EL MERCURIO
MINERÍA & COMUNIDAD

Fecha: 18/03/2025 Audiencia: 320.543 Sección: ESPECIALES
Vpe: $7.659.635 Tirada: 126.654 Frecuencia: OTRAS
Vpe pág: $20.570.976 Difusión: 126.654
Vpe portada: $20.570.976 Ocupación: 37,24%

PARA EMPRESAS DE INFRAESTRUCTURA CRÍTICA:

Nuevas exigencias legales aumentan la demanda de talentos en ciberseguridad

Se estima que la necesidad de especialistas crecerá cerca de 30% entre 2024 y 2025 en Latinoamérica, por lo que instituciones educativas, organizaciones e, incluso, el Ejército, se alían para apoyar la formación.

CATERINNA GIOVANNINI

El 2 de enero pasado comenzó a operar la Agencia Nacional de Ciberseguridad (ANCI), creada para supervisar el cumplimiento de la nueva Ley Marco de Ciberseguridad; y este mes, se publicó en el Diario Oficial que todas las empresas y organizaciones que prestan servicios esenciales deberán informar a la agencia en caso de ciberataques o incidentes de ciberseguridad.

"Eso supone una presión muy importante en términos de madurez de los equipos y de la cantidad de talento que se necesita", asegura Rocío Ortiz, subdirectora de Industrias del Futuro del Centro de Innovación UC y directora ejecutiva de Ciberlab. Sobre todo, porque ahora existe la normativa que deben cumplir las empresas de infraestructura crítica, como es el caso de la minería, explica.

Esta es una tendencia en toda América Latina. De hecho, se espera que la demanda de expertos en ciberseguridad, como arquitectos de seguridad, analistas de vulnerabilidades, ingenieros de seguridad y gestores de SOC (centros de operaciones de seguridad), con conocimientos en regulaciones de privacidad de datos y capacidad para garantizar el cumplimiento normativo, crezca entre 25 y 30% entre 2024 y 2025, según un estudio de IT-Talent.

Esto, justo cuando, según datos del Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (Csirt, por sus siglas en inglés), ala fecha en Chile hay un déficit de 28.000 especialistas en ciberseguridad. "La presión de los nuevos reglamentos no da un tiempo muy amplio ni un margen de holgura para cometer errores o tener procesos muy largos de formación de talentos, y exige tener gente capacitada", agrega Ortiz.

Lo positivo es que el 68,8% de los encuestados por IT-Talent dice querer mantenerse actualizado sobre oportunidades de formación continua en tecnología y el 54,7% se ha capacitado o tiene ganas de hacerlo. Para ello, el 44,8% prefiere programas de certificación profesional, y el 39,7% lo haría a través de cursos en línea como Udemy, Coursera, etc.

Una característica particular de la ciberseguridad en minería es que abarca a las tecnologías de operación, como infraestructura, sensores y maquinaria.

"En el sector minero es trascendental comprender los alcances de la minería 4.0", dice Ramón Salas, asociado de la Alianza Chilena de Ciberseguridad y gerente general de eBD.

Ortiz, por su parte, subraya la necesidad de que quienes forman el equipo de ciberseguridad conozcan la cadena de suministro en las mineras. "Lo que ha aumentado mucho en el último tiempo son los ataques a las grandes empresas, y como estas ya cuentan con equipos de ciberseguridad, los atacantes intentan ingresar por medio de los proveedores", explica.

Además, en minería hay riesgos que van más allá del intento de ingresar con alguna contraseña o de forma remota a los sistemas, como el peligro de que personas externas puedan afectar físicamente a las faenas. "Esto ocurre porque una característica particular de la minería es que también implica una parte de OT, que son las tecnologías de operación, como infraestructura, sensores y maquinaria", agrega Ortiz.

El problema es que "hoy, los plazos para crear perfiles especializados en ciberseguridad son muy cortos, más exigentes y no se ajustan a los itinerarios tradicionales, ya sea en las universidades o los centros de formación técnica", explica.

Salas estima que el trabajo conjunto es la premisa para enfrentar la brecha, "mediante alianzas entre gobierno y las empresas privadas, como universidades, mineras y proveedores tecnológicos, a fin de permitir el conocimiento específico", asegura.

ESPACIO NEUTRAL

El año pasado, con el objetivo de generar alianzas y programas centrados en capacidades prácticas, se creó el Laboratorio de Ciberdefensa para la Protección de Infraestructuras Críticas (Ciberlab), una iniciativa del Centro de Innovación UC, el Ejército de Chile, la Corporación de Ciberseguridad Minera, y otros. Fue concebido como un espacio neutral para generar modelos de formación más ágiles y competencias aplicadas, lo que "nos va a permitir seguirle el ritmo a lo que está ocurriendo", dice Ortiz.

En este laboratorio se desarrollan competencias mediante seminarios, talleres, programas personalizados y ejercicios de gestión de crisis, simulacros, proyectos y pilotos, dirigidos a profesionales que quieren especializarse o reinventarse.

En países como Chile, Brasil y México, los incentivos para dedicar tiempo a este tipo de formación están dados por los salarios, que son los más altos de la región para los profesionales de TI. Y hay un segmento que aún no se ha explorado lo suficiente. En Latinoamérica, menos del 30% de los profesionales de TI son mujeres, pero IT-Talent estima que esta cifra crecerá hasta 35% este año. Según el estudio, las empresas que inviertan en programas de inclusión, tanto para aumentar la representación femenina como para integrar a más jóvenes, estarán mejor posicionadas para afrontar los desafíos tecnológicos del futuro.