LITORALPRESS

Fecha: 29-04-2026
Medio: El Mercurio
Supl. : El Mercurio - Chile Tecnológico
Tipo: Noticia general
Título: **El riesgo en el uso desmedido de herramientas digitales en la oficina**

Pág. : 5
Cm2: 442,6

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

FENÓMENO CONOCIDO COMO *SHADOW AI*:

El riesgo en el uso desmedido de herramientas digitales en la oficina

La mayor amenaza en ciberseguridad que enfrentan las empresas chilenas hoy no viene de *hackers* sofisticados, sino de sus propios empleados que usan herramientas de inteligencia artificial sin control.

MARÍA PASTORA SANDOVAL

Un trabajador abre ChatGPT, carga el contrato de un cliente y le pide al *chat* que lo resuma. Ahorra veinte minutos. Lo que no sabe (o no dimensiona) es que acaba de enviar información confidencial a un servidor fuera de Chile, donde podría convertirse en dato de entrenamiento para futuros modelos de inteligencia artificial. La empresa, en ese instante, perdió el control de esa información.

Esto no es un escenario hipotético, es el patrón más común que observan hoy los especialistas en ciberseguridad que trabajan con empresas chilenas. Y tiene nombre propio: *shadow AI*, o el uso no autorizado de herramientas de inteligencia artificial dentro de las organizaciones.

"Ya dejó de ser emergente; es un problema recurrente y de rápido crecimiento", advierte Sebastián Ávila, jefe del Csirt del Grupo Tecnológico ITQ. "La intención del empleado suele ser buena, pero el riesgo es altísimo", agrega.

Un informe de Microsoft de octubre de 2025 reveló que el 71% de los trabajadores usa herramientas de IA no aprobadas por su compañía. Otro estudio de TechRepublic detectó que el 77% ha compartido datos sensibles con ChatGPT u otras plataformas similares. Las violaciones de políticas asociadas al uso de IA generativa se duplicaron año a año, con una media de 223 incidentes mensuales por empresa.

UN ESTUDIO DE TECHREPUBLIC detectó que el 77% de los trabajadores ha compartido datos sensibles con ChatGPT u otras plataformas similares.

EL ESLABÓN MÁS DÉBIL

Para Juan Francisco Acuña, gerente general de Timix, el fenómeno no es un problema de personas, sino de liderazgo: "Los empleados están buscando ser más productivos y la IA les da esa capacidad inmediata, pero las organizaciones no han avanzado al mismo ritmo en gobernanza ni en políticas. Cuando no hay estrategia de IA, aparece la *shadow AI*".

El perfil de las empresas más expuestas abarca todos los tamaños, pero el impacto es especialmente grave en sectores que manejan grandes volúmenes de documentos críticos, como servicios financieros, estudios de abogados, salud y recursos humanos. En nuestro país, el problema tiene una dimensión adicional.

"Chile es un blanco de alto perfil por su avanzada digitalización. Las filtraciones de datos en el país han crecido un 188% y gran parte se debe al fenómeno de la *shadow AI*. Aunque nuestra infraestructura es sólida, el comportamiento del usuario sigue siendo el eslabón más débil", señala Víctor Belaúnde, gerente de Operaciones y CISO de Ecosistemas Global.

Técnicamente, el mecanismo es simple y preocupante: cuando un empleado sube un documento a una plataforma gratuita como ChatGPT, ese archivo viaja a la nube del proveedor y, según sus términos de servicio, puede pasar a ser parte de los datos de entrenamiento para futuros modelos. Ávila lo explica en simple: "Un fragmento de esos datos confidenciales podría ser aprendido por la IA y aparecer en la respuesta de otro usuario en cualquier parte del mundo".

> "Las filtraciones de datos en el país han crecido un 188% y gran parte se debe al fenómeno de la *shadow AI*".
>
> **VÍCTOR BELAÚNDE**
> Gerente de Operaciones y CISO de Ecosistemas Global

El panorama regulatorio chileno aún no logra ponerse al día. Belaúnde reconoce que la Ley Marco de Ciberseguridad y la nueva Ley de Protección de Datos Personales son avances históricos, pero aclara que "no es una solución mágica" y que "las leyes castigan la consecuencia". Sin embargo, indica que la prevención depende de la gobernanza interna de cada organización.

Según Acuña, menos del 30% de las empresas chilenas cuenta hoy con políticas maduras y operativas sobre el uso de IA. Herramientas de gobernanza de IA y plataformas de monitoreo de *shadow IT* pueden aportar control y, un paso más allá, adoptar instancias privadas de IA, donde los datos no salen del entorno seguro de la empresa, garantizando que la productividad no sacrifique la confidencialidad.

¿Qué puede hacer una empresa mediana sin grandes inversiones? Los expertos coinciden en un mismo camino: primero, redactar una política de uso de IA clara (qué herramientas están permitidas y qué datos jamás pueden ingresarse); segundo, capacitar a los equipos para que entiendan por qué es peligroso (no solo que está prohibido), y, tercero, si el negocio requiere usar estas plataformas, adquirir licencias corporativas donde el proveedor garantiza por contrato que los datos no serán usados para entrenar modelos públicos.

Y si el error ya ocurrió, la respuesta es una sola: reportarlo de inmediato. "Perder el miedo a la represalia y avisar al área de TI es lo más importante. Ocultar el error siempre agravará el problema", dice Ávila; lo que Belaúnde reafirma destacando que "la transparencia es vital". En ciberseguridad, el tiempo apremia.