LITORALPRESS

Fecha: 18-02-2025
Medio: El Mercurio
Supl. : El Mercurio - Minería y Comunidad
Tipo: Noticia general
Título: Mayor uso de la nube en la industria impone reforzar medidas de protección digital

Pág. : 4
Cm2: 715,7

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

CIBERSEGURIDAD:

Mayor uso de la nube en la industria impone reforzar medidas de protección digital

Los ambientes *cloud* permiten mejorar la sostenibilidad de las operaciones mineras, pero también requieren integrar estrategias para proteger los datos críticos y garantizar la continuidad operativa.

CATERINNA GIOVANNINI

En la minería chilena, muchos de los proyectos implementados en la nube tienen el mismo objetivo: garantizar la trazabilidad y el seguimiento del *stock* y la producción mediante una tecnología que, si bien permite visualizar y almacenar los registros de rendimiento en tiempo real, también exige tener la capacidad de detectar un ciberataque en el momento.

La adopción de estos sistemas forma parte de la transformación digital que se está produciendo en un sector que destaca por ser uno de los que más invierte en innovación tecnológica. De hecho, según un informe de Accenture, en 2022, el 85% de las empresas mineras ya había incorporado el uso de la nube.

Gracias a ella, se "simplifica la implementación de plataformas y servicios de apoyo al negocio en ambientes donde recurrentemente existen complicaciones a la hora de proveer nueva infraestructura", explica Luis Porta, director ejecutivo de Accenture Chile.

LAS VENTAJAS

Los expertos coinciden en que el uso de la nube en minería mejora la eficiencia operativa, la sostenibilidad y la competitividad, ya que permite monitorear datos y tomar decisiones desde cualquier ubicación, lo que reduce los tiempos de respuesta.

Eduardo Bouillet, director del Centro de Ciberinteligencia (CCI) de Entel Digital, asegura que "el uso de la nube en minería es estratégico", ya que también implica una reducción de costos al eliminar grandes infraestructuras físicas mediante modelos escalables según la demanda, y facilita la colaboración entre equipos dispersos. "Se optimiza el análisis de grandes volúmenes de datos y se agiliza la adopción de tecnologías emergentes como la inteligencia artificial y el internet de las cosas", agrega el ejecutivo.

LAS VULNERABILIDADES

Sin embargo, la sensibilidad de las operaciones de una industria como la minería aumenta el riesgo que se corre al migrar datos a ambientes *cloud*.

Por ejemplo, puede ser afectada por problemas de conectividad, ya que la minería a menudo se realiza en áreas remotas, lo que podría impedir que las operaciones dependan de la nube en tiempo real.

Otro aspecto a tener en cuenta es que la conexión de redes IT (tecnologías de la información) y OT (tecnologías operativas) aumentarían el riesgo de sufrir incidentes y ciberataques que comprometan la seguridad de los trabajadores, si llegaran a afectar sistemas críticos. "Las empresas que utilizan plataformas en la nube son particularmente vulnerables a los ataques dirigidos, ya que los atacantes pueden estar interesados en robar información valiosa o interrumpir las operaciones", afirma Diego Toro, especialista en Negocios Estratégicos de ITQ Latam.

El aumento de los ciberataques y la integración de las tecnologías operativas con la nube plantean nuevas necesidades, que van desde los sistemas de control hasta la capacitación permanente.

EN 2022,
el 85 % de las empresas mineras ya había incorporado el uso de la nube, según un estudio de Accenture.

LOS CONTROLES

La prevención cobra especial importancia en un contexto en que los riesgos han aumentado debido al incremento de ciberataques al sector industrial y la integración de OT con la nube, según el Reporte de Ciberseguridad 2025 elaborado por el CCI de Entel Digital.

Por eso, estos avances deben implementarse priorizando las mejoras de seguridad, con modelos *zero trust*, donde, "utilizando *edge computing*, se logra un mayor control de las conexiones remotas, tanto de empleados como de terceras partes", explica Luis Porta.

El director ejecutivo de Accenture agrega que "acá toma relevancia conocer correctamente el estado de ciberseguridad de mi empresa, poner a prueba la efectividad de los controles que tengo implementados y contar con una estrategia para el desarrollo de los niveles de madurez de ciberseguridad de mi compañía".

Y, en el caso de llegar a sufrir un ataque, se recomiendan medidas como mantener copias de seguridad regulares de los datos críticos para evitar pérdidas, contar con un plan claro para reaccionar y tener un equipo especializado para detectar incidentes de seguridad de manera proactiva.