

Reglamento (UE) 2025/38, del Parlamento Europeo y del Consejo, de 19 de diciembre de 2024, por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar ciberamenazas e incidentes, prepararse y responder a ellos y por el que se modifica el Reglamento (UE) 2021/694 (Reglamento de Ciberseguridad) [DOUE L 2025/38, de 15-I-2025]

1. INTRODUCCIÓN

Al analizar el Reglamento (UE) 2025/38, publicado en el *Diario Oficial de la Unión Europea* el 15 de enero de 2025, me resulta imposible no percibirlo como una respuesta ambiciosa y urgente a la creciente interdependencia digital que define nuestra era y, con ella, a las amenazas cibernéticas que desafían la estabilidad de las economías, las sociedades y las democracias de la Unión Europea. Entiendo que este instrumento, fundamentado en los artículos 173.3 y 322.1.a) del Tratado de Funcionamiento de la Unión Europea, no se limita a ser una mera actualización técnica del marco de ciberseguridad de la Unión, sino que encarna un esfuerzo deliberado por fortalecer la solidaridad entre los Estados miembros frente a un panorama de riesgos que trasciende fronteras y sectores. La magnitud y la frecuencia de los incidentes de ciberseguridad, desde ataques a la cadena de suministro hasta programas de secuestro masivos, han puesto de manifiesto la vulnerabilidad de las infraestructuras críticas y la necesidad de un enfoque colectivo que vaya más allá de las capacidades nacionales individuales.

El legislador europeo parece haber captado que, en un mercado único digital donde la interconectividad es tanto una fortaleza como un punto débil, la preparación y la respuesta a las ciberamenazas no pueden seguir siendo un mosaico de esfuerzos fragmentados. Lo anterior me sugiere que el Reglamento (UE) 2025/38, conocido como el Reglamento de Ciberseguridad, aspira a consolidar un sistema de defensa cibernética más robusto y coordinado, integrando herramientas como el Sistema Europeo de Alerta de Ciberseguridad, el Mecanismo de Emergencia en materia de Ciberseguridad y el Mecanismo Europeo de Revisión de Incidentes de Ciberseguridad. Este enfoque no solo busca proteger a los ciudadanos, las empresas y las administraciones públicas, sino también posicionar a la Unión como un actor competitivo en la economía digital global, un objetivo que resuena con las recomendaciones de la Conferencia sobre el Futuro de Europa. A continuación, desglosaré las disposiciones clave de esta norma, explorando sus implicaciones jurídicas y los retos que plantea su implementación, desde una perspectiva crítica y detallada.

2. MARCO NORMATIVO Y OBJETIVOS

El Reglamento (UE) 2025/38 se inscribe en un contexto normativo ya sólido, que incluye instrumentos como el Reglamento (UE) 2019/881, la Directiva (UE) 2022/2555 (SRI 2) y la Recomendación (UE) 2017/1584, pero introduce un enfoque distintivo al priorizar la solidaridad y la capacidad colectiva frente a las ciberamenazas (considerando 5). Considero que esta norma responde a la necesidad de superar las limitaciones de los marcos previos, que, aunque efectivos en la reducción de vulnerabilidades específicas, no abordaban suficientemente la dimensión transnacional y la rapidez de propagación de los incidentes cibernéticos. Su fundamento jurídico en el artículo 173.3, relativo a la competitividad industrial, y en el artículo 322.1.a), sobre normas financieras, refleja una visión integradora que combina objetivos económicos con la gestión presupuestaria, lo que me lleva a deducir que el legislador busca alinear la ciberseguridad con la resiliencia del mercado interior.

Los objetivos del reglamento, establecidos en el artículo 1, se centran en detectar, prevenir y responder a ciberamenazas e incidentes significativos o a gran escala, un ámbito que trasciende las responsabilidades nacionales y exige una acción coordinada a escala de la Unión. La creación del Sistema Europeo de Alerta de Ciberseguridad (artículos 3-9), el Mecanismo de Emergencia en materia de Ciberseguridad (artículos 10-20) y el Mecanismo Europeo de Revisión de Incidentes (artículo 21) constituyen los pilares operativos de esta estrategia. Entiendo que esta estructura tripartita no solo busca reaccionar ante crisis, sino también anticiparse a ellas mediante una mayor conciencia situacional y capacidades compartidas, un enfoque que se alinea con las Conclusiones del Consejo de mayo de 2022 y la Comunicación sobre la política de ciberdefensa de noviembre de 2022 (considerandos 5 y 6). Sin embargo, la voluntariedad de la participación en el Sistema de Alerta (considerando 14) introduce una variable de flexibilidad que podría limitar su eficacia si no se logra una adhesión generalizada entre los Estados miembros.

La modificación del Reglamento (UE) 2021/694, que rige el Programa Europa Digital, evidencia una voluntad de integrar estas medidas en un marco financiero y operativo ya existente (artículo 22). Esta integración me parece un acierto estratégico, ya que aprovecha recursos y estructuras preestablecidas, como el Centro Europeo de Competencia en Ciberseguridad (ECCC), para evitar duplicidades y optimizar la inversión. No obstante, la dependencia del presupuesto de la Unión plantea interrogantes sobre la sostenibilidad a largo plazo, especialmente ante la imprevisibilidad de los recursos necesarios para responder a crisis cibernéticas de magnitud variable (considerando 12), un aspecto que analizaré más adelante.

3. EL SISTEMA EUROPEO DE ALERTA DE CIBERSEGURIDAD

El Sistema Europeo de Alerta de Ciberseguridad, regulado en los artículos 3 a 9, representa una de las innovaciones más significativas del Reglamento (UE) 2025/38.

Entiendo que su objetivo de crear una red de centros cibernéticos nacionales y transfronterizos interoperables responde a la necesidad de una detección proactiva y una puesta en común de información que trascienda las capacidades individuales de los Estados miembros. La designación de un centro cibernético nacional por cada Estado participante (artículo 4) como punto de referencia para la coordinación y la recopilación de datos sobre ciberamenazas me parece un paso lógico para centralizar y racionalizar la inteligencia cibernética a nivel nacional, mientras que los centros transfronterizos (artículo 5), integrados por al menos tres Estados miembros, buscan maximizar los beneficios de la colaboración transnacional.

La puesta en común de datos, que puede incluir telemetría, indicadores de compromiso y alertas específicas (considerando 19), tiene el potencial de transformar la capacidad de la Unión para anticiparse a las amenazas, complementando redes existentes como la de CSIRT y la EU-CyCLONE (considerando 18). Considero que esta interoperabilidad, respaldada por herramientas de vanguardia como la inteligencia artificial (artículo 6), podría posicionar a la Unión como líder en la soberanía tecnológica en ciberseguridad, un objetivo explícito del reglamento (considerando 24). Sin embargo, la voluntariedad de la participación y la falta de obligatoriedad en la entrega de datos por parte de entidades privadas (artículo 4.2) me obligan a deducir que la eficacia del sistema dependerá en gran medida de la voluntad de colaboración de los actores involucrados, un desafío que podría mitigarse con incentivos claros, pero que el texto no detalla suficientemente.

La financiación conjunta a través del ECCC (artículo 5.5) y las restricciones a la participación de entidades controladas por terceros países, salvo excepciones justificadas (artículo 22, modificando el artículo 12 del Reglamento (UE) 2021/694), reflejan un equilibrio entre la apertura a la innovación y la protección de los intereses de seguridad de la Unión. Asumo que estas salvaguardias buscan evitar riesgos estratégicos, pero podrían limitar el acceso a tecnologías avanzadas si la capacidad interna de la Unión no logra satisfacer la demanda, un riesgo que la cartografía periódica de ENISA (artículo 9.4) deberá monitorizar cuidadosamente. La cooperación con la red de CSIRT y la EU-CyCLONE (artículo 7) refuerza la complementariedad, pero la necesidad de acuerdos específicos para la puesta en común de información (artículo 5.6) podría ralentizar la respuesta en situaciones de crisis si no se estandarizan con rapidez.

4. MECANISMO DE EMERGENCIA EN MATERIA DE CIBERSEGURIDAD

El Mecanismo de Emergencia en materia de Ciberseguridad, regulado en los artículos 10 a 20, constituye el núcleo operativo del Reglamento (UE) 2025/38, diseñado para ofrecer apoyo financiero y técnico ante incidentes significativos o a gran escala. Entiendo que su enfoque en la preparación, la respuesta y la recuperación inicial

(artículo 10) responde a la imprevisibilidad y el impacto devastador de los ciberataques, como los dirigidos a infraestructuras críticas o servicios esenciales (considerando 2). La inclusión de la Reserva de Ciberseguridad de la Unión Europea (artículo 14), compuesta por servicios contratados a proveedores de confianza, me parece una solución pragmática para garantizar una respuesta rápida y especializada, complementando los recursos nacionales y otras estructuras como el UCPM o la EU-CyCLONE (considerando 30).

Las acciones de preparación, como las pruebas coordinadas en sectores de alta criticidad (artículo 11), buscan armonizar la resiliencia en el mercado interior mediante metodologías comunes, un aspecto que considero esencial para evitar vulnerabilidades asimétricas entre Estados miembros. Sin embargo, la voluntariedad de las entidades participantes (artículo 11.6) y la falta de poderes coercitivos para implementar planes correctores me sugieren que el impacto real de estas medidas dependerá de la proactividad de los actores privados, un punto débil que podría limitar su eficacia frente a amenazas sistémicas. La asistencia mutua entre Estados miembros (artículo 18) y el apoyo a terceros países asociados al Programa Europa Digital (artículo 19), regulado mediante actos de ejecución del Consejo, refuerzan el principio de solidaridad, pero la complejidad del procedimiento de autorización (artículo 19.4) podría retrasar la respuesta en situaciones críticas, un riesgo que el reglamento no mitiga completamente.

La Reserva de Ciberseguridad, gestionada por la Comisión y parcialmente delegada a ENISA (artículo 14.5), introduce un modelo híbrido que combina compromiso previo de servicios con flexibilidad para convertirlos en acciones de preparación si no se utilizan (artículo 16.5). Esta adaptabilidad me parece un acierto, pero la dependencia de proveedores privados de confianza (artículo 17), con estrictos criterios de seguridad y certificación, podría reducir el *pool* de oferentes disponibles, afectando la capacidad de respuesta en un contexto de alta demanda. La evaluación de solicitudes en un plazo de 48 horas (artículo 16.1) es ambiciosa, pero su viabilidad operativa dependerá de la coordinación entre múltiples actores, un desafío que el reglamento deja en manos de futuros actos de ejecución (artículo 15.7).

5. MECANISMO EUROPEO DE REVISIÓN DE INCIDENTES

El Mecanismo Europeo de Revisión de Incidentes de Ciberseguridad (artículo 21) completa el enfoque del reglamento al centrarse en la evaluación retrospectiva de incidentes significativos o a gran escala. Entiendo que su objetivo de extraer conclusiones para prevenir futuros eventos responde a la necesidad de un aprendizaje continuo en un ámbito donde las amenazas evolucionan rápidamente. La implicación de ENISA, con el apoyo de la red de CSIRT y la aprobación de los Estados miembros afectados, me parece un enfoque equilibrado que respeta las competencias nacionales mientras fomenta una perspectiva unificada a nivel de la Unión.

La elaboración de informes detallados, que incluyen causas, vulnerabilidades y recomendaciones (artículo 21.3), tiene un valor evidente para la mejora de la ciberresiliencia, pero la opcionalidad de la anonimización y la exclusión de datos sobre vulnerabilidades activas (artículo 21.3) reflejan una cautela que podría limitar la utilidad práctica de los informes en situaciones de crisis en curso. Asumo que esta prudencia busca proteger la seguridad operativa, pero podría dificultar la difusión inmediata de información crítica. La publicación de informes (artículo 21.5) fomenta la transparencia, aunque el requisito de consentimiento de los Estados miembros afectados podría generar versiones descafeinadas, reduciendo su impacto educativo.

Diego FIERRO RODRÍGUEZ
Letrado de la Administración de Justicia
Codirector de la revista *Acta Judicial*
diego.fierro.ius@juntadeandalucia.es