LITORALPRESS

Fecha: 14-07-2025
Medio: Revista Nueva Minería & Energía
Supl. : Revista Nueva Minería & Energía
Tipo: Noticia general
Título: CIBERATAQUES Y LA DEFENSA INTELIGENTE

Pág. : 8
Cm2: 483,7

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

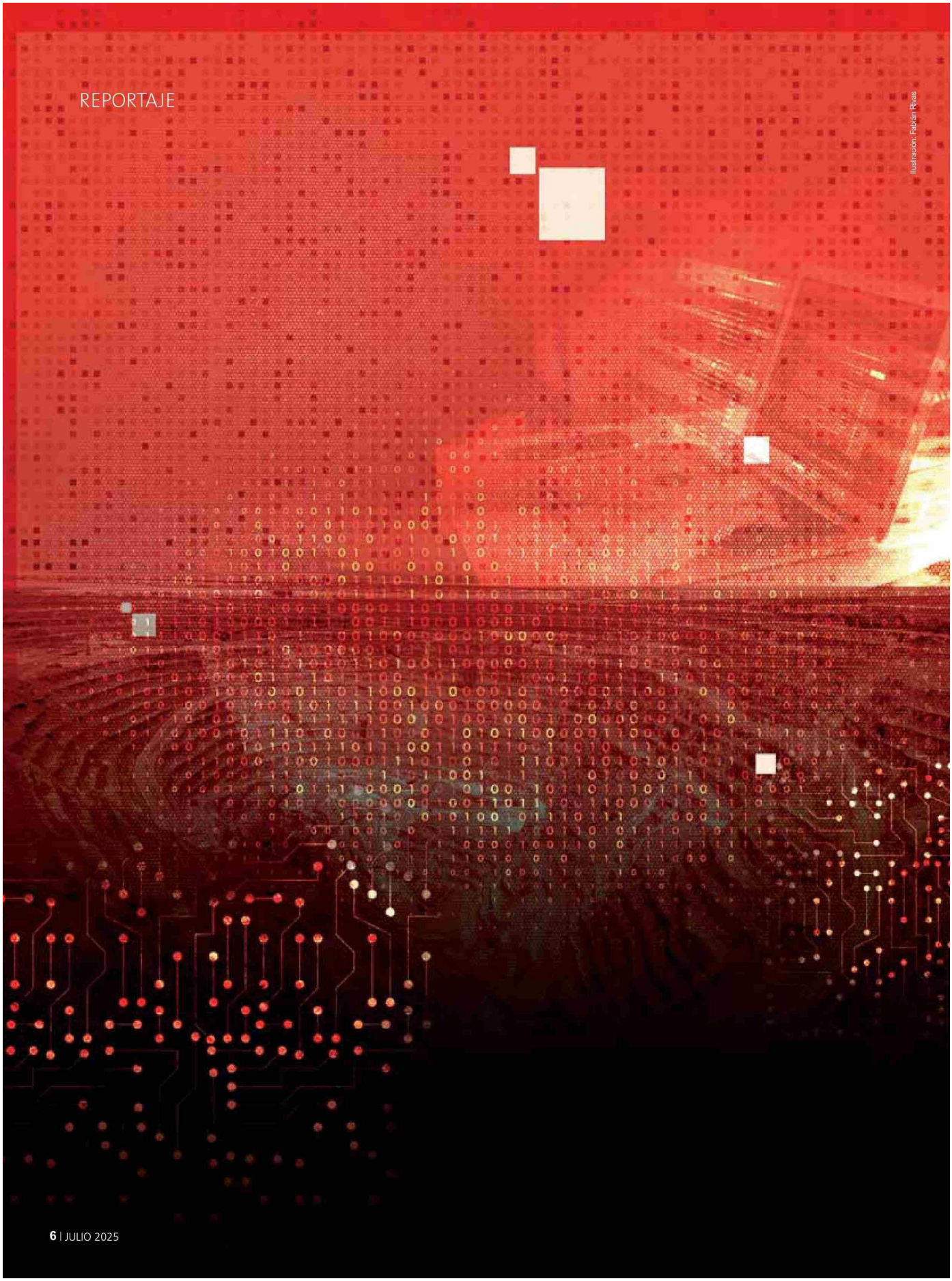

Ilustración: Fabián Rivas

LITORALPRESS

Fecha: 14-07-2025
Medio: Revista Nueva Minería & Energía
Supl. : Revista Nueva Minería & Energía
Tipo: Noticia general
Título: CIBERATAQUES Y LA DEFENSA INTELIGENTE

Pág. : 9
Cm2: 298,5

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

LA NUEVA VULNERABILIDAD MINERA:

CIBERATAQUES Y LA DEFENSA INTELIGENTE

Frente a un escenario de riesgos cibernéticos crecientes, la inteligencia artificial emerge como una herramienta clave para anticipar ataques, fortalecer las defensas y resguardar los procesos esenciales de las faenas. *Por Horacio Acuña*

En plena revolución de la Minería 4.0, donde sensores inteligentes, digital twins y flotas autónomas transforman los yacimientos en ecosistemas altamente digitalizados, emerge con fuerza una preocupación que hasta hace poco era secundaria: los ciberataques. Así, la creciente integración de tecnologías de inteligencia artificial (IA) en la operación minera no solo abre oportunidades de eficiencia, sino además nuevas puertas de entrada a amenazas digitales cada vez más sofisticadas.

Esta amenaza, que parecía lejana hace solo una década, se ha transformado en una preocupación transversal en la industria, así como también en otros sectores y tipos de instalaciones críticas. Un caso emblemático es el de Colonial Pipeline, ocurrido en mayo de 2021, que expuso los alcances reales de una brecha digital: un ransomware paralizó el principal oleoducto de la costa este de Estados Unidos durante días, generando escasez de combustible, caos logístico y pérdidas millonarias. Si un hecho similar ocurriera en una operación minera chilena, no solo se detendría la producción: podría afectar el suministro eléctrico, la cadena de exportación o incluso la estabilidad de contratos internacionales.

Durante el último tiempo, Chile ha dado pasos significativos en materia de ciberseguridad. En marzo de 2024 se cumplió un año desde la promulgación de la Ley 21.663, el nuevo marco legal chileno en esta área. Esta normativa, que comenzó a aplicarse de manera progresiva desde enero y marzo de 2025, establece obligaciones para las empresas designadas como proveedores de servicios esenciales u operadores de importancia vital (OIV), una categoría en la que es altamente probable que se encuentren numerosas compañías del sector minero.

Esta norma obliga a dichas empresas a contar con protocolos robustos de respuesta ante incidentes, reportar vulneraciones de forma obligatoria y cumplir estándares definidos por la Agencia Nacional de Ciberseguridad (ANCI). Para la minería, donde los sistemas SCADA (Control de Supervisión y Adquisición de Datos), IoT industrial y plataformas cloud son hoy parte estructural de la operación, la implementación de estas exigencias se vuelve urgente, impulsando una transformación cultural y tecnológica sin precedentes en la industria.

PARQUE LEGADO

No obstante, entre la norma y la realidad operativa persisten brechas importantes. “ Todavía, cuando voy a una empresa para hacer algún tipo de diagnóstico en el mundo industrial me encuentro con computadores que operan

LITORALPRESS

Fecha: 14-07-2025
Medio: Revista Nueva Minería & Energía
Supl. : Revista Nueva Minería & Energía
Tipo: Noticia general
Título: CIBERATAQUES Y LA DEFENSA INTELIGENTE

Pág. : 10
Cm2: 380,7

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

Foto: LinkedIn

Patrick Rinski, socio y líder de ciberseguridad para América Latina de McKinsey & Company.

Foto: LinkedIn

Katherina Canales, directora ejecutiva de la Corporación Minera de Ciberseguridad (CCMIN).

con Windows 95 o Windows 98. Es decir, es una realidad de la industria" , advierte Patrick Rinski, socio y líder de ciberseguridad para América Latina de McKinsey & Company.

Estos sistemas operativos integran de lo que se conoce como parque legado o sistemas legados, que corresponden a tecnologías, equipos o plataformas informáticas antiguas, tanto de software como de hardware, pero aún en uso, que fueron desarrolladas con tecnologías ya obsoletas o desactualizadas, sin soporte ni actualizaciones, lo que las vuelve extremadamente vulnerables a ataques cibernéticos. Sin embargo, no han sido reemplazadas porque siguen cumpliendo funciones críticas dentro de una organización y no es sencillo ni económico sustituirlas.

Rinski subraya que numerosas compañías diseñan planes, pero no ejecutan simulacros ni definen una cadena de mando para enfrentar una crisis. En ese sentido, muchas empresas tienen " planes de respuesta que quedan en papel" , pero " cuando ocurre un incidente, nadie sabe quién toma el mando ni cómo aislar el sistema afectado" .

> "Hoy en día tenemos ataques cibernéticos que son ejecutados por **inteligencia artificial.** ¿Estamos preparados para responder a eso?", plantea Patrick Rinski de McKinsey & **Company.**

HERRAMIENTA ESTRATÉGICA

Respecto al origen de los incidentes, entre el 70% y el 95% de los estudios en el mundo dicen que la principal causa de ataques cibernéticos son errores humanos.

La cadena de suministro es otro punto ciego. " Tres de cada cuatro ciberataques al sector minero ingresan por esta vía" , alerta Katherina Canales, directora ejecutiva de la Corporación Minera de Ciberseguridad (CCMIN). En este grupo, se considera a los proveedores que acceden a sistemas corporativos desde plataformas externas, muchas veces sin cumplir estándares de seguridad equivalentes.

Frente a este panorama, la IA ha pasado de ser una herramienta de optimización a convertirse en un pilar estratégico para detectar, prevenir y mitigar ciberataques.

Su capacidad para identificar comportamientos anómalos, correlacionar eventos en múltiples sistemas y reaccionar automáticamente ante patrones de riesgo permite anticiparse a posibles ataques antes de que generen daño. Además, hace posible proteger con mayor precisión las llamadas " joyas de la corona" : los activos digitales más sensibles de una organización, como sistemas SCADA, redes OT, datos de producción y comunicaciones críticas.

MONITOREO PERMANENTE

Actualmente, existen varias funciones en las que puede ayudar la IA, principalmente para el monitoreo de comportamientos anómalos, explica Walter Montenegro, gerente regional de ciberseguridad en Cisco.

" En los sistemas legados pueden existir dos problemas: o no pueden recibir actualizaciones o es muy riesgoso hacerlo. Por ende, se requiere un monitoreo constante que identifique comportamientos sospechosos. En ese sentido, la IA también aporta en la integración IT/OT (Tecnologías de la Información / Tecnologías de Operación), particularmente en cómo fluye el intercambio de datos, pudiendo encontrar potenciales ataques y/o acciones predictivas" , asegura.

Y añade: " tenemos que entender que los modelos de IA se basan en detectar amenazas nuevas y cosas desconocidas sin un patrón estándar.

LITORALPRESS

Fecha: 14-07-2025
Medio: Revista Nueva Minería & Energía
Supl. : Revista Nueva Minería & Energía
Tipo: Noticia general
Título: CIBERATAQUES Y LA DEFENSA INTELIGENTE

Pág. : 11
Cm2: 390,3

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

Foto: Cisco

Walter Montenegro, gerente regional de ciberseguridad en Cisco.

Foto: Senado

Kenneth Pugh, senador.

Foto: LinkedIn

Marcelo Concha, senior management en Metso.

Con ello, evidentemente ayudan a disminuir los riesgos en el mundo industrial" .

Según el ejecutivo, las soluciones actuales no solo resguardan los modelos de IA, sino al mismo tiempo permiten usarla para fortalecer la protección. " Esto obviamente se extiende a los entornos industriales. Por ejemplo, tenemos incorporada la IA en nuestra solución de XDR y en Talos, para la detección de amenazas y comportamientos anómalos que vengan de un tercero, lo cual nos permite disminuir los riesgos y proteger la infraestructura del cliente final" , asevera.

SEGMENTACIÓN Y CAPACITACIÓN

Asimismo, destaca la importancia de contar con una política de segmentación para el entorno IT/OT y dentro del ámbito OT. " Tenemos elementos que nos permiten aplicar una arquitectura 'Zero Trust', limitando el impacto en caso de que algún ataque ingrese a través de la cadena de suministro" . Lo anterior, entendido como un modelo que elimina la confianza implícita dentro de una red o sistema, basándose en el principio de " nunca confiar, siempre verificar" .

" Sumado a ello, nuestras plataformas pueden detectar el tráfico lateral (este-oeste) que se podría estar propagando desde un tercero hacia los activos industriales, o cuando ingresa algún contratista a administrar plataformas. Así, no se pone en riesgo la infraestructura del cliente final" , agrega.

Por otra parte, el representante de Cisco enfatiza que la seguridad no se implementa solo en el plano tecnológico. " Debe ir de la mano con la capacitación constante para que los colaboradores tengan conciencia plena sobre la protección de los activos de las empresas" , asegura.

Adicionalmente, Montenegro explica que hoy existen asistentes en tiempo real dentro de las soluciones tecnológicas, que apoyan a los operadores en múltiples procesos, tales como respuestas a incidentes y tareas de configuración. Además, es posible generar escenarios simulados de ataques con IA, adaptados a distintos roles y niveles técnicos, para poner a prueba los equipos.

AVANCES EN EL PAÍS

Pese a estos retos, el ecosistema chileno muestra avances. Desde 2021, una alianza multisectorial -integrada por BHP, Anglo American, Teck, Collahuasi y Antofagasta Minerals- trabaja en modelos colaborativos de defensa digital, incorporando simulaciones de ciberataques con IA para entrenar a sus equipos. En paralelo, iniciativas como la formación gratuita en ciberseguridad para mineras medianas en Canadá demuestran que la combinación de

" La IA proporciona información interesante para la protección de las llamadas 'joyas de la corona', que en los ambientes OT puede ser mediante los sistemas SCADA o los PLC (Controladores Lógicos Programables)", afirma Walter Montenegro de Cisco.

LITORALPRESS

Fecha: 14-07-2025
Medio: Revista Nueva Minería & Energía
Supl. : Revista Nueva Minería & Energía
Tipo: Noticia general
Título: CIBERATAQUES Y LA DEFENSA INTELIGENTE

Pág. : 12
Cm2: 366,3

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

IA y capacitación puede elevar la resiliencia, incluso con presupuestos limitados.

Desde el ámbito legislativo, el senador Kenneth Pugh (independiente), impulsor de la Ley Marco, insiste en que la minería actual no solo debe ser "verde" o sostenible, sino también segura. "Si logramos eso, Chile va a poder ser el ejemplo en la región y para el resto del mundo en este campo", puntualiza.

Por otro lado, Marcelo Concha, senior management en Metso, plantea que es necesario abordar una brecha existente entre la cultura organizacional y la digitalización, para impulsar la adopción de la inteligencia artificial a la ciberseguridad. En su opinión, es preciso conectar las decisiones directivas con el trabajo en terreno, porque debido a este "gap" cultural, en las oficinas corporativas se prioriza esta materia, pero aguas abajo se percibe aún como lejana.

"Si hablas con un mantenedor y requiere tal o cual servicio, te dice que no puede obtenerlo argumentando que el encargado de ciberseguridad no le permite enviar los datos afuera. A su vez, si vas donde la persona a cargo de ciberseguridad y le dices 'esto es lo que voy a extraer', puedes encontrarte con que no posee una diferenciación de los datos", sostiene el ejecutivo. Por ende, el desafío es alinear visión estratégica y operación práctica en faena.

UN CAMBIO CULTURAL

Entonces, ¿por qué no se ha adoptado la IA con mayor fuerza en la ciberseguridad minera?

El senador Pugh considera, a pesar de que todavía se empleen tecnologías obsoletas, como el Windows 95, que los datos que se manejan representan "oro", por su importancia crítica. "Entonces si están manejando oro con un Windows 95, ¿por qué no hacen una pequeña inversión? Porque culturalmente no hemos cambiado y creemos que este es un tema a cargo de la unidad de TI (Tecnología de la Información) o de administración y finanzas, y eso es un error", advierte el legislador.

Con todo, expertos coinciden en que el principal escollo para poder impulsar la adopción masiva de la IA en ciberseguridad es que no se ha asumido con la dimensión de un cambio cultural. Es decir, no basta con la tecnología: se necesita gobernanza, compromiso ejecutivo y transformación del mindset organizacional.

La incorporación de IA a la ciberseguridad minera no es hoy, por lo tanto, una opción táctica, sino un imperativo estratégico. Para que Chile mantenga su liderazgo en el sector extractivo y se proyecte como referente en minería verde y segura, será necesario avanzar con ambos pies, asevera el senador Pugh: transformación digital y seguridad cibernética.

"Pensemos en que esto tenemos que adaptarlo de tal manera que sea una parte del ecosistema de nuestra organización y un componente de lo que queremos transmitir. Con eso, vamos a asegurar no solo el éxito de nuestra producción presente, sino también de la futura", concluye Katherina Canales.

"No se trata solo de un tema de política pública, sino también de política empresarial. Es decir, entender la importancia de ver la ciberseguridad como un tema estratégico", destaca el senador Kenneth Pugh.

Foto: Freepik

Las mineras son blancos frecuentes de ransomware, phishing y ataques a la cadena de suministro. La IA permite escalar las capacidades de defensa en ciberseguridad sin necesidad de rediseñar toda la infraestructura.