacidades más complejas, incluyendo flujos de trabajo completos.

Sin embargo, este avance viene acompañado de un desafío significativo: la ciberseguridad. A medida que los agentes de IA adquieren mayor autonomía y acceso a sistemas críticos, surge una nueva categoría de amenaza interna. Y es que tradicionalmente el concepto "amenaza interna" se vinculaba a personas dentro de una organización capaces de causar daño a través de una amplia gama de acciones, desde fraude y robo hasta sabotaje y espionaje. Hoy los agentes de IA, con niveles de acceso similares, podrían ser manipulados para ejecutar acciones similares, explicó Claudio Ordoñez, Director de Ciberseguridad de PwC Chile.

"Para el caso de los agentes de IA el riesgo es mayor porque, a diferencia del software tradicional, estos agentes interpretan instrucciones, toman decisiones y actúan de manera autónoma y en tiempo real. Su capacidad de operar a gran escala y velocidad puede convertir cualquier manipulación en un incidente de alto impacto", explicó Ordoñez. Sostuvo que actualmente existe una brecha importante en la gestión de estos riesgos. Aunque algunas organizaciones ya cuentan con experiencia en amenazas internas humanas y prácticas de ciberseguridad, la protección de agentes de IA se encuentra todavía en una etapa incipiente.

¿Qué medidas adoptar?

Frente a este escenario, según el ejecutivo de PwC Chile, las organizaciones deben adoptar medidas proactivas. Entre ellas se encuentran tratar a los agentes como usuarios internos con privilegios mínimos, establecer límites claros a sus acciones, implementar controles con intervención humana para decisiones críticas y monitorear su comportamiento mediante mecanismos independientes.

Del mismo modo, es fundamental entrenar a los agentes en las políticas y valores de la empresa, actualizar constantemente el inventario de agentes y aplicar revisiones periódicas. Prácticas innovadoras como DLP y monitoreo de actividad también refuerzan la protección.

"La adopción de agentes de IA presenta oportunidades excepcionales para aumentar la productividad, mejorar la toma de decisiones y transformar procesos. No obstante, para capturar plenamente su valor, las organizaciones deben avanzar con responsabilidad y con una estrategia de seguridad digital robusta."

Para Claudio Ordoñez, "reconocer y mitigar los riesgos asociados a estos nuevos colaboradores digitales es esencial para garantizar que la IA sea un habilitador de crecimiento y no una fuente de vulnerabilidad".