C/2026/3795

16.7.2026

# AVISO DE LA JUNTA EUROPEA DE RIESGO SISTÉMICO

## de 25 de junio de 2026

## sobre los ciberriesgos sistémicos derivados de modelos de inteligencia artificial de frontera

## (JERS/2026/3)

(C/2026/3795)

LA JUNTA GENERAL DE LA JUNTA EUROPEA DE RIESGO SISTÉMICO,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Acuerdo sobre el Espacio Económico Europeo ([1]), en particular el anexo IX,

Visto el Reglamento (UE) n.º 1092/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, relativo a la supervisión macroprudencial del sistema financiero en la Unión Europea y por el que se crea una Junta Europea de Riesgo Sistémico ([2]), en particular el artículo 3, apartado, 2, letra c), y los artículos 16 y 18,

Vista la Decisión JERS/2011/1 de la Junta Europea de Riesgo Sistémico, de 20 de enero de 2011, por la que se adopta el Reglamento interno de la Junta Europea de Riesgo Sistémico ([3]), en particular los artículos 18 y 19,

Considerando lo siguiente:

(1) Los principales proveedores de inteligencia artificial (IA) han desarrollado modelos de IA de frontera (FAIM, por sus siglas en inglés), que tienen una gran capacidad en el ámbito de la ciberseguridad y pueden llevar a cabo ciberataques totalmente automatizados contra sistemas complejos, en particular mediante el descubrimiento de vulnerabilidades y el desarrollo y el uso como arma de los aprovechamientos, cambiando así radicalmente el panorama de ciberamenazas.

(2) Los FAIM son significativamente mejores que los modelos de IA anteriores a la hora de encontrar formas de llevar a cabo ciberataques, superando a los modelos anteriores en coste, rapidez y precisión, lo que actualmente rivaliza con los principales expertos humanos.

(3) Los FAIM tienen la capacidad de amenazar los sistemas que sustentan los entornos de tecnologías de la información y la comunicación (TIC) de los que depende la infraestructura financiera, aumentando la probabilidad y la gravedad de ciberincidentes con repercusiones sistémicas.

(4) Los FAIM han demostrado la capacidad para descubrir vulnerabilidades y crear nuevos aprovechamientos, exponiendo así a los principales sistemas operativos y programas informáticos utilizados en casi todas las organizaciones al riesgo de ciberataques.

(5) Históricamente, el descubrimiento de estas vulnerabilidades ha sido poco frecuente y, a menudo, las han detectado investigadores de seguridad, lo que ha permitido aplicar medidas correctivas específicas. En esos casos, a los proveedores de programas informáticos se les concede a menudo un plazo normalizado —por lo general, 90 días— para corregir la vulnerabilidad antes de que se haga pública. Sin embargo, es probable que los FAIM aumenten el volumen de vulnerabilidades detectadas.

(6) Las prácticas actuales del sistema financiero para corregir vulnerabilidades son predominantemente reactivas y se basan en actualizaciones periódicas y respuestas ad hoc a las vulnerabilidades reveladas. Este enfoque funciona en un entorno de amenazas en el que el tiempo permite que el descubrimiento de vulnerabilidades siga siendo manejable. No obstante, con el aumento del volumen de vulnerabilidades, las prácticas actuales pueden resultar insuficientes para mantener la resiliencia operativa.

(7) Este aumento del volumen también expone a los actuales procesos de corrección de vulnerabilidades a una sobrecarga, ya que priorizan las medidas correctoras basadas en el riesgo y requieren pruebas de los parches de software antes de su aplicación para garantizar la estabilidad operativa. Si se descubren demasiadas vulnerabilidades con repercusiones graves en un breve plazo de tiempo, de modo que se incremente sustancialmente el número de parches de software críticos necesarios, las entidades financieras pueden tener que decidir entre quedar expuestas a riesgos cibernéticos significativos o reducir los requisitos relativos a las pruebas de parcheado, con el consiguiente riesgo de incidentes operativos e interrupciones.

([1]) DO L 1 de 3.1.1994, p. 3, ELI: http://data.europa.eu/eli/agree_internation/1994/1/oj.
([2]) DO L 331 de 15.12.2010, p. 1, ELI: http://data.europa.eu/eli/reg/2010/1092/oj.
([3]) DO C 58 de 24.2.2011, p. 4.

(8) Anteriormente, la creación de aprovechamientos utilizados como arma se realizaba en gran medida manualmente y a los expertos humanos les requería días o semanas, mientras que ahora los FAIM pueden hacerlo en cuestión de minutos u horas. Esto supone un colapso de los márgenes de tiempo defensivos, que son necesarios para mantener la continuidad de las funciones esenciales e importantes durante la corrección del problema.

(9) Con la proliferación de aprovechamientos utilizados como armas correspondientes a vulnerabilidades críticas impulsados por la IA y la correspondiente reducción de los márgenes de tiempo defensivos, el riesgo para las funciones y entidades esenciales o importantes individuales aumenta considerablemente. Si estos riesgos se materializan de forma simultánea entre esas funciones y entidades, podría producirse un aumento permanente del ciberriesgo sistémico para el que, en la actualidad, no se dispone de un marco de mitigación plenamente eficaz. Debido a la fuerte interconexión dentro del sector financiero de la Unión, así como entre dicho sector y otros sectores y jurisdicciones, esta situación plantea un riesgo sistemático y puede crear fragilidades sistémicas.

(10) Además, solo un pequeño número de proveedores de IA están desarrollando FAIM, y varios de ellos han manifestado su preocupación por que los futuros FAIM puedan ser demasiado potentes como para permitir un acceso público sin restricciones.

(11) Agentes malintencionados ya están haciendo uso de la IA para mejorar los ciberataques. Es probable que estos agentes acaben obteniendo, ya sea a través de filtraciones, robos, desarrollo independiente o acceso abierto, modelos de IA con capacidades comparables a las actualmente desplegadas en entornos defensivos controlados.

(12) Si bien los FAIM pueden aumentar significativamente las capacidades ofensivas y la probabilidad de ciberataques sofisticados, también reforzarán las capacidades defensivas, en particular en lo que respecta al descubrimiento de vulnerabilidades, la correlación de datos y las medidas correctoras por parte de las distintas instituciones. Sin embargo, a corto y medio plazo, es probable que el aumento de la velocidad, la escala y la precisión de las capacidades ofensivas supere los beneficios.

(13) El rápido desarrollo de los FAIM hace necesario abordar sin demora los riesgos para la estabilidad financiera identificados, con el fin de evitar su materialización o, al menos, mitigar sus posibles repercusiones. Para garantizar la estabilidad financiera en los mercados financieros de la Unión, todos los miembros de la Junta Europea de Riesgo Sistémico (JERS) deben considerar las implicaciones de los FAIM en la capacidad operativa y la resiliencia de las entidades financieras en el contexto de sus medidas de política macroprudencial y microprudencial. Esto se entiende sin perjuicio de los mandatos de política monetaria de los bancos centrales de la Unión. Por ejemplo, y entre otras iniciativas actuales de las autoridades, el BCE, en su función de supervisor bancario, ha solicitado a las entidades significativas que evalúen sin demora las repercusiones del panorama de amenazas en constante evolución y que elaboren, a más tardar el 31 de octubre de 2026, un plan de acción exhaustivo en el que se describan medidas concretas para hacer frente a dichos riesgos. ([4])

(14) A medida que la tecnología de IA prolifera, es importante garantizar que todas las infraestructuras esenciales, y especialmente las entidades financieras, estén preparadas para hacer frente a los ciberataques provocados por los FAIM, y adopten las medidas oportunas y adecuadas. No obstante, estos esfuerzos defensivos por parte de entidades individuales resultarían insuficientes. Una respuesta eficaz y la mitigación del riesgo requieren una respuesta coordinada en la que participen todas las partes afectadas, incluidos los proveedores de IA, los proveedores de software, las empresas de seguridad, los responsables del mantenimiento de proyectos de código abierto, las entidades financieras y las autoridades tanto a escala nacional como de la Unión.

(15) Al abordar las cuestiones anteriores, es importante recordar los marcos jurídicos y políticos pertinentes de la Unión, en particular el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo ([5]), el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo ([6]), el Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo ([7]) y la Recomendación de la Junta Europea de Riesgo Sistémico (JERS/2021/17) ([8]).

([4]) La carta dirigida a las entidades significativas está disponible en la dirección de internet de Supervisión Bancaria del BCE en http://www.bankingsupervision.europa.eu/home/html/index.en.html.

([5]) Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011 (DO L 333 de 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L 2024/1689 de 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.º 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia) (DO L 2024/2847 de 20.11.2024, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

([8]) Recomendación de la Junta Europea de Riesgo Sistémico, de 2 de diciembre de 2021, sobre un marco paneuropeo de coordinación de ciberincidentes sistémicos para las autoridades pertinentes (JERS/2021/17) (DO C 134 de 25.3.2022, p. 1).

(16) El Reglamento (UE) 2022/2554 establece un marco exhaustivo para que las entidades financieras identifiquen, gestionen, supervisen y mitiguen los riesgos relacionados con las TIC, incluidos los riesgos derivados de ciberataques. Dada la interconexión del sector financiero y su dependencia de los sistemas de TIC y de proveedores de servicios terceros, un ciberataque eficaz que afecte a una o varias entidades financieras o a sus proveedores de servicios esenciales podría tener implicaciones sistémicas significativas. Las autoridades de supervisión financiera deben dar la prioridad adecuada a las actividades de supervisión en este ámbito, teniendo en cuenta las posibles repercusiones de dichos ciberataques en la estabilidad, la integridad y la fiabilidad del sistema financiero, así como los daños operativos, financieros y para los consumidores que puedan ocasionar.

(17) El Reglamento (UE) 2024/1689 establece normas armonizadas para la introducción en el mercado, la puesta en servicio y el uso de sistemas de IA y modelos de IA de uso general en la Unión, incluidos, en determinadas circunstancias, los sistemas y modelos de IA ofrecidos por proveedores de IA establecidos en terceros países cuando el resultado generado por el sistema de IA se utilice en la Unión, o un modelo de IA se integre en un sistema introducido en el mercado de la Unión. Este reglamento también establece normas específicas, incluido un régimen regulador más estricto, para los modelos clasificados como modelos de IA de uso general con riesgo sistémico.

(18) El Reglamento (UE) 2024/2847 introduce requisitos obligatorios de ciberseguridad para los fabricantes que comprenden la planificación, el diseño, el desarrollo y el mantenimiento de productos de hardware y software con elementos digitales introducidos en el mercado de la Unión. También exige que los fabricantes se ocupen de las vulnerabilidades durante el ciclo de vida de sus productos. Una vez sea plenamente aplicable en diciembre de 2027, las entidades financieras que introduzcan dichos productos en el mercado de la Unión también tendrán que garantizar que estos cumplen estos requisitos.

(19) La Recomendación JERS/2021/17 recomendaba que las Autoridades Europeas de Supervisión (AES) desarrollaran conjuntamente, a través del Comité Mixto y junto con el Banco Central Europeo (BCE), la JERS y las autoridades nacionales pertinentes, una respuesta coordinada eficaz a escala de la Unión en caso de ciberincidente transfronterizo grave o amenaza conexa que pudiera tener efectos sistémicos en el sector financiero de la Unión. Esto dio lugar a la creación del marco paneuropeo de coordinación de ciberincidentes sistémicos (EU-SCICF), que proporciona una valiosa plataforma operativa para el intercambio de información y la coordinación entre las autoridades financieras.

(20) En este contexto, la JERS adopta un aviso de carácter general que aborda los importantes riesgos para la estabilidad financiera amplificados por el desarrollo de los FAIM. El aviso tiene en cuenta los trabajos analíticos de la nota de la JERS titulada «Addressing Frontier AI Models with cyber capabilities from a financial stability perspective», publicada en junio de 2026 ([9]).

EMITE EL PRESENTE AVISO:

SECCIÓN 1

**Aviso**

*Nuevo panorama de riesgos*

El rápido desarrollo de modelos de IA de frontera (FAIM) con cibercapacidades conlleva cambios significativos en el panorama de riesgos para el sistema financiero de la Unión. Los datos actuales indican que los FAIM son capaces de detectar vulnerabilidades, generar aprovechamientos operativos y ejecutar de forma autónoma ciberataques a gran escala con una velocidad, una magnitud y un nivel de precisión muy superiores a los de los modelos de IA anteriores. Esto constituye un cambio de paradigma en el ámbito de la ciberseguridad y un punto de inflexión respecto a la capacidad de IA.

La JERS considera que esta evolución es una fuente de riesgos sistémicos para el sistema financiero, pudiendo generar efectos adversos significativos en la ciberseguridad debido al descubrimiento acelerado de vulnerabilidades, la reducción del tiempo disponible para la respuesta y la defensa eficaz, el aumento de la magnitud y la sofisticación de los ciberataques, y la aparición de nuevas dependencias y riesgos de concentración en el sistema financiero. Si bien la JERS reconoce el refuerzo de las capacidades defensivas que ofrecerán los FAIM a las entidades financieras, es probable que estas capacidades se vayan materializando gradualmente a lo largo de los próximos años, lo que requerirá que las entidades financieras operen durante un período transitorio caracterizado por un elevado riesgo, una gran incertidumbre y un panorama tecnológico en rápida evolución. Dado el carácter altamente digitalizado e interconectado del sistema financiero, estos efectos adversos en la ciberseguridad podrían propagarse rápidamente, afectando a funciones esenciales e importantes en todas las entidades financieras, y, en última instancia, provocando perturbaciones sistémicas y pérdida de confianza en el sistema financiero.

([9]) Disponible en la dirección de la JERS en internet, www.esrb.europa.eu.

Los nuevos FAIM aumentan el riesgo inherente relacionado con las TIC, lo que da lugar a un debilitamiento de la resiliencia operativa en todo el sector financiero, en particular en cuatro ámbitos: a) el tiempo, incluida la capacidad de aplicar parches a sistemas complejos rápidamente sin provocar fallos operativos, teniendo en cuenta la desaparición de los márgenes de tiempo defensivos entre el descubrimiento de vulnerabilidades y la utilización de los aprovechamientos como arma; b) la capacidad de los expertos en ciberseguridad, incluida su capacidad para realizar pruebas de seguridad automatizadas y manuales asistidas por FAIM, así como su capacidad para proteger, detectar y responder a las amenazas derivadas del uso de FAIM adversarios; c) la concentración, incluida la dependencia de un número limitado de proveedores de IA, dependientes a su vez de proveedores en la nube, componentes de código abierto y otro software de uso generalizado, y d) la capacidad de las autoridades, incluida su calibración de las expectativas, las pruebas de resistencia y las medidas de preparación de acuerdo con el desarrollo de los FAIM, de modo que los fallos operativos no se conviertan en una mayor fuente de inestabilidad.

Además, es difícil establecer y mantener la visibilidad del uso de la IA en cualquier entidad financiera, incluido el pleno entendimiento de dónde y cómo se utiliza la IA, teniendo en cuenta que se utiliza en las interfaces de clientes, los agentes internos, los procesos empresariales y la integración con terceros.

*Evaluación sistémica*

Los desarrollos identificados pueden alterar sustancialmente tanto la magnitud como la estructura del riesgo cibernético, aumentando los riesgos tanto directos como indirectos para la estabilidad financiera. Las capacidades de los FAIM pueden someter a los marcos de resiliencia existentes a una presión considerable, especialmente si los incidentes son generalizados y se producen simultáneamente. Los incidentes también pueden propagarse rápidamente en todas las entidades y mercados financieros si se ven afectados proveedores terceros esenciales, ecosistemas tecnológicos compartidos o componentes de código abierto ampliamente utilizados, lo que aumenta el riesgo de perturbaciones conexas con implicaciones sistémicas.

Los FAIM alteran tres fuentes de asimetría en el sector financiero: la primera entre jurisdicciones, la segunda entre expertos en ciberseguridad y atacantes y la tercera entre entidades financieras mejor dotadas y menos equipadas.

En primer lugar, la actual concentración geográfica de los principales proveedores de IA fuera de la Unión deja a esta expuesta a una dependencia estratégica y a un riesgo geopolítico. Con el fin de mitigar la asimetría tecnológica y de conocimientos entre jurisdicciones, es necesario adoptar medidas para facilitar un acceso adecuado y proporcionado de la Unión y sus Estados miembros a los FAIM de reciente creación. Dichas medidas deben ser oportunas, coherentes y eficientes, tanto en términos de política como de aplicación, y deben tener debidamente en cuenta los diferentes sectores financieros de la Unión, aprovechando la experiencia de las AES correspondientes. Esto aliviará no solo la asimetría entre la Unión y las jurisdicciones de terceros países, sino también entre entidades financieras establecidas en diferentes Estados miembros, preservando unas condiciones de competencia equitativas dentro y fuera de la Unión y minimizando el riesgo sistémico. Los acuerdos que facilitan el acceso a los FAIM solo para determinadas categorías de entidades o en jurisdicciones seleccionadas contribuirían a la fragmentación del mercado único de las finanzas, reduciendo su liquidez y profundidad.

En segundo lugar, por lo que se refiere a la asimetría entre atacantes y expertos en ciberseguridad, los FAIM reducen el precio de admisión de los atacantes. Es probable que los agentes de riesgo recurran cada vez más a los FAIM para llevar a cabo las partes más avanzadas técnicamente e intensivas en mano de obra de las operaciones ofensivas, reduciendo los costes. En cambio, los expertos en ciberseguridad se ven limitados por los requisitos operativos, las dependencias y las obligaciones reglamentarias, lo que limita el efecto y la magnitud respecto a lo que pueden beneficiarse de los FAIM a corto y medio plazo, lo que en última instancia requiere períodos más largos para ajustarse.

En tercer lugar, existen diferencias en la manera en que las entidades financieras cuentan con los recursos y los equipos necesarios para hacer frente a los retos que plantean los FAIM. Estas diferencias pueden deberse a costes fijos en lugar de escalonados, a limitaciones de recursos y a un acceso limitado a especialistas. Cuando existe una asimetría en la capacidad de hacer frente a tales retos, el eslabón más débil de la cadena puede afectar a la estabilidad del sistema.

*Implicaciones*

Es esencial garantizar que los sistemas de pago y liquidación de importancia sistémica y las infraestructuras de los mercados financieros sigan estando protegidos frente a las vulnerabilidades derivadas del uso y el desarrollo de FAIM. Los operadores públicos y privados deben revisar y actualizar exhaustivamente sus marcos de ciberseguridad para tener en cuenta dichas vulnerabilidades. Las autoridades encargadas de la supervisión o vigilancia deben adoptar medidas para garantizar que los sistemas estén adecuadamente protegidos. Se debe fomentar la cooperación entre las autoridades y las entidades financieras privadas siempre que sea necesario para aumentar la seguridad y la resiliencia del sistema financiero de la Unión.

En su informe de 2020 sobre ciberriesgos sistémicos ([10]), la JERS identificó la velocidad, la magnitud y la intención maliciosa de las ciberamenazas como posibles fuentes de propagación del riesgo sistémico. Las autoridades deben ser conscientes de que, si bien los FAIM representan una nueva fuente de propagación, también amplifican las fuentes ya identificadas anteriormente, y deben integrar esta idea en sus medidas de política monetaria. Teniendo en cuenta todos los riesgos para la estabilidad financiera derivados de la exposición operativa al ciberriesgo en el sector financiero, es importante garantizar que las preocupaciones señaladas en el presente aviso se reflejen en el trabajo de supervisión y vigilancia y en las posiciones políticas adoptadas por las autoridades pertinentes, en el marco de sus respectivos mandatos.

Las autoridades pertinentes, dentro de sus respectivas competencias y específicamente en el marco establecido por el Reglamento (UE) 2022/2554, deben ser conscientes de las tres fuentes de asimetría mencionadas anteriormente introducidas por los FAIM en el sector financiero. Para reducir estas asimetrías, deben considerarse acuerdos de cooperación y coordinación sectorial junto con los marcos de pruebas existentes ([11]). Las autoridades financieras también deben garantizar que los consejos de las entidades financieras privadas se comprometan plenamente a mitigar los ciberriesgos derivados de los FAIM, que existan marcos claros de gobierno y rendición de cuentas y que las respuestas oportunas se planifiquen adecuadamente, junto con las inversiones internas correspondientes.

Varios posibles desarrollos considerados en este aviso —ya sean las repercusiones sistémicas, el riesgo geopolítico o el cambio de equilibrio entre atacantes y expertos en seguridad— pueden afectar al funcionamiento del sistema financiero y a la confianza en él. Para evaluarlos continuamente, la JERS considerará la necesidad de reflejar estos desarrollos en las evaluaciones de riesgos, los marcos de pruebas y las expectativas de supervisión, así como en la evolución de los escenarios futuros. La JERS también realizará un seguimiento del uso y el desarrollo de los FAIM y sus repercusiones en el sector financiero desde la perspectiva del riesgo sistémico. Además, la JERS volverá a evaluar la evolución de cada evaluación trimestral de riesgos de la Junta General y estudiará otras medidas cuando sea necesario.

SECCIÓN 2

**Definiciones**

A efectos del presente aviso, se entenderá por:

1) «proveedor de IA», el definido en el artículo 3, punto 3, del Reglamento (UE) 2024/1689;

2) «modelos de IA de frontera (FAIM)», modelos de IA de uso general más avanzados que pueden afectar significativamente a ciberoperaciones ofensivas o defensivas;

3) «ciberataque», el definido en el artículo 1 del Reglamento (UE) 2019/796 del Consejo ([12]), incluso cuando se origine en la Unión;

4) «vulnerabilidad», la definida en el artículo 3, punto 16, del Reglamento (UE) 2022/2554;

5) «aprovechamiento», herramienta, técnica o método utilizado para aprovechar una o varias vulnerabilidades con el fin de obtener acceso no autorizado a los sistemas, modificarlos o perturbarlos o dar lugar a riesgos o incidentes relacionados con las TIC;

6) «uso como arma», la preparación o adaptación de los aprovechamientos que permitan la explotación sistemática o escalable de las vulnerabilidades;

7) «función esencial o importante», la definida en el artículo 3, punto 22, del Reglamento (UE) 2022/2554;

8) «modelo de IA de uso general», el definido en el artículo 3, punto 63, del Reglamento (UE) 2024/1689;

9) «modelo de IA de uso general con riesgo sistémico», un modelo de uso general clasificado como de riesgo sistémico con arreglo al artículo 51, apartado 1, del Reglamento (UE) 2024/1689;

10) «incidente relacionado con las TIC», el definido en el artículo 3, punto 8, del Reglamento (UE) 2022/2554;

([10]) Véase «Systemic cyber risk», JERS, febrero de 2020, disponible en inglés en la dirección de la JERS en Internet: www.esrb.europa.eu.

([11]) Por ejemplo, marco para ataques cibernéticos controlados basados en inteligencia de seguridad (TIBER), la prueba de penetración basada en amenazas (TLPT), la simulación de ataques avanzada (ART) y las pruebas de resistencia de ciberresiliencia (CyRST).

([12]) Reglamento (UE) 2019/796 del Consejo, de 17 de mayo de 2019, relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros (DO L 129 I de 17.5.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11) «riesgo relacionado con las TIC», el definido en el artículo 3, punto 5, del Reglamento (UE) 2022/2554;

12) «resiliencia operativa», la resiliencia operativa digital definida en el artículo 3, punto 1, del Reglamento (UE) 2022/2554;

Hecho en Fráncfort del Meno el 25 de junio de 2026.

*El Jefe de la Secretaría de la JERS,*
*en nombre de la Junta General de la JERS,*
Francesco MAZZAFERRO