



La seguridad tecnológica exige conexiones físicamente independientes y autonomía en la toma de decisiones y en la priorización estratégica



Los satélites pueden mantener las comunicaciones prioritarias durante una crisis, aunque su capacidad limitada obliga a tratarlos como una solución de respaldo



La independencia física de las conexiones y la capacidad de mantener funciones críticas influirán cada vez más en el seguro, la financiación y la valoración de los activos digitales

DE CABLES A SATÉLITES: LA BATALLA DE EUROPA POR LA RESILIENCIA DIGITAL

Raúl VIÑAS ABADÍA

Afi

Los cables submarinos transportan la inmensa mayoría del tráfico intercontinental de internet, pero su vulnerabilidad física y las crecientes tensiones geopolíticas ponen en riesgo la conectividad global. Europa es especialmente vulnerable por su dependencia de proveedores externos para la capacidad, el mantenimiento y el respaldo satelital. Reforzar su resiliencia exige diversificar proveedores y rutas, mejorar la capacidad de reparación y garantizar el control sobre las alternativas disponibles en caso de crisis. Los satélites pueden mantener los servicios críticos durante una interrupción, pero no sustituir a gran escala a la fibra óptica. La conectividad física adquiere así una importancia económica creciente, a medida que las entidades financieras y los inversores la incorporan a sus evaluaciones de riesgos y activos estratégicos.

Introducción

La soberanía digital europea descansa sobre una infraestructura física vulnerable y, en buena medida, sobre proveedores extranjeros que aportan capacidad, mantenimiento y respaldo satelital. Esta combinación convierte la conectividad en una cuestión de control estratégico: multiplicar el número de conexiones no garantiza la continuidad operativa si Europa carece de capacidad para redirigir el tráfico y restablecer el servicio durante una crisis.

Muchas aplicaciones que un usuario europeo percibe como globales se sirven desde centros de datos situados en Europa, aunque el proveedor sea estadounidense. Además, los grandes operadores replican datos y cargas críticas en varias regiones para reducir su exposición a fallos físicos. Esa redundancia amortigua el impacto de averías aisladas, pero no elimina la dependencia de las rutas intercontinentales

La evaluación de riesgos de la Comisión Europea para 2025 estima que los hiperescaladores estadounidenses concentran en torno al 90 % de la capacidad entre Estados Unidos y Europa, y prevé que su influencia siga creciendo en otras regiones

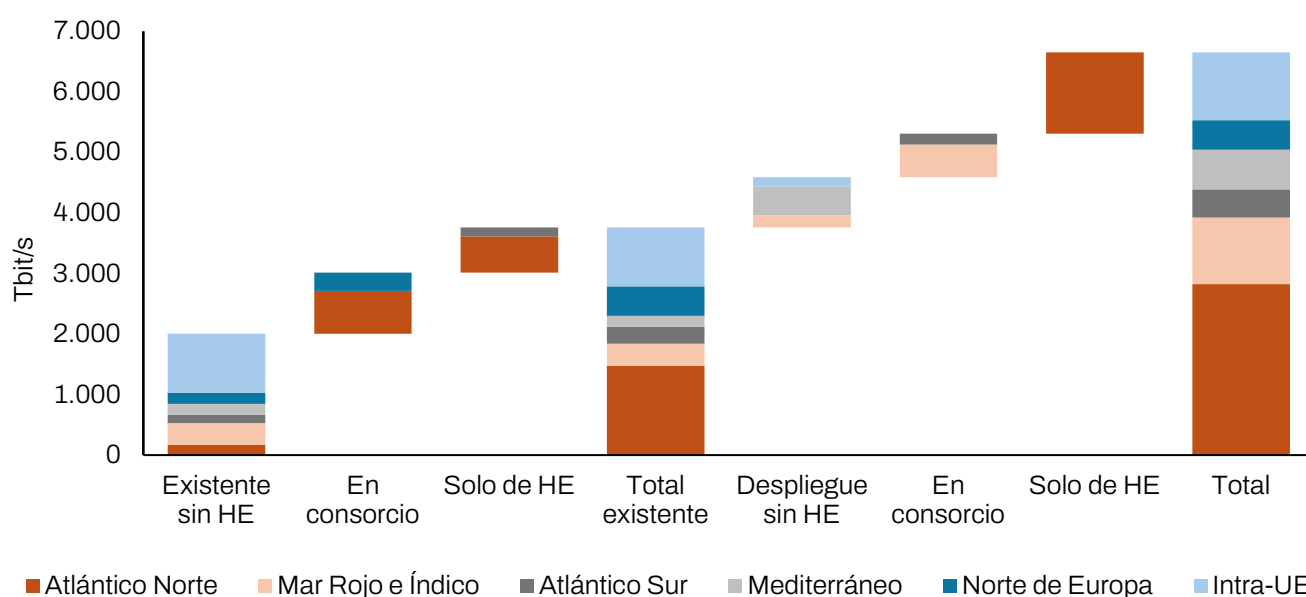
ni del control operativo sobre ellas. Los cables submarinos son decisivos cuando el tráfico cruza océanos: sincronización entre centros de datos, acceso a copias alojadas fuera de Europa, operaciones financieras internacionales, ciberseguridad, telemetría, tráfico entre nubes y comunicaciones empresariales globales.

Más del 99 % del tráfico internacional de datos que cruza océanos viaja por cables submarinos, esenciales para la expansión de la inteligencia artificial, los servicios financieros digitales y la ciberseguridad. [Su exposición física añade un riesgo de “zona gris”, ya que los daños deliberados pueden camuflarse entre las cerca de 200 averías anuales de la red mundial, el 80 % de ellas causadas por la pesca o el fondeo¹](#). Los incidentes registrados en el Báltico en los últimos años han reforzado la idea de que la seguridad depende de mantener la capacidad de respuesta cuando una ruta deja de funcionar.

Conectividad europea, control exterior

Los hiperescaladores estadounidenses han transformado la infraestructura submarina al financiar cables que conectan directamente sus centros de datos y plataformas. [La evaluación de riesgos de la Comisión Europea para 2025 estima que estas empresas concentran alrededor del 90 % de la capacidad entre Estados Unidos y Europa, y prevé que su peso siga creciendo en otras regiones²](#). Esta inversión privada permite ampliar la capacidad con rapidez y responde a una lógica operativa clara: los hiperescaladores conectan sus propios centros de datos para reducir la latencia, asegurar la disponibilidad y controlar mejor sus servicios. La vulnerabilidad europea surge cuando esa capacidad intercontinental, la nube, la priorización del tráfico y parte de las alternativas de continuidad dependen de un ecosistema empresarial muy concentrado y mayoritariamente estadounidense.

Figura 1 - Capacidad de cables submarinos conectada a la UE por región y participación de los hiperescaladores (HE), 2025

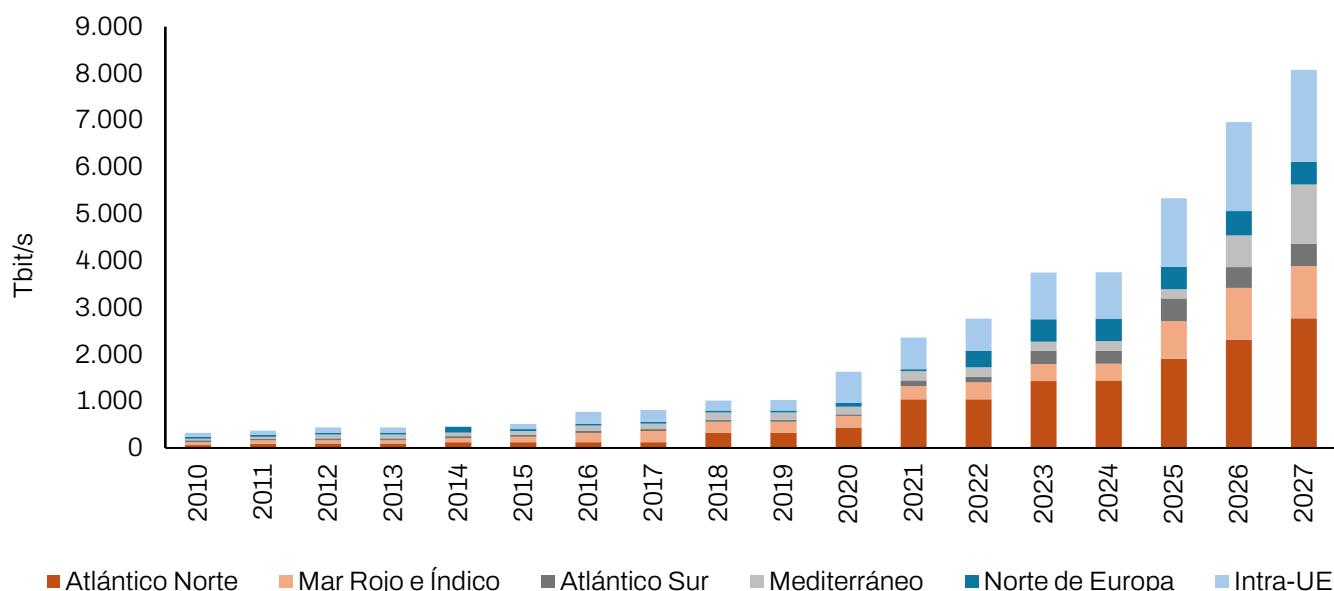


Fuente: Elaboración propia a partir de Comisión Europea (2025), Seguridad y resiliencia de las infraestructuras de cables submarinos de la UE: mapeo, evaluaciones de riesgo y pruebas de resistencia.

Para Europa, esta concentración afecta sobre todo a la autonomía de decisión y a la posibilidad de sustituir capacidades críticas durante una crisis. Ante una interrupción grave, la UE podría depender de intereses externos para restablecer el tráfico de datos o de que otros prioricen los incidentes según sus propias necesidades operativas. Por ello, la diversificación de la red europea no debe medirse por el número de cables, sino por el grado de concentración de proveedores, de servicios de mantenimiento y de alineamientos geopolíticos.

Las empresas chinas tienen menos peso directo en la capacidad transatlántica y están menos integradas en el ecosistema digital europeo, pero han ganado mucha presencia en la fabricación y el despliegue de sistemas submarinos, así como en proyectos de terceros países clave para la UE. En este contexto, la respuesta europea empieza a trasladarse a la política industrial. [A finales de 2024, Francia compró el 80 % de Alcatel Submarine Networks, una de las pocas compañías del mundo capaces de diseñar, instalar y mantener sistemas submarinos completos, que había desplegado ya más de 750.000 kilómetros de cable³](#). La operación no resuelve la dependencia europea, pero preserva la capacidad industrial para diseñar, tender y reparar sistemas submarinos sin depender por completo de proveedores externos.

Figura 2 - Capacidad de los cables submarinos que llegan al menos a un Estado miembro de la UE (2010-2027)



Fuente: Analysys Mason.

Recuperar el servicio antes de que la interrupción se agrave

[Los datos de la Unión Internacional de Telecomunicaciones \(UIT\) muestran que el tiempo medio mundial para iniciar una reparación pasó de menos de 20 días en 2012 a más de 50 en 2024, pese a que el número de reparaciones y de buques disponibles se mantuvo relativamente estable⁴](#). Los permisos y las restricciones operativas explican una parte importante de ese deterioro. Las diferencias entre regiones son considerables: el Reino Unido, por ejemplo, inicia las reparaciones en unos ocho días

de media porque parte de los permisos marítimos, medioambientales y de acceso a zonas costeras se tramitan antes del incidente. En estos casos, el retraso no depende solo de que haya un buque disponible, sino también de que pueda operar legalmente y con rapidez en el punto de avería. Una mayor atención política a estas infraestructuras debería contribuir a extender este tipo de procedimientos y a reducir parte de los retrasos administrativos, aunque persistirán límites más difíciles de abordar, como la disponibilidad de buques especializados, las condiciones marítimas o la distancia hasta el punto de avería.

Europa parte de una posición comparativamente favorable en disponibilidad de buques. Según la evaluación de la Comisión, entre 2022 y 2024 solo alrededor del 2-3 % de los incidentes europeos sufrieron retrasos porque el buque necesario estaba ocupado en otra reparación. Esa ventaja puede erosionarse si aumentan los cortes simultáneos y la demanda sobre una flota muy especializada. Una campaña deliberada podría buscar precisamente esa saturación y convertir una capacidad suficiente en condiciones normales en un cuello de botella.

[La Comisión ha reservado 347 millones de euros en 2026 para reforzar la seguridad de los cables, con financiación para proyectos estratégicos, monitorización y módulos de reparación desplegados desde puertos europeos⁵](#). La primera fase prioriza el Báltico y prevé extender esa capacidad al Mediterráneo y al Atlántico. El cambio de enfoque es relevante porque traslada acertadamente parte de la respuesta desde la gestión de la emergencia hacia la preparación previa al incidente.

El satélite compra tiempo; la fibra transporta el volumen

Las constelaciones de órbita baja (LEO) pueden mantener una conectividad esencial durante una emergencia, pero no tienen capacidad para absorber el volumen que transportan los cables submarinos. La capacidad agregada de una red de satélites es muy inferior a la de los grandes sistemas de fibra y, además, debe repartirse entre usuarios y territorios muy dispersos. Aunque los satélites LEO han reducido considerablemente la latencia, su rendimiento empeora con las variaciones de congestión y cobertura, así como durante los cambios de enlace entre satélites. Por último, siguen necesitando infraestructura terrestre para conectar el tráfico con centros de datos y redes locales, por lo que no eliminan por completo los puntos físicos de fallo. Si varios cables de gran capacidad quedaran fuera de servicio al mismo tiempo, la red orbital permitiría sostener funciones prioritarias, pero no absorbería el tráfico perdido.

La utilidad económica del respaldo satelital será mayor en los servicios en los que una interrupción breve pueda tener efectos desproporcionados. En el sector financiero, mantener operativos determinados sistemas de pagos, comunicaciones críticas o accesos a infraestructuras remotas puede bastar para mitigar parte del impacto mientras se recupera la conectividad submarina. Esto convierte a las constelaciones satelitales en una capa de continuidad selectiva, cuya importancia crecerá a medida que aumente la dependencia de los servicios digitales y se reduzca la tolerancia a interrupciones prolongadas.

Las constelaciones de órbita baja (LEO) pueden mantener conectividad esencial durante una emergencia, pero no tienen capacidad para absorber el volumen que transportan los cables submarinos

La valoración de activos digitales incorporará previsiblemente esta dimensión a medida que aumenten la concentración tecnológica y la exposición geopolítica

Esta nueva capa de resiliencia introduce, sin embargo, otra concentración estratégica. Si buena parte de la capacidad orbital disponible depende de unas pocas constelaciones privadas, como Starlink, la diversificación tecnológica puede seguir descansando en un número reducido de operadores y jurisdicciones. [Ucrania ya lo ha experimentado: en 2022, SpaceX se negó a activar la cobertura de Starlink cerca de Crimea que requería un ataque ucraniano, conforme a criterios propios de la compañía⁶](#). [Europa intenta reducir esa dependencia con IRIS²⁷](#) (Infraestructura de resiliencia, interconectividad y seguridad por satélite de la UE), un proyecto que ha cobrado impulso en 2026 con el inicio de su despliegue a gran escala, aunque sus primeros servicios no llegarán hasta finales de la década.

De la conectividad al riesgo financiero

[DORAⁱ obliga a bancos, aseguradoras y otras entidades financieras europeas a identificar dependencias tecnológicas críticas, evaluar concentraciones en terceros y preparar mecanismos de continuidad y recuperación⁸](#). En este marco, conviene tener en cuenta que el deterioro de las conexiones con centros de datos, sistemas de pagos o infraestructuras de mercado puede obligar a recurrir a capacidad alternativa y retrasar operaciones. También puede tener efectos financieros sin llegar a una interrupción total: pagos más lentos, retrasos en la conciliación de operaciones, menor acceso a datos de mercado, dificultades en las llamadas de margen o problemas en funciones alojadas en la nube. En los sistemas de pagos, una interrupción que provoque la acumulación de órdenes pendientes aumenta la presión sobre la liquidación y la liquidez intradía cuando se recupera el servicio. [El BCE ha advertido, además, de que una entidad bien capitalizada puede afrontar problemas graves si pierde funciones críticas durante un shock operativo⁹](#).

El perfil de riesgo de un centro de datos puede variar significativamente según la independencia física de sus conexiones, el acceso previamente acordado a servicios de reparación y la capacidad de respaldo disponible para mantener funciones críticas. A medida que estas diferencias sean más visibles, es razonable que influyan también en el coste del seguro, en la financiación o en las exigencias de los inversores. Un activo que dependa de rutas concentradas, de proveedores externos poco sustituibles o de tiempos de reparación inciertos presentará un perfil distinto al de otro con alternativas contratadas de antemano y mayor claridad sobre sus puntos físicos de fallo. Esta evolución sería coherente con el énfasis que DORA y los marcos de resiliencia bancaria ya ponen en las dependencias críticas y en la continuidad ante disrupciones graves.

Durante los próximos cinco años, supervisores y aseguradoras podrían exigir más información sobre el recorrido físico de las conexiones y el tiempo necesario para restablecerlas. El cambio empezaría a ser visible cuando los ejercicios de resiliencia comenzaran a distinguir entre rutas realmente independientes y enlaces que comparten corredores vulnerables. Los contratos podrían incorporar progresivamente capacidad de reparación reservada y respaldo satelital para funciones prioritarias. Hacia mediados

i. Digital Operational Resilience Act, el Reglamento de Resiliencia Operativa Digital de la UE.

de la próxima década, los activos incapaces de acreditar estas garantías podrían afrontar primas más elevadas y peores condiciones de financiación. La señal decisiva para Europa será la velocidad con la que las inversiones en módulos de reparación e IRIS² aporten capacidad disponible durante una crisis. Si la infraestructura aumenta mientras el control operativo sigue concentrado, la autonomía avanzará mucho menos de lo que sugieren las cifras de capacidad. **FI**

Referencias

1. International Telecommunication Union (ITU) (2026). International Advisory Body on Submarine Cable Resilience – Report of the Working Groups 2026. <https://www.itu.int/hub/publication/s-iab-wg-2026/>
2. European Commission, Submarine Cable Infrastructures Expert Group (2025). Security and Resilience of EU Submarine Cable Infrastructures – Mapping, Risk Assessments, Stress Tests. <https://digital-strategy.ec.europa.eu/en/library/report-security-and-resilience-eu-submarine-cable-infrastructures>
3. Nokia (2025). Nokia completes its sale of its leading submarine networks business, ASN (Alcatel Submarine Networks), to the French State. <https://www.nokia.com/newsroom/nokia-completes-its-sale-of-leading-submarine-networks-business-asn-alcatel-submarine-networks-to-the-french-state/>
4. International Telecommunication Union (ITU) (2026). International Advisory Body on Submarine Cable Resilience – Report of the Working Groups 2026. <https://www.itu.int/hub/publication/s-iab-wg-2026/>
5. European Commission (2026). Commission boosts submarine cable security with a €347 million investment and a new toolkit. <https://digital-strategy.ec.europa.eu/en/news/commission-increases-submarine-cable-security-eu347-million-investment-and-new-toolbox>
6. Associated Press (2023). Elon Musk's refusal to have Starlink support Ukraine's attack in Crimea raises questions for the Pentagon. <https://apnews.com/article/fde93d9a69d7dbd1326022ecfdb53c2>
7. European Space Agency (ESA) (2026). IRIS² reinforced and accelerated as implementation advances. https://www.esa.int/Applications/Connectivity_and_Secure_Communications/IRIS2_reinforced_and_accelerated_as_implementation_advances
8. European Union (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (Digital Operational Resilience Act, DORA). <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>
9. European Central Bank (2026). Elderson, F., 'Strengthening operational resilience for the age of AI'. Keynote speech at the Goldman Sachs European Financials Conference 2026, Zurich, 3 June 2026. <https://www.ecb.europa.eu/press/key/date/2026/html/ecb.sp260603~5b8e67f237.en.html>