Electricidad
La revista energética de Chile

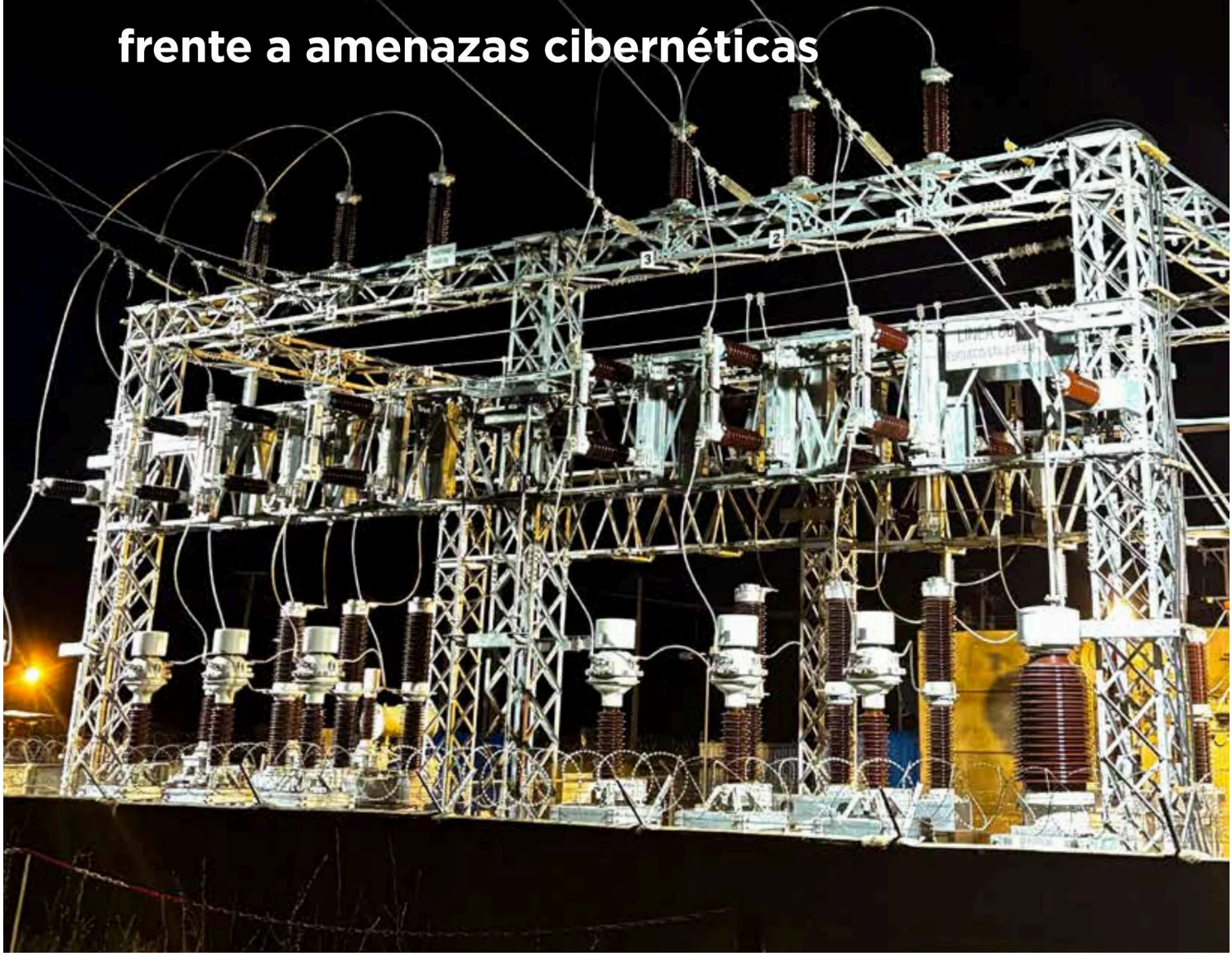
Fecha: 26/03/2026 Audiencia: 0 Sección: ACTUALIDAD
Vpe: $108.534 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $124.656 Difusión: 0
Vpe portada: $124.656 Ocupación: 87,07%

REPORTAJE

Subestaciones:

Blindaje eléctrico

frente a amenazas cibernéticas



Electricidad
La revista energética de Chile

Fecha: 26/03/2026 Audiencia: 0 Sección: ACTUALIDAD
Vpe: $85.989 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $124.656 Difusión: 0
Vpe portada: $124.656 Ocupación: 68,98%

LA CRECIENTE AUTOMATIZACIÓN DE INSTALACIONES CRÍTICAS IMPULSA AL SECTOR ENERGÉTICO A FORTALECER SUS ESQUEMAS DE PROTECCIÓN, CON FOCO EN RESILIENCIA OPERATIVA Y DEFENSA EN MÚLTIPLES CAPAS.

El avance tecnológico en los sistemas eléctricos ha incrementado su exposición a ataques informáticos, elevando la urgencia de resguardar activos estratégicos.

Ante este escenario, la industria ha intensificado la adopción de estándares y capacidades para anticipar y enfrentar incidentes.

En este contexto, "desde Coordinador Eléctrico Nacional vemos que el avance de la digitalización en la industria eléctrica, junto con el aumento de amenazas cibernéticas a nivel global, obliga al sector a reforzar de manera permanente esta protección", menciona Patricio Leyton, director de la Unidad de Ciberseguridad e Infraestructura Crítica de esta institución.

En línea con este rol, cabe recordar que esta organización posee un rol de coordinación sectorial, promoviendo la colaboración entre las empresas del Sistema Eléctrico Nacional, el intercambio de información sobre amenazas y el fortalecimiento de capacidades para prevenir, detectar y responder ante incidentes de ciberseguridad.

A partir de este enfoque, es así como, desde 2020, la industria opera bajo el Estándar de Ciberseguridad para el Sector Eléctrico, basado en estándar de la norma norteamericana NERC-CIP, que establece requisitos obligatorios para proteger los ciberactivos que sustentan la operación del sistema, incluyendo centros de control, sistemas SCADA y subestaciones eléctricas. Este marco se ve hoy reforzado por la Ley Marco de Ciberseguridad N°21.663, bajo la cual 147 entidades del sector eléctrico han sido calificadas como Operadores de Importancia Vital (OIV), lo que fortalece las obligaciones en materia de gestión de riesgos, protección de sistemas y reporte de incidentes.

En la práctica, "la protección de activos críticos como las subestaciones -cada vez más digitalizadas y automatizadas- exige combinar medidas tecnológicas, organizacionales y operacionales, entre ellas la segmentación de redes, el monitoreo especializado de entornos ope-

Electricidad
La revista energética de Chile
Fecha: 26/03/2026 Audiencia: 0 Sección: ACTUALIDAD
Vpe: $84.992 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $124.656 Difusión: 0
Vpe portada: $124.656 Ocupación: 68,18%

racionales, el control de accesos remotos, la gestión de vulnerabilidades y la capacitación continua del personal. A ello se suma un desafío emergente: el uso creciente de tecnologías como la inteligencia artificial por parte de actores maliciosos, lo que puede facilitar ataques más rápidos, amplios y de mayor impacto", explica Leyton.

Gestión sectorial

Más allá de los marcos normativos y técnicos, la defensa de la infraestructura eléctrica es algo gravitante, por el hecho que si una subestación se ve afectada, "el impacto se siente en hospitales, semáforos, telecomunicaciones, servicios básicos y en la operación de miles de empresas. Por eso, frente a un entorno más digital y con amenazas crecientes, el sector energético está redoblando esfuerzos para pasar de una lógica de "cumplimiento" a una lógica de ciberresiliencia: prevenir, resistir y recuperar sin perder la continuidad operacional", comenta Luz María García, gerenta general de la Asociación Chilena de Empresas de Tecnologías de Información (ACTI A.G.).

FOTO: GENTILEZA COORDINADOR ELÉCTRICO NACIONAL

PATRICIO LEYTON, director de la Unidad de Ciberseguridad e Infraestructura Crítica del Coordinador Eléctrico Nacional.

FOTO: GENTILEZA ACTI

LUZ MARÍA GARCÍA, gerenta general de la Asociación Chilena de Empresas de Tecnologías de Información

A ello se suma un elemento adicional que hoy cobra creciente relevancia: "Hoy muchas organizaciones están ajustando su manera de gestionar el riesgo por la volatilidad internacional, y eso se traduce en decisiones más exigentes sobre seguridad, cadena de suministro tecnológica y capacidades de respuesta. En energía, esa presión es mayor porque hablamos de infraestructura crítica, donde un incidente puede escalar rápidamente a efectos sistémicos", advierte la autoridad gremial.

En ese sentido, "desde ACTI, el punto de fondo es que esta agenda no es sólo tecnológica: es de coordinación y capacidades país. Requiere institucionalidad que impulse estándares, intercambio de información, preparación de talento OT/IT y ejercicios de respuesta para que, cuando ocurra un incidente, la operación pueda sostenerse y recuperarse con rapidez", subraya Luz María.

Bajo este escenario, el sector

Electricidad
La revista energética de Chile

Fecha: 26/03/2026 Audiencia: 0 Sección: ACTUALIDAD
Vpe: $104.344 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $124.656 Difusión: 0
Vpe portada: $124.656 Ocupación: 83,71%

Entidades como el Coordinador Eléctrico Nacional propician la vinculación de los diversos actores del sector.

FOTO: GENTILEZA COORDINADOR ELÉCTRICO NACIONAL.

> **El sector energético está redoblando esfuerzos para pasar de una lógica de "cumplimiento" a una lógica de ciberresiliencia", Luz María García**

eléctrico ha venido fortaleciendo su estrategia de ciberseguridad a partir de un enfoque integral que combina estándares técnicos, cumplimiento regulatorio, monitoreo continuo y gestión avanzada de riesgos, como explican Jorge Villar, Leonardo Prado y Chantal Bass, integrantes de la Mesa de Ciberseguridad de ISA Energía en Chile.

Desde una perspectiva operativa, "en Chile, la industria ha sido pionera en la adopción de estándares internacionales como la normativa NERC CIP y marcos de gestión basados en normas tales como ISO 27001 o ISO 22316, que han permitido robustecer los mecanismos de protección y resiliencia de los activos críticos del sistema, incluyendo subestaciones y sistemas de control. Esta adopción no sólo fortalece la defensa frente a amenazas conocidas, sino que también mejora la preparación

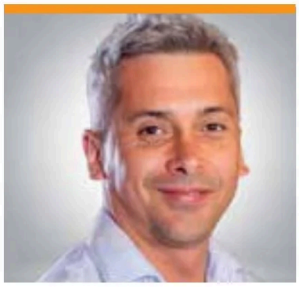
Electricidad
La revista energética de Chile
Fecha: 26/03/2026 Audiencia: 0 Sección: ACTUALIDAD
Vpe: $90.777 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $124.656 Difusión: 0
Vpe portada: $124.656 Ocupación: 72,82%

La protección de activos críticos como las subestaciones exige combinar medidas tecnológicas, organizacionales y operacionales", Patricio Leyton

ante ataques avanzados dirigidos a sistemas industriales", menciona Jorge Villar, especialista de TI de ISA Energía en Chile.

Este enfoque es complementado por Leonardo Prado, director de Operaciones de ISA Energía en Chile, quien subraya que, en el caso del sistema eléctrico, "la estrategia de defensa ha evolucionado desde enfoques centrados principalmente en la protección perimetral hacia modelos de seguridad basados en defensa en profundidad, incorporando capas sucesivas de protección física, lógica y operacional, que consideran la gestión continua de riesgos, la resiliencia operacional, el monitoreo permanente de los sistemas que soportan la operación de la red y los modelos de continuidad del negocio".

FOTO: GENTILEZA ISA ENERGÍA



JORGE VILLAR, especialista de TI de ISA Energía en Chile.

FOTO: GENTILEZA ISA ENERGÍA

LEONARDO PRADO, director de Operaciones de ISA Energía en Chile.

En paralelo, la ciberseguridad y los esfuerzos detrás de la misma han dejado de ser exclusivo de un nicho o área de la organización, adquiriendo un carácter transversal.

Desde el ámbito organizacional, Chantal Bass, especialista legal de ISA Energía en Chile, visualiza que este enfoque multidisciplinario permite fortalecer la capacidad del sector para anticipar y responder frente a amenazas cibernéticas cada vez más sofisticadas y evolutivas.

En esta misma línea, "la protección de activos críticos, tales como las subestaciones, se ha ido consolidando como un esfuerzo colaborativo entre personas, empresas, autoridades y actores técnicos del sistema eléctrico", añade la profesional.

Estrategia

A este escenario se suma una visión desde la ciberseguridad especializada, como la de Katherina Canales, COO de Aura Cybersecurity, quien advierte que el sector energético enfren-

Electricidad
La revista energética de Chile

Fecha: 26/03/2026 Audiencia: 0 Sección: ACTUALIDAD
Vpe: $95.566 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $124.656 Difusión: 0
Vpe portada: $124.656 Ocupación: 76,66%

ta hoy una tormenta perfecta.

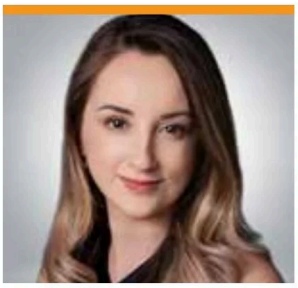
"Entre 2022 y 2024 se registraron 119 incidentes cibernéticos relevantes a nivel global en el sector, los ataques a empresas de servicios públicos en EE.UU. crecieron casi un 70% entre 2023 y 2024, y en América Latina más del 20% de los sistemas de control industrial sufrieron intentos de infección solo en el segundo trimestre de 2025. A eso se suma la dimensión geopolítica: los conflictos modernos tienen al sector eléctrico como objetivo explícito en el ciberespacio", detalla.

En particular, en su visión, el desafío particular de activos como las subestaciones está en la convergencia IT/OT, debido a que se trata de equipos con ciclos de vida de 20 a 30 años, diseñados para disponibilidad y no para seguridad, que hoy se conectan a redes corporativas, ampliando la superficie de ataque.

FOTO: GENTILEZA ISA ENERGÍA

CHANTAL BASS,
especialista legal de ISA Energía en Chile.

FOTO: GENTILEZA AURA CYBERSECURITY.



KATHERINA CANALES,
COO de Aura Cybersecurity.

Frente a este panorama, Canales considera que el sector avanza en cuatro frentes: "Primero, la adopción de estándares como el de CNE y NIST CSF aplicados al entorno industrial, que permiten estructurar una defensa en profundidad realista para entornos OT. Segundo, la segmentación de redes y monitoreo pasivo mediante herramientas especializadas que otorgan visibilidad sin interferir en la operación. Tercero, el control riguroso de la cadena de suministro, dado que muchos vectores de ataque ingresan por proveedores con accesos remotos mal gestionados. Y cuarto, y donde estoy trabajando directamente con empresas del sector, el desarrollo de planes de continuidad operacional con foco OT, que van más allá del BCP corporativo tradicional y contemplan escenarios de degradación controlada y recuperación de configuraciones de campo".

> **La protección de activos críticos, tales como las subestaciones, se ha ido consolidando como un esfuerzo colaborativo", Chantal Bass**