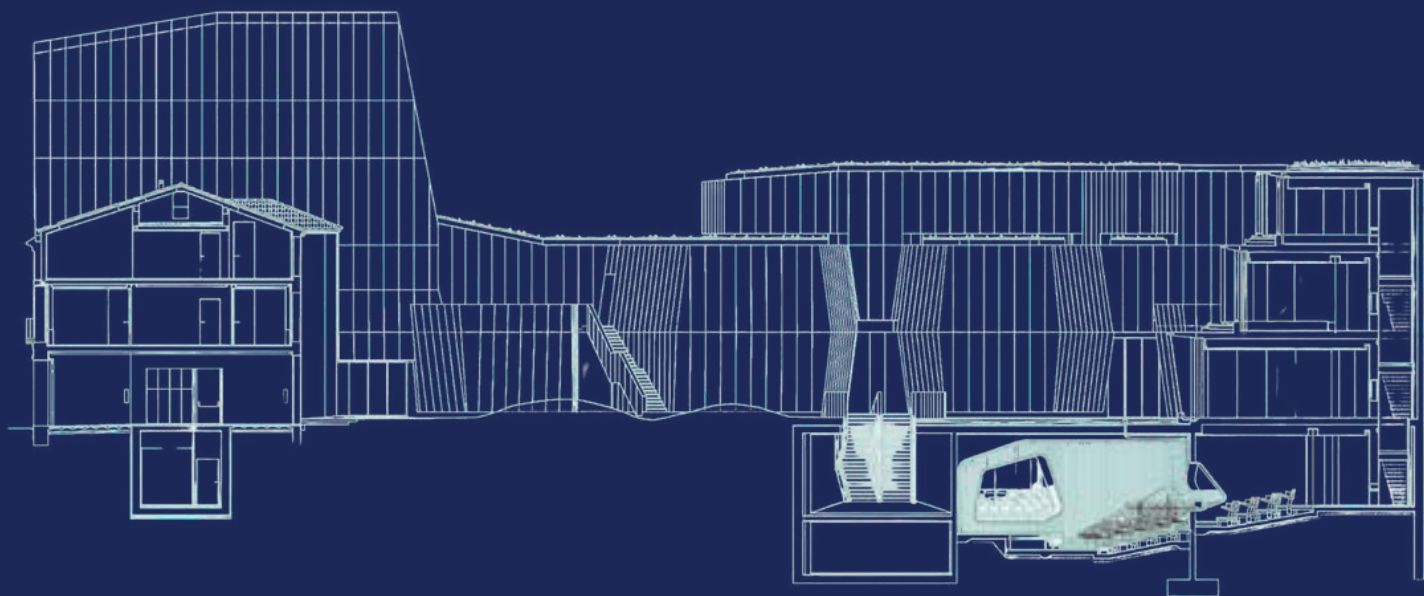


III Foro #WholesaleSpain

Resiliencia y futuro en las infraestructuras digitales



La disponibilidad infinita



El apagón ibérico demostró la dependencia crítica de nuestra sociedad respecto a las infraestructuras digitales y la fragilidad de su resiliencia.

Durante el evento, las redes fijas dejaron de cursar tráfico en minutos y las estaciones base móviles fueron apagándose a medida que agotaban sus baterías.

La situación replicó un suceso previo en Chile, donde el regulador Subtel documentó el proceso con datos públicos y reportes en tiempo real. España, en cambio, carecía de mecanismos equivalentes de comunicación y gestión coordinada¹.

Catástrofes naturales, sabotajes y ciberataques recientes - desde los cortes de cables submarinos en el Mar Rojo hasta ataques a aeropuertos europeos - evidencian que la resiliencia digital es hoy un asunto de interés público y estratégico.

Este documento propone repensar el concepto desde una perspectiva sistémica y colaborativa, tomando como base los debates del **III Foro #WholesaleSpain**.

El 28 de abril de 2025, una interrupción del suministro eléctrico dejó sin luz a más de 50 millones de personas en España, Portugal y el sur de Francia.





Resiliencia digital: un concepto multidimensional

Hablar de resiliencia en el ámbito digital implica algo más que disponer de redundancia técnica. Significa asegurar la continuidad, adaptabilidad y confianza de los servicios esenciales sobre los que se apoya la sociedad. Hay tres dimensiones que son inseparables:

Técnica

Resistencia a fallos físicos o cibernéticos, recuperación rápida, redundancia de red y suministro energético seguro.

Económica

Sostenibilidad del modelo de negocio para mantener inversiones en seguridad, mantenimiento y modernización.

Social y geoestratégica

Soberanía digital, colaboración entre actores públicos y privados, y equidad territorial.



La Ley General de Telecomunicaciones (2022) ya incorporó el mandato de reforzar la seguridad y la resiliencia de las redes, y el Ministerio para la Transformación Digital y la Función Pública ha lanzado en 2025 una consulta pública específica para desarrollar ese marco².

A nivel europeo, la ENISA (European Union Agency for Cybersecurity) ha identificado la infraestructura digital como el tercer sector más atacado por actores maliciosos, detrás de la administración pública y la sanidad³.

Un diagnóstico necesario: vulnerabilidades y tensiones del sistema

Las infraestructuras digitales europeas demostraron gran robustez durante la pandemia de 2019, pero el contexto actual – marcado por la consolidación industrial y la presión sobre costes – ha alterado los equilibrios.

Entre las palancas de eficiencia adoptadas por el sector (compartición de redes, apagado de tecnologías legacy, migración a la nube, concentración de proveedores, externalización de servicios) requieren nuevos equilibrios en torno a la resiliencia. Podrían reducir redundancias y crean dependencias cruzadas difíciles de gestionar en situaciones de crisis.

Incluso el marco de datos del que disponemos para medir y entender el impacto es muy limitado. Algunos datos que nos permiten contextualizar esta evolución pueden encontrarse a continuación:

- La tasa media de disponibilidad de los servicios fijos y móviles se mantiene por encima del 99,9%, según los indicadores de Calidad de Servicio de la CNMC (último informe 2024)⁴. No obstante los informes trimestrales de calidad de servicio si registran un impacto claro en el número de avisos de avería para redes fijas en el 4 trimestre del 24 y el segundo del 25 asociados, según el propio informe a la DANA y al apagón. Para algunos operadores la tasa se multiplica más que por 8.
- La duración media de las interrupciones registradas aumentó un 7% entre 2022 y 2024, con un tiempo medio de restauración de 4,8 horas.
- El capex sectorial total (telecomunicaciones fijas y móviles) se ha estabilizado en torno a los 6.000 millones de euros anuales.
- Las zonas rurales presentan una cobertura NGA del 74%, frente al 98% urbano (Informe de Cobertura de Banda Ancha 2024⁶).

Durante el apagón Ibérico el tráfico IP en España se redujo en más de 80% (un 90% para algunos operadores), por debajo de los mínimos nocturnos.


En ese mismo día, según Ookla más del 30% de los clientes de algún operador se quedaron sin ningún tipo de cobertura móvil, frente a los valores prácticamente inapreciables de un período normal.

Estos datos apuntan a una brecha de resiliencia territorial y estructural: aunque las redes mantienen niveles de disponibilidad altos, la falta de inversión diferencial y redundancia geográfica podría amplificar el impacto de eventos extremos.

La visión de la industria: cuatro aproximaciones complementarias

- * **Infraestructuras críticas y soberanía:** los cables submarinos, que transportan más del 95% del tráfico internacional, son vulnerables tanto física como geopolíticamente. Europa necesita diversificar rutas y reforzar mecanismos de protección física y ciberseguridad. Sin embargo, los requisitos de independencia geostratégica podrían estar ya encareciendo la tecnología y su despliegue, remarcando la necesidad de encontrar nuevos equilibrios.
- * **Resiliencia operativa:** en redes de radiodifusión y torres compartidas, la continuidad depende de la gestión coordinada de clientes y servicios, y de protocolos unificados ante incidencias. Si se debe extender el nivel de baterías en los emplazamientos de redes móviles surgen de nuevo contradicciones: más allá del evidente coste de las mismas, es dudoso que exista la capacidad para fabricarlas en un plazo breve o incluso de ubicarlas en las estaciones base más críticas que disponen de poco espacio y muchas dificultades para crecer.
- * **Resiliencia tecnológica:** la disponibilidad energética y las conexiones multi-proveedor son claves en los centros de datos, son el nuevo núcleo de la resiliencia digital. Estos elementos altamente redundados por diseño forma parte de una cadena mucho mayor en la que cada eslabón cuenta.
- * **Resiliencia territorial:** las redes rurales contribuyen a la cohesión nacional y actúan como respaldo en situaciones de emergencia. La descentralización de infraestructura aumenta la capacidad de recuperación. Las redes de “larga distancia” o backhaul son elementos claves para la resiliencia, más aún en entornos rurales.

CADA VISIÓN APORTA UNA PIEZA DISTINTA AL MISMO RETO: CONVERTIR LA INTERDEPENDENCIA EN FORTALEZA, NO EN FRAGILIDAD.



Gobernanza y regulación: del cumplimiento a la colaboración

La regulación sobre resiliencia se expande en Europa, pero su eficacia depende del equilibrio entre exigencia y cooperación.

*

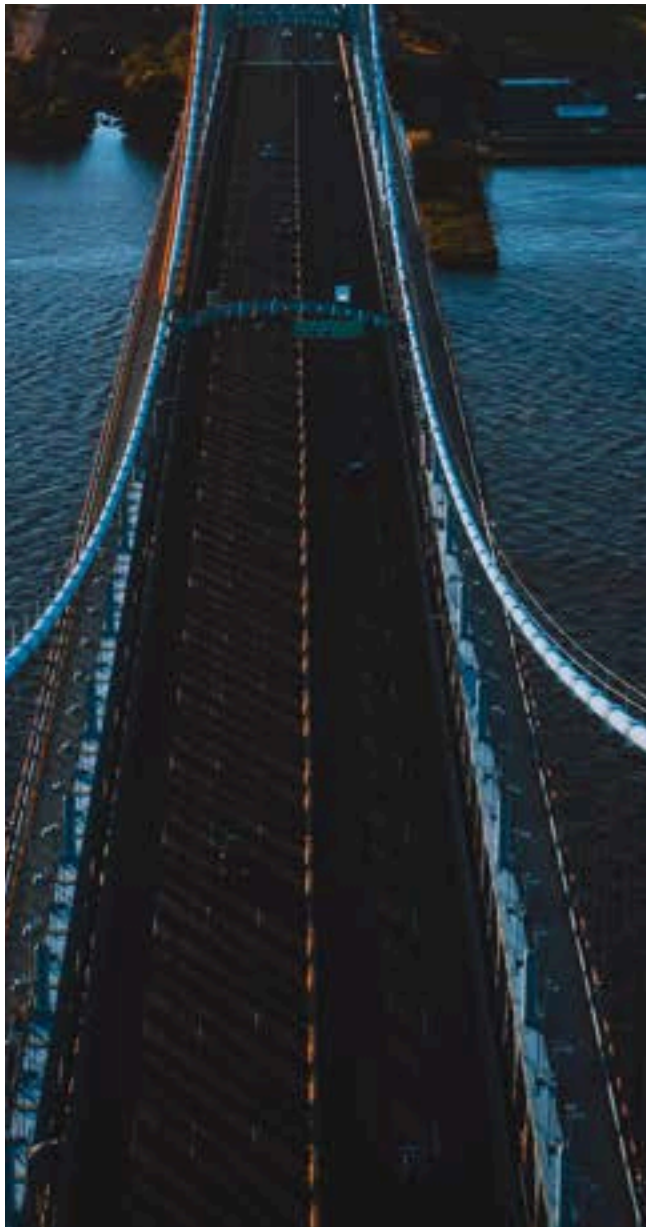
El ****Ofcom Resilience Framework (UK, 2024)**⁷** estimó que dotar de baterías adicionales a las estaciones base del país costaría alrededor de 1.000 millones de libras. Este ejemplo ilustra la magnitud del esfuerzo que supone “blindar” infraestructuras críticas.

Sin embargo, reforzar la resiliencia no puede depender solo de obligaciones regulatorias. Experiencias como el roaming nacional de emergencia - ya operativo en Chile o Finlandia - muestran que la colaboración entre operadores puede mejorar la disponibilidad sin requerir inversiones masivas. Durante el apagón ibérico, los usuarios en roaming experimentaron mejor conectividad al poder usar la red más funcional en cada momento.

España podría incorporar en su futura norma un sistema de cooperación y priorización nacional para tráfico de emergencia, y un reporting coordinado de incidentes al estilo del UK Communications Resilience Group.

Hacia un marco sistémico de resiliencia

El reto no consiste solo en reforzar la infraestructura existente, sino en diseñar una arquitectura institucional que incentive la resiliencia.



NIVEL DE OPERADOR:

1. Planes de continuidad y simulacros conjuntos.
2. Redes de emergencia y priorización de tráfico esencial.
3. Evaluaciones periódicas de riesgo integradas en el diseño.

NIVEL DE ECOSISTEMA:

1. Mecanismos de roaming nacional de emergencia.
2. Protocolos de ayuda mutua entre operadores y proveedores energéticos.
3. Centros de coordinación intersectoriales para incidentes digitales.

NIVEL DE POLÍTICA PÚBLICA:

1. Incentivos fiscales o de inversión en redundancia y seguridad.
2. Inclusión de indicadores de resiliencia en los informes de CNMC y ENISA.
3. Estrategia nacional de comunicación de crisis digitales, con información transparente para la ciudadanía.

Una posible evolución sería crear un Índice Nacional de Resiliencia Digital, compuesto por cinco métricas:

disponibilidad, redundancia, tiempo de recuperación, cobertura equitativa y cooperación institucional.

Este índice permitiría comparar avances año a año y serviría de referencia en Europa.

Fuentes y referencias

¹ Subtel Chile. “Informe sobre eventos de interrupción de servicios y medidas de resiliencia” (2024).

² Ministerio para la Transformación Digital y de la Función Pública (España). Consulta pública sobre seguridad y resiliencia de redes y servicios (2025).

³ ENISA. Threat Landscape Report 2024 — Infrastructure under attack. Disponible en <https://www.enisa.europa.eu>

⁴ CNMC. Indicadores de Calidad de Servicio – Informes trimestrales 2022–2024. Dataset: “Interrupciones y disponibilidad de servicios electrónicos”.

⁵ CNMC. Panel de Hogares. Volumen de tráfico IP por tipo de acceso y dispositivo (2022–2024).

⁶ CNMC & Secretaría de Estado de Telecomunicaciones. Informe de Cobertura de Banda Ancha 2024.

⁷ Ofcom. Resilience and Emergency Planning Framework (Londres, 2024).

THERE IS
A LIGHT
THAT NEVER
GOES OUT

CONCLUSIONES: UNA LUZ QUE NUNCA SE APAGA

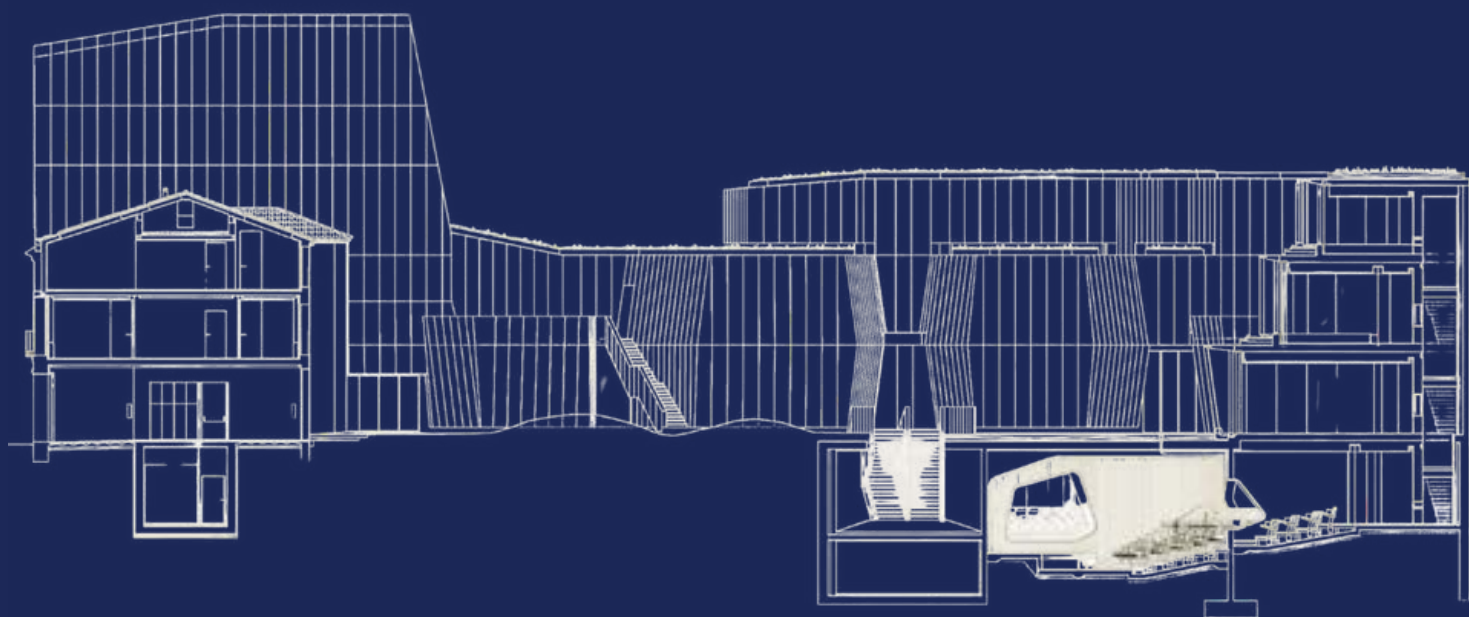
El futuro de las redes pasa por integrar la resiliencia en el corazón del modelo de negocio y de la política pública. No como un coste, sino como una inversión en confianza, estabilidad y competitividad, sin olvidarnos de los equipos humanos que las gestionan. Una vez más es necesaria una regulación efectiva y eficiente, que dote de un marco general en donde prime la cooperación versus el detalle normativo en donde la colaboración público-privada sea el pilar que vertebre los próximos años

* La resiliencia no es solo un atributo técnico: es una forma de cooperación.

* De su fortalecimiento dependerá que, como en el título de la canción, nuestras redes sigan siendo una luz que nunca se apaga.

“La resiliencia es ya un eje transformador para las infraestructuras digitales que debe ser abordado no solo desde una perspectiva tecnológica, sino también económica, social, regulatoria y geopolítica”

Gracias



Joaquín Guerrero

joaquin.guerrero@nae.global

[in /jguerrer/](#)

[Website Nae](#)

Icíar Martínez

iciar.martinez@onivia.net

[in /iciar-martinez/](#)

[Website Onivia](#)