MÁSTER EN ANALISTA DE INTELIGENCIA

Informe sobre la Ley de Coordinación y Gobernanza de la ciberseguridad NIS 2

Autores:

Iris Teresa Obiang Pérez

Gonzalo Rojas Martínez

Gustavo Horna Zamora

Adrián Cisneros Jiménez

1 de noviembre de 2025

Introducción

La Directiva (UE) 2022/2555, conocida como NIS 2 (Directiva SRI 2) se ha constituido como la piedra angular de la normativa europea en materia de ciberseguridad. Su objetivo fundamental es garantizar un elevado nivel común de ciberseguridad y ciberresiliencia en toda la Unión para mejorar el funcionamiento del mercado interior. Esta directiva surge como una evolución y refuerzo de la anterior Directiva NIS (Directiva (UE) 2016/1148), la cual había mostrado deficiencias en su aplicación fragmentada y disparidad en los niveles de ciberresiliencia entre los Estados miembros.

Como modificación fundamental podemos señalar que la NIS2 amplía significativamente el alcance de los sectores y entidades cubiertas en comparación con NIS 1.

Amplia el objeto de entidades a las que se dirige, siendo éstas, entidades públicas o privadas que operen en la UE y pertenezcan a sectores definidos, y que generalmente son medianas o grandes empresas (más de 50 empleados y 10 millones de euros de volumen de negocios/balance).

La directiva clasifica las entidades en dos categorías basadas en la criticidad de su sector: entidades esenciales y entidades importantes.

Las entidades esenciales incluyen sectores como energía (electricidad, gas, hidrógeno), transporte, banca, infraestructura de mercados financieros, sector sanitario, infraestructura digital, y gestión de servicios TIC (de empresa a empresa), y debido a su criticidad están sujetas a supervisión proactiva.

Las entidades importantes incluyen servicios de correo y mensajería, gestión de residuos, fabricación (alimentos, productos sanitarios, informáticos, maquinaria, vehículos de motor), y proveedores de servicios digitales, entre otros. Aquí la supervisión será reactiva, siendo monitorizados después de que se notifique un incidente de incumplimiento.

La NIS 2 establece requisitos rigurosos para la gestión de los riesgos y obligaciones de notificación con un marco temporal en varias etapas, así como directrices en múltiples áreas: gobernanza, políticas de seguridad y análisis de riesgos, para la continuidad de las actividades, seguridad de la cadena de suministro, uso de criptografía, control de acceso, autenticación multifactorial (MFA) y prácticas básicas de ciberhigiene y formación.

La Directiva obliga también a los Estados miembros a la implementación en la transposición de un régimen sancionador y medidas de supervisión eficaces, proporcionales y disuasorias como inspecciones, auditorias, políticas y por supuesto sanciones.

Análisis

1. Contexto y Antecedentes

1.1. Evolución de la ciberseguridad en la UE

La ciberseguridad ha ganado un papel central en la agenda estratégica de la Unión Europea (UE) a medida que la digitalización se ha acelerado y extendido a todos los sectores económicos y sociales. La primera respuesta normativa integral fue la Directiva (UE) 2016/1148, también conocida como NIS, que estableció un marco común para reforzar la ciberinteligencia de las infraestructuras críticas y esenciales dentro del mercado único digital. Esta directiva obligó a los Estados miembros a:

- Adoptar estrategias nacionales de ciberseguridad.
- Designar autoridades competentes y equipos de respuesta a incidentes de seguridad informática (CSIRT).
- Exigir a ciertos operadores de servicios esenciales y proveedores digitales la aplicación de medidas de gestión de riesgos y notificación de incidentes.

La Directiva NIS supuso un punto de partida importante, pero su aplicación práctica reveló debilidades significativas, como una implementación desigual entre países y un alcance limitado en sectores y entidades cubiertas.

1.2. De la Directiva NIS (2016/1148) a NIS 2 (2022/2555)

Tras una revisión exhaustiva, la Comisión Europea propuso en 2020 una actualización integral, que resultó en la adopción de la Directiva (UE) 2022/2555 (NIS 2). Esta nueva normativa fue adoptada oficialmente el 14 de diciembre de 2022 y deroga a la anterior.

NIS 2 representa una evolución significativa en la gobernanza de la ciberseguridad al:

- Ampliar el número de sectores y entidades cubiertos, incluyendo sanidad, servicios postales, gestión de aguas y espacio, entre otros.
- Clasificar las entidades como esenciales o importantes, con requisitos diferenciados.
- Establecer un enfoque más armonizado y menos discrecional para los Estados miembros.
- Reflejar un cambio de paradigma: de la protección individual a un enfoque sistémico de resiliencia cibernética en toda la UE.

1.3. Amenazas cibernéticas actuales y necesidad de actualización normativa

El crecimiento exponencial de ciberataques, en especial durante la pandemia de COVID-19, ha puesto de manifiesto las vulnerabilidades estructurales de las sociedades digitalizadas. Los incidentes relacionados con ransomware, el ciberespionaje, los ataques a la cadena de suministro y las interrupciones de servicios críticos han aumentado en volumen y sofisticación.

Estas amenazas generan:

- Pérdidas económicas significativas.
- Interrupciones en servicios esenciales.
- Riesgos para la seguridad nacional y la confianza ciudadana en las infraestructuras digitales.

Ante este panorama, la NIS 2 establece un marco actualizado para hacer frente a riesgos sistémicos y transfronterizos, con una perspectiva preventiva, coordinada y basada en riesgos, reforzando tanto las capacidades nacionales como la cooperación a escala europea.

2. Análisis de la Directiva (UE) 2022/2555 (NIS 2)

2.1. Objetivos principales

La Directiva NIS 2 tiene como propósito garantizar un elevado nivel común de ciberseguridad en toda la Unión Europea, abordando las deficiencias observadas en la anterior Directiva NIS (2016/1148). Sus objetivos fundamentales son:

- Ampliar y armonizar los requisitos de ciberseguridad en los Estados miembros.
- Reducir la fragmentación normativa del mercado interior.
- Reforzar la resiliencia de los sectores críticos, incluyendo nuevos ámbitos clave.
- Mejorar la cooperación y respuesta ante incidentes mediante mecanismos coordinados a nivel europeo.

2.2. Ámbito de aplicación

Uno de los cambios más sustanciales introducidos por la Directiva NIS 2 respecto a su predecesora radica en la expansión de su ámbito de aplicación. Mientras que la Directiva NIS original se centraba en un número limitado de operadores de servicios esenciales y proveedores de servicios digitales, la nueva normativa amplía significativamente la cobertura sectorial, institucional y empresarial. Esta expansión responde a la necesidad de abordar un panorama de amenazas cibernéticas cada vez más complejo e interconectado, en el que los vectores de riesgo no se limitan a sectores tradicionalmente considerados críticos.

NIS 2 incorpora una gama más amplia de sectores clave, incluyendo salud, gestión de aguas, residuos, servicios postales, fabricación de productos críticos, infraestructura digital como redes de telecomunicaciones y servicios en la nube, y hasta el sector espacial, reflejando una visión más integral de la economía digital. Esta inclusión no se limita a sectores por sí mismos, sino que también contempla el tipo de actividad desempeñada y su impacto potencial en la sociedad y el mercado interior.

Para determinar si una entidad está sujeta a las obligaciones de la directiva, NIS 2 establece un criterio objetivo: quedan comprendidas todas aquellas entidades que superen el umbral de una mediana empresa, aunque también se prevé la inclusión de organizaciones más pequeñas si prestan servicios de especial importancia. Esta aproximación basada en criterios uniformes sustituye al sistema anterior,

en el que los Estados miembros tenían mayor discrecionalidad para definir qué organizaciones debían ser consideradas operadores esenciales.

No obstante, la Directiva también establece ciertas excepciones. Quedan fuera de su ámbito las entidades cuya actividad esté estrechamente vinculada a la seguridad nacional, la defensa, la seguridad pública o las funciones policiales. Esta exclusión busca respetar las competencias estatales en materias sensibles, preservando al mismo tiempo la coherencia con el resto del marco normativo europeo en materia de seguridad.

2.3. Entidades esenciales y entidades importantes

Para facilitar la implementación y supervisión de las obligaciones de ciberseguridad, la Directiva NIS 2 introduce una clasificación estructurada de los sujetos obligados. Este modelo dual distingue entre entidades esenciales y entidades importantes, en función de la criticidad del sector en el que operan y del tipo de servicio que prestan.

Las entidades esenciales son aquellas cuya actividad se considera de vital importancia para el funcionamiento de la sociedad, la economía o los servicios públicos. Incluyen operadores en sectores como la energía, el transporte, la sanidad, las infraestructuras digitales, el suministro de agua y la administración pública. Estas entidades, dada su relevancia estratégica, están sujetas a una supervisión más estricta, continua y proactiva por parte de las autoridades competentes, que pueden realizar inspecciones, auditorías y otras medidas preventivas incluso sin indicios previos de incumplimiento.

Por su parte, las entidades importantes también realizan funciones relevantes desde el punto de vista económico o social, pero con un nivel de criticidad menor o con un impacto potencial más limitado en caso de incidente. En su caso, la supervisión es más flexible y se activa principalmente a través de mecanismos reactivos, es decir, tras la ocurrencia de incidentes significativos o la detección de posibles fallos en el cumplimiento de las obligaciones.

Esta diferenciación no implica diferencias sustanciales en cuanto a las medidas de seguridad exigidas, pero sí en lo referente al control administrativo y la intensidad del seguimiento, lo que permite una implementación más proporcional y eficiente de los recursos de supervisión.

2.4. Obligaciones de seguridad y notificación

Uno de los pilares centrales de la Directiva NIS 2 es el establecimiento de obligaciones reforzadas para las entidades incluidas en su ámbito. Estas obligaciones no se limitan a la reacción ante incidentes, sino que exigen una estrategia preventiva basada en la gestión integral del riesgo.

Cada entidad debe adoptar medidas técnicas y organizativas adecuadas para proteger sus sistemas de redes y de información frente a ciberamenazas. Estas medidas deben estar adaptadas a la naturaleza de los riesgos que enfrentan y contemplar aspectos como la seguridad de la cadena de suministro, la protección frente a vulnerabilidades conocidas, la formación del personal, y la implementación de prácticas de ciberhigiene sostenidas en el tiempo.

Además, se exige la elaboración de planes de continuidad operativa y recuperación ante desastres que garanticen la prestación de los servicios esenciales incluso en situaciones de crisis cibernética. Esto implica no solo disponer de infraestructuras resilientes, sino también de protocolos claros de toma de decisiones y comunicación interna y externa.

Una novedad relevante de NIS 2 es el endurecimiento de los requisitos de notificación de incidentes. Las entidades deben informar sin demora injustificada a las autoridades competentes o al CSIRT nacional cuando sufran un incidente de seguridad con impacto significativo. Esta notificación debe realizarse preferiblemente en un plazo máximo de 24 horas desde que se tenga conocimiento del incidente, lo que exige una capacidad de detección y respuesta muy ágil por parte de las organizaciones. Este enfoque busca fortalecer la capacidad colectiva de reacción del sistema europeo de ciberseguridad, permitiendo respuestas coordinadas y efectivas ante amenazas comunes.

2.5. Supervisión, ejecución y sanciones

La Directiva NIS 2 introduce un marco más robusto de supervisión y cumplimiento, que refuerza las facultades de las autoridades nacionales en materia de ciberseguridad. A diferencia de la anterior directiva, donde el margen de aplicación era más discrecional y la vigilancia dependía en gran medida del enfoque de cada Estado miembro, la nueva normativa armoniza los criterios de control y dota a los organismos supervisores de herramientas más eficaces.

Las autoridades competentes podrán realizar auditorías periódicas, inspecciones in situ, entrevistas técnicas y requerimientos de documentación o pruebas de cumplimiento. La intensidad de estas acciones dependerá, como se ha señalado, de si se trata de una entidad esencial o importante, pero en ambos casos el objetivo es garantizar que las obligaciones se traduzcan en prácticas efectivas.

En cuanto a las consecuencias del incumplimiento, la Directiva establece un régimen sancionador armonizado a escala europea, que permite imponer multas significativas. Las sanciones pueden alcanzar los 10 millones de euros o el 2% del volumen de negocios anual global de la entidad infractora, adoptando así un modelo similar al que ya se aplica en el ámbito de la protección de datos con el Reglamento General de Protección de Datos (RGPD). Esta dimensión económica busca ejercer un efecto disuasorio, especialmente en sectores donde las medidas de ciberseguridad podrían ser relegadas por prioridades comerciales.

Además, se contemplan mecanismos específicos para la gestión de incidentes con impacto transfronterizo, mediante canales de notificación conjuntos y cooperación entre autoridades de diferentes Estados miembros. Esto permite que una amenaza detectada en un país pueda ser gestionada de forma coordinada con otros, mitigando riesgos sistémicos y evitando respuestas fragmentadas.

2.6. Gobernanza europea: rol de la ENISA y cooperación entre Estados Miembros

La NIS 2 establece una estructura de gobernanza cibernética más robusta, en la que destacan:

- ENISA (Agencia de Ciberseguridad de la UE): proporciona apoyo técnico, emite directrices, coordina con los CSIRT y participa en el análisis de riesgos y amenazas.

- Grupo de Cooperación: compuesto por representantes de los Estados miembros, la Comisión y ENISA. Su función es facilitar el alineamiento normativo, el intercambio de buenas prácticas y la planificación estratégica.
- Red de CSIRT: facilita la respuesta operativa coordinada ante incidentes.
- EU-CyCLONe: nuevo mecanismo para la gestión de crisis cibernéticas a gran escala a nivel de la UE.

Este sistema refuerza la interoperabilidad, confianza y respuesta conjunta ante incidentes que pueden tener repercusiones transfronterizas.

3. Estado de la transposición de la Directiva NIS2 en España

La transposición de la Directiva NIS 2 al derecho nacional debía completarse antes del 18 de octubre de 2024. España ha promovido un Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad que debería constituirse en esa transposición, pero a fecha de elaboración del presente informe todavía no se ha aprobado, siendo sancionada conforme señala la normativa europea en estos supuestos.

Conviene destacar que la falta de transposición genera un riesgo aún más grave, al provocar una notable inseguridad jurídica para los sujetos obligados, que carecen de un marco legislativo nacional claramente definido que les permita adaptarse de manera precisa y efectiva a las exigencias de la norma. Debido al objeto que regula, los riesgos asociados a esa inseguridad son elevados porque esta Directiva busca fundamentalmente la implementación de medidas para aumentar el nivel de seguridad en las redes y sistemas de información de las empresas obligadas, sectores ya definidos como críticos, y mejorar la gestión de riesgos cibernéticos así como el establecimiento de mecanismos comunes de ciberdefensa en la Unión Europea que permitan garantizar la continuidad y la integridad de los servicios digitales ante cualquier amenaza o incidente de seguridad. Por ello, la falta de obligaciones concretas y homogéneas a nivel nacional puede aumentar la vulnerabilidad de las organizaciones obligadas a su cumplimiento, incrementando al mismo tiempo su riesgo de sufrir ciberataques al no disponer de mecanismos adecuados de prevención y gestión de riesgos ni de políticas adecuadas de seguridad que exige la normativa europea.

El Anteproyecto de la norma que debe realizar dicha transposición designa al Centro Nacional de Ciberseguridad como autoridad competente en España, siendo señalada como la encargada de la gestión de crisis y punto de contacto único, coordinando a los CSIRT nacionales (como CCN-CERT, INCIBE-CERT, ESPDEF-CERT y OCC-Policía Judicial del Mº del Interior). En relación con la clasificación establecida por la NIS2, el Anteproyecto también contiene algunas modificaciones como la inclusión del sector de la industria nuclear y las empresas de seguridad privada.

A la hora de analizar la NIS2 y su transposición a través del Anteproyecto mencionado hay que tener en cuenta también la Estrategia Nacional de Ciberseguridad (ENCS), la cual debe alinearse con las

pautas establecidas por la UE, tanto en la Estrategia europea de ciberseguridad 2020, como con las distintas políticas y recomendaciones emitidas. Entre esos puntos y recomendaciones conviene destacar la Política de Ciberdefensa de la UE de 2022, el 5G, la certificación, la protección de cables submarinos o el "pacto cuántico". Tanto el articulado de la Directiva como su transposición nacional tienen que concretar en buena parte los elementos que la Estrategia Nacional de Ciberseguridad de los Estados miembros debe contener, incluyendo: políticas concretas para luchar contra el auge de los ciberataques de tipo ransomware, para el fomento de la ciberprotección activa o aquellas dirigidas a la protección específica de los servicios públicos básicos digitalizados.

A fecha actual, España aún no ha completado la transposición de la Directiva (UE) 2022/2555 (NIS2), cuyo plazo expiró el 17 de octubre de 2024. El Consejo de ministros aprobó el 14 de enero de 2025 el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, actualmente en tramitación parlamentaria. La Comisión Europea ha iniciado un procedimiento de infracción contra España por el retraso en la transposición, lo que sitúa al país bajo presión política y jurídica para acelerar su aprobación.

Hasta que la nueva ley entre en vigor, continúan aplicándose el Real Decreto-ley 12/2018, que incorporó la anterior Directiva NIS1, su desarrollo reglamentario (Real Decreto 43/2021) y la Ley 8/2011 sobre protección de infraestructuras críticas.

El Anteproyecto introduce un nuevo modelo de gobernanza, con la creación de un Centro Nacional de Ciberseguridad y una estructura reforzada de coordinación entre autoridades, CSIRTs y operadores críticos. España se encuentra, por tanto, en una fase de transición normativa en la que conviven el marco vigente y el proceso de adaptación a NIS2, lo que genera un escenario regulatorio híbrido y cierta incertidumbre operativa.

El texto refuerza las exigencias en gestión de riesgos, notificación de incidentes y cumplimiento de medidas de seguridad, e introduce un régimen sancionador alineado con los estándares europeos. Además, consolida los mecanismos de cooperación internacional, garantizando la plena integración de España en las redes europeas de alerta y respuesta.

El modelo español de ciberseguridad se articula en torno a una red de actores públicos y privados. La autoridad nacional corresponde al Ministerio para la Transformación Digital y la SEDIA, que coordina organismos como el Centro Criptológico Nacional (CCN-CERT), el Instituto Nacional de Ciberseguridad (INCIBE-CERT) y el Mando Conjunto del Ciberespacio (MCCE). Estos organismos conforman la red nacional de CSIRTs, que garantiza la cooperación técnica y la gestión coordinada de incidentes. En el ámbito privado, la ley amplía las obligaciones a un mayor número de entidades esenciales e importantes (energía, transporte, salud, banca, agua o infraestructuras digitales), que deberán cumplir con estándares más estrictos de seguridad y notificación. Hasta su integración plena en el nuevo marco, los operadores críticos seguirán rigiéndose por la Ley 8/2011 y su normativa de desarrollo.

La ley establece una arquitectura de gobernanza que articula tres niveles de actuación: estratégico, operativo y técnico. En el nivel político-estratégico, el Consejo Nacional de Ciberseguridad se consolida como órgano superior de coordinación, responsable de definir directrices, evaluar riesgos y gestionar crisis de ciberseguridad. En el nivel operativo, la red nacional de CSIRTs centraliza el intercambio de información y la respuesta coordinada ante incidentes, mientras que el futuro Centro Nacional de Ciberseguridad actuará como punto de apoyo técnico y de enlace con las instituciones europeas.

La norma promueve la cooperación público-privada y la supervisión continua del cumplimiento normativo, generando un sistema más integrado, ágil y resiliente. Asimismo, establece un sistema de supervisión proactiva basado en inspecciones, auditorías y planes de cumplimiento. Las entidades esenciales e importantes deberán acreditar su capacidad de gestión del riesgo y mantener actualizados sus procedimientos internos. Se refuerzan los mecanismos de notificación de incidentes y la capacidad de respuesta coordinada a través del Centro Nacional de Ciberseguridad y los CSIRTs sectoriales.

El enfoque se desplaza de la reacción a la prevención, promoviendo la cooperación, la transparencia y la mejora constante de las capacidades nacionales

4. Implicaciones estratégicas y operativas en la transposición nacional: Situación de España

La nueva Ley de Coordinación y Gobernanza de la Ciberseguridad, que transpone la Directiva NIS2 al ordenamiento jurídico español, transformará profundamente la estructura de la ciberseguridad en España. Su aprobación permitirá reforzar el papel del Estado, promover una gestión más preventiva y continua del riesgo, y establecer un sistema más cohesionado e integrado con los mecanismos europeos de respuesta ante incidentes.

En el plano estratégico, la norma representa un paso decisivo hacia la consolidación de un modelo nacional de gobernanza que unifique criterios, refuerce la coordinación interinstitucional y eleve los estándares de resiliencia digital. Además, su implementación contribuirá a una mayor trazabilidad de la información, una cooperación más sólida entre organismos públicos y privados y una integración plena con las redes europeas de alerta y respuesta.

Esta transformación tendrá efectos significativos tanto en el sector público como en el privado. En el primero, exigirá una revisión profunda de las políticas de seguridad, un refuerzo de las capacidades técnicas y una mejora en la coordinación entre los distintos niveles administrativos. En el segundo, las empresas verán ampliadas sus obligaciones, especialmente aquellas que se incorporan por primera vez al marco regulatorio, lo que implicará inversiones en tecnología, formación, gestión del riesgo y cumplimiento normativo. Aunque el cumplimiento supondrá mayores costes, también incrementará

la resiliencia, la confianza y la competitividad del ecosistema digital español. En conjunto, la ley consolidará un modelo de cooperación estable entre autoridades y operadores, impulsando un entorno más maduro, colaborativo y seguro.

Sin embargo, la aplicación efectiva de la NIS2 en España plantea diversos desafíos estratégicos y operativos. Uno de los más relevantes es la fragmentación institucional, especialmente en un país con una estructura descentralizada, donde la coordinación entre los niveles autonómico y estatal resulta compleja. Superar este reto exigirá voluntad política, marcos de gobernanza claros y mecanismos de cooperación interinstitucional sólidos que garanticen la coherencia en la implementación.

Otro desafío importante está relacionado con la capacidad técnica y económica de las entidades obligadas. No todas disponen de los recursos humanos, tecnológicos o financieros necesarios para cumplir con los nuevos estándares, lo que resulta especialmente crítico en sectores como el sanitario, el educativo o la gestión de aguas, donde la digitalización avanza de forma desigual. Por ello, la supervisión deberá ir acompañada de estrategias de acompañamiento y refuerzo institucional que permitan equilibrar el nivel de preparación, evitando una visión puramente sancionadora.

A todo ello se suma el reto de fomentar una cultura de ciberseguridad sólida y transversal. La correcta notificación de incidentes, el análisis de vulnerabilidades o la adopción de medidas preventivas requieren un cambio cultural que sitúe la seguridad digital como una prioridad estratégica en todas las organizaciones, públicas y privadas.

Asimismo, la nueva normativa demanda la consolidación de infraestructuras legales y técnicas todavía incipientes, como sistemas automatizados de notificación, bases de datos nacionales de vulnerabilidades y mecanismos de cooperación transfronteriza, que deberán desarrollarse plenamente para garantizar la eficacia y la coherencia del nuevo marco normativo.

Pese a los retos, la transposición de la NIS2 representa una oportunidad estratégica para modernizar la arquitectura institucional de la ciberseguridad en España, profesionalizar el talento, fortalecer el sector industrial y consolidar la cooperación europea. Además, impulsa una cultura de corresponsabilidad y sitúa la ciberseguridad en el centro de la agenda estratégica nacional. Si se implementa con una visión de largo plazo, esta norma podrá convertir a España en un actor relevante y autónomo dentro del ecosistema europeo de seguridad digital, transformando las obligaciones normativas en una auténtica ventaja estratégica y competitiva.

5. Gestión de Crisis

Partiendo y dejando a un lado lo ya señalado en cuanto a la actuación proactiva o reactiva en base al tipo de entidad, la gestión en el tratamiento de un incidente de ciberseguridad conforme a la NIS2 y el Anteproyecto tiene en cuenta dos marcos principales: las fases de notificación obligatoria a las autoridades competentes y las medidas de gestión interna y respuesta que la entidad debe implementar.

En primer lugar, el proceso se inicia cuando ocurre un incidente que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por sistemas de redes y de información o accesibles a través de ellos, y que éste sea significativo, y se considera significativo cuando se cumpla uno de los dos siguientes:

1. Ha causado o puede causar graves perturbaciones operativas de los servicios o pérdidas económicas para la entidad afectada.
2. Ha afectado o puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales o inmateriales considerables.

En el marco de fases de notificación, la cual se convierte en obligatoria, y que debe realizarse al CSIRT o CERT (Equipo de Respuesta a Incidentes de Seguridad Informática) y a la autoridad competente, sin demora indebida, se establece en la Directiva una cronología:

Fase	**Plazo Máximo**	**Contenido de la Notificación**
Alerta Temprana	24 horas desde que se haya tenido constancia del incidente	Debe indicar si se sospecha que el incidente responde a una acción ilícita o malintencionada o si puede tener repercusiones transfronterizas
Notificación del Incidente	72 horas desde que se haya tenido constancia del incidente	Debe exponer una evaluación inicial del incidente (incluyendo gravedad e impacto) e indicadores de compromiso, cuando estén disponibles
Informe Intermedio	A instancia del CSIRT o autoridad competente	Contiene las actualizaciones pertinentes sobre la situación del incidente
Informe Final	A más tardar un mes después de la Notificación del Incidente (la de 72 horas)	Debe incluir una descripción detallada (gravedad e impacto), el tipo de amenaza o causa principal, las medidas paliativas aplicadas y en curso, y las repercusiones transfronterizas, si proceden. Si el incidente sigue en curso en ese momento, se debe presentar un informe de situación, y el informe final se presenta un mes después de haber gestionado el incidente.

6. Comparativa internacional (NIS 2 vs otras normativas)

La Directiva NIS 2 se configura como uno de los marcos regulatorios más ambiciosos y amplios en materia de ciberseguridad a nivel internacional. No obstante, coexiste con otros instrumentos normativos en diferentes regiones del mundo, cada uno con características propias que responden a sus contextos políticos, económicos y jurídicos. Comparar NIS 2 con estas normativas permite entender mejor su alcance, sus fortalezas y sus limitaciones, así como anticipar su interacción con organizaciones internacionales y empresas globalizadas.

- **NIS 2 vs CCPA (California Consumer Privacy Act, EE.UU.)**

Aunque no centrada exclusivamente en ciberseguridad, la CCPA incluye disposiciones relativas a la protección de datos personales y la respuesta a incidentes de seguridad. A diferencia de NIS 2, se trata de una ley de privacidad más que de ciberseguridad, pero su aplicación en el estado de California —una economía equivalente a la de muchos países— la convierte en un referente global.

La diferencia fundamental es que NIS 2 es una norma de ciberseguridad sectorial y estructural, mientras que la CCPA pone el foco en los derechos individuales del consumidor. NIS 2 impone requisitos técnicos y organizativos a operadores de servicios esenciales, incluyendo notificación de incidentes, supervisión y sanciones. CCPA, en cambio, establece obligaciones sobre el uso, recopilación y venta de datos, con énfasis en el consentimiento y la transparencia, y su respuesta ante brechas de datos es más limitada.

- **NIS 2 vs CIRCIA (Cyber Incident Reporting for Critical Infrastructure Act, EE.UU.)**

Aprobada en 2022, CIRCIA representa un avance en la normativa federal de ciberseguridad estadounidense, especialmente en el ámbito de la notificación de incidentes en infraestructuras críticas. Obliga a entidades cubiertas a reportar incidentes significativos al CISA (Cybersecurity and Infrastructure Security Agency) en un plazo de 72 horas, con ciertos criterios de aplicación.

En comparación, NIS 2 impone una ventana más estrecha de notificación (24 horas) y un espectro más amplio de sectores afectados. Además, CIRCIA aún se encuentra en proceso de reglamentación detallada, mientras que NIS 2 establece una estructura normativa completa, incluyendo mecanismos de supervisión, gobernanza europea coordinada y categorización de entidades.

Otra diferencia clave es que NIS 2 promueve una armonización transnacional entre Estados miembros, mientras que el modelo estadounidense se basa en la coexistencia de normativas estatales y federales, lo que puede generar solapamientos o fragmentación.

- **NIS 2 vs ISO/IEC 27001**

La norma ISO/IEC 27001 no es un instrumento legal, sino un estándar internacional voluntario para la gestión de la seguridad de la información. Muchas organizaciones lo adoptan como marco de buenas prácticas, y en algunos países es exigido por los reguladores como parte de la estrategia de cumplimiento.

NIS 2, sin embargo, es jurídicamente vinculante y va más allá de la gestión interna del riesgo, estableciendo un entorno normativo con obligaciones legales, auditorías y sanciones. Aunque ambos comparten principios comunes (como el enfoque basado en riesgos, la mejora continua o la protección de activos críticos) NIS 2 incorpora además mecanismos de cooperación internacional, notificación obligatoria y supervisión institucional, lo que lo convierte en un marco mucho más estructurado y exigente.

- **NIS 2 vs Cybersecurity Law de China (2017)**

  La Ley de Ciberseguridad de la República Popular China es una de las normativas más severas y centralizadas del mundo. Establece exigencias estrictas de localización de datos, control gubernamental sobre redes e infraestructuras críticas, y censura sobre contenidos considerados sensibles.

  En contraste, NIS 2 mantiene un equilibrio entre seguridad y derechos fundamentales, particularmente la privacidad, la protección de datos y la transparencia. Mientras que la ley china se fundamenta en una lógica de seguridad nacional y control estatal, NIS 2 responde a los principios del mercado interior, la protección de infraestructuras críticas y la cooperación institucional europea, con fuertes garantías para los operadores y los ciudadanos.

En conjunto, NIS 2 sitúa a la Unión Europea a la vanguardia de la ciberregulación global, al integrar normas técnicas exigentes, gobernanza multinivel y protección de derechos fundamentales. Frente a modelos más centralistas, parciales o voluntarios, NIS 2 representa un equilibrio sofisticado entre seguridad, cooperación institucional y valores democráticos.

Conclusiones

La transposición de la NIS2 a la normativa nacional va a resultar crucial por sus implicaciones normativas, estratégicas y geopolíticas, constituyéndose como una necesidad urgente para dotar de instrumentos que garanticen la ciberseguridad en España y en el conjunto de la UE, en un momento en que se ha revelado que la materia es crucial en el ámbito de la seguridad de los países, no solo con la amenaza de actores que buscan el lucro personal sino otros que persiguen objetivos de injerencias que afecten a la posición de las naciones y a sus sistemas de gobierno.

La implantación va a conllevar unos costes e implica una mayor complejidad en los sistemas de seguridad, pero los beneficios a largo plazo justifican la inversión con una mayor resiliencia operativa y una reducción exponencial de riesgos.

Por otro lado, la transposición implica un desafío tecnológico y operativo para los sistemas industriales existentes, asimismo existe un problema estructural de falta de personal calificado en ciberseguridad, y por último nos arriesgamos también a una existencia de sobrerregulación y burocracia que pueda generar fatiga en el cumplimiento.

El Anteproyecto de Ley que plantea la legislación española se alinea estrechamente con los requisitos de la NIS e incorpora elementos de gobernanza como la expansión a sectores específicos no contemplados.

Igualmente establece figuras específicas de gestión de la seguridad como el Centro Nacional de Ciberseguridad designado como autoridad competente única y último responsable de la gestión de

crisis coordinando a otras autoridades y CSIRTs, así como los Responsables de la Seguridad de la Información con funciones específicas de coordinación técnica y supervisión.

Pero todo ello debería conjugar con la principal problemática antes expuesta que podemos resumir en facilitar su aplicación a unos sectores que ya se encuentran sobrerregulados y con muchos obstáculos burocráticos y de gestión.