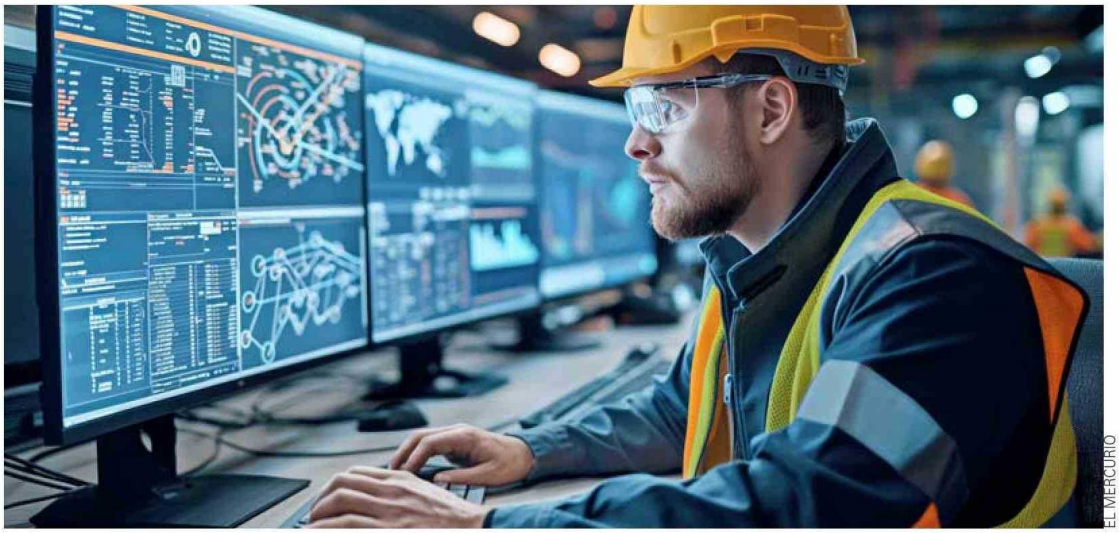
LITORALPRESS

Fecha: 28-08-2025
Medio: El Mercurio
Supl. : El Mercurio - Minería y Comunidad
Tipo: Noticia general
Título: **Los ciberataques ponen en jaque continuidad operacional**

Pág. : 6
Cm2: 369,1

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida



EL MERCURIO

**98% de las compañías mineras** carece de la capacidad para enfrentar ciberataques impulsados por IA, según el informe "State of Cybersecurity Resilience 2025: Natural Resources Industry".

### ATAQUES EN AUMENTO EN RUBRO MINERO:

# Los ciberataques ponen en jaque continuidad operacional

**PAULA MONTEBRUNO**

El ataque a la División Gabriela Mistral de Codelco en 2023, que paralizó la operación de sus camiones autónomos durante 72 horas, es un caso recordado que dejó al descubierto la fragilidad de los entornos OT/IT (tecnología industrial y de la información) en la minería chilena. "Este tipo de incidentes demuestran que los ciberataques ya no solo generan pérdidas económicas, sino que también pueden comprometer la continuidad operacional e incluso la seguridad de las personas en faenas", advierte Martín Tavil, director ejecutivo para la Industria Minera de Accenture Chile.

Para el experto, la creciente adopción de IoT (internet de las cosas), automatización, robótica y sistemas de control como SCADA (*supervisory control and data acquisition*) incrementa la superficie de ataque y expone a las compañías a interrupciones de procesos críticos. Al respecto, el Global Cybersecurity Outlook 2025, del World Economic Forum (WEF) y Accenture, señala que los principales riesgos para la minería incluyen la exposición de las cadenas de suministro (54%), la expansión de ciberataques con IA generativa (47%) y el *ransomware*, considerado la mayor amenaza por el 45% de los encuestados. "Factores como las tensiones geopolíticas, la proliferación de ataques de *phishing* —42% de las organizaciones sufrió uno exitoso en el último año— y la creciente brecha de talento —solo el 14% afirma tener las competencias necesarias— amplifican la exposición del sector minero", agrega Tavil.

Douglas Corona, arquitecto de ciberseguridad en ITQ Latam, coincide al señalar que hoy el mayor riesgo es la interrupción de la continuidad operativa. "Un ataque de *ransomware* o un ataque a la cadena de suministro podría detener la producción, con un impacto económico millonario en cuestión de horas", afirma. Y advierte que la masiva integración de OT e IoT crea nuevos puntos vulnerables: "Los equipos de perforación autónoma, los sensores y la infraestructura de control están conectados a la red, y si estos sistemas no están debidamente protegidos, se convierten en una puerta de entrada para los ciberdelincuentes".

## AMENAZA DE LA IA

El panorama es aún más desafiante. Según Tavil, "el 98% de las compañías mineras carece de la capacidad para enfrentar ciberataques impulsados por IA, cifra que supera el promedio global de 90%. Además, nueve de cada diez no cuentan con prácticas básicas de seguridad de datos e IA para proteger modelos críticos, *pipelines* de datos e infraestructura en la nube".

Algo a considerar, ya que el MM-ISAC (Mining and Metals Information Sharing and Analysis Centre) estima que los ataques al sector minero, a nivel global, se triplicaron entre 2023 y 2024, impulsados, entre otras cosas, por la inteligencia artificial.

Tavil estima que en un sector altamente digitalizado y dependiente de la analítica avanzada, estas brechas representan vulnerabilidades de alto riesgo para la operación.