

07

Pedro Cuadros-Solas

CUNEF Universidad y Funcas

Nuria Suárez

Universidad Autónoma de Madrid y Funcas



Ciberriesgo y resiliencia operativa en banca: el papel de la inteligencia artificial

Este artículo analiza la exposición del sector bancario europeo al ciberriesgo, sus implicaciones para la resiliencia operativa y el papel que puede desempeñar la inteligencia artificial (IA) para mitigar o amplificar esta fuente de riesgo operacional. A partir de datos de EuRepoC y de la Autoridad Bancaria Europea (EBA), se muestra que los bancos concentran una parte sustancial de los ciberataques registrados en el sector financiero europeo y que el riesgo cibernético constituye su principal preocupación operacional. Aunque la proporción de entidades que declara haber sufrido ataques recientes se ha reducido, las pérdidas materializadas por cibereventos han aumentado. La IA puede reforzar la detección de vulnerabilidades y la respuesta defensiva, pero también facilitar ataques más rápidos, automatizados y sofisticados.

Ciberriesgo, resiliencia operativa e IA

La digitalización está transformando profundamente la actividad bancaria. Una proporción creciente de las operaciones tiene lugar a través de canales digitales. Los pagos se procesan en tiempo real, los empleados acceden a aplicaciones y datos desde múltiples entornos y las entidades dependen de redes complejas de proveedores de servicios tecnológicos, infraestructuras de mercado y plataformas en la nube. Ciertamente, esta transformación permite reducir costes, mejorar la experiencia del cliente y ampliar la oferta de servicios, pero también incrementa la superficie susceptible de sufrir fallos o ataques.

El ciberriesgo ha dejado de ser una cuestión meramente técnica para convertirse en una fuente central de riesgo operacional. Un incidente puede impedir el acceso de los clientes a sus cuentas, interrumpir pagos, comprometer información confidencial, alterar la integridad de los datos o facilitar operaciones fraudulentas. La resiliencia operativa, por tanto, no consiste únicamente en impedir que se produzcan incidentes. Supone identificar funciones críticas, anticipar escenarios adversos, contener el impacto de una perturbación y recuperar el servicio. Por ello, el Reglamento de Resiliencia Operativa Digital (DORA), aplicable desde el 17 de enero de 2025, refuerza la gestión del riesgo tecnológico, la notificación de incidentes, las pruebas de resistencia y el control de los proveedores tecnológicos externos (Unión Europea, 2022).

Las herramientas basadas en IA pueden mejorar la detección de anomalías, analizar grandes volúmenes de alertas, identificar vulnerabilidades y acelerar la respuesta de las entidades ante incidentes. Sin embargo, esas mismas capacidades también pueden ser utilizadas por actores maliciosos. La EBA considera que el rápido

desarrollo de modelos de IA de frontera puede amplificar los riesgos operacionales y cibernéticos mediante el uso malicioso de herramientas basadas en IA.

El objetivo de este artículo es analizar la relevancia del ciberriesgo para la banca europea y su relación con la resiliencia operativa. En primer lugar, se estudia la posición de los bancos como objetivo de los ciberataques dirigidos al sector financiero. A continuación, se examinan la percepción del riesgo operacional y la evolución reciente de los ataques sufridos por las entidades. Finalmente, se analiza el doble papel de la IA como herramienta defensiva y como posible amplificador de las amenazas.

El sector bancario en el punto de mira de los ciberdelincuentes

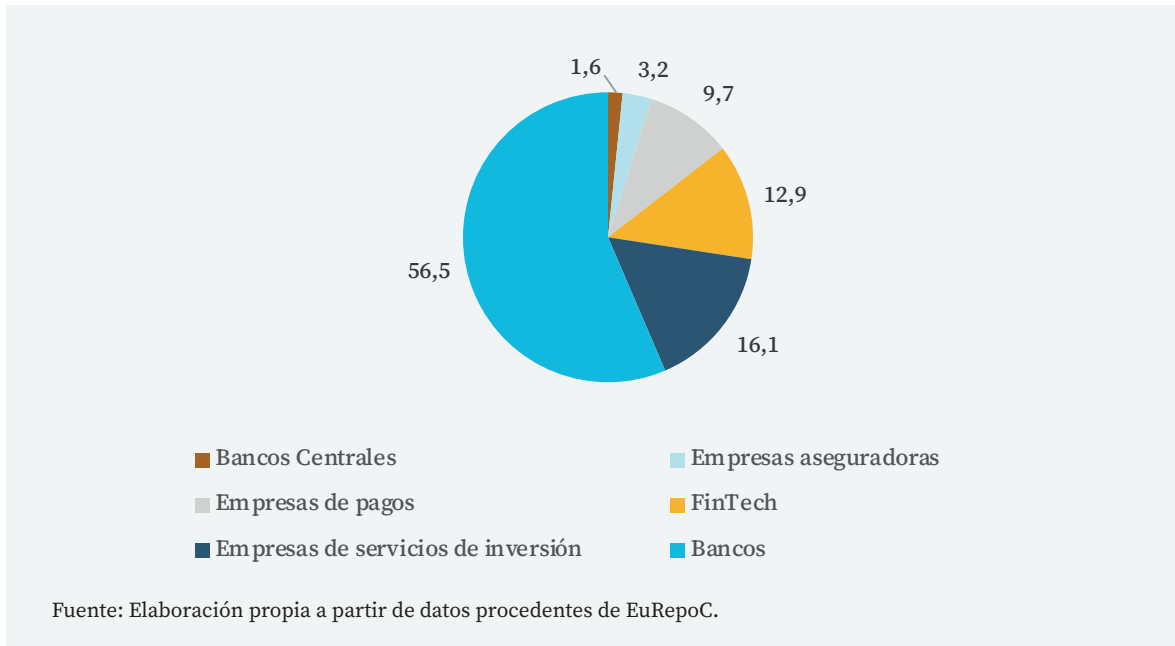
Los bancos constituyen un objetivo especialmente atractivo para los ciberdelincuentes. Gestionan dinero, datos personales y credenciales, desempeñan una función central en los sistemas de pagos, mantienen conexiones con numerosos clientes, empresas, administraciones y proveedores y prestan servicios cuya interrupción es inmediatamente visible. Un ciberataque podría producir simultáneamente un beneficio económico para el atacante, un elevado coste para la entidad y un efecto reputacional significativo.

El gráfico 1 muestra la distribución de los ciberataques registrados en el sector financiero europeo a partir de la información de EuRepoC. Los bancos concentran el 56,5 % del total. A considerable distancia aparecen las empresas de servicios de inversión (16,1 %); las fintech (12,9 %); y las empresas de pagos (9,7 %). Las aseguradoras representan el 3,2 % y los bancos centrales el 1,6 %.

Gráfico 1

Distribución de ciberataques en el sector financiero europeo

Porcentajes



El acceso ilegítimo a una cuenta o a las credenciales de un empleado puede facilitar transferencias, fraude o extorsión. La banca opera sobre infraestructuras digitales de gran escala, con un elevado número de usuarios y conexiones, por lo que, cuantos más puntos de acceso, aplicaciones, interfaces y proveedores intervienen en la prestación del servicio, mayor es la superficie potencial de ataque. La necesidad de operar de manera casi ininterrumpida aumenta el coste de los ataques a la disponibilidad, como los de denegación de servicio o el *ransomware*.

La subcontratación de servicios, el uso de *software* común, la computación en la nube y la conexión con infraestructuras de pagos crean dependencias compartidas. Un fallo o ataque a un proveedor puede transmitirse a varias entidades al mismo tiempo. El primer informe anual europeo de incidentes tecnológicos graves bajo DORA

contabilizó 3.383 incidentes en 2025 en el conjunto del sector financiero europeo, alrededor de un tercio con impacto transfronterizo. Los fallos de sistemas y los eventos externos fueron los principales desencadenantes, y cerca de un tercio tuvo su origen en fallos de terceros. La resiliencia digital exige, por tanto, abordar tanto los ataques maliciosos como los fallos tecnológicos y las dependencias del ecosistema (Autoridades Europeas de Supervisión, 2026a).

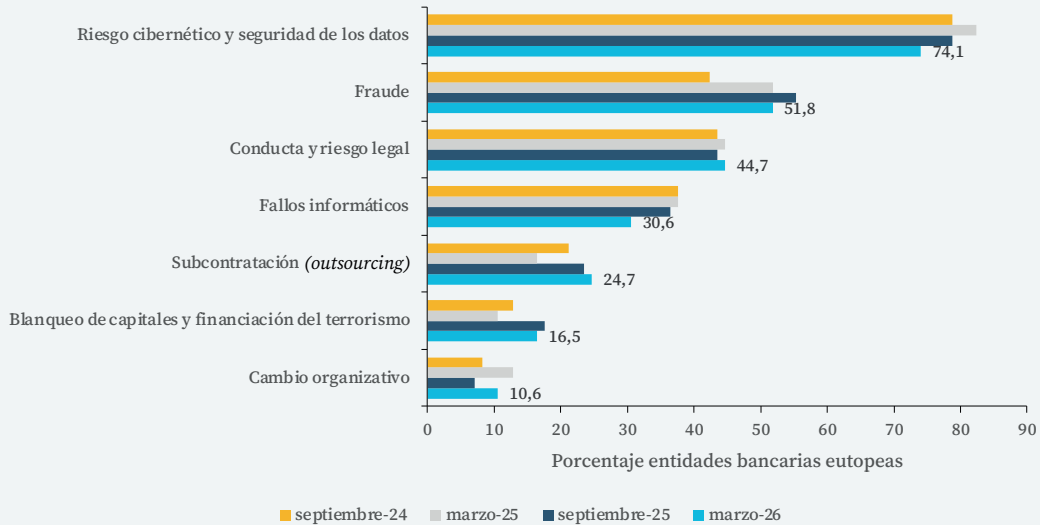
Riesgo cibernético: determinante del riesgo operacional y su materialización

La centralidad del ciberriesgo se observa en las respuestas de las entidades a la encuesta semestral de la EBA, realizada a una muestra de 85 bancos de la Unión Europea y el Espacio Económico Europeo. El gráfico 2 presenta el

Gráfico 2

Fuentes del riesgo operacional

Porcentaje de bancos europeos encuestados que responden afirmativamente



Fuente: Elaboración propia a partir de datos procedentes de la EBA.

porcentaje de entidades que identifica afirmativamente distintas fuentes de riesgo operacional. Las categorías no son excluyentes, ya que un mismo banco puede considerar relevantes varios riesgos al mismo tiempo (EBA, 2026a).

En marzo de 2026, el 74,1 % de los bancos situaba el riesgo cibernético y la seguridad de los datos entre las principales fuentes de riesgo operacional, encontrándose 22,3 puntos porcentuales por encima del fraude, mencionado por el 51,8 % de las entidades. A continuación, aparecen la conducta y el riesgo legal (44,7 %); los fallos informáticos (30,6 %) o la subcontratación (24,7 %). El riesgo cibernético y la seguridad de los datos representaban el 78,8 % en septiembre de 2024, aumentaron hasta el 82,4 % en marzo de 2025, volvieron al 78,8 % en septiembre de 2025 y se situaron en el 74,1 % en marzo de 2026. El descenso desde el máximo es visible. Sin embargo,

en todas las oleadas, el ciberriesgo ocupa la primera posición (EBA, 2026a). En cualquier caso, el descenso de la percepción del ciberriesgo desde marzo de 2025 puede responder a la estabilización del número de ataques, el refuerzo de las defensas, una mayor madurez en la gestión del riesgo o a la adaptación al marco de DORA.

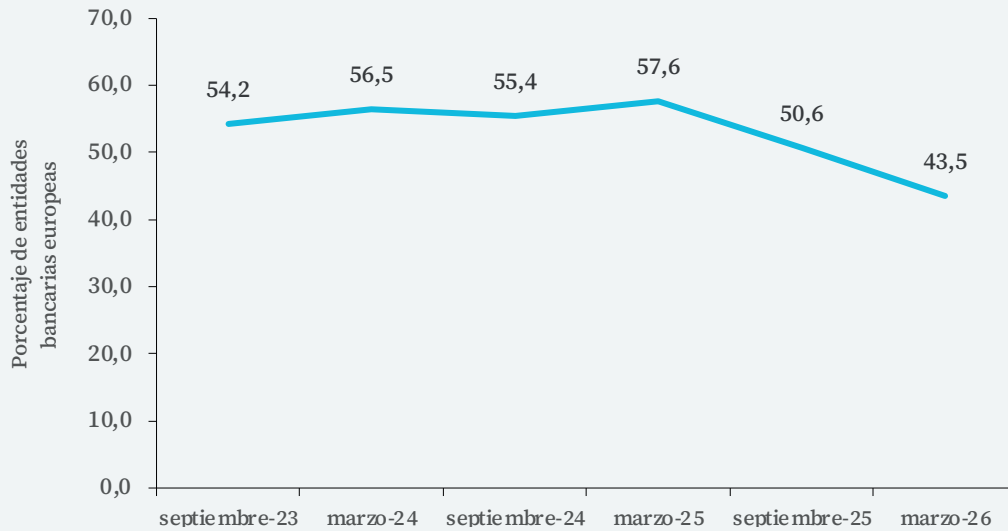
En marzo de 2026, el 74,1 % de los bancos situaba el riesgo cibernético y la seguridad de los datos entre las principales fuentes de riesgo operacional, encontrándose 22,3 puntos porcentuales por encima del fraude, mencionado por el 51,8 % de las entidades

El gráfico 3 recoge la evolución del porcentaje de bancos europeos que, durante los seis meses

Gráfico 3

Bancos europeos víctimas de al menos un ciberataque en los últimos seis meses

Porcentaje sobre el total



Fuente: Elaboración propia a partir de datos procedentes de la EBA.

anteriores, habrían sufrido al menos un ciberataque capaz de provocar un incidente tecnológico grave. Este porcentaje pasó del 54,2 % en septiembre de 2023 al 50,6 % en septiembre de 2025 y al 43,5 % en marzo de 2026 (EBA, 2026a). Aunque la tendencia es descendente, el nivel continúa siendo elevado: en marzo de 2026, más de cuatro de cada diez entidades habrían afrontado al menos un ataque con capacidad real o potencial de convertirse en un incidente grave durante el semestre anterior.

A pesar de esta reducción en el número de entidades afectadas, las pérdidas económicas derivadas de nuevos cibereventos aumentaron, alcanzando aproximadamente 730 millones de euros en 2025, frente a los 650 millones registrados en 2024. Estas pérdidas también crecieron como proporción del capital ordinario de nivel 1 (CET1), aunque se mantuvieron en un

nivel agregado reducido, cercano al 0,04 %. Por tanto, los costes directos de los ciberataques no parecen representar, por sí solos, una amenaza significativa para la solvencia del sector bancario europeo. No obstante, el promedio agregado puede ocultar impactos importantes en determinadas entidades y no refleja completamente costes indirectos como la pérdida de negocio, las compensaciones a clientes, el daño reputacional o las inversiones necesarias para recuperar y reforzar los sistemas (EBA, 2026b).

El papel de la IA: ¿aliada o enemiga?

La IA amplía las capacidades de prevención, detección y respuesta de las entidades bancarias, a la par que proporciona a los atacantes herramientas más potentes y accesibles. La cuestión relevante no es, por tanto, si la IA es intrínsecamente

beneficiosa o perjudicial, sino qué actores la utilizan, con qué objetivos y bajo qué controles.

|
Se pone de manifiesto que un modelo capaz de encontrar una vulnerabilidad puede ayudar a corregirla, pero también podría facilitar su explotación por actores maliciosos
|

En el ámbito defensivo, los sistemas de IA pueden analizar de forma continua grandes cantidades de registros, tráfico de red y patrones de transacciones para identificar comportamientos anómalos que pasarían inadvertidos mediante reglas estáticas. También pueden ayudar a priorizar alertas, detectar código malicioso, revisar *software*, resumir información sobre amenazas y automatizar algunas tareas iniciales de contención. En materia de fraude, permiten combinar señales de múltiples fuentes y adaptar los modelos a patrones cambiantes. Su principal ventaja

es que pueden procesar información a una velocidad difícilmente alcanzable por equipos humanos, reservando la intervención de los especialistas para los casos de mayor riesgo (FSB, 2024; FSB, 2026a).

El caso de Anthropic ilustra con claridad este potencial. En abril de 2026, la compañía anunció Project Glasswing, iniciativa para utilizar su modelo de vanguardia Claude Mythos Preview en la identificación y corrección de vulnerabilidades de *software* crítico. Entre los socios iniciales figuraban empresas tecnológicas y de ciberseguridad y una entidad financiera sistémica como JPMorganChase. El modelo identificó miles de vulnerabilidades de alta gravedad, alcanzando una tasa de éxito del 83,1 % en CyberGym, una prueba de reproducción de vulnerabilidades, frente al 66,6 % de Claude Opus 4.6. El acceso se articuló como una prueba de investigación restringida y orientada a usos defensivos (Anthropic, 2026; Rodríguez Fernández, 2026). A la par, se pone de manifiesto que un modelo

Cuadro 1

Papel de la IA en la gestión del ciberriesgo

Mitigador	Amplificador
• Análisis continuo de registros, tráfico de red y transacciones. • Capacidad de prevención, detección y respuesta. • Priorización de alertas y facilidad para detectar amenazas y fraudes. • Revisión de <i>software</i>, resumen de amenazas y automatización de tareas de contención.	• Automatización y personalización de ataques. • Rapidez en el descubrimiento y aprovechamiento de vulnerabilidades. • Mayor eficacia de ataques basados en la ingeniería social. • Concentración de servicios en proveedores comunes: riesgo de correlación y contagio.

Fuente: Elaboración propia.

capaz de encontrar una vulnerabilidad puede ayudar a corregirla, pero también podría facilitar su explotación por actores maliciosos. Si el tiempo necesario para descubrir un fallo cae por debajo del que necesitan las organizaciones para validarlo, desarrollar un parche y desplegarlo de manera segura, la ventaja puede desplazarse hacia el atacante.

La IA generativa también reduce el coste de la ingeniería social. Permite redactar mensajes convincentes y personalizados en distintos idiomas, imitar estilos de comunicación y producir audio o vídeo sintético. Esto puede elevar la eficacia del *phishing*, la suplantación de directivos o proveedores y el robo de credenciales. La combinación de información obtenida de fuentes abiertas, datos robados y generación automática facilita ataques dirigidos a empleados concretos con acceso a

pagos, sistemas o información sensible. Los *deepfakes* y otras formas de suplantación generadas mediante IA ilustran cómo el riesgo tecnológico puede materializarse a través de la manipulación de las personas, y no necesariamente mediante la intrusión directa en un sistema.

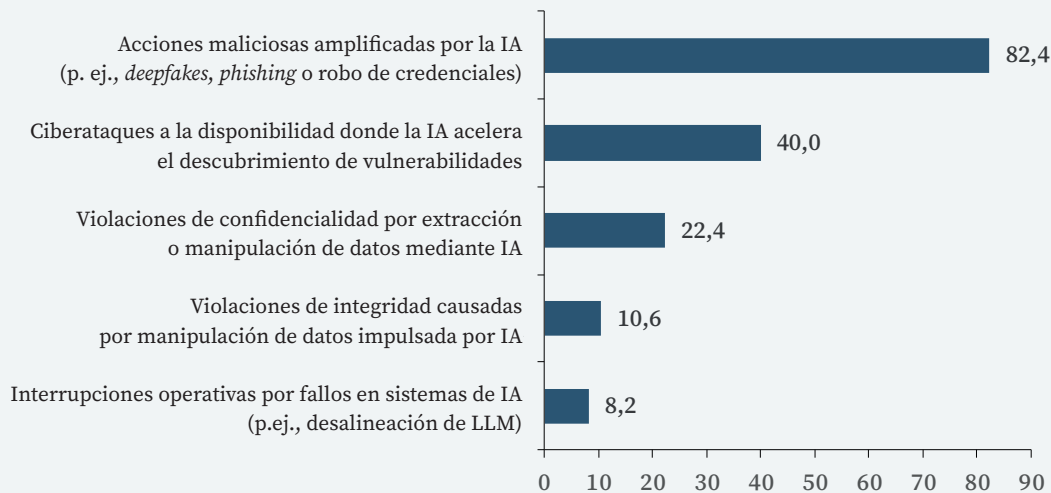
|
*Si numerosos bancos utilizan
infraestructuras similares,
un fallo o una vulnerabilidad puede
generar efectos correlacionados*
|

El gráfico 4 recoge cómo perciben los bancos europeos las distintas formas en que la IA puede amplificar el impacto negativo de los incidentes tecnológicos. La preocupación dominante son las acciones maliciosas potenciadas por IA

Gráfico 4

Entidades bancarias europeas que afirman que el impacto de los siguientes tipos de incidentes tecnológicos puede verse amplificado por la IA

Porcentaje



Fuente: Elaboración propia a partir de datos procedentes de la EBA.

—incluidos los *deepfakes*, el *phishing* automatizado y el robo de credenciales—, señaladas por el 82,4 % de las entidades. Esta proporción refleja que el principal temor no se centra aún en un fallo autónomo de los modelos, sino en la capacidad de la IA para hacer más escalables, creíbles y eficaces técnicas de ataque ya conocidas.

A ello se suma que muchas entidades dependen de un número reducido de proveedores de nube,

modelos, *hardware* y *software*. El FSB ha señalado que la IA puede amplificar vulnerabilidades asociadas a las dependencias de terceros, el ciberriesgo y el riesgo de modelo. Si numerosos bancos utilizan infraestructuras similares, un fallo o una vulnerabilidad puede generar efectos correlacionados. La gestión de la IA no puede limitarse, por ello, a validar cada aplicación individual, debe identificar también dependencias comunes, posibilidades de sustitución y planes de continuidad (FSB, 2024).

Conclusiones

El ciberriesgo ocupa una posición central en la agenda bancaria europea. La IA puede reforzar la defensa mediante una mejor detección de anomalías, análisis de amenazas, identificación de vulnerabilidades y rapidez de respuesta. Sin embargo, también puede facilitar usos maliciosos. Por ello, no sorprende que el 82,4 % de los bancos considere que la IA puede amplificar las acciones maliciosas y el 40 % destaque su impacto sobre ataques a la disponibilidad y sobre explotación de vulnerabilidades.

La respuesta, por tanto, debe apoyarse en cuatro principios:

- Prevención y reducción de la superficie de ataque: *software* actualizado, control estricto de accesos, protección del código y gestión continua de vulnerabilidades.
- Detección y respuesta a la velocidad de la amenaza: monitorización permanente, uso defensivo de IA,

equipos cualificados y protocolos de escalado claros.

- Resiliencia ante fallos propios y de terceros: copias verificadas, recuperación probada y planes de salida frente a proveedores críticos.
- Gobernanza de la IA: inventario de modelos, evaluación de cada caso de uso, calidad y seguridad de los datos, pruebas adversariales, trazabilidad y supervisión humana proporcional a la criticidad.

Las dependencias comunes de proveedores de infraestructuras tecnológicas pueden transformar un incidente individual en una perturbación correlacionada. La cooperación entre bancos, autoridades y proveedores resulta, por tanto, esencial. En último término, la IA no elimina la necesidad de controles tradicionales de ciberseguridad, sino que eleva su exigencia. El resultado dependerá de la rapidez defensiva de los bancos, de la calidad de la gobernanza tecnológica y de la capacidad supervisora para identificar dependencias comunes.

Referencias

- ANTHROPIC. (2026). *Project Glasswing: Securing critical software for the AI era*. 7 de abril.
- AUTORIDAD BANCARIA EUROPEA —EBA—. (2025). *Risk Assessment Report. Autumn 2025*.
- AUTORIDAD BANCARIA EUROPEA —EBA—. (2026a). *Risk Assessment Questionnaire Results. Spring 2026*.
- AUTORIDAD BANCARIA EUROPEA —EBA—. (2026b). *Risk Assessment Report. Spring 2026*.
- AUTORIDADES EUROPEAS DE SUPERVISIÓN. (2026a). *2025 Report on Major ICT-related Incidents*.
- AUTORIDADES EUROPEAS DE SUPERVISIÓN. (2026b). *Toward a Consistent and Risk-based Approach for ICT Risks from Frontier AI Models*. 31 de julio.
- EUROPEAN REPOSITORY OF CYBER INCIDENTS —EuRepoC—. (2026). *Database of Cyber Incidents*.
- FINANCIAL STABILITY BOARD —FSB—. (2024). *The Financial Stability Implications of Artificial Intelligence*.
- FINANCIAL STABILITY BOARD —FSB—. (2026a). *Sound Practices for Financial Institutions' Responsible AI Adoption: Consultation Report*.
- FINANCIAL STABILITY BOARD —FSB—. (2026b). *FSB Chair's Letter to G20 Finance Ministers and Central Bank Governors. August 2026*.
- RODRÍGUEZ FERNÁNDEZ, F. (2026). *Inteligencia artificial y estabilidad financiera: los riesgos bancarios en la era de la IA de vanguardia. Una evaluación comparativa de España, la Unión Europea y Estados Unidos*. Investigaciones de Funcas, 40/2026. https://www.funcas.es/documentos_trabajo/inteligencia-artificial-y-estabilidad-financiera-los-riesgos-bancarios-en-la-era-de-la-ia-de-vanguardia-una-evaluacion-comparativa-de-espana-la-union-europea-y-estados-unidos/
- UNIÓN EUROPEA. (2022). Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, sobre la resiliencia operativa digital del sector financiero (DORA).