

Expertos analizan los riesgos de la IA, desinformación y ciberseguridad planteados por el Foro Económico Mundial

■ El Informe de Riesgos Globales 2026 advirtió que la aceleración tecnológica está impactando desde la confianza pública hasta la seguridad digital.

POR MARCO ZECCHETTO

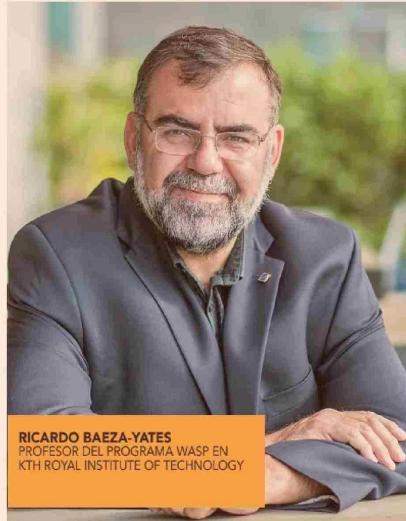
Hace unos días, el Foro Económico Mundial publicó su Informe de Riesgos Globales 2026, en el que posicionó a la confrontación geo-económica como el principal riesgo global para este año, en un contexto marcado por crecientes tensiones entre potencias.

En ese escenario, el documento situó a la información falsa y la desinformación como el segundo mayor riesgo a dos años, ubicó a la inseguridad cibernética entre los principales riesgos estructurales, y alertó sobre el fuerte ascenso de las consecuencias adversas de la inteligencia artificial (IA), que escaló hasta el quinto lugar en el horizonte de 10 años.

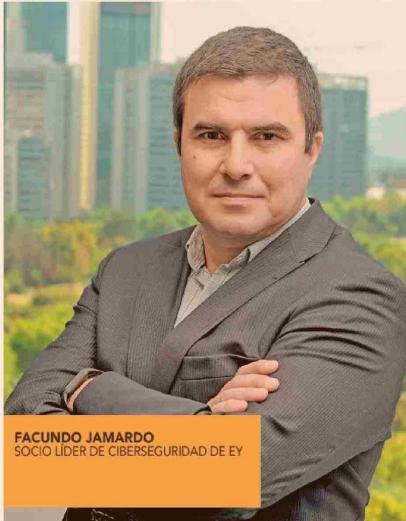
En particular, el informe advirtió que la integridad de las noticias en línea y la información en general está "cada vez más amenazada", debido a la creciente dificultad para distinguir entre contenido real y material sintético generado por IA.

Además, señaló que la proliferación de imágenes, audios y videos falsificados (*deepfakes*), junto con el mayor consumo de noticias a través de redes sociales y herramientas basadas en IA, está afectando la confianza pública y profundizando la polarización política y social, con impactos directos en procesos democráticos e institucionales.

El profesor del programa Wahlenberg IA, Sistemas Autónomos y Software (WASP) en KTH Royal Institute of Technology, Ricardo Baeza-Yates, afirmó que el mundo "ya entró" en una crisis global de confianza en la información,



RICARDO BAEZA-YATES
PROFESOR DEL PROGRAMA WASP EN
KTH ROYAL INSTITUTE OF TECHNOLOGY



FACUNDO JAMARDO
SOCIO LÍDER DE CIBERSEGURIDAD DE EY

TOP 10 RIESGOS GLOBALES, SEGÚN SU GRAVEDAD	
CORTO PLAZO (DOS AÑOS)	LARGO PLAZO (10 AÑOS)
1) Confrontación geoeconómica	1) Fenómenos meteorológicos extremos
2) Información falsa y desinformación	2) Pérdida de biodiversidad y colapso del ecosistema
3) Polarización social	3) Cambio crítico en los sistemas terrestres
4) Fenómenos meteorológicos extremos	4) Información falsa y desinformación
5) Conflictos armados en los Estados	5) Consecuencias adversas de las tecnologías de IA
6) Inseguridad cibernética	6) Escasez de recursos naturales
7) Desigualdad	7) Desigualdad
8) Deterioro de los derechos humanos y/o de las libertades civiles	8) Inseguridad cibernética
9) Contaminación	9) Polarización social
10) Migraciones o desplazamientos involuntarios	10) Contaminación

FUENTE: INFORME DE RIESGOS GLOBALES 2026, FORO ECONÓMICO MUNDIAL

marcada por el rol de la IA en las campañas de desinformación ante los procesos electorales de 2024 y 2025, y que el avance de esta tecnología está complicando la capacidad de verificar la legitimidad de imágenes e información que se

difunde en línea.

El también cofundador y CSO de Theodora AI indicó que los medios, las plataformas y las democracias "están muy poco preparadas" para enfrentar el aumento en la proliferación de *deepfakes* y la

humanas con mayor rapidez.

Por otro lado, el académico indicó que la IA está ampliando la brecha digital, debido a que "el 55% de la población" no cuenta con acceso o habilidades para beneficiarse de estas tecnologías, y agregó que su mayor adopción amplificará otros riesgos, como la polarización social y la influencia en los problemas de salud mental, aludiendo a los casos de suicidio asistidos por modelos de IA.

Inseguridad cibernética

En el ámbito de la inseguridad cibernética, el reporte indicó que la digitalización y la automatización de la infraestructura crítica está creando un nuevo frente de vulnerabilidad "ciberfísica", donde los sistemas y dispositivos de control industrial pueden llegar a estar "insuficientemente protegidos y supervisados".

El documento advirtió que estas amenazas resultan especialmente atractivas para actores gubernamentales y cibercriminales, al permitir negar responsabilidad y dificultar respuestas diplomáticas y legales.

En este escenario, el socio líder de Ciberseguridad de EY, Facundo Jamardo, destacó el rol de la consolidación de la ciberguerra y el uso intensivo de IA para automatizar ataques, lo que ha reducido los tiempos necesarios para identificar y explotar vulnerabilidades. Señaló que hoy los ciberataques operan de manera continua, y con una velocidad que supera la capacidad de respuesta de muchas organizaciones.

"Hoy tienes agentes con la capacidad de operar como un hacker que trabaja 24/7, que permiten conseguir resultados de vuelta razonables y en muy poco tiempo, sobre todo teniendo en cuenta que las empresas no tienen todavía un músculo de protección 24/7. Entonces, hay mucha infraestructura que no ha tenido el nivel de securización adecuado", afirmó.

Jamardo agregó que uno de los principales desafíos para los próximos años será la demanda de capacidades humanas y técnicas para operar esquemas de protección frente a la digitalización de procesos, junto con establecer controles de seguridad de terceros y proveedores en cadenas productivas y de servicios.

"La gran mayoría de las empresas en Chile no han hecho nada respecto a cómo saber el nivel de seguridad de terceros", añadió.