SECTOR ELÉCTRICO · INFRAESTRUCTURA CRÍTICA

Tres meses sin reconectarse

Lo que el caso Huatacondo revela sobre cómo medimos la resiliencia en infraestructura crítica en Chile. El dato relevante no es la intrusión. Es el tiempo de retorno.

Por **Álvaro Rojas Espinoza** CISA · CISM · CDPSE · ISO 27001 LA

16 de noviembre de 2026 Lectura: 8 minutos

El 27 de agosto de 2026, a las 13:10, el parque fotovoltaico Huatacondo y su sistema de almacenamiento en baterías quedaron fuera del Sistema Eléctrico Nacional. En el mismo minuto se desconectó el transformador TR1 220/23 kV de la subestación Santa Rita. La bitácora del Coordinador Eléctrico Nacional registró la causa declarada por las empresas coordinadas: ciberataque.

Desde el 28 de agosto, la planta y las baterías figuran con 0% de disponibilidad en los informes diarios del Coordinador. A fines de octubre seguían así, y al cierre de este artículo no he encontrado registro público de su reconexión. Son cerca de tres meses.

EL CASO, EN DATOS VERIFICABLES

Instalación	Parque fotovoltaico Huatacondo, 103 MW, comuna de Pozo Almonte, Región de Tarapacá. Unas 150 hectáreas y cerca de 365 mil paneles. En operación desde 2019.
Almacenamiento	Sistema de baterías de 98 MW / 312 MWh, en etapa de puesta en servicio al momento del incidente.
Evento	27 de agosto de 2026, 13:10. Desconexión forzada de la planta y del BESS, más el transformador TR1 220/23 kV de la subestación Santa Rita en el mismo minuto.
Causa registrada	«Ciberataque», según la causa declarada por las empresas coordinadas en la bitácora del Coordinador Eléctrico Nacional.
Estado	0% de disponibilidad en los informes diarios del Coordinador desde el 28 de agosto. Sin registro público de reconexión al 16 de noviembre de 2026.

El propio Coordinador ha señalado que sus informes diarios registran la causa que comunica el operador y no constituyen una investigación técnica. Ninguno de los datos anteriores debe leerse como una conclusión sobre responsabilidades.

Conviene decir también lo que no consta. No hay declaración pública sobre qué sistemas fueron comprometidos: si el ataque alcanzó el entorno TI corporativo, el SCADA, el sistema de control de planta o el enlace de comunicación con el Coordinador. No hay información sobre el vector de entrada. No hay mención de ransomware ni de demanda de rescate. No hay atribución.

Llevo más de veinte años revisando programas de riesgo tecnológico y he aprendido a desconfiar de los análisis que rellenan esos vacíos con suposiciones. Así que este artículo no trata de cómo entraron. Trata de lo único que sí está documentado y que, en mi opinión, es el dato más incómodo de todo el caso: el tiempo.

01

El costo de la opacidad

Antes de seguir, vale la pena detenerse en el silencio.

El Coordinador calificó el episodio como un caso excepcional y ha mantenido reserva mientras la investigación sigue en curso. Es una posición defendible. La información sobre un incidente activo puede facilitar un segundo ataque, y existen obligaciones contractuales y de confidencialidad que nadie puede ignorar por conveniencia analítica.

Pero la reserva tiene un costo, y ese costo es colectivo. Una revisión pública de los informes diarios del Coordinador del último año no encontró otros eventos explícitamente atribuidos a ciberataques. Ese hallazgo admite dos lecturas muy distintas: que no los hubo, o que no quedaron registrados de esa forma. La diferencia importa, porque el resto del sector está tomando decisiones de inversión sobre esa base.

En banca aprendimos esta lección hace años. La RAN 20-10 de la CMF obliga a compartir información técnica de incidentes con la industria, precisamente porque una técnica que funciona contra una institución funciona contra todas. El sector eléctrico chileno todavía no tiene ese reflejo instalado. La norma técnica que está en consulta propone un CSIRT sectorial que podría empezar a construirlo, y ojalá llegue pronto.

02

La asimetría que casi nadie mide

Cuando evalúo un programa de seguridad —y he evaluado muchos, en banca, minería, retail y energía— encuentro casi siempre la misma distribución del esfuerzo. El inventario de controles preventivos es detallado: segmentación, gestión de accesos, *hardening*, monitoreo, detección. Hay métricas, hay reportes mensuales, hay tendencia. Y después está la capacidad de volver a operar, que normalmente ocupa una línea en un plan de continuidad, con un objetivo de tiempo de recuperación que alguien escribió hace tres años y que nunca se probó en condiciones reales.

Esa asimetría tiene una explicación razonable. La prevención es un proyecto; la recuperación es un ensayo. Los proyectos se financian, se ejecutan y se cierran con un entregable. Los ensayos interrumpen la operación, cuestan producción y rara vez tienen un dueño dispuesto a empujarlos contra la resistencia del área operativa.

El problema es que el riesgo no se distribuye igual. En un entorno de TI, la diferencia entre un buen y un mal programa de recuperación se mide en horas o días. En un entorno de tecnología de operación, se mide en semanas o meses. Y el impacto no es la caída de un servicio administrativo: es energía que no se genera, compromisos que no se cumplen y una posición en el sistema que alguien más tiene que cubrir.

> **Huatacondo pone ese número sobre la mesa. No sé cuál era su tiempo objetivo de recuperación. Sospecho que no eran tres meses.**

03

Por qué volver en OT no se parece a volver en TI

Esta es la parte que, en mi experiencia, peor se traduce a un directorio. Conviene decirla sin tecnicismos.

En TI, la restauración es un problema de datos. Si tengo respaldos íntegros y aislados, reinstalo, restauro y vuelvo a operar. El criterio de éxito es que la información esté completa y consistente.

En OT, la restauración es un problema de confianza. El criterio de éxito no es que los sistemas arranquen: es poder demostrar que la red de control está limpia y que la lógica que gobierna el equipamiento es la correcta. Son cosas distintas, y la segunda es mucho más difícil de probar.

Pensemos en lo que eso implica en la práctica. Hay que verificar la integridad de la lógica de control y de los parámetros de operación, que no siempre están versionados ni respaldados con el mismo rigor que una base de datos. Hay que descartar persistencia en equipos que muchas veces no admiten un agente de seguridad ni un análisis forense convencional. Hay que revisar los accesos remotos de fabricantes e integradores, que son parte legítima del modelo operativo y no una anomalía. Y hay que volver a validar el comportamiento del activo frente al sistema: un generador no se reconecta porque su dueño decida que ya está listo, sino cuando puede demostrarlo ante quien coordina la operación.

Cada uno de esos pasos es defendible por separado. Sumados, explican por qué una instalación puede quedar meses fuera sin que nadie esté actuando con negligencia. Y explican por qué el tiempo de retorno en OT no se puede estimar desde un plan de continuidad escrito en el lenguaje de TI.

04

El detalle que más me preocupa

Hay un dato lateral que ha recibido mucha menos atención que la planta y que, para mí, es el más relevante de toda la cobertura.

La semana anterior al incidente de Huatacondo se reportó en el sector otro evento: un proveedor de ingeniería y sistemas de control con acceso a instalaciones de terceros. No voy a especular sobre si existe relación entre ambos, porque no hay base pública para afirmarlo. Pero el patrón merece atención, porque es el mismo que encuentro en casi todas las evaluaciones de riesgo de terceros que hago en entornos industriales.

El acceso del integrador es, casi siempre, el punto más débil y el menos gobernado de la arquitectura OT. Es permanente donde debería ser temporal. Es compartido donde debería ser nominativo. Queda fuera del inventario de cuentas privilegiadas porque «es del proveedor». Y nadie lo revisa, porque revisarlo

significa negociar con el único actor capaz de reparar el equipamiento un domingo a las tres de la mañana.

Si una organización va a hacer una sola cosa después de leer esto, que sea esa: levantar el inventario real de accesos de terceros a la red de control, con nombre, propósito, vigencia y registro de actividad. Es la medida de mayor retorno por peso invertido que conozco en este ámbito.

05

Lo que viene por el lado regulatorio

El contexto normativo del sector ya cambió y va a cambiar más.

Por un lado, la Ley 21.663 está plenamente operativa. La generación, la transmisión y la distribución eléctrica figuran como servicios esenciales, y la ANCI cerró dos etapas de calificación de Operadores de Importancia Vital. Para quien quedó calificado, las obligaciones son concretas: delegado de ciberseguridad, sistema de gestión de seguridad de la información y reporte de incidentes con alerta temprana dentro de tres horas, actualización a las 72 horas —24 si el servicio esencial se ve afectado— e informe final a los 15 días.

Por otro, la Comisión Nacional de Energía sometió a consulta pública, a fines de agosto de 2026, el proyecto de Norma Técnica de Ciberseguridad y Seguridad de la Información del sector eléctrico, un proceso que arrastra desde 2021. Su arquitectura es interesante. Un capítulo de gestión de seguridad de la información dirigido a las empresas que no son OIV, con clasificación de impacto alto, medio o bajo, certificación ISO 27001 para las de impacto alto y un conjunto de controles mínimos para el resto. Y un capítulo de ciberseguridad industrial que alcanza a todas las empresas eléctricas, incluidos los OIV y el propio Coordinador, construido sobre el modelo NERC CIP.

Hay que leer bien esa estructura, porque tiene una consecuencia práctica que ya he visto malinterpretar: ser OIV no exime del capítulo industrial. Una empresa calificada que dé por cerrado su cumplimiento con lo que exige la ANCI se va a encontrar con un segundo conjunto de obligaciones, con otra lógica de clasificación —por activo, no por tipo de cliente— y con otro supervisor.

Dicho eso, quiero ser honesto sobre el alcance de todo esto. La regulación que viene mide gobernanza: que exista una unidad responsable, una política, un alcance definido, una medición de madurez. Es necesario y es un avance real. Pero ninguna de esas exigencias responde la pregunta que Huatacondo deja planteada, que es cuánto tarda una instalación crítica en volver a operar después de un incidente y si alguien lo midió antes de que ocurriera.

Eso sigue siendo una decisión de gestión y no una obligación normativa. Por eso mismo es una decisión de directorio.

06

Seis preguntas para el directorio

Estas son las preguntas que llevo a los comités con los que trabajo. No son técnicas: no hace falta saber qué es un PLC para evaluar la calidad de la respuesta.

01	¿Cuál es nuestro tiempo objetivo de retorno para la instalación más crítica, y cuándo fue la última vez que lo probamos de verdad, no en escritorio?
02	Si tuviéramos que demostrar mañana que nuestra red de control está limpia, ¿con qué evidencia contamos? ¿Quién la produce y en cuánto tiempo?
03	¿Está respaldada y versionada la lógica de control y la parametrización de operación, con el mismo rigor que los datos del ERP?
04	¿Cuántos accesos de terceros existen hoy a nuestra red de control, quién los autorizó, cuándo vencen y dónde queda registro de lo que hacen?
05	¿Quién, con nombre y apellido, declara un incidente a la ANCI dentro de las tres horas, y qué ocurre si el evento cae un sábado a las dos de la mañana?
06	¿Cuánto nos cuesta un día fuera de operación, y en qué punto esa cifra justifica la inversión que llevamos tres años postergando?

Cómo leer las respuestas. Si las seis se responden con datos, el programa de resiliencia es real. Si tres o más se responden con «habría que revisarlo», lo que existe es un documento, no una capacidad.

07

El número que yo llevaría al directorio

El valor de un caso como Huatacondo no está en el morbo del ataque. Está en que entrega una métrica que normalmente no tenemos: cuánto puede durar realmente la indisponibilidad de un activo crítico cuando el problema no es físico, sino de confianza en la red de control.

Cerca de tres meses. Ese es el número que yo pondría sobre la mesa en la próxima sesión. No para asustar a nadie, sino para hacer una sola pregunta: si nos pasara a nosotros, ¿tenemos cómo saber si seríamos más rápidos?

La madurez en ciberseguridad industrial no se demuestra evitando todos los incidentes. Eso no lo logra nadie. Se demuestra sabiendo, antes de que ocurran, cuánto vamos a tardar en volver.

FUENTES

1. **ESS News (pv magazine)**, «Chile solar and battery system remain offline after cyberattack», 29 de octubre de 2026. Bitácora e informes diarios del Coordinador Eléctrico Nacional, capacidad del BESS y revisión de informes del último año.
2. **Diario Financiero (Señal DF)**, «Coordinador Eléctrico registró ciberataque en planta solar Huatacondo», 23 de octubre de 2026. Hora del evento, transformador TR1 de Santa Rita y disponibilidad en informes diarios.
3. **SolarQuarter**, «Cyberattack Forces 103 MW Huatacondo Solar Farm And Battery Storage Offline In Chile», 30 de octubre de 2026.
4. **T13**, «Ciberataques en Chile: el ataque que dejó desconectada una planta eléctrica», 16 de noviembre de 2026. Declaraciones del Coordinador Eléctrico Nacional.
5. **EnergySage**, «Grid cybersecurity: Chile's draft regulation reaches consultation», 31 de agosto de 2026. Estructura de la Norma Técnica de la CNE, clasificación de impacto y plazos de implementación.
6. **Electrominería**, «Ciberseguridad: Norma Técnica de la CNE contempla siete pilares», 4 de octubre de 2023. Contenidos y CSIRT sectorial.
7. **Anguita Osorio**, «RAN 20-10: ciberseguridad bancaria», actualizado al 10 de septiembre de 2026. Obligación de compartir información técnica de incidentes con la industria.

Nota metodológica: este artículo se apoya en fuentes de prensa especializada que citan los informes diarios del Coordinador Eléctrico Nacional. No se ha accedido a los documentos originales del Coordinador ni a declaraciones de las empresas involucradas. La Norma Técnica de la CNE se encontraba en consulta pública a la fecha de las fuentes consultadas; su estado a noviembre de 2026 no pudo verificarse en fuente oficial. Ninguna afirmación de este texto debe interpretarse como una imputación de responsabilidad a las empresas mencionadas.

SOBRE EL AUTOR

De la conversación técnica a la decisión de directorio

En Mindoria acompañamos a organizaciones de servicios financieros, minería, energía, retail e industria productiva a construir programas de riesgo y ciberseguridad que resisten la prueba del incidente, no solo la de la auditoría. Trabajamos en el lenguaje del directorio y en el detalle del control.

- Estrategia y gobierno de ciberseguridad · vCISO
- Gestión de riesgo operacional y tecnológico (TI/OT)
- Auditoría TI y assessments ISO 27001, NIST CSF y COBIT
- Continuidad operacional y resiliencia
- Cumplimiento Ley 21.663 / ANCI y normativa sectorial
- Gobierno de datos personales y gestión de terceros

Álvaro Rojas Espinoza

CISA · CISM · CDPSE · ISO 27001 LEAD AUDITOR

Más de 20 años en riesgo tecnológico y ciberseguridad.
Ex Accenture, Deloitte y Falabella.

Conversemos
[sitio web] · [correo de contacto]
LinkedIn: Álvaro Rojas Espinoza