

## Del ciberataque a la interrupción del suministro: el riesgo creciente para el sector energético

- El reto para las empresas energéticas consiste en aprovechar las ventajas de la digitalización sin poner en riesgo la continuidad del suministro.



La preocupación por las amenazas cibernéticas emergentes ha aumentado tras la invasión rusa de Ucrania.

<https://elperiodicodelaenergia.com/del-ciberataque-a-la-interrupcion-del-suministro-el-riesgo-creciente-para-el...>

Carlos Castañeda-Marroquín

**Viernes, 16 octubre 2026**

### El reto para las empresas energéticas consiste en aprovechar las ventajas de la digitalización sin poner en riesgo la continuidad del suministro

El cierre durante cuatro días de una pequeña central eléctrica en el Reino Unido tras un ciberataque el pasado mes de julio dejó una advertencia clara para el sector energético europeo. Una amenaza digital ya no tiene por qué quedarse en el mundo digital. Cuando alcanza la tecnología operativa (OT), puede tener consecuencias físicas, y España no es ajena a este tipo de amenaza.

En España, el ataque al Sistema de Información de Puntos de Suministro (SIPS) del pasado 7 de septiembre puso de nuevo el foco en la exposición del sector energético. El atacante afirmó haber extraído más de 40 millones de registros de la base de datos de la Comisión Nacional de los Mercados y la Competencia (CNMC), que almacena información técnica, comercial y de consumo de los puntos de suministro de electricidad y gas natural en España. Este tipo de incidentes plantea una cuestión a las empresas energéticas españolas: ¿conocen realmente todos los activos OT de los que dependen sus operaciones y saben cómo podrían ser atacados? La respuesta importa porque las redes eléctricas son cada vez más digitales y están más conectadas.

La convergencia entre las tecnologías de la información (IT) y las tecnologías operativas (OT) permite intercambiar datos entre activos de generación, centros de control, redes inteligentes,

instalaciones renovables y plataformas externas. Esta conectividad aporta numerosas ventajas operativas, pero también abre nuevas vías de entrada para los atacantes. Se podría decir que la superficie de ataque crece mientras la IA acelera las posibles vías de ataque. El reto para las empresas energéticas consiste en aprovechar las ventajas de la digitalización sin poner en riesgo la continuidad del suministro.

## **El reto de proteger las infraestructuras**

En 2025, el Instituto Nacional de Ciberseguridad (INCIBE) gestionó 122.223 incidentes en España, un 26 % más que el año anterior. Para el sector energético, el riesgo presenta una dimensión particular, ya que los activos OT controlan procesos físicos relacionados con la generación, el transporte y la distribución de energía. Por otra parte, estos activos están dispersos geográficamente, por lo que las subestaciones, las instalaciones de energías renovables y las plantas de generación más pequeñas suelen gestionarse de forma remota, a menudo con pocas medidas de seguridad. Paralelamente, los fabricantes de equipos, los proveedores de mantenimiento y los socios de ingeniería también requieren acceso remoto a los sistemas.

La protección de los sistemas OT requiere un enfoque distinto del utilizado para salvaguardar los sistemas de tecnologías de la información (IT), en los que priman la confidencialidad y la protección de los datos. En este ámbito operativo del sector energético, el foco está en la seguridad, la integridad, la disponibilidad y la continuidad del servicio, dado que un incidente en este entorno puede llegar a detener una operación física.

## **Proteger el entorno OT**

La protección de la infraestructura OT debe comenzar por una pregunta sencilla: ¿qué tenemos conectado? Cada acceso a estos sistemas debería responder a una necesidad operativa clara. Las conexiones que ya no sean necesarias y las cuentas inactivas deben eliminarse, mientras que los accesos legítimos deben limitarse a los sistemas y tareas que realmente los requieran. Un inventario actualizado permite saber qué hardware, software, firmware y protocolos industriales forman parte del entorno, además de identificar las conexiones de red, sus responsables y las dependencias operativas.

El siguiente paso consiste en determinar qué activos son críticos y qué ocurriría si dejaran de funcionar o se vieran comprometidos. Esta visibilidad permite concentrar los esfuerzos de seguridad allí donde una interrupción tendría mayores consecuencias. También hace posible supervisar de forma continuada la infraestructura industrial para detectar comportamientos anómalos. Esto resulta especialmente relevante cuando un atacante intenta pasar de un sistema corporativo comprometido a operaciones críticas. Todo ello debe hacerse teniendo en cuenta una característica esencial de la OT: la seguridad no puede poner en peligro la operación. Un parche incompatible, un reinicio inesperado o una medida mal diseñada pueden interrumpir procesos críticos. La ciberseguridad industrial debe adaptarse a esa realidad.

## **Estar preparado**

Incluso la planificación más rigurosa no garantiza que una organización pueda evitar todos los ataques. Por eso, la formación y la preparación previa forman parte de la protección. Un plan de respuesta específico para OT debe establecer cómo detectar y contener un incidente y cómo restablecer la actividad tras él. Su desarrollo no puede recaer únicamente en el equipo de ciberseguridad. Los responsables de operaciones y los ingenieros deben participar, junto con los proveedores pertinentes. En este contexto, los ejercicios periódicos ayudan a comprobar qué ocurriría ante escenarios reales, como la pérdida de visibilidad remota, la propagación de ransomware desde IT hacia OT o el compromiso del acceso de un tercero. Más allá de estar bien preparada frente a un ciberataque, una organización debe contar con un plan de contingencia que le permita seguir operando cuando algo sale mal. Conocer y controlar los activos OT es una cuestión de resiliencia operativa.

El objetivo de la digitalización de los entornos TI y OT es acceder a datos para supervisar las operaciones, mejorar la eficiencia e impulsar nuevas iniciativas en tiempo real. De cara a las amenazas digitales, el sector energético necesita identificar los activos críticos, saber quién puede acceder a ellos y tener claro cómo responder si se ven comprometidos. La verdadera medida del éxito no será cuántos controles de ciberseguridad se hayan implantado, sino algo mucho más tangible: que, incluso frente a un ataque, la energía siga llegando allí donde España la necesita.

***Carlos A. Castañeda-Marroquín es director de Soluciones e Innovación en Integrity360 España.***