LITORALPRESS

Fecha: 05-05-2025
Medio: Revista Gerencia
Supl. : Revista Gerencia
Tipo: Especiales
Título: "La colaboración pública-privada y de la academia es clave para fortalecer la resiliencia nacional frente a amenazas cibernéticas"

Pág. : 24
Cm2: 585,3
VPE: $ 825.314

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

ESPECIAL

Ciberseguridad OT

Rocío Ortiz, Directora Ejecutiva de Ciberlab y Subdirectora de Industrias del Futuro Centro de Innovación UC

"La colaboración pública-privada y de la academia es clave para fortalecer la resiliencia nacional frente a amenazas cibernéticas"

Rocío Ortiz, Ciberlab.

La ciberseguridad industrial enfrenta desafíos crecientes como la obsolescencia tecnológica, integración de sistemas críticos y nuevas amenazas en la cadena de suministro. Todos retos en los que Ciberlab se enfoca al impulsar la colaboración público-privada y académica como eje clave para construir una infraestructura más resiliente.

Desde Ciberlab, ¿cómo evalúan el estado actual de la ciberseguridad industrial en Chile?

El nivel de madurez de la ciberseguridad industrial en Chile es heterogéneo. Sectores críticos como el energético, y en particular el sector eléctrico, muestran avances importantes, adoptando estándares internacionales de manera proactiva. Sin embargo, en industrias como la logística o la minería, persiste una mayor dispersión. Uno de los principales retos es la presencia de tecnologías "legacy", cuya actualización es compleja y que introduce vulnerabilidades, especialmente en entornos donde el hardware tiene un rol central.

¿Cuáles son las principales amenazas que enfrenta este sector?

Las amenazas más relevantes incluyen la obsolescencia tecnológica, la convergencia de redes TI y OT sin adecuada segmentación, y los riesgos de seguridad física en plantas. También destaca el creciente ataque a la cadena de suministro, donde los cibercriminales buscan vulnerabilidades en proveedores para acceder a las organizaciones principales.

¿Cómo ven el marco regulatorio actual en materia de ciberseguridad?

La promulgación de la Ley Marco de Ciberseguridad representa un avance significativo. Sin embargo, es necesario un mayor detalle en la reglamentación específica para el ámbito industrial, que defina claramente estándares, sanciones y requisitos aplicables a sistemas críticos como SCADA y PLC. Sin duda, la puesta en marcha de la Agencia Nacional de Ciberseguridad (ANCI) será clave en este proceso.

¿Qué tendencias o desafíos observan en la ciberseguridad del sector?

Entre los principales desafíos está la gestión de infraestructuras distribuidas y centros de control remoto, así como la incorporación de tecnologías emergentes como Inteligencia Artificial y computación cuántica. Esto plantea una alta demanda de talento especializado, capaz de integrar conocimientos de ciberseguridad, procesos industriales y nuevas tecnologías.
Muchos sectores industriales y nuestras ciudades comparten infraestructuras críticas y proveedores de servicios. Pensar en su integración es clave y es uno de los retos que enfrentamos, ya que impacta directamente en el diseño de anillos industriales y en la planificación de las ciudades del futuro.

¿Cómo nace Ciberlab y cuáles son sus principales objetivos?

El Laboratorio de Ciberdefensa para la Protección de Infraestructuras Críticas (Ciberlab) nace en Julio de 2024 como una iniciativa del área de Industrias del Futuro del Centro de Innovación UC y el Ejército de Chile, en conjunto con representantes de los sectores público, privado y la academia. Su objetivo es ser un espacio neutral donde se articulen capacidades entre los diferentes actores, para el desarrollo de manera

LITORALPRESS

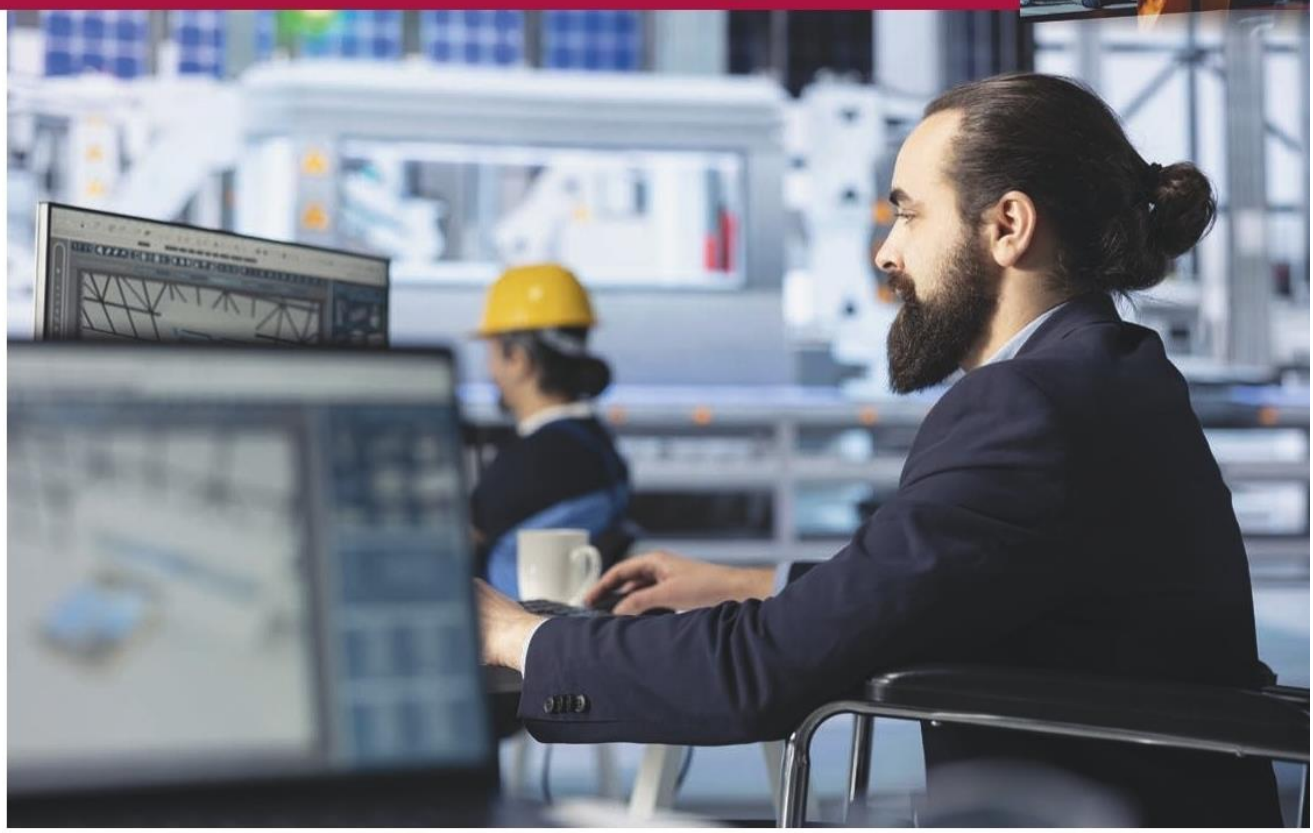
Fecha: 05-05-2025
Medio: Revista Gerencia
Supl. : Revista Gerencia
Tipo: Especiales
Título: “La colaboración pública-privada y de la academia es clave para fortalecer la resiliencia nacional frente a amenazas cibernéticas”

Pág. : 25
Cm2: 582,1
VPE: $ 820.704

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

ESPECIAL

Ciberseguridad OT



asociativa de formación, pruebas de concepto y pilotajes tecnológicos. Actualmente cuenta con 17 partners, incluyendo actores de tecnología, defensa e infraestructuras críticas, como el Coordinador Eléctrico Nacional (CEN), la Corporación de Ciberseguridad Minera (CCMIN), la Asociación de Bancos e Instituciones Financieras de Chile (ABIF), Aguas Andinas y Conecta Logística, entre otros.

¿Qué necesidades detectaron?

Primero, detectamos varias brechas y oportunidades desde el inicio del proyecto, siguiendo una hoja de ruta. Una de las principales era la falta de preparación frente a la llegada de la Ley Marco, especialmente en temas formativos, de capacitación, certificaciones y desarrollo de ejercicios, áreas que en ese momento no estaban suficientemente cubiertas en el país. También había una brecha en espacios de testeo tecnológico, ya que hay una asimetría respecto a la disponibilidad de tecnología que tienen, por ejemplo, grandes empresas v/s medianas o pequeñas. Además, detectamos una brecha importante en formación. Los programas tradicionales, como diplomados y cursos, están en constante búsqueda frente a las necesidades prácticas de los equipos de respuesta, especialmente considerando la velocidad con que evoluciona la tecnología en ciberseguridad y ciberdefensa.

"La promulgación de la Ley Marco de Ciberseguridad representa un avance significativo. Sin embargo, es necesario un mayor detalle en la reglamentación específica para el ámbito industrial, que defina claramente estándares, sanciones y requisitos"

¿Qué iniciativas destacaría entre las que hoy lidera Ciberlab?

Principalmente, los ejercicios de gestión de crisis, que buscan capacitar a las organizaciones en la toma de decisiones frente a incidentes cibernéticos. En octubre de 2024, se realizó el primer ejercicio nacional con más de 150 participantes. Además, trabajamos en el desarrollo de pilotajes de tecnología mediante células de trabajo que enfocan el uso de software y hardware en casos de uso específicos para sectores como el eléctrico, financiero y logístico.
En este sentido, seguiremos trabajando para impulsar modelos de colaboración público-privados y académicos que son fundamentales para fortalecer la resiliencia nacional frente a amenazas cibernéticas, generar espacios de confianza, compartir conocimientos y realizar ejercicios prácticos conjuntos, elementos esenciales para preparar mejor a las organizaciones frente a los desafíos futuros.G