

DE PUÑO  
Y LETRA

**CATALINA  
MERTZ**

Economista

# Tranquilidad artificial

Hoy es común que en diversos foros de conversación se comente que la adopción de la inteligencia artificial (IA) por parte de las empresas ha sido más lenta de lo esperado. Por ejemplo, un semanario internacional acuña el término "pilotitis" como una actual tendencia, consistente en pilotear, pero nunca escalar, el uso de la IA de manera relevante, y en otros medios y foros se describe que en demasiados casos las adopciones se ejecutan en procesos secundarios, mas no en los que hay mayores problemas a resolver o beneficios que cosechar.

Más allá de las razones detrás de este fenómeno, que van desde la dificultad de generar los datos necesarios u orquestrar o integrar adecuadamente sistemas y fuentes de datos generados inorgánicamente en el pasado y llegan hasta una cultura aversa al riesgo, considerar este hecho como una descripción exhaustiva del nivel de penetración de la IA trae consigo un riesgo importante: despreocuparse de cómo nuestras organizaciones están integrando la IA. Mientras las empresas se muestran reacias, las personas han adoptado la IA a un ritmo sin precedentes. En el caso de ChatGPT, su adopción fue vertiginosa, alcanzando un millón de usuarios en cinco días y llegando hoy a más de 200 millones de usuarios activos mensuales. En Chile, algunas encuestas estiman que el 80% de los chilenos lo está usando. ¿Acaso dejan de usarlo al cruzar la puerta de la oficina o ingresar a las plataformas de trabajo? La ganancia en productividad en una multiplicidad de tareas es tal que lo más probable es que no sea así. Y si reaccionamos irreflexivamente, prohibiendo su uso para evitar la fuga de información de la empresa, será una decisión incomprensible y resistida, y además contradictoria con la búsqueda constante de mejoras en la eficiencia.

La IA es mucho más que ChatGPT, herramienta que es además solo una de entre varias disponibles, pero su popularidad permite ilustrar bien lo urgente que es el que todas las organizaciones, independientemente de su tamaño e industria, pongan la IA como tema sobre la mesa. La divergencia entre las tasas de adopción de las personas en comparación con la de las empresas puede ser un buen punto de partida en esta conversación, al acotar una primera ronda

de preguntas a cómo la organización integrará el uso que las personas hacemos de las herramientas disponibles, ya sea adoptando las configuraciones de privacidad y de almacenamiento y uso de información que ofrecen, u optando por versiones empresariales con medidas de seguridad más avanzadas. Esa primera ronda también desencadenará otras preguntas prácticas sobre cómo se organizarán estas tareas, tales como las personas a cargo de diseñar e implementarlas, y generar tanto directrices, en forma de políticas o reglamentos, como prácticas de aseguramiento de que se estén cumpliendo. Si la alta dirección genera el espacio necesario, como debiera, probablemente surgirán, también, reflexiones sobre la estrategia de adopción de la IA de la empresa, y cómo hacerlo de manera segura.

Y es que el uso de la IA trae consigo, necesariamente, tanto oportunidades como riesgos. No solamente están los desafíos relacionados con la protección de datos personales que implican estos grandes modelos de lenguaje o con las denominadas alucinaciones —respuestas incorrectas o ficticias— que, sin revisión, pueden inducir a decisiones equivocadas, sino que la IA modifica sustancialmente el paisaje de riesgos de la seguridad de la información, al menos en tres sentidos. En primer lugar, hay más incógnitas. La evolución de la IA, y el mayor uso de agentes de IA "conversando" entre ellos, generará nuevas categorías de riesgo, que no nos imaginamos todavía. Por otra parte, se amplía la denominada "superficie de ataque" para los ciberdelincuentes, ya que, al haber más interconexión de datos, y haciendo un símil con una casa, las ventanas por donde pueden entrar son más, y también el botín al que pueden tener acceso es mayor. Y, por último, el poder de la IA de aprender y evolucionar rápidamente está habilitando la creación de tipos de ataques totalmente nuevos.

Ya hay estudios que correlacionan el crecimiento de las empresas con su capacidad de construir seguridad y confianza digital. Dejar atrás la "tranquilidad artificial" y enfrentar el desafío de la IA será lo que diferencie a las empresas que perduren de aquellas que se queden rezagadas en el nuevo entorno digital.

**MIENTRAS LAS EMPRESAS SE  
MUESTRAN REACIAS, LAS PERSONAS  
HAN ADOPTADO LA IA A UN RITMO  
SIN PRECEDENTES.**