

84
Septiembre
2026

CUA DER NOS *DE ENERGÍA*

GARRIGUES

40  de la Energía

Deloitte.

De proteger infraestructuras a garantizar la prestación de los servicios esenciales: la resiliencia del sector energético ante un nuevo escenario de riesgos

José Luis Pérez Pajuelo

Director del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC)

La transformación energética que está teniendo lugar en los últimos años, la profunda transformación digital de la sociedad y un entorno geopolítico más exigente obligan a evolucionar desde la protección de activos concretos hacia un concepto integral de resiliencia. En ese cambio de modelo, que ya se anticipó en el contexto de la protección de infraestructuras críticas, la energía constituye uno de los mejores ejemplos de cómo seguridad, continuidad del servicio y cooperación público-privada se han convertido en dimensiones inseparables. Es la energía, por tanto, mucho más que un sector estratégico.

No muchas actividades reflejan mejor la complejidad de las sociedades modernas que el suministro energético del que se les dota. Detrás de un gesto cotidiano como encender una luz, cargar un vehículo eléctrico, utilizar un teléfono móvil, seleccionar un producto alimenticio del refrigerador o acceder a un servicio sanitario existe una extensa red de infraestructuras, empresas, tecnologías y profesionales cuya actividad debe mantenerse de manera continua bajo cual-

quier circunstancia.

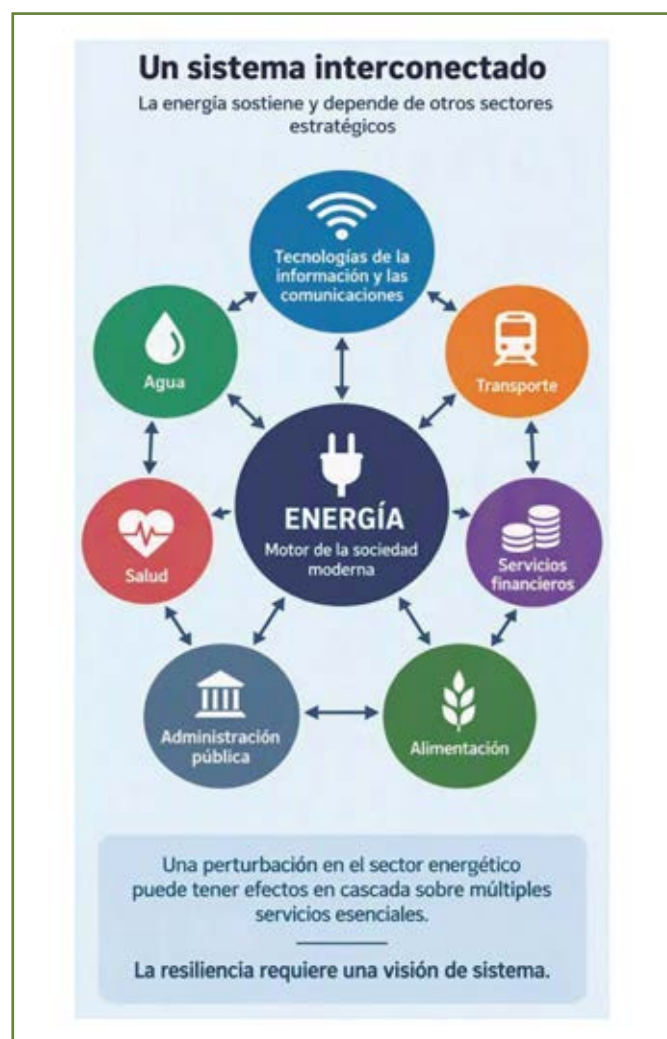
Por ello, hablar de seguridad energética ya no es sólo hablar de asegurar la disponibilidad de determinadas fuentes de suministro, mirada pasada y que ha sido totalmente superada desde hace años. Significa también asegurar la capacidad de generación, su transporte, el almacenamiento y la distribución; y también proteger los sistemas físicos y digitales que hacen posible su operación, pero, sobre todo, en el actual contexto, significa garantizar la continuidad de los servicios esenciales que dependen de ellos.

Esta realidad adquiere cada día una mayor importancia porque **las infraestructuras actuales están profundamente interconectadas**. La propia legislación española sobre protección de infraestructuras críticas ya advertía en 2011 de la creciente dependencia de las sociedades respecto de las infraestructuras que sostienen los servicios esenciales y del riesgo de que una perturbación pueda propagarse por sus efectos en cascada entre sistemas interdependientes. Esa

interdependencia se asume hoy todavía con una mayor dimensión. Sectores como el de la energía y el de las tecnologías de la información y las comunicaciones dependen el uno del otro; los sistemas de transporte necesitan de la energía y comunicaciones; el abastecimiento de agua requiere electricidad; numerosos servicios financieros, sanitarios y administrativos dependen simultáneamente del suministro eléctrico y de las redes digitales.

La energía es, por tanto, un sector sobre el que descansan muchos otros sectores estratégicos para el normal desarrollo de la vida de la ciudadanía de los estados modernos.

Figura 1.



Esta característica explica que la búsqueda de su máxima resiliencia no sea únicamente una cuestión empresarial o sectorial, sino una materia directamente relacionada con la seguridad de la sociedad en su conjunto, de la seguridad nacional.

El entorno en el que operan las infraestructuras energéticas se ha transformado sustancialmente durante los últimos años. Las amenazas intencionadas tradicionales no han desaparecido, pero conviven ahora con riesgos de naturaleza muy diversa que en otros tiempos no suponían una dimensión de riesgos tan aguda.

En primer lugar, el escenario geopolítico ha devuelto al primer plano la dimensión estratégica de la energía. Las tensiones internacionales han demostrado nuevamente que las materias primas fuentes de energía, rutas de suministro, sus interconexiones, las instalaciones energéticas y las cadenas logísticas constituyen elementos de extraordinario valor estratégico.

A esto se suma la consolidación de las amenazas híbridas, caracterizadas precisamente por combinar instrumentos de distinta naturaleza para provocar el incidente, lo complejo de su atribución, dificultar la identificación de los límites entre seguridad física, seguridad digital, presión económica, influencia informativa o acciones de naturaleza encubierta.

Paralelamente debería observarse el componente climático, que cobra una importancia creciente en la última década. Fenómenos meteorológicos extremos, incendios forestales de sexta generación, inundaciones devastadoras, sequías o episodios de temperaturas especialmente elevadas pueden afectar simultáneamente a diferentes instalaciones o comprometer las condiciones necesarias para su normal funcionamiento.

Pero a todo esto, hay que añadir un cuarto factor que resulta determinante: la profunda digitalización que está sufriendo el sector. La transformación digital del sector energético proporciona importantes beneficios en términos de eficiencia, flexibilidad y capacidad de gestión. Las redes inteligentes, la sensorización avanzada, automatización, telecontrol, almacenamiento, generación distribuida o gestión digital de

la demanda permiten un sistema energético mucho más sofisticado y eficaz que el de hace apenas unas décadas disfrutábamos.

Pero, al igual que toda evolución, esa misma conectividad

amplió su superficie de exposición ante nuevas amenazas. Actualmente resulta muy complicado, por no decir imposible, establecer una separación entre seguridad física o tradicional y ciberseguridad. Un incidente que comienza en el ámbito digital puede generar efectos físicos, y una perturbación física puede afectar a sistemas de comunicaciones y control imprescindibles para gestionar la recuperación, por no hablar de elementos internos que puedan sabotear los sistemas tanto físicos como tecnológicos para alterar el funcionamiento de la propia instalación.

Esta convergencia constituye uno de los grandes cambios conceptuales de la protección moderna de infraestructuras estratégicas, y que fue abordada por el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) a medida que evolucionó el propio Sistema nacional PIC.

Durante años, la política de seguridad de las infraestructuras críticas se ha construido fundamentalmente alrededor de la protección integral de los activos. Se trata, de manera simplificada, de identificar aquellas instalaciones cuya perturbación puedan producir consecuencias especialmente graves y de establecer medidas capaces de evitar o reducir dicha posibilidad, y, de hecho, **la protección sigue siendo imprescindible**. Sin embargo, el entorno actual obliga a ir un paso más allá, considerando que todos los incidentes no pueden evitarse. Y de esta concepción de imposibilidad de una total protección nace la necesidad de tratar el escenario que se genere ante la materialización de uno de estos riesgos.

Una infraestructura puede verse afectada por una inundación extraordinaria, un fallo tecnológico, una interrupción de su cadena logística, un ciberincidente o una combinación de varios acontecimientos, y frente a esta realidad, la pregunta clave ya no es exclusivamente saber cómo podemos impedir que ocurra un incidente; ahora aparecen interrogantes adicionales, como saber si somos capaces de mantener el servicio, limitar sus efectos, adaptarnos o recuperar rápidamente la normalidad en su funcionamiento. Esto es, esencialmente, **el cambio hacia la resiliencia**.

La Unión Europea ha incorporado formalmente esta transformación conceptual mediante la Directiva (UE) 2022/2557

Figura 2.



del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas, que sustituye el enfoque anterior establecido mediante la Directiva 2008/114/CE del Consejo, sobre la identificación y designación de infraestructuras críticas europeas. El legislador europeo parte de la constatación de que concentrar las medidas de protección exclusivamente sobre activos individuales resulta insuficiente en una economía crecientemente interconectada.

En esta ocasión la aspiración europea es mucho más amplia: conseguir que las entidades críticas tengan capacidad para prevenir, protegerse, responder, resistir, mitigar, absorber, adaptarse y recuperarse ante aquellos incidentes susceptibles de alterar la prestación de los servicios esenciales, es decir, de adoptar el concepto de resiliencia en las organizaciones. No se abandona la protección, sino que se integra dentro de un concepto superior.

La aprobación de la Directiva (UE) 2022/2557, conocida como Directiva CER, constituye uno de los principales hitos de esta evolución, y cambia el paradigma regulatorio. Su objeto consiste en **reducir la vulnerabilidad y aumentar la resiliencia de las entidades críticas responsables de servicios esenciales para la economía y las funciones sociales**. Su ámbito comprende once sectores, todos ellos ya estudiados en el sistema español PIC, puesto que, desde la Secretaría de Estado de Seguridad, con el CNPIC como motor tractor de esta normativa, los identificó e incluyó en la transposición de la primera de las directivas europeas. Ahora, la energía comprende específicamente electricidad, calefacción y refrigeración urbanas, petróleo, gas e hidrógeno, elementos que, de una u otra forma, ya suponen servicios esenciales contemplados y estudiados.

Pero lo más significativo y particularmente novedoso, supone que el objeto principal sobre el que se construye el sistema deja de ser únicamente la infraestructura estratégica para situarse adicionalmente sobre la entidad responsable de prestar el servicio esencial a través de estas infraestructuras. En otras palabras, **se pasa progresivamente de proteger el activo a garantizar la resiliencia de la organización para asegurar la continuidad del servicio esencial**.

Esto no es una cuestión meramente semántica, sino que tiene profundas consecuencias prácticas, puesto que una organización resiliente necesita conocer no solamente las amenazas dirigidas contra una instalación, sino también sus dependencias, proveedores críticos, recursos humanos esenciales, sistemas tecnológicos, comunicaciones,

Figura 3.



suministros alternativos y capacidades de recuperación. Un análisis mucho más profundo al que asistía cuando lo que se pretendía era proteger un activo concreto. Y es aquí donde el análisis de riesgos adquiere así una dimensión transversal.

Ahora, las entidades críticas de los sectores estratégicos deben adoptar medidas técnicas, organizativas y de seguridad adecuadas y proporcionadas para garantizar su resiliencia.

Pero esta transformación no puede entenderse sin otra pieza fundamental de la arquitectura europea, la Directiva (UE) 2022/2555, del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, conocida como NIS2, evolución de la anterior Directiva NIS.

Mientras CER aborda de forma integral la resiliencia de las entidades críticas, NIS2 eleva el nivel común de ciberseguridad en la Unión, estableciendo obligaciones relacionadas con la gestión de riesgos, la notificación de incidentes, la supervisión y la cooperación en el ámbito de la ciberseguridad, es decir, que cuestión más técnica en el marco de la ciberseguridad se concentra en esta norma, que debe convivir con la perspectiva más estratégica que pudiera derivarse de la CER.

Debido a la implementación de las tecnologías de la información y las comunicaciones en el sector energético, este sector ocupa un lugar central en la NIS2, y figura entre los sectores de alta criticidad, abarcando los mismos ámbitos que se indican en la CER.

CER y NIS2 deben contemplarse, por consiguiente, como dos dimensiones complementarias de una estrategia europea común de resiliencia desde las perspectivas que cada una abarca.

En este contexto analizado, la primera lección práctica para cualquier operador energético resulta evidente: ya no parece razonable gestionar en compartimentos estancos la seguridad física, la ciberseguridad, la seguridad interna, la continuidad de negocio, la gestión de crisis o la recuperación ante incidentes sistémicos. **Ahora se hace necesario**

un modelo verdaderamente resiliente que integre todas sus perspectivas.

Pero España es un alumno aventajado en este marco, y no parte de cero en este proceso. La Ley 8/2011, de 28 de abril, estableció hace quince años el marco nacional de protección de las infraestructuras críticas, y su posterior desarrollo reglamentario, mediante el Real Decreto 704/2011, de 20 de mayo, articuló un sistema en el que participan administraciones públicas y operadores privados y desarrolló diferentes instrumentos de planificación, incluidos los Planes Estratégicos Sectoriales, Planes de Seguridad del Operador y Planes de Protección Específicos. De esta forma, la normativa española construyó una arquitectura “piramidal” basada en varios elementos que mantienen plena vigencia conceptual: identificación de infraestructuras críticas, análisis de riesgos, planificación, coordinación administrativa y, especialmente, cooperación público-privada. Además, incluía, e incluye, la dimensión de la ciberseguridad de las infraestructuras críticas formalmente designadas.

Dentro de esta arquitectura, el CNPIC ha sido el órgano del Ministerio del Interior encargado de impulsar, coordinar y supervisar todas las actividades atribuidas a la Secretaría de Estado de Seguridad en relación con la protección de las infraestructuras críticas en España, y la experiencia acumulada proporciona una base especialmente relevante para afrontar el nuevo escenario.

En 2026 España ha dado un paso decisivo para adaptar este sistema al nuevo marco europeo, puesto que el 17 de marzo, el Consejo de Ministros aprobó, a propuesta del Ministerio del Interior, el proyecto de *Ley de Protección y Resiliencia de Entidades Críticas*, destinado a incorporar al ordenamiento español la Directiva CER, que será remitido a las Cortes Generales para su tramitación.

Este proyecto refleja perfectamente el cambio de paradigma señalado anteriormente, donde la Secretaría de Estado de Seguridad seguirá asumiendo la condición de autoridad nacional competente a través del futuro **Centro Nacional para la Protección y Resiliencia de las Entidades Críticas (CNPREC)**, evolución del actual CNPIC. El proyecto contempla asimismo la elaboración y actualización de un catálogo

de entidades estratégicas y amplía los sectores contemplados, incorporando expresamente, entre otros, el hidrógeno y los sistemas urbanos de calefacción y refrigeración, que, como se indicó anteriormente, ya estaban subsumidos de forma alguna en los sectores que se incluyeron en la ley PIC, además de otros sectores novedosos como el de Seguridad Privada.

Pero no estamos ante un simple cambio de denominación del CNPIC, estamos ante la evolución de un modelo donde las infraestructuras críticas eran el foco principal, hasta el nuevo, donde lo serán las entidades críticas; donde la protección será abordada, para ampliarse hasta la resiliencia, y dónde los activos estratégicos no serán sólo las infraestructuras, sino la propia organización que deberá proteger la provisión del servicio esencial.

El reto consiste ahora en aprovechar toda la experiencia adquirida durante años dentro del Sistema nacional de Protección de Infraestructuras Críticas y proyectarla sobre un modelo más amplio, transversal e integrado.

En este nuevo contexto, el sector energético es probablemente uno de los ámbitos en los que mejor puede observarse esta transformación. La transición energética está modificando simultáneamente la estructura, la tecnología y los actores del sistema.

A las instalaciones tradicionales se suman progresivamente otras de generación distribuida, almacenamiento, autoconsumo, redes inteligentes, nuevas interconexiones, infraestructura de recarga y, tímidamente, tecnologías vinculadas al hidrógeno. Paralelamente, millones de dispositivos y sistemas digitales participan cada vez más activamente en la gestión energética. Además, la descentralización puede suponer un aumento de la resiliencia del sistema, al reducir determinadas concentraciones de riesgo, pero también crea nuevas dependencias y superficies de exposición. De la misma manera, la digitalización proporciona capacidades extraordinarias de monitorización y gestión, pero también incrementa la dependencia respecto de otros sectores como el de las telecomunicaciones, incluyendo también sus propios riesgos y amenazas.

La resiliencia no debe entenderse como una resistencia al cambio tecnológico, sino como una condición necesaria para que ese cambio sea seguro y sostenible, aunque esto conlleve un gran esfuerzo para adaptarse a este nuevo contexto de riesgos y amenazas. Y precisamente en este nuevo contexto surgen nuevas preguntas para los operadores energéticos, además de la natural, saber si su instalación está suficientemente protegida. Ahora hay que cuestionarse qué servicio esencial depende de ella; qué otras infraestructuras necesita para funcionar; qué proveedores resultan irremplazables; durante cuánto tiempo podría mantener la operación ante una perturbación de gran magnitud; qué alternativas existen; cómo debería realizarse su recuperación; o con qué autoridades y operadores debería coordinarse durante una crisis. Ahora, **la resiliencia se transforma en una cuestión de gobernanza empresarial, no exclusivamente de seguridad.**

Existe además una cuestión que merece especial atención, que es la que aborda la seguridad, mal entendida, en muchas ocasiones, como un coste inevitable asociado al cumplimiento regulatorio. Este paso hacia la resiliencia como concepto superior invita a cambiar definitivamente esta percepción de la seguridad que, como se ha indicado anteriormente, se ha transformado en un asunto de vital importancia para los resultados operativos de la organización, que conoce sus dependencias, diversifica suministros, dispone de alternativas, entrena a sus equipos, ensaya escenarios de crisis y puede recuperar rápidamente sus operaciones, sencillamente, una organización mejor preparada para competir y sobrevivir en un entorno incierto como el actual.

La resiliencia protege instalaciones, pero también inversión, reputación, clientes, conocimiento empresarial y capacidad productiva.

La directiva CER proporciona una inmejorable oportunidad para revisar íntegramente los modelos organizativos y **eleva la resiliencia hasta el nivel de decisión estratégica**, que es donde realmente se convierte en una herramienta que aporte su valor añadido. Esa es la esencia del nuevo paradigma.

Tras el análisis anterior, parece claro que **el sector energético reúne todos los elementos que hacen especialmente**

necesaria esta evolución: infraestructuras distribuidas por todo el territorio, elevada digitalización, interdependencia con prácticamente todos los servicios esenciales, transformación tecnológica acelerada y exposición simultánea a riesgos naturales, tecnológicos, cibernéticos y geopolíticos.

En un sistema energético cada vez más complejo, interconectado y decisivo para el futuro económico y estratégico de España esa capacidad de resiliencia que se busca constituye probablemente una de nuestras mejores inversiones en seguridad, donde existen varios **principios** que son propicios para desarrollar una **nueva cultura de resiliencia energética**, entre los que pueden considerarse particularmente relevantes:

1. Pensar en servicios, no solamente en infraestructuras.

Una infraestructura adquiere carácter crítico por las consecuencias que tendría su perturbación sobre la sociedad, y por ello, el punto de partida debe ser el servicio esencial que proporciona a la sociedad, y las capacidades necesarias para mantenerlo.

2. Comprender la importancia de las interdependencias.

Una entidad puede conocer perfectamente sus propias vulnerabilidades y, sin embargo, desconocer suficientemente aquellas derivadas de terceros. Electricidad, telecomunicaciones, agua, transporte, tecnologías digitales y cadenas de suministro forman hoy redes de dependencia extraordinariamente complejas con impactos sistémicos en otros sectores, si uno de sus servicios falla.

3. Adoptar un enfoque multirriesgo.

La Directiva CER consagra precisamente un marco frente a todo tipo de riesgos, naturales y provocados por el ser hu-

mano, accidentales o intencionados, y esto obliga a superar los análisis compartimentados actuales. El escenario más exigente puede derivar no de una única amenaza, sino de la coincidencia o concatenación de varias, donde las amenazas híbridas cobran un especial sentido.

4. Integración de la seguridad.

Las directivas CER y NIS2 ofrecen una expresión jurídica de algo que operacionalmente ya era evidente: la separación entre ambos mundos ha perdido sentido. Por esto, precisamente, un programa de resiliencia energética debe integrar seguridad física, ciberseguridad, seguridad interna, continuidad del negocio, gestión de crisis, protección de las personas y recuperación, es decir, disponer de una visión mucho más amplia que la se venía adoptando en términos de seguridad.

5. Cooperar antes para gestionar la crisis con solvencia.

La cooperación público-privada no puede improvisarse cuando sucede un incidente, sino que debe construirse previamente mediante intercambio de información, ejercicios, procedimientos conocidos, relaciones de confianza y una clara definición de responsabilidades.

Este es, precisamente, uno de los principales valores de la experiencia desarrollada durante años por el sistema español de protección de infraestructuras críticas.

Por último, y a pesar de toda esta evolución, hay que señalar **que el objetivo último permanece inalterable**, proteger aquello que permite que nuestra sociedad funcione, con la única diferencia que hoy sabemos que proteger ya no consiste únicamente en levantar “barreras” frente a una amenaza, sino que significa también anticiparse, prepararse, resistir, adaptarse y recuperar cuanto antes la normalidad.



84
Septiembre
2026

GARRIGUES



**Club Español
de la Energía**

Deloitte.

Hermosilla, 3
28001 Madrid
Tel. 91 514 5200
Fax. 91 399 2408
www.garrigues.com

Paseo de la Castellana, 257, 1ª Planta
28046 Madrid
Tel. 91 323 7221
Fax. 91 323 0389
www.enerclub.es

Plaza Pablo Ruiz Picasso, 1
Torre Picasso. 28020 Madrid
Tel. 91 514 5000
Fax. 91 514 5180
www.deloitte.es