LITORALPRESS

Fecha: 21-01-2026
Medio: El Mercurio
Supl. : El Mercurio - Minería y Comunidad
Tipo: Noticia general
Título: **Bajo amenaza: cómo el cibercrimen se infiltra en el coraazón de la minería**

Pág. : 1
Cm2: 577,8
VPE: $ 7.590.219

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

LOS NUEVOS OBJETIVOS DE LA DELINCUENCIA

Bajo amenaza: cómo el cibercrimen se infiltra en el corazón de la minería

La acelerada digitalización de las faenas mineras ha expuesto a un sector clave para la economía del país a riesgos y delitos cibernéticos, provocando paralizaciones operacionales, filtración de información y pérdidas que superan los cientos de miles de dólares.

CLAUDIA BETANCOURT M.

La ciberseguridad se ha convertido en un tema crítico para la industria minera nacional. Las amenazas cibernéticas, además de interrumpir operaciones, dañar equipos y sistemas, pueden alcanzar un altísimo costo en dólares.

De hecho, un 70% de las organizaciones reportan pérdidas de US$ 100.000 o más, y un 30% supera US$ 1.000.000, según las cifras de la Corporación de Ciberseguridad Minera (CCMIN). Estas pérdidas van en directa relación con el tamaño de la operación y la paralización de una faena minera, si es parcial o total.

La minería no solo está expuesta a los riesgos IT, de tecnologías de la información de datos y sistemas, sino que, además, a los riesgos OT, es decir, de tecnologías de operación como equipos e infraestructura, sostiene Fernando Lucchini, director ejecutivo de CCMIN.

"Esto convierte a la ciberseguridad de la minería en un esfuerzo primordial para mantener tanto la continuidad operacional como la seguridad de las personas que trabajan en ella", recalca el ejecutivo.

A juicio de los expertos, la digitalización del sector, que ha avanzado rápidamente en los últimos años en una transformación digital (4.0), les ha permitido a las compañías mayor eficiencia y sostenibilidad, pero también ha posibilitado el avance del cibercrimen.

Es que conexiones y herramientas digitalizadas asociadas a la automatización de procesos, operación remota, sensores (IoT), sistemas en la nube y análisis de grandes volúmenes de datos en tiempo real, entre otros, son potencialmente vulnerables.

Al respecto, Daniel Cattaneo, líder digital de la Corporación Alta Ley, sostiene que si bien las nuevas tecnologías digitales habilitan una mejora en la eficiencia y competitividad de la industria minera, también aumentan la exposición de los sistemas.

"La mayor conexión entre sistemas y plataformas, y una mayor exposición de las organizaciones por el uso de los servicios en la nube, amplía la superficie y la posibilidad de sufrir ciberataques. Además de lo anterior, existe un aumento global del cibercrimen con foco en sectores como la minería, con alta capacidad financiera y alto impacto operacional", afirma.

Para Eduardo Bouillet, director del Centro de Ciberinteligencia de Entel Digital, en América Latina, la minería se ha consolidado como uno de los blancos preferidos para los delincuentes informáticos, debido a su alta dependencia de procesos continuos y su impacto económico.

"Ya no se trata de ataques aislados, sino de verdaderas empresas criminales digitales que operan con modelos profesionales y apuntan directamente a sectores estratégicos de la economía", revela.

Si bien desde Codelco comparten las observaciones, Soledad Bastías, gerenta corporativa de Ciberseguridad IT/OT y Riesgo Tecnológico de la empresa, advierte que "si la tecnología se incorpora con un enfoque de ciberseguridad por diseño, no debiese incrementar los riesgos".

La especialista de la cuprífera estatal precisa que debe existir una evaluación permanente debido al contexto de las amenazas y tipos de ciberataques, que están en constante evolución. "En síntesis, la minería 4.0 reduce riesgos operacionales, pero puede incrementar riesgos cibernéticos si no existe un sistema de ciberseguridad industrial maduro", asegura.

ESTUDIO PICEL

Ya no se trata de ataques aislados, sino de verdaderas empresas criminales digitales.

BAJO ATAQUE

Según un informe del Mining and Metals Information Sharing and Analysis Centre (MM-ISAC), las mineras experimentan un promedio de dos a tres incidentes de ciberseguridad por mes, lo que suma entre 24 y 36 incidentes anuales.

Uno de los principales tipos de ciberataques es el *ransomware*, que busca bloquear sistemas y/o infraestructura de la compañía, lo que puede comprometer seriamente sus operaciones, un costo económico de millones de dólares y de reputación de la empresa minera.

También está el *phishing*, donde el atacante utiliza el engaño y técnicas creativas para acceder a información sensible; o, bien, la fuga de datos sobre operaciones, recursos y otros.

La suplantación de identidad de personas que trabajan en la misma organización es otro de los delitos que se mencionan entre los más recurrentes. Los ataques a la cadena de suministro, como proveedores de la minería con sistemas comprometidos, es otra de las amenazas que se aluden.

A pesar de que muchas empresas mineras han comenzado a realizar inversiones en soluciones de ciberseguridad y capacitar a sus trabajadores, aún estas acciones han sido insuficientes.

Uno de los casos más recientes es el ataque que sufrió el Servicio Nacional de Geología y Minería (Sernageomin) en diciembre de 2025, donde su sistema informático y el portal institucional fueron afectados por un ataque cibernético a sus servidores, lo que provocó la interrupción temporal del servicio.

Un año antes, los sistemas de la minera Antofagasta Minerals fueron vulnerados con el fin de emitir seis facturas falsas modificando las claves ante el SII, lo que gatilló un fraude de cercano a los $373 millones.

El ciberataque que afectó a los camiones autónomos de la División Gabriela Mistral (DGM) de Codelco es otro de los casos registrados. Lo anterior llevó a una suspensión de actividades por aproximadamente 72 horas y cuantiosas pérdidas financieras.

MEDIDAS URGENTES

Los especialistas insisten en que, este año, la industria minera chilena deberá enfrentar desafíos en torno a la ciberseguridad, en un sector que es responsable de más del 10% del PIB y cerca del 60% de las exportaciones, de acuerdo con las cifras de la Sociedad Nacional de Minería (Sonami).

Entre las medidas perentorias mencionan elevar la seguridad a un nivel estratégico y de gobernanza corporativa, y cerrar la brecha de talento especializado en torno al TI/TO.

José Antonio Lagos, socio principal de Cybertrust Latam, plantea que el reto es más bien cultural, en el sentido de que el sector esté consciente de estos nuevos riesgos. Y recomienda "avanzar desde una visión reactiva y tecnológica hacia un enfoque de resiliencia integral, colaboración sectorial e integración de la ciberseguridad en la gestión global de riesgos".

Fernando Lucchini enfatiza que las compañías no pueden abarcar las amenazas por sí solas. "El compartir información de ciberinteligencia para generar alertas y respuestas temprana, y concientización y coordinación con la cadena de suministro, es primordial", dice.

"YA NO HABLAMOS SOLO DE DINERO, SINO DE REPUTACIÓN PAÍS".

El subprefecto y jefe nacional del Cibercrimen de la PDI, Marcelo Wong, explica que la industria minera pasó a ser profundamente digital, lo que le dio bastante eficiencia y productividad, pero también abrió una nueva superficie de ataque.

¿Cómo afecta un ciberincidente en la confianza de los inversionistas?

"Un incidente no solo es la caída de un servidor, puede significar muchas veces la detención completa de una planta, la alteración de un proceso químico, o la pérdida de un control de ventilación o transporte. Y cuando eso ocurre, ya no hablamos solo de dinero, hablamos de reputación país y, en algunos escenarios, el riesgo directo para la vida de las personas".

Comparándonos con la región, ¿cuál es la situación de Chile ante estos delitos?

"Chile —me atrevería a decir— está bien preparado. En el último informe de la OEA de Ciberseguridad hemos aumentado nuestro índice de seguridad. Estamos mucho mejor posicionados en Latinoamérica, y eso significa también que somos un referente para nuestros vecinos. Esto tiene mucho que ver con la inversión que ha habido en Chile y la educación en temas de ciberseguridad".