

## Por qué la resiliencia energética requiere un nuevo enfoque

- Según DNV, la resiliencia de las infraestructuras energéticas se ha convertido en una condición indispensable para que la transición pueda avanzar sin interrupciones.



Por qué la resiliencia energética requiere un nuevo enfoque

<https://elperiodicodelaenergia.com/por-que-la-resiliencia-energetica-requiere-un-nuevo-enfoque/>

José A. Roca

**Martes, 01 septiembre 2026**

### Según DNV, la resiliencia de las infraestructuras energéticas se ha convertido en una condición indispensable para que la transición pueda avanzar sin interrupciones

La transición desde los combustibles fósiles hacia un sistema energético descarbonizado se enfrenta a un desafío que va mucho más allá de reducir las emisiones. El denominado “trilema energético” obliga a compatibilizar tres objetivos: sostenibilidad y neutralidad climática, seguridad del suministro y precios asequibles. En este contexto, la resiliencia de las infraestructuras energéticas se convierte en una condición indispensable para que la transición pueda avanzar sin interrupciones, según el nuevo documento *“From the concern to control: Rethinking energy resilience for the new threat era”*, de DNV. \*\*

La resiliencia no equivale simplemente a garantizar la fiabilidad cotidiana de una red eléctrica. Implica que el sistema sea capaz de resistir, responder y recuperarse ante acontecimientos extremos, como catástrofes naturales, ciberataques, sabotajes físicos o conflictos híbridos. Para ello es necesario anticipar riesgos, proteger las infraestructuras, disponer de mecanismos de defensa y contar con planes eficaces de recuperación.

El reto se ha agravado por la creciente complejidad e interconexión de los sistemas energéticos. La electrificación, el despliegue de renovables y la digitalización aumentan las oportunidades de eficiencia, pero también crean nuevas dependencias y puntos vulnerables. Un fallo localizado puede

desencadenar efectos en cadena que afecten a otros sectores esenciales, como las telecomunicaciones, el transporte o la sanidad.

## Un panorama de amenazas cambiante

El panorama de amenazas también ha cambiado. Las infraestructuras críticas son cada vez más objeto de ataques deliberados, desde operaciones de ciberdelincuencia hasta acciones vinculadas a Estados y conflictos de "zona gris". Redes eléctricas, gasoductos, cables submarinos y terminales de gas natural licuado pueden convertirse en objetivos de sabotajes, drones, misiles o bloqueos. A ello se suman riesgos no intencionados, como infraestructuras envejecidas, falta de capacidad y flexibilidad de las redes, deficiencias de mantenimiento o incertidumbres regulatorias y comerciales.

El cambio climático añade otra capa de vulnerabilidad. Las olas de calor, sequías, inundaciones y otros fenómenos extremos son cada vez más frecuentes e intensos, poniendo a prueba unas infraestructuras de las que depende una economía cada vez más electrificada. Las olas de calor registradas en Europa occidental durante el verano de 2026 volvieron a evidenciar cómo los problemas de las redes pueden propagarse más allá de las fronteras. En Ecuador, la sequía de 2024 llegó a provocar un deterioro extremo del sistema eléctrico, altamente dependiente de la generación hidroeléctrica.

Paradójicamente, la resiliencia climática continúa recibiendo menos atención e inversión que amenazas más visibles, como los ciberataques o la seguridad física. Según el análisis de DNV citado en el documento, menos de la mitad de los líderes del sector considera que sus organizaciones disponen de estrategias de resiliencia claramente definidas y actualizadas de forma periódica.

La experiencia demuestra, además, que los grandes incidentes energéticos rara vez quedan confinados a una única empresa. El apagón que afectó a España y Portugal en abril de 2025 interrumpió servicios de transporte y telecomunicaciones y tuvo repercusiones en hospitales. La investigación posterior apuntó a una combinación de factores técnicos y relacionados con el control de la red, poniendo de manifiesto la necesidad de abordar la resiliencia desde una perspectiva sistémica.

La transición energética también introduce nuevas dependencias en las cadenas de suministro. El crecimiento de las renovables exige equipos, componentes y materias primas cuya producción puede concentrarse en determinados países. Una crisis geopolítica, una disputa comercial o una interrupción logística podría comprometer el suministro. Por ello, empresas y gobiernos están recurriendo a estrategias como el *reshoring*, el *nearshoring* y el *friendshoring* para diversificar proveedores y reducir riesgos.

## Mayores exigencias de resiliencia

En paralelo, la regulación está elevando las exigencias de resiliencia. En Europa, las directivas sobre resiliencia de entidades críticas y ciberseguridad buscan reforzar la protección física y digital de los servicios esenciales. Estados Unidos, por su parte, está tratando la red eléctrica cada vez más como una cuestión de seguridad nacional, impulsando medidas para ampliar la capacidad industrial y garantizar el suministro de componentes estratégicos.

Ante este escenario, DNV propone un enfoque basado en sistemas y no en activos aislados. Su Resilience Framework pretende proporcionar un lenguaje común para empresas, operadores, reguladores y administraciones públicas. La premisa es que ningún actor puede controlar por sí solo todas las amenazas y que la resiliencia debe construirse mediante cooperación a lo largo de toda la cadena energética.

El marco se articula en cuatro pasos. El primero consiste en analizar los riesgos y construir un perfil actualizado de amenazas. Para ello no basta con estudiar accidentes o fenómenos meteorológicos: también deben considerarse las capacidades e intenciones de posibles actores maliciosos. El análisis contempla cinco dimensiones: organización, personas, infraestructura física, sistemas digitales y ciberseguridad, y cadena de suministro.

El segundo paso es priorizar las inversiones. No se trata de gastar indiscriminadamente en seguridad, sino de identificar las medidas capaces de reducir más riesgo y las vulnerabilidades estructurales que requieren inversiones de mayor alcance. La resiliencia debe integrarse en los planes financieros y operativos de las compañías y traducirse en una hoja de ruta clara.

El tercer paso es aplicar las medidas. Los planes deben convertirse en capacidades reales mediante barreras preventivas, alternativas operativas y procedimientos documentados de respuesta, reinicio y recuperación. La resiliencia, sostiene DNV, no debe funcionar como un proyecto independiente, sino incorporarse a la gestión habitual de los activos y a la ejecución de nuevos proyectos.

Finalmente, el cuarto paso exige comprobar y validar continuamente el sistema. Los escenarios de crisis deben ensayarse, las dependencias críticas ponerse a prueba y los procedimientos de recuperación revisarse periódicamente. La resiliencia no es un estado permanente ni una certificación puntual, sino un proceso de mejora continua condicionado por un entorno geopolítico, tecnológico y climático cambiante.

En definitiva, la seguridad energética del futuro dependerá tanto de la descarbonización como de la capacidad para resistir las perturbaciones que acompañarán a ese proceso. La digitalización, la electrificación y las renovables pueden acelerar la transición, pero también aumentan la interdependencia del sistema. Por ello, la resiliencia debe incorporarse desde el diseño de las infraestructuras y convertirse en una responsabilidad compartida entre empresas, gobiernos y reguladores. El objetivo final es pasar de una cultura reactiva, centrada en responder a las crisis, a otra basada en la anticipación, la preparación y la recuperación. Solo así será posible construir un sistema energético simultáneamente limpio, seguro y asequible.