LITORALPRESS

Fecha: 05-06-2024
Medio: Revista Electro Industria
Supl. : Revista Electro Industria
Tipo: Noticia general
Título: Un desafío crucial para la continuidad del suministro eléctrico

Pág. : 26
Cm2: 409,6

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

Tensiones en la ciberseguridad

Un desafío crucial para la continuidad del suministro eléctrico

A pesar de los avances en la continuidad del suministro eléctrico, expertos alertan sobre la falta de progreso en ciberseguridad, señalando que los ataques podrían aumentar debido a la vulnerabilidad de algunas empresas del sector. Con la reciente promulgación de la Ley Marco de Ciberseguridad, se imponen nuevos desafíos y exigencias a las empresas generadoras y distribuidoras para proteger sus infraestructuras tecnológicas.

Según el último Estudio de Continuidad de Suministro 2023, del Coordinador Eléctrico Nacional, la Región Metropolitana goza de la mejor continuidad del suministro eléctrico en el país: se corta menos la luz y por menos tiempo. El mencionado informe indica que los cortes de energía en la capital tuvieron un tiempo promedio de 24 minutos durante el año anterior, casi la mitad en comparación con el año anterior. Mientras tanto, en la Región del Maule, la duración de estos eventos fue 3,3 veces mayor en relación con la capital en 2022, y en La Araucanía, 2,8 veces más larga.

En el último registro, la mayoría de los cortes se produjo por eventos climáticos fuera del alcance del diseño (lluvia, viento, temporales) y, en segundo lugar, por origen no determinado. Según explica Víctor Vilche, Gerente General de Conecta Ingeniería, este último indicador incluye vulneraciones de ciberseguridad.

Para el experto, este número podría incrementarse por eventuales ciberataques. "Es preocupante ver la falta de previsión de algunas empresas generadoras y distribuidoras en términos de seguridad de la información. Muchas no están cumpliendo lo que exige la norma y están expuestas a ataques cibernéticos. Entendemos que no es un tema fácil de enfrentar, porque la normativa tiene varias aristas y es necesario coordinar a más de un área al interior de las empresas", subraya.

En ese contexto, Eduardo Morales, académico en Ciberseguridad Industrial de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile, agrega que la Ley Marco de Ciberseguridad, recientemente promulgada, impone nuevos desafíos a las empresas generadoras y distribuidoras: "Sin duda tendrán más exigencias en ciberseguridad para sus infraestructuras tecnológicas, tanto IT como OT, las que estarán orientadas a la prevención, contención, resolución y respuesta a incidentes de ciberseguridad". Más allá de esta legislación, desde julio de 2020 se está aplicando el nuevo estándar en este ámbito para la industria eléctrica, donde se exigen requisitos mínimos de resguardo en esta materia. "La mayoría de las empresas que no cumple la normativa es porque tienen la percepción de que deben renovar su tecnología y que se trata de un proceso caro y complejo. Sin embargo, es un prejuicio y es posible encontrar soluciones funcionales en el mercado", aclara Guillermo Velarde Zapater, VP Business Development LATAM de NovaTech Automation.

Un escenario en constante cambio

En ciberseguridad, los riesgos son constantes y dinámicos, por lo que, independientemente de los marcos legales, los actores de la industria están expuestos a eventos que pueden provocar diversos menoscabos. "Se enfrentan a pérdidas económicas, reputaciones con sus clientes, de productividad, entre otras, lo que obliga a las empresas del rubro a redoblar los presupuestos y recursos destinados a la ciberseguridad. La Ley Marco de Ciberseguridad, sin duda, viene a proteger a los ciudadanos que dependen de las infraestructuras críticas ya presentes en el ciberespacio y por el cual hoy los servicios esenciales de la ciudadanía están en riesgo", explica Morales.

El académico detalla que, de no cumplir con la ley, las multas asociadas pueden oscilar entre 5.000 y 40.000 UTM. "Es importante que los distintos actores de la industria conozcan los riesgos a los que se exponen para prevenir y/o mitigar potenciales ciberamenazas que pongan en riesgo la seguridad y continuidad del servicio de energía eléctrica. Sobre todo, hoy en día que contamos con herramientas que facilitan la integración de la ciberseguridad a la operación", concluye Vilche.

Artículo gentileza de Conecta Ingeniería.