La Directiva NIS2: implicaciones normativas, estratégicas y prospectivas para la ciberseguridad europea

Índice

Resumen/Abstract

El presente estudio analiza la Directiva (UE) 2022/2555 (NIS2), pieza esencial de la arquitectura de ciberseguridad comunitaria, desde una perspectiva multidisciplinar que combina enfoques jurídico, estratégico y geopolítico. Se examinan sus principales innovaciones respecto a la anterior Directiva NIS1, los desafíos de implementación, y su interacción con otras normas relevantes como el DORA, el RGPD o el Reglamento de Ciberresiliencia. Asimismo, se evalúan las amenazas actuales identificadas por las autoridades europeas como el ENISA, poniendo énfasis en la creciente sofisticación de los ciberataques, el protagonismo de actores no estatales y la dependencia tecnológica de la Unión Europea.

El proyecto identifica los principales riesgos y debilidades que plantea la situación de ciberseguridad europea en relación a la implementación de la NIS2, a la vez que resalta los beneficios y oportunidades derivados de su implementación. Finalmente, y atendiendo a la dimensión prospectiva, se proponen recomendaciones estratégicas y posibles escenarios de evolución, con el objetivo de aportar una visión útil sobre la importancia de garantizar la resiliencia digital y estratégica de la Unión.

This study analyses the Directive (EU) 2022/2555 (NIS2), essential corner of the Union's cybersecurity architecture, from the multidisciplinar perspective that combine legal, strategic and geopolitical approaches. It examines the mains innovations from the previous Directive (NIS1), the challenges of its implementations, and the interactions with others relevant frameworks such as DORA, RGPD or the Cyber resilience Act. In addition, it evaluates the currents threats which are identifies by the European authorities like ENISA, with particular emphasis on the growing sophistication of the cyberattacks, the rising prominence of the non-state actors, and the Union's technological dependency.

This project identifies the main risks and weaknesses affecting the European cybersecurity in relation to the NIS2's implementation, while also highlights its benefits and opportunities it entails. Finally, in the line with this study's prospective purpose, it formulates strategic recommendations and potential scenarios, aiming to provide a comprehensive insight the importance of ensuring Europe's digital and strategic resilience.

Palabras Clave

NIS2. Ciberseguridad. Unión Europea. Resiliencia Digital. Inteligencia estratégica. Autonomía estratégica. Autonomía tecnológica. Ciberamenazas. ENISA. Prospectiva.

Introducción

En un mundo cada vez más interconectado, donde la seguridad y la estabilidad están estrechamente entrelazadas, la ciberseguridad adquiere un protagonismo central. En el marco de la llamada Cuarta Revolución Industrial, en la que amplios sectores económicos, sociales e institucionales dependen de infraestructura digitales y redes de telecomunicaciones, la ciberseguridad se erige como pilar indispensable de la seguridad nacional e internacional.

A esta realidad se suma un contexto geopolítico complejo para la Unión Europea. Los ciberataques constantes, muchos de ellos dirigidos contra infraestructuras críticas y sectores estratégicos, ponen en riesgo la estabilidad de los miembros, la seguridad de sus ciudadanos y la resiliencia de sus economías. Esta creciente exposición evidencia la necesidad de reforzar al máximo los mecanismos de protección ya existentes y de consolidar un enfoque común en materia de ciberseguridad.

En este escenario, la Unión Europea aprobó en diciembre del pasado 2022 la Directiva 2022/2555 del Parlamento Europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, más conocida como Directiva NIS2. Esta Directiva no solo responde a las exigencias técnicas derivadas del avance tecnológico, sino que también se inscribe en el proyecto de Autonomía Estratégica Europea. Su objetivo es reforzar la continuidad de los servicios considerados esenciales, proteger las cadenas de suministro y consolidar al Bloque como actor de referencia en este ámbito.

El presente artículo aborda la NIS2 desde una perspectiva multidisciplinar, analizando no solo sus implicaciones normativas, sino también sus dimensiones estratégicas y geopolíticas. Asimismo, se evaluarán sus fortalezas y debilidades, así como las amenazas y oportunidades que plantea el contexto internacional actual, con el fin de ofrecer una lectura crítica orientada al a inteligencia y prospectiva estratégica.

Marco Normativo y Contextualización de la Directiva NIS2

En los años previos a la aprobación de la NIS2, la situación de la ciberseguridad en la Unión Europea estaba marcada por un incremento constante en la frecuencia y sofisticación de los ciberataques. El *ENISA Threat Landscape 2021* reflejaba este panorama, donde el ransomware se consolidaba como la principal amenaza, afectando tanto a organismos públicos como a empresas privadas. Al mismo tiempo, la cibercriminalidad se expandía hacia nuevas formas de monetización, en particular la sustracción y el blanqueo de criptomonedas. Paralelamente, el criptohacking alcanzó niveles récord para la época, mientras que los ataques de denegación de servicio distribuido (DDoS) se volvieron más enfocados, persistentes y multivectoriales.

Otro fenómeno relevante fue la diversificación del malware, con actores maliciosos empleando lenguajes de programación poco comunes para evadir la detección. En paralelo, la pandemia del Covid-19 actuó como un multiplicador de riesgos, ya que aumentaron las brechas de datos en sectores críticos como el sanitario, y proliferaron las campañas de phishing aprovechando la crisis contextual. Todo ello puso de manifiesto la notable vulnerabilidad de sectores esenciales, sanidad, energía, transporte… evidenciando las limitaciones de la normativa vigente.

La Directiva 2016/1148 (NIS1), tenía como objetivo reducir las amenazas a los sistemas de redes y de información utilizados para servicios esenciales, garantizando su continuidad y contribuyendo tanto a la seguridad de la Unión como al correcto funcionamiento del Mercado Interior. La NIS1 supuso un avance en su momento, ya que estableció la base para los marcos nacionales de ciberseguridad, fomentó las capacidad reguladoras y creó mecanismos de cooperación entre los EE.MM como el Grupo de Cooperación y la Red de CSIRTs, y luego ampliado por la NIS2 con la creación del CyCLONe.

No obstante, la aplicación de la NIS1 mostró notables deficiencias. Su ámbito de aplicación ambiguo generaba interpretaciones divergentes entre los Estados miembros, lo que comprometía la homogeneidad del Mercado Interior. Además, dejaba una excesiva discrecionalidad en la aplicación de obligaciones de seguridad y notificación de incidentes, así como en las disposiciones de supervisión y cumplimiento. Estas debilidades afectaban a la ciberresiliencia colectiva de la Unión

Europea, ya que la vulnerabilidad de un Estado miembro podía comprometer la seguridad de los demás.

Para corregir estas deficiencias, la Unión Europea aprobó en diciembre del 2022 la Directiva 2022/2555, conocida como NIS2, respaldada jurídicamente por el artículo 114 del TFUE. La nueva norma introduce innovaciones sustanciales como, la superación de la rígida y obsoleta clasificación entre Operadores de Servicios Esenciales (OES) y Proveedores de Servicios Digitales (DSP), ya que esta distinción conceptual no reflejaba la actual incidencia de estos últimos en los procesos socioeconómicos del Mercado Interior, ya que estos desempeñan un papel vertebrador del sistema productivo.

Otra de las innovaciones fue el establecimiento de unos nuevos criterios que determinasen el ámbito de aplicación, basado estos en tres parámetros. En primer lugar el criterio de actividad, mediante el que se distingue entre Entidades Esenciales (EE) y Entidades Importantes (EI), con base en el impacto potencial en la cadena de suministro en el supuesto de su interrupción. En segundo lugar, el criterio del tamaño[1], ya que esta Directiva somete a las medianas empresas (50-250 empleados o facturación entre 10 y 50 millones de euros) y grandes empresas (más de 250 empleados o más de 50 millones de ingresos). En tercer lugar, el criterio de criticidad, que permite incluir incluso a pequeñas empresas que no estuviesen contempladas en los anexos de la Directiva, si su función es estratégica en la cadena de suministro.

Otra de las novaciones, consecuencia directa de las anteriores fue la ampliación de los sectores sometidos a su régimen jurídico, ya que la Directiva abarca 11 sectores como energía, transporte, sanidad, espacio, banca, infraestructuras financieras, administración pública, abastecimiento y gestión de aguas, infraestructuras digitales y TIC, como esenciales. También incorpora actividades como importantes, como servicios postales, residuos, industria química y manufacturera, investigación, alimentación y servicios digitales.

Por último, otra de las innovaciones a destacar es el refuerzo de las obligaciones y sistema sancionador, a fin de garantizar el cumplimiento de la Directiva, ya que el régimen jurídico impone a las entidades sometidas la adopción de medidas que cumplan unos mínimos más altos, aunque no

[1] Unión Europea. Recomendación 2003/361/CE sobre la definición de microempresas, pequeñas y medianas empresas. (6 de mayo de 2003).

exigiendo ninguna tecnología en concreto, solo medidas, tales como análisis de riesgos, protocolos de seguridad, planes de gestión de crisis, pruebas de penetración, sistemas de respaldo, entre otras. Además, introduce la responsabilidad jurídica directa sobre los órganos de dirección, reforzando así la obligación sobre la gobernanza interna de las empresas.

Así pues, la NIS2 no solo pretende corregir las deficiencias de la normativa predecesora, sino que representa también la ambición comunitaria de dirigir las políticas públicas hacia una ciberresiliencia más integrada y armonizada. Al mismo tiempo, pretende responder a una dimensión estratégica mayor, consolidando así una mayor autonomía tecnológica y la resiliencia de Bruselas en un escenario global caracterizado por el aumento de ciberamenazas de una pluridad de actores que abarcan desde sujetos criminales a Estados hostiles.

No obstante, la NIS2 no ha de entenderse de forma aislada, sino como el eje vertebrador de un cuerpo normativo mucho más amplio y que está en constante expansión. El Reglamento 2022/2554 (DORA) sobre resiliencia operativa digital, que refuerza las capacidades del sector financiero para resistir ciberincidentes evitando así riesgos sistémicos, el Reglamento 2025/38 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, el Reglamento 2019/881 relativo a ENISA y a la certificación de ciberseguridad, que consolidó el papel de la Agencia Europea de Ciberseguridad y estableció un marco europeo de certificación de productos y servicios TIC. Otras normativas complementarias como el Reglamento General de Protección de Datos (RGPD 2016/679), la Directiva 2002/58, o la Directiva 97/67 sobre normativa postal, que aunque no se centren en el campo de la ciberseguridad, interactúan de manera clave con esta en diversas materias. En conjunto, este marco normativo refleja la voluntad de la UE de fortalecer sus capacidades y garantizar una cohesión jurídica.

Situación Actual de la Ciberseguridad

La Directiva 2022/2555 (NIS2), aprobada en diciembre del 2022, fijaba un plazo de transposición, como cualquier Directiva, hasta el 17 de octubre del 2024. Sin embargo, a mayo del 2025, la Comisión Europea se vio obligada a instar y advertir formalmente a 19 Estados miembros a completar o encaminar la transposición mediante el envío de las respectivas cartas de

emplazamiento, otorgándoles un plazo de dos meses para adoptar las medidas necesarias. En caso contrario, la Comisión podría acudir al Tribunal de Justicia de la Unión Europea para exigir el cumplimiento de las obligaciones que se derivan de los Tratados. No obstante, la mayoría de Estados miembros ya han iniciado los procedimientos legislativos internos para preparar dicha transposición. Sin embargo esto no es óbice para evidenciar una de las grandes deficiencias del bloque europeo, la carencia de agilidad en la toma de decisiones y acciones así como la demora burocrática que en si misma perjudica gravemente, en este caso, la seguridad de los ciudadanos.

En cuanto al contexto de amenazas y riesgos en materia de ciberseguridad en la Unión, el Reporte sobre el Estado de la Ciberseguridad en la UE del 2024 y el Índice de Ciberseguridad de la UE del mismo año, destacan que las principales amenazas siguen siendo los ataques de denegación de servicio (DDoS), los ataques de ransomware y las instrucciones en bases de datos, que en su conjunto representan más del 50% de los incidentes registrados y comunicados. Asimismo, cobran especial relevancia las campañas de desinformación e injerencia extranjera, protagonizadas principalmente por grupos cercanos a los intereses rusos y chinos, destacándose sobretodo los primeros, cuyas acciones están dirigidas a influir en la opinión pública, especialmente en momentos de gran sensibilidad, como procesos electorales o movilizaciones sociales, con el fin de fomentar división y socavar la resiliencia comunitaria.

Los informes también subrayan el incremento de los ataques a las cadenas de suministro y a las instituciones públicas, así como la creciente incidencia del ciberdelito interno, fenómenos cuya evolución requiere un seguimiento constante y el refuerzo de las capacidades de respuesta. Ello pasa necesariamente por la transposición efectiva de la NIS2 y la aplicación práctica de sus disposiciones.

Por otro lado, el índice de Ciberseguridad de la UE 2024, que combina indicadores cuantitativos como cualitativos con puntuaciones de 0 a 100, situó el nivel agregado de la Unión en 62,65 puntos, con una desviación entre Estados miembros de tan solo 3,76 puntos, lo que indica cierta homogeneidad en el desempeño. Los mejores resultados se registraron en indicadores como la ciberseguridad empresarial, la protección sobre la divulgación de información sensible y la resiliencia en la gestión de datos, todos ellos con más de 90 puntos. También destacan positivamente indicadores relativos al comportamiento ciudadano en el uso seguido de internet y la colaboración transfronteriza basada en la red CSIRT y CyCLONe.

En contraste, los peores resultados se concentran en aspectos estratégicos como la inversión en ciberdefensa, la certificación formal de los CSIRT, las evaluaciones de riesgos en ciberseguridad y la asignación de fondos a I+D en el ámbito cibernético, ninguno de los cuales supera los 35 puntos sobre 100. Estos déficits ponen en relieve la brecha existente entre el marco regulatorio avanzado que impulsa la UE y la realidad de su implementación práctica, especialmente en ámbitos que requieren recursos sostenidos y una visión estratégica a largo plazo.

Más allá del panorama actual, los informes de ENISA incorporan una perspectiva prospectiva a 2030. La Agencia Europea advierte que, en los próximos años, el desarrollo de tecnologías como la computación cuántica y la inteligencia artificial añadirán una mayor complejidad al entorno de amenazas, lo que exigirá a los Estados miembros y a la propia Unión Europea reforzar sus capacidades.

Entre las tendencias identificadas destacan, un creciente protagonismo de actores no estatales; la previsión de que las amenazas actuales como los ataques a la cadena de suministro o las campañas de desinformación experimenten un leve descenso en su frecuencia pero mantengan su posición preeminente; y un aumento del peso de vulnerabilidades estructúrales, entre ellas los errores humanos, la explotación de sistemas obsoletos y las disrupciones medioambientales. En conjunto, estas tendencias reflejan que la ciberseguridad europea deberá evolucionar y aumentar su inversión.

Implicaciones para la Inteligencia en Ciberseguridad

La alerta temprana[2] es una de las mayores implicaciones, en un sentido amplio, para la inteligencia en ciberseguridad. Si bien esta figura se constituye como una de las obligaciones principales para todas aquellas entidades que sufran cualquier tipo de vulnerabilidad y/o ataque cibernético. En un plazo de 24 horas, han de retransmitir la información que tengan sobre el incidente al CSIRT o autoridad correspondiente. Así pues, un informe sobre la evolución de la situación conforme se vayan desarrollando las circunstancias y, en un plazo máximo de un mes, un informe final que ha de

[2] Unión Europea. Directiva 2022/2555 del Parlamento Europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (Artículo 23º)

contener la descripción del incidente y su gravedad para la cadena de suministro y/o el funcionamiento del Estado, el tipo de amenaza o ataque que haya desencadenado el incidente, las medidas que se hayan adoptado e implementado, si es necesario, las repercusiones transfronterizas del incidente. En cualquier caso, el CSIRT ha de ofrecer asistencia y entablar unas comunicaciones estables con todo los entes involucrados, así como comunicar a las autoridades pertinentes a efectos de posibles responsabilidades jurídicas que se pudieren derivar de las circunstancias, además de la posibilidad de incoar un proceso de investigación.

Todo esto, como se ha expuesto anteriormente, tiene una relevancia muy significativa para la generación de inteligencia, ya que la NIS2 impone la obligación de establecer sistemas y mecanismos de evaluación de riesgos e incidentes, de cuyos informes se tomarán como base para la mejora en la prevención, comunicación, gestión, coordinación e investigación de dichos incidentes, y en última instancia, generará inteligencia para optimizar la toma de decisiones. Asimismo, para la resiliencia de las instituciones es esencial la generación de este tipo de conocimiento, así como prever situaciones futuras en el contexto prospectivo, determinando patrones, encaminando así las medidas a adoptar tomando como base dichos informes. Por lo tanto, las implicaciones prospectivas y de inteligencia son amplias, pero resumibles en estos puntos: La creación de estrategias para la mejor resolución de incidencias, así como mejorar los sistemas de prevención y retroalimentación.

Como se especifica en la Directiva, los Estados miembros han de disponer y crear, en relación a las demás obligaciones y mecanismos que exige la normativa comunitaria, una Estrategia Nacional de Ciberseguridad (ENC)[3]. Por lo tanto, cada Estado miembro será en última instancia responsable de sus propias capacidades. No obstante, y como es tradicional en la Unión, no todos los Estados avanzan al mismo ritmo, pudiendo considerarse que actualmente hay nueve Estados miembros con estrategias de tercera generación, catorce con estrategias de segunda generación, y otros cuatro que presentan por primera vez sus propias estrategias. Independientemente de las diferencias entre las ENCs, hay una serie de objetivos comunes que se transforman en capacidades y que luego se materializarán en base a los recursos que se destinen por cada Estado miembro.

[3] Unión Europea. Directiva 2022/2555 del Parlamento Europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (Artículo 7º)

En lo que respecta a las implicaciones geopolíticas y geoestratégicas, la información derivada de los incidentes y de las obligaciones de notificación no se limita únicamente a reforzar las propias entidades afectadas, sino que constituye uno de los mayores activos estratégicos para la Unión Europea en su conjunto. Los datos recogidos permitirán anticipar campañas de injerencia extranjera, identificar patrones atribuidos a todo tipo de actores y evaluar más eficaz y eficientemente los riesgos en sectores e infraestructuras críticas de relevancia geoestratégica. En este sentido, la inteligencia generada no solo contribuye a la resiliencia estructural e institucional propia, sino que también fortalece el proyecto de autonomía estratégica de la UE en un contexto caracterizado por una mayor presencia de conflictividad híbrida.

Riesgos, Debilidades y Desafíos Potenciales

Pese a los aspectos positivos que introduce una norma de tal calibre como la NIS2, es innegable que también plantea una serie de riesgos y desafíos que potencialmente pueden afectar a las capacidades de ciberseguridad de los actores comprendidos en su ámbito de aplicación.

En primer lugar, la sobrerregulación. La NIS2 no debe entenderse como una norma aislada, sino como parte vertebral de un entramado normativo denso y complejo. Ello supone un riesgo evidente para las pequeñas y medianas empresas, pymes, que con frecuencia carecen de los medios y del personal suficientemente cualificado para adaptarse de manera eficiente a los requisitos. El exceso de reporting es un ejemplo claro, puede general “fatiga de cumplimiento”, reduciendo la calidad de la información transmitida y desvirtuando los objetivos de la propia Directiva. En consecuencia, la ciberseguridad corre el riesgo de convertirse en una mera obligación legal, en lugar de una oportunidad de mejora real en los servicios.

En segundo lugar, la vasta carga burocrática. La Unión Europea arrastra una dinámica característica propia, procesos lentos, complejos y pesados que retrasan y dificultan la toma de decisiones, que convierten a la Unión en un actor rezagado en un entorno global extremadamente dinámico y cambiante. A ello se suma la lentitud en la transposición de las Directivas, que acentúa la fragmentación y da lugar a una Europa de varias velocidades. Cuanto mayor es la carga burocrática y documental, mayor es la ventana de vulnerabilidad que pueden aprovechar tanto actores estatales como no estatales hostiles al bloque.

Directamente vinculado con lo anterior se encuentra el riesgo de fallo en la interoperabilidad transnacional. Aunque la NIS2 busca armonizar los marcos normativos, en la práctica persisten divergencias entre los Estados miembros en función de sus prioridades, capacidades y estrategias nacionales de ciberseguridad. Estas divergencias en última instancia, dificultan la coordinación en un área tan crítica como la ciberseguridad comunitaria. Si la interoperabilidad falla, el riesgo para el conjunto de la Unión es severo.

Otro desafío vital es la financiación. La implementación de las obligaciones derivadas de la NIS2 requiere importantes recursos económicos. Esto obliga a los Estados miembros a intervenir para apoyar a su tejido empresarial y sectores afectados, pero no todos cuentan con las mismas capacidades presupuestarias. En consecuencia, surgen desigualdades tanto en la inversión como en el desarrollo de capacidades, reflejandose, por ejemplo, en la dispar fortaleza de los CSIRTs nacionales.

El déficit de talento constituye asimismo un problema estructural. El capital humano especializado es esencial en todo proceso de ciberseguridad, y la demanda de perfiles crece a un ritmo que supera la capacidad de formación y atracción de profesionales. Conviene destacar que no solo se requieren ingenieros e informáticos, sino también perfiles no técnicos como analistas de inteligencia, especialistas en cumplimiento normativo, juristas, politólogos, gestores de riesgo, cuya escasez limita aún más la capacidad de respuesta. Sin una estrategia clara de captación y retención, este déficit amenaza con convertirse en un cuello de botella permanente.

Por último, la fragmentación tecnológica y dependencia externa siguen siendo uno de los mayores puntos débiles del bloque. La UE continúa siendo principalmente compradora y no productora, de buena parte de los componentes tecnológicos estratégicos. Esta dependencia conlleva vulnerabilidades estructúrales y riesgos geopolíticos de primer orden, al no garantizarse una autonomía estratégica digital, los intereses europeos permanecen expuestos a la influencia de actores externos, lo que limita la capacidad de la UE para garantizar su propia seguridad en el nuevo campo de conflicto, el ciberespacio.

Oportunidades y Beneficios

Tras haber analizado los principales riesgos y debilidades que persisten en la arquitectura de ciberseguridad europea, resulta imprescindible señalar también los beneficios y oportunidades que introduce la Directiva NIS2.

En primer lugar, la NIS2 consolida y amplia los mecanismos de cooperación y coordinación ya iniciados con la NIS1, contribuyendo de manera decisiva a la mejora de la resiliencia de la Unión Europea frente a incidentes cibernéticos. Estos instrumentos buscan precisamente reducir la fragmentación y reforzar la capacidad de respuesta conjunta, uno de los principales objetivos estratégicos de la Directiva.

En segundo término, la Directiva, junto con el resto de normativa complementaria, DORA, Reglamento de Ciberresiliencia, Reglamento de Certificación, entre otros, establecen un marco común de estándares mínimos de ciberseguridad, que se traduce en una mayor armonización de procedimientos de protección, detección y respuesta. Este marco común no solo eleva los niveles de exigencia técnica, sino que también garantiza una mayor previsibilidad para empresas y administraciones.

Otro de los beneficios clave es el impulso a sistemas de alerta temprana, comunicación fluida con autoridades y protocolos de gestión de incidentes. Gracias a una mayor coordinación transfronteriza, la UE puede reaccionar con mayor agilidad ante ataques de carácter transnacional, mitigando así los efectos disruptivos y reforzando la prevención.

La Directiva también contribuye al fortalecimiento del tejido empresarial europeo, al imponer obligaciones que elevan el nivel de protección de empresas grandes, medianas e incluso pequeñas entidades estratégicas. Esto no solo mejora su resiliencia frente a ataques, sino que incrementa la competitividad y atractivo del mercado europeo en un contexto global cada vez más dependiente de la confianza digital.

Otro beneficio fundamental es el fomento de la cooperación público-privada, favoreciendo el intercambio de información y de buenas prácticas entre empresas, administraciones nacionales y

organismos comunitarios. Este ecosistema colaborativo genera sinergias que multiplican la eficacia de las respuestas frente a ciberamenazas.

La NIS2 también impulsa una cultura de ciberseguridad más transversal, al exigir que los organismos de dirección de las entidades asuman responsabilidades directas en materia de gobernanza digital. Esto favorece la integración de la seguridad no solo en el ámbito técnico, sino en los niveles estratégicos y organizativos.

Por último, la Directiva se enmarca en la estrategia de autonomía estratégica europea, reforzando la capacidad del bloque para depender menos de actores externos en servicios críticos. En este sentido, la NIS2 no es únicamente un instrumento normativo, sino también un vector para avanzar hacia una verdadera independencia tecnológica y operativa de la Unión.

Recomendaciones Estratégicas y Escenarios

Para dar por cumplida la función estratégica y prospectiva del presente estudio, es necesario proponer una serie de recomendaciones que permitan reforzar las capacidades de ciberseguridad de la unión Europea en el marco de aplicación de la NIS2. La primera de ellas pasa por la reducción de la carga burocrática que caracteriza a las instituciones comunitarias. Bruselas debe aligerar los procedimientos administrativos y evitar duplicidades que terminan por generar fenómenos como la fatiga regulatoria, especialmente en las pymes, que carecen de los recursos suficientes para atender a procesos administrativos tan exigentes. Un exceso de reporting o de trámites formales no solo retrasa la implementación de medidas críticas y necesarias, sino que también degrada notoriamente la calidad de la información que se transmiten a las autoridades competentes.

En segundo lugar, resulta prioritario aumentar la asistencia técnica y económica a las pymes, verdadero motor económico de la Unión y, al mismo tiempo, uno de los eslabones más vulnerables en términos de ciberseguridad. La creación de programas específicos de financiación, capacitación y acceso a herramientas tecnológicas adaptadas es fundamental para que estas empresas puedan cumplir con los estándares exigidos y, además, transformen la ciberseguridad en una clara ventaja competitiva en lugar de percibirla únicamente como una carga normativa.

Una tercera línea estratégica se centra en reforzar la inversión en la cultura de defensa y, más específicamente, en la cultura de ciberseguridad. La resiliencia digital no puede depender únicamente de medidas técnicas, sino que exige un cambio cultural sostenido en el tiempo. Incluir contenidos de ciberseguridad en los sistemas educativos y fomentar la corresponsabilidad en el uso seguro de la tecnología son medidas que contribuyen a generar un ecosistema social más consciente y preparado a los riesgos del presente y del futuro.

Al mismo tiempo, es esencia del desarrollo de una verdadera industria europea de ciberseguridad. La dependencia de proveedores externos, tanto en hardware como en software, constituye una vulnerabilidad anteriormente explicada y que limita su autonomía estratégica. Fomentar la innovación, apoyar a startups y financiar proyectos de I+D+i en el ámbito de la ciberseguridad contribuiría a reforzar la base tecnológica propia, capaz de sostener la competitividad y la resiliencia a largo plazo.

Otra de las recomendaciones fundamentales consiste en avanzar en la armonización normativa y de requisitos. La fragmentación nacional interna limita la eficacia de la NIS2 y perpetúa asimetrías en la aplicación de medidas entre los Estados miembros. Resulta imprescindible, por tanto, trabajar hacia estándares comunes más detallados, reforzando los ENSs y garantizar la interoperabilidad real de los sistemas de notificación, evaluación de riesgos y supervisión. Solo de esta manera se podrá asegurar una respuesta homogénea y eficaz a nivel comunitario.

En paralelo, debe reforzarse el papel de ENISA, que ha de evolucionar hacia un rol más operativo. Dotar a esta agencia de competencias ejecutivas en materia de gestión de crisis, supervisión de cumplimiento e incluso sanción, siempre en estrecha coordinación con las autoridades comunitarias y los CSIRTs nacionales, permitiría reducir la dispersión de competencias y agilizar la toma de decisiones en contextos de amenaza creciente.

Finalmente, el déficit de talento constituye otro de los grandes retos que deben abordarse. La Unión necesita políticas activas para atraer y retener capital humano, no solo en perfiles técnicos, como ingenieros, sino también en ámbitos más estratégicos, de gestión, de riesgo y de cumplimiento normativo. Ampliar programas de movilidad y becas, mejorar las condiciones laborales e introducir

incentivos fiscales puede contribuir a revertir una situación que actualmente limita el desarrollo de las capacidades en ciberseguridad.

En lo que respecta a los escenarios que se dilucidan de cara al horizonte 2030, se contemplan tres escenarios prospectivos para la ciberseguridad de la Unión Europea en relación con la NIS2:

- Escenario Optimista: En este escenario, la Directiva NIS2 es transpuesta de manera eficaz, homogénea y coordinada en todos los Estados miembros, lo que permite superar las habituales asimetrías normativas de la Unión Europea. La cooperación transfronteriza se consolida, los CSIRTs nacionales alcanzan plena interoperabilidad y se refuerza la coordinación de las ENSs, e inclusive se plantea la creación de una única Estrategia de Seguridad a nivel europeo. Paralelamente, emerge una industria europea de ciberseguridad con creciente capacidad competitiva, apoyada por fondos específicos destinados a reforzar este programa, así como el aumento de la dotación de los fondos destinados a mejorar la resiliencia cibernética de las pymes. Esta dinámica reduce progresivamente la dependencia tecnológica de actores externos y convierte a la Unión en un referente mundial en materia de ciberseguridad y gobernanza digital. En este sentido, Bruselas comenzaría a exportar sus estándares regulatorios y reforzaría su posición a nivel global. No obstante, dadas las condiciones actuales de fragmentación e inestabilidad política, incapacidad en captar y mantener talento y las notables limitaciones presupuestarias y de implementación normativa, este escenario se presenta con una probabilidad altamente reducida.

- Escenario Neutral: En este escenario, la implementación de la NIS2 avanza con resultados desiguales entre los Estados miembros. Aunque persisten algunas divergencias normativas, se logran avances sustanciales en la cooperación transfronteriza, en la coordinación de los ENSs y la generación de una cultura de ciberseguridad más arraigada. Se financias proyectos de industria cibernética europea, pero estos no alcanzan la competitividad y solidez necesaria frente a potencias tecnológicas externas, limitando el impacto del proyecto de autonomía estratégica digital. La Unión alcanza un mayor grado de resiliencia frente a los ciberataques, lo que impulsa modificaciones posteriores de la Directiva. La Unión mejora su cohesión normativa y preventiva, aunque sin conseguir una plena independencia tecnológica. En consecuencia el bloque continúa condicionado por influencias externas, especialmente de Estados Unidos y Taiwán. Este escenario se perfila como el más probable teniendo en cuenta el contexto actual.

- Escenario Pesimista: En este escenario, la transposición e implementación de la NIS2 se ve obstaculizada por la sobrerregulación, la falta de recursos financieros y las persistentes divergencias entre Estados miembros. La fragmentación normativa, y el déficit de talento limitan la operatividad tanto de los CSIRTs como de los demás entes público-privados, además de que la ausencia de un apoyo consolidado y suficiente a las pymes e industrias impide el desarrollo de un ecosistema europeo sólido de ciberseguridad. La Unión permanece altamente dependiente de Estados Unidos además de otros actores para su suministro tecnológico, lo que compromete su autonomía estratégica y capacidad de toma de decisión internacional. En este escenario, los ciberataques aumentan en frecuencia y gravedad, afectando a infraestructuras críticas, debilitando la competitividad económica europea y erosionando la confianza ciudadana en las instituciones comunitarias. La falta de resiliencia digital alimenta divisiones internas, reduciendo la capacidad de Bruselas de ejercer influencia geopolítica en el ciberespacio, afectando a su vez al proyecto de integración europea. Este escenario sigue siendo posible si no se aborda de manera urgente las problemáticas ya identificadas tanto por parte de los Estados miembros como por parte de las instituciones y autoridades europeas.

Conclusiones

La NIS2 constituye un salto cualitativo en el proyecto de construir una Europa más resiliente, consciente de que en el contexto de esta cuarta revolución industrial, la ciberseguridad se ha convertido en un elemento inseparable de la seguridad nacional, económica y social. Sin embargo, la Directiva por si sola no consigue resolver los problemas estructurales del bloque, como las asimetrías entre los Estados miembros, la lentitud burocrática y de actuación, la escasez de captación y retención del talento y la dependencia tecnológica extranjera. Si bien nos ofrece un marco regulatorio amplio y avanzado, su éxito depende en gran medida de su implementación y aplicación, de forma coherente, coordinada y de compromiso a largo plazo, tanto por la Unión Europea como por sus Estados miembros.

La NIS2 no debe entenderse meramente como una herramienta jurídica, sino como una de las formas en las que la Unión Europea está pretendiendo avanzar en su programa de Autonomía Estratégica en un mundo caracterizado por la conflictividad hibrida, las estrategias de zona gris y la competencia tecnológica. Si Bruselas logra abarcar las recomendaciones propuestas, entre otras, la

NIS2 podrá convertirse en el pilar de un futuro ecosistema digital europeo más seguro, resiliente, competitivo e independiente.

Bibliografía

I. *Agencia de la Unión Europea para la Ciberseguridad*. (s. f.). European Union. de https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_es

II. Carrasco, E. B. (2025, septiembre 25). *ENISA en la nueva arquitectura de ciberseguridad europea*. LISA News. https://www.lisanews.org/ciberseguridad/el-papel-de-enisa-en-la-nueva-arquitectura-de-ciberseguridad-europea/

III. *Ciberdefensa*. (21 de marzo del 2025). Consejo Europeo y Consejo de la Unión Europea. https://www.consilium.europa.eu/es/policies/cyber-defence/

IV. *El 'Índice de Ciberseguridad de la UE' 2024 revela carencias en ciberseguridad pese a los avances en políticas digitales*. (20 de junio de 2025). Red Seguridad. https://www.redseguridad.com/actualidad/ciberseguridad/el-indice-de-ciberseguridad-de-la-ue-2024-revela-mejoras-en-ciberseguridad-pese-a-los-avances-en-politicas-digitales_20250620.html

V. ENISA. (2024). The EU-Cybersecurity Index 2024. EU-level insights and next steps.

VI. ENISA. (2024). 2024 Report on the State of Cybersecurity in the Union.

VII. ENISA. (2025). ENISA Cybersecurity Maturity & Criticality Assessment of NIS2 sectors.

VIII. *EU CyCLONe*. (s. f.). Europa.Eu. de https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cyclone

IX. IT Digital Media Group. (2025, junio 24). *¿Qué implicaciones tiene la NIS2 para las estrategias de ciberseguridad?* IT Digital Media Group. https://www.itdigitalsecurity.es/infraestructuras-criticas/2023/10/que-implicaciones-tiene-la-nis2-para-las-estrategias-de-ciberseguridad

X. Leonés, E. (2024, marzo 25). *Directiva NIS 2*. Ingertec.com; INGERTEC. https://ingertec.com/ciberseguridad/directiva-nis-2/?6609039339&nis2&gad_source=1&gad_campaignid=23009107354&gbraid=0AAAAAD-aDzn_jqljKnoxhMwTkwygR7cA0&gclid=Cj0KCQjw58PGBhCkARIsADbDilwWEdkkqZk4dDPDo2y7MFdlj5oemGRsU5cWkqOZMvn1BRaAegKiiZgaAqOfEALw_wcB

XI. *NIS2: todo sobre la directiva de ciberseguridad de la UE*. (2024, noviembre 7). IONOS Digital Guide. https://www.ionos.es/digitalguide/servidores/seguridad/directiva-nis2/?itc=3VVVRR75-HUKYUQ-66GYJ6Z&utm_source=google&utm_medium=cpc&utm_campaign=SGE-ES-ECL-ECLX-PMX--PrivateCloud---&utm_content=PrivateCloud&gclsrc=aw.ds&gad_source=1&gad_campaignid=22761044537&gbraid=0AAAAAo6N9g_kBhBFZJ7W37j9tveF3BLmd&gclid=Cj0KCQjw58PGBhCkARIsADbDilzF01t4UROshL2QM-4oWcaNRcWzoJzoVuYTetFvGmkU6neBb-7QH1saAp2uEALw_wcB

XII. *Transposición de la Directiva SRI 2 en los países de la UE*. (s. f.). Configurar el futuro digital de Europa. de https://digital-strategy.ec.europa.eu/es/policies/nis-transposition

XIII. Unión Europea. Directiva 97/67/CE relativa a las normas comunes para el desarrollo del mercado interior de los servicios postales de la Comunidad y la mejora de la calidad del servicio. (15 de diciembre de 1997). https://www.boe.es/buscar/doc.php?id=DOUE-L-1998-80098

XIV. Unión Europea. Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). (12 de julio de 2002). https://www.boe.es/doue/2002/201/L00037-00047.pdf

XV. Unión Europea. Directiva 2022/2555 del Parlamento Europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). (14 de diciembre del 2022). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022L2555

XVI.Unión Europea. Recomendación 2003/361/CE sobre la definición de microempresas, pequeñas y medianas empresas. (6 de mayo de 2003). https://www.boe.es/buscar/doc.php?id=DOUE-L-2003-80730

XVII.Unión Europea. Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). (27 de abril de 2016). https://www.boe.es/doue/2016/119/L00001-00088.pdf

XVIII.Unión Europea. Reglamento 2019/881 relativo a ENISA y a la certificación de ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) no 526/2013. (17 de abril de 2019). https://www.boe.es/buscar/doc.php?id=DOUE-L-2019-80998

XIX.Unión Europea. Reglamento 2025/38 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 Cibersolidaridad). (19 de diciembre de 2024). https://www.boe.es/buscar/doc.php?id=DOUE-L-2025-80049

XX.Unión Eurpea. Reglamento 2022/2554 del Parlamento Europeo y del Consejo sobre la resiliencia operativa digital del sector financiero. (14 de diciembre de 2022). https://eur-lex.europa.eu/eli/reg/2022/2554/oj?eliuri=eli%3Areg%3A2022%3A2554%3Aoj&locale=es