

Schneider Electric impulsa la ciberseguridad a través de un enfoque colaborativo energético y sostenible

Se trata de **Cyber On Community**, un espacio que busca fortalecer la seguridad digital y promover la confianza en diversas industrias y sectores productivos.

En la última década, la digitalización, el auge de la inteligencia artificial y el avance de la transición energética, acompañados por los cambios en el comportamiento de las personas durante la pandemia, han promovido un crecimiento sin precedentes en la interacción digital. Este nuevo entorno ha empujado a las organizaciones a avanzar tecnológicamente para mantenerse competitivas, pero también ha revelado un desafío crítico: la ciberseguridad.

En este sentido, Adriana Fonseca, *Industrial Automation Business Leader* de Schneider Electric, explica que "los países sudamericanos han comenzado a desarrollar políticas y recursos para fortalecer sus capacidades. Sin embargo, la región aún enfrenta desafíos en talento e infraestructura. Chile, en particular, ocupa el puesto 74 en el índice global de ciberseguridad entre casi 200 países".

Un enfoque colaborativo hacia la ciberseguridad

En respuesta a estos desafíos, Schneider Electric creó **Cyber On Community**, un espacio colaborativo donde los miembros de diversas empresas e industrias pueden compartir experiencias, aprender sobre vulnerabilidades potenciales y convertirse en asesores de sus propias organizaciones en temas de ciberseguridad. Este espacio, desarrollado en la región y que se extenderá a otros países a partir de 2025 (Chile entre ellos), fomenta el aprendizaje compartido y el análisis de casos de



éxito, ayudando a fortalecer la cultura de ciberseguridad organizacional. Además, tiene un enfoque especialmente relevante en sectores críticos como la minería, donde la diversidad de la fuerza laboral y los constantes cambios suponen un reto adicional en la implementación de estas estrategias.

En suma, Fonseca señala que el principal desafío en ciberseguridad es cultural. "Es crucial que las personas comprendan los riesgos asociados a sus funciones y cómo pueden contribuir a proteger la organización. Esto exige una gobernanza sólida en cada empresa, con la ciberseguridad integrada en sus políticas corporativas. También es esencial contar con un plan de gestión de riesgos que incluya respuesta a contingencias y estrategias de mitigación. Finalmente, la inversión en ciberseguridad debe ir más allá de los recursos

económicos, incorporando capacitación continua y el compromiso de la dirección", afirma.

Con base en esto, la estrategia de ciberseguridad de Schneider Electric se construye sobre pilares sólidos que abarcan tanto la seguridad digital, operativa y física como un enfoque integral de gestión de riesgos que permita proteger a la organización desde todos los frentes. "Además, como compañía reforzamos constantemente nuestra seguridad a través de soluciones de *hardware*, *software* y servicios, otorgando a la industria una protección dinámica y en evolución con la que buscamos generar confianza a lo largo de toda la cadena de valor y garantizar el cumplimiento de las regulaciones locales en cada país donde operamos, afianzando así la relación con nuestros clientes y aliados", explica la ejecutiva.