

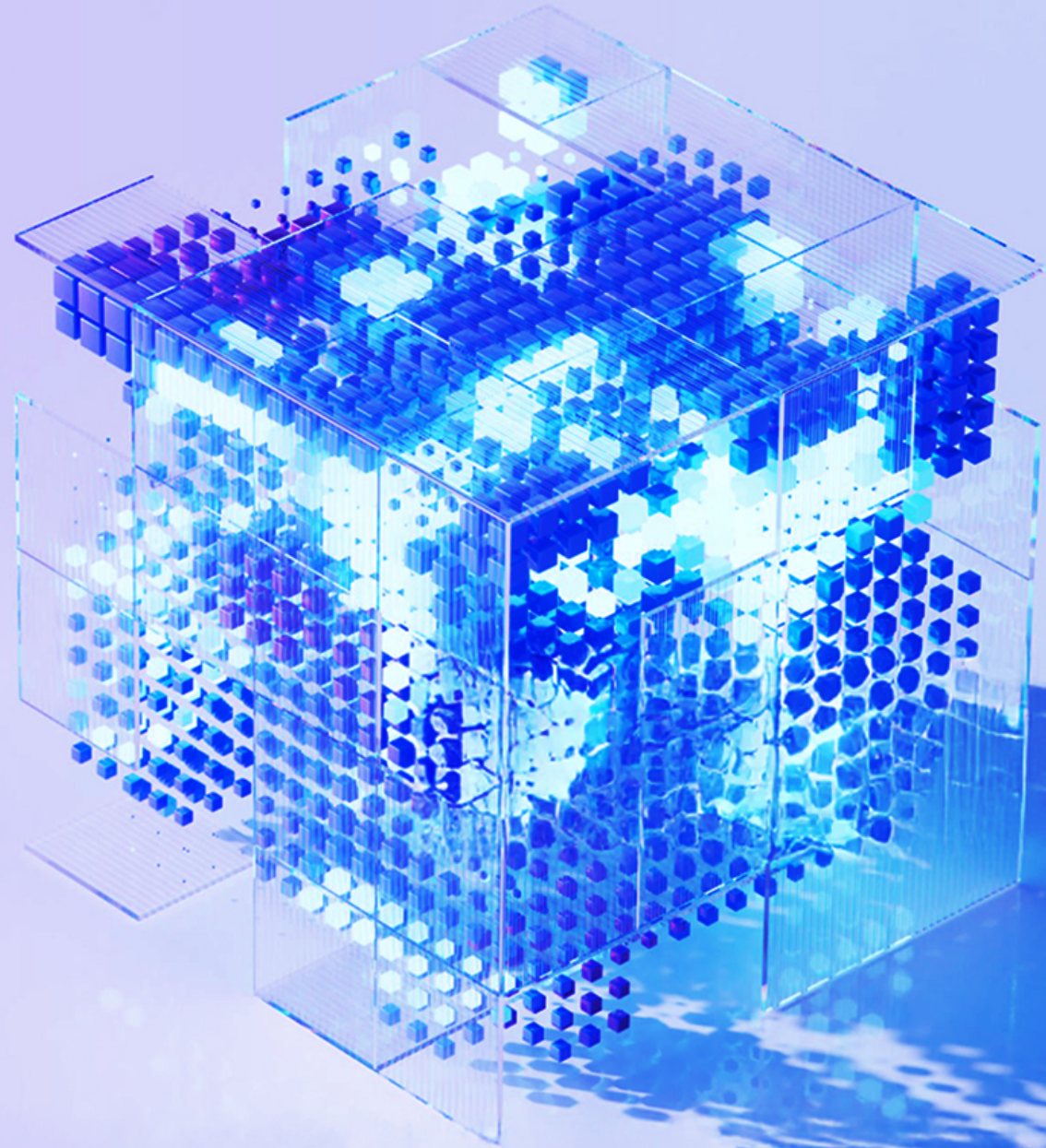


# Claves para cumplir con la Directiva NIS2

**KPMG. Make the Difference.**

Diciembre 2024

---



# La ciberseguridad ha escalado posiciones entre las principales preocupaciones para las compañías:

El **90%**

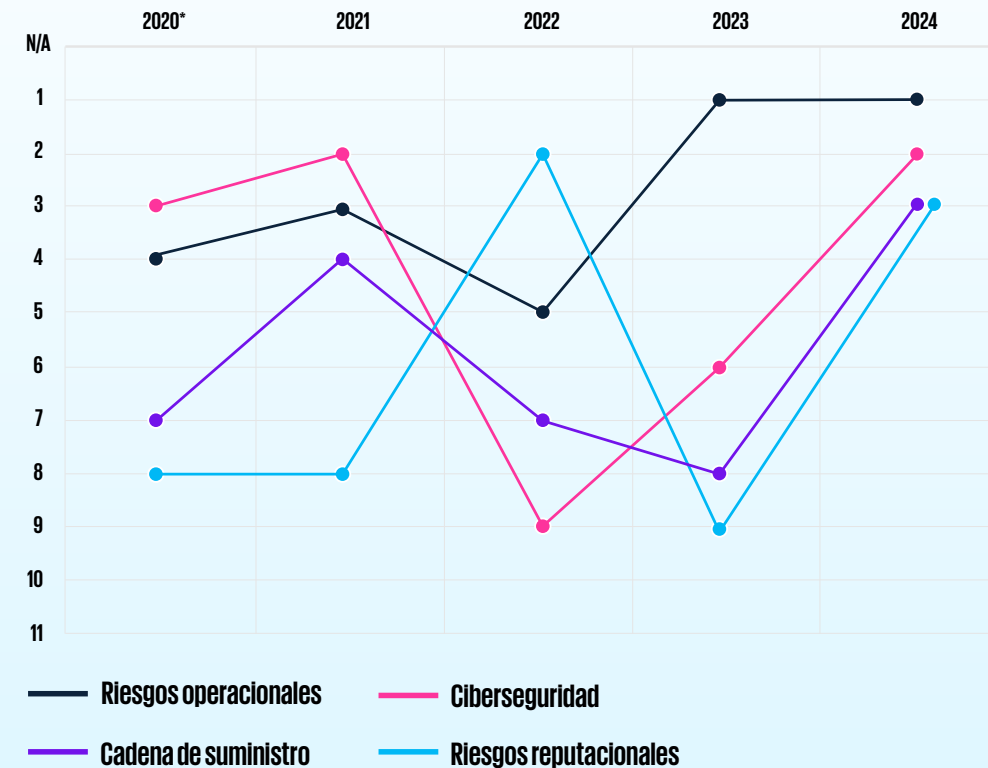
de las empresas prevé un aumento de ciberataques, por lo que han aumentado su presupuesto en ciberseguridad (el gasto medio en TI por organización aumentó a 15 millones de euros en 2023, **duplicándose el presupuesto en ciberseguridad**). [ENISA \(European Union Agency for Cybersecurity\)](#) en su Informe "NIS Investments 2024".

En **2024**

la ciberseguridad se consolida como el **segundo riesgo más relevante para el crecimiento de las organizaciones en España:**

## Evolución en los últimos diez años de los principales riesgos para el crecimiento identificados en España en 2024

Puesto definido en base al porcentaje de respuesta registrado por cada una de estas opciones en las distintas ediciones



\* Porcentajes previos al estallido de la pandemia/La edición de 2020 fue exclusivamente Global  
Fuente: KPMG 2024 CEO Outlook



## Objetivo:

### reforzar la resiliencia colectiva europea contra las ciber amenazas

Como consecuencia de todo ello, se han puesto en marcha diferentes normativas para **regular y armonizar el cumplimiento de los requisitos relacionados con la ciberseguridad**, como son la Ley de Ciberresiliencia (CRA) o la **Directiva NIS2**, que amplía el alcance de la directiva original (NIS1), que cubría principalmente operadores de servicios esenciales.

Desde su elaboración, esta Directiva constituye un eje importante en la Estrategia de Ciberseguridad de la Unión Europea, y favorece el objetivo de **reforzar la resiliencia colectiva europea contra las ciber amenazas**. Además, ayuda a que todos los ciudadanos y empresas puedan contar con unos servicios y herramientas digitales de confianza.

Concretamente, la **Directiva NIS2 introduce una ampliación** a raíz de la cual sectores adicionales como proveedores de servicios digitales y varias industrias estratégicas deberán cumplir **con mayores exigencias de ciberseguridad**, lo que añade presión al proceso de adecuación legislativa.

En vigor desde enero de 2023, **la Directiva NIS2 ya es vinculante** y, sin embargo, las empresas españolas aún **no tienen un marco legislativo**

**La Directiva NIS2 ya es vinculante y, sin embargo, las empresas españolas aún no tienen un marco legislativo nacional claro que les permita adaptarse**

**nacional claro que les permita adaptarse**. La razón es el retraso en el proceso de trasposición en España, como ha ocurrido en otros países, por complejidades legislativas y la necesaria adaptación de las estructuras y normativa actuales (el 17 octubre finalizó el plazo para su trasposición).

**Ante lo cual surgen interrogantes, que esclarecemos a continuación:**

# 1. Hasta que llegue la trasposición, ¿qué debo hacer?



La respuesta recae en el **Reglamento de Ejecución**: el mismo día que terminaba el plazo de trasposición de la Directiva para los Estados miembro (17 de octubre de 2024) la Comisión Europea publicaba un Reglamento de Ejecución que será **aplicable de forma directa a las entidades afectadas** (esenciales e importantes de sectores concretos, denominadas entidades relevantes) y que se debería **tomar como punto de partida para que cualquier organización pueda prepararse para cumplir con NIS2**.

Este Reglamento de Ejecución, que **convivirá con las normativas de trasposición de la Directiva de los distintos Estados Miembros**, una vez sean aprobadas, tiene como

**Hasta la llegada de la trasposición, el Reglamento de Ejecución deberá tomarse como punto de partida para que cualquier organización pueda prepararse para cumplir con la NIS2.**

objetivo principal establecer los **requisitos técnicos y metodológicos de gestión**, así como la especificación con más detalle de los casos en los que un incidente tendrá la consideración de significativo.

**Para aquellos sectores aplicables, el Reglamento de Ejecución publicado el 17 de octubre, incluye requisitos específicos de aplicación de la Directiva NIS2 que deberán cumplir las entidades pertinentes, pertenecientes a los sectores que implica el propio Reglamento.**



## Los sectores a los que aplica el Reglamento de Ejecución son los siguientes\*:

Proveedores de servicios DNS

Proveedores de motores de búsqueda en línea

Proveedores de servicios de computación en la nube

Proveedores de mercados en línea

Proveedores de servicios de centros de datos

Proveedores de servicios gestionados y seguridad gestionada

Registros de nombres TLD

Proveedores de redes de distribución de contenido

Proveedores de plataformas de servicios de redes sociales

Proveedores de servicios de confianza

## 2. ¿Cómo sé si me aplica la normativa?



A diferencia de la situación con la Directiva NIS1, **las propias organizaciones serán responsables de analizar y determinar si es un sujeto obligado** al cumplimiento de la Directiva NIS2 y, en su caso, su clasificación como entidad esencial o importante.

Así, teniendo en cuenta el Artículo 2 de la propia Directiva sobre sujetos obligados, **identificamos los siguientes criterios** para determinar si una organización es entidad esencial o importante:

- Entidad esencial, suma de criterios entre gran empresa y sector aplicable.
- Entidad importante, determinados sectores o por no ser gran empresa.

**Las propias organizaciones serán responsables de analizar y determinar si es un sujeto obligado al cumplimiento de la Directiva NIS2 y, en su caso, su clasificación como entidad esencial o importante.**

### Entidades esenciales\*

Gran empresa:

+250 trabajadores

volumen de negocios anual  
+50M

balance general anual +43M

Son criterios individuales

Sectores aplicables:

Energía

Sector sanitario

Gestión de servicios TIC

Transporte

Agua potable

Administración pública

Banca

Aguas residuales

Espacio

Mercados financieros

Infraestructura digital

### Entidades importantes

- Entidades de los sectores del Anexo I que no cumplen los requisitos de categorización de entidad esencial.
- Entidades de los sectores del Anexo II.
- Identificación directa del estado a través de un listado que, según la propia Directiva, deberá ser publicado por el Estado antes del 17 de abril del 25.

Sumados ambos criterios, una empresa será considerada esencial a ojos de la Directiva.

\*Existen, entre otras, casuísticas particulares como la designación ad-hoc de una entidad como esencial por parte de los Estados Miembros.

Estos criterios son individuales y cualquiera de ellos puede provocar que una empresa sea considerada entidad importante.

### 3. ¿Qué diferencias hay entre entidades esenciales e importante?



La diferencia principal no se centra en las obligaciones que aplican a cada una de estas entidades, puesto que son las mismas a nivel general, sino más bien en el nivel de supervisión que tendrán cada una de las entidades. En concreto, las principales diferencias existentes entre ambos tipos de entidades son las siguientes:

#### Entidades esenciales - Medidas de supervisión por parte de las autoridades más exigentes:

Medidas de supervisión y ejecución a priori y a posteriori

Auditorías específicas y periódicas

Auditorías ad hoc

Actuación por parte de la autoridad en el mismo instante de inspección/auditoria

Suspensión temporal de una certificación o autorización de servicios o actividad

#### Entidades importantes – Medidas de supervisión menos exigentes:

Las autoridades solamente actuarán cuando existan pruebas o indicios de incumplimiento

Medidas de supervisión a posteriori

Auditorías específicas, pero no periódicas

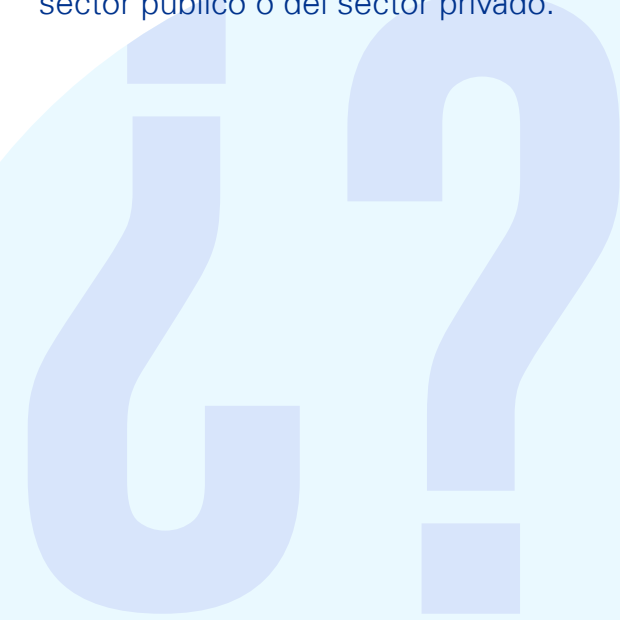
No se contemplan auditorías ad hoc

No tienen la obligación de documentar sistemáticamente la conformidad con las medidas para la gestión de riesgos de ciberseguridad

### 4. ¿Cuál es la entidad supervisora?



Actualmente **no se encuentra definido a nivel nacional** y seguramente sea objeto de la normativa de transposición de la Directiva, pero en caso de tener un incidente significativo, existen varios organismos para ser notificados, entre los que destacan el **CCN-CERT e INCIBE**, dependiendo de si la entidad prestadora de los servicios se engloba dentro del sector público o del sector privado.



# 5. ¿Qué obligaciones tengo que cumplir?

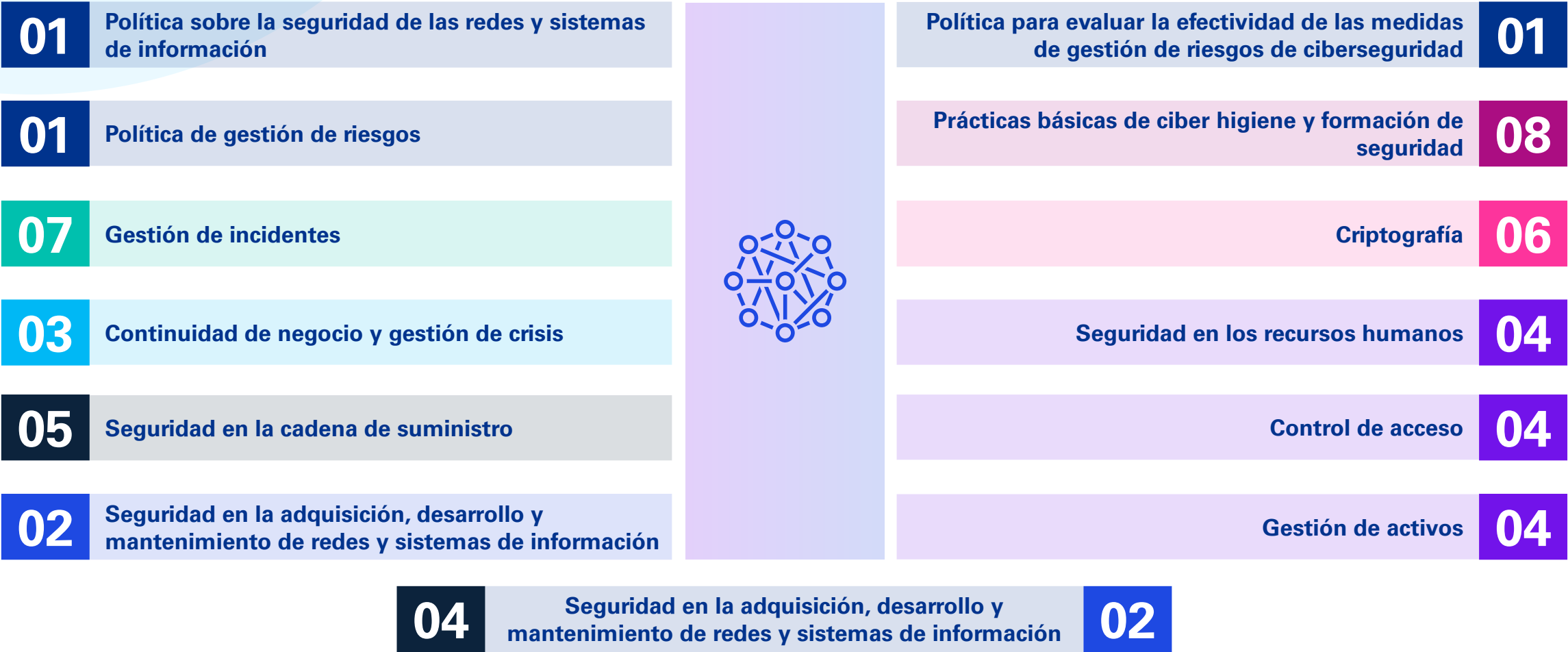


Teniendo en cuenta que las obligaciones a las que están sujetas las diferentes entidades son las mismas a nivel general, **actualmente las obligaciones principales surgen de la Directiva** y, en caso de aplicación, del **Reglamento de Ejecución que desarrolla en mayor detalle estas obligaciones**, siendo las principales las siguientes:

- 01** Desarrollar **políticas de sistemas de información** que incluyan el análisis de los riesgos.
- 02** **Garantizar la seguridad de la información y sistemas de redes** mediante la implementación de dicha seguridad en la adquisición, el desarrollo y el mantenimiento de sistemas de redes y de información, incluida la gestión y divulgación de vulnerabilidades.
- 03** **Mejorar la continuidad de negocio**, atendiendo a la gestión de copias de seguridad y la recuperación en caso de catástrofe, así como de gestión de crisis.
- 04** **Revisar la seguridad en los recursos humanos, políticas de control de acceso y gestión de activos**, teniendo en consideración las altas/bajas y modificaciones en los sistemas considerados dentro de este alcance.
- 05** **Garantizar la seguridad en la cadena de suministro**, gestionando los riesgos de la misma mediante una priorización que determine la criticidad de los diferentes proveedores y sus riesgos;
- 06** **Implementar el uso de criptografía**, introducida como una medida específica ante la necesidad de que las entidades prevean políticas y procedimientos relativos al buen uso de la utilización de la misma y, en su caso, del cifrado.
- 07** **Gestionar incidentes, estableciendo una política y los correspondientes procesos de gestión**, monitorización y recopilación de aquellos que puedan acontecer, y siempre teniendo en cuenta los nuevos requerimientos de notificación;
- 08** **Definir formación en ciberseguridad**, mediante una estrategia para adoptar una cultura organizativa consistente y llevando a cabo una formación y concienciación para todos los empleados.

Además, el Reglamento de Ejecución aterriza con más detalle esas obligaciones, e identifica los principales dominios establecidos con los requisitos mencionados:

Además, el Reglamento de Ejecución aterriza con más detalle esas obligaciones, e identifica los **principales dominios** establecidos con los requisitos mencionados:





## 6. ¿Quién deberá ser el responsable dentro de la organización?



La normativa establece que **debe existir un responsable**, pero se incluye como novedad **la supervisión de los órganos directivos de las empresas** para garantizar el cumplimiento con la normativa. En concreto, se exige:

- que los órganos de dirección de las organizaciones aprueben las medidas de gestión de los riesgos de ciberseguridad adoptadas por dichos órganos para cumplir lo dispuesto en el artículo 21
- que supervisen la aplicación de dichas medidas
- que puedan llegar a ser incluso responsables de las infracciones previstas en dicho artículo

## 7. ¿Me pueden sancionar si incumplo?



Siguiendo la línea de otras normativas europeas, **existen sanciones económicas o no económicas** según la gravedad del incumplimiento

### SANCIONES ECONÓMICAS

**Entidades esenciales:** las sanciones económicas pueden alcanzar los **10 millones para entidades esenciales o hasta el 2% del volumen de negocios** total anual a escala mundial de la empresa a la que pertenezca la entidad esencial en el ejercicio precedente, optándose por la de mayor cuantía.

**Entidades importantes:** las sanciones pueden alcanzar los **7 millones de 7.000.000 euros o el 1,4% del volumen de negocios total anual a nivel mundial de la empresa** a la que pertenece la entidad importante en el ejercicio precedente, optándose por la de mayor cuantía.

### ENTIDADES NO ECONÓMICAS

Ordenar el cese de una conducta que infrinja la Directiva.

Ordenar que se garanticen las medidas de gestión de riesgos o las obligaciones de información de manera y en un plazo determinados.

Imponer multas administrativas.

## 8. ¿Esta normativa afecta a mis proveedores?



Dentro de las obligaciones de la Directiva, se incluye la **gestión de los riesgos de seguridad de los proveedores o prestadores de servicios directos**.

En este sentido, el **Reglamento de Ejecución**, de aplicabilidad directa a los proveedores de servicios DNS, registros de nombres TLD, proveedores de servicios de computación en la nube, proveedores de servicios de centros de datos,

proveedores de redes de distribución de contenido, proveedores de servicios, proveedores de servicios de seguridad gestionados, proveedores de mercados en línea, de motores de búsqueda en línea y de plataformas de servicios de redes sociales, y proveedores de confianza proveedores de servicios, especifica los **requisitos aplicables a la seguridad de la cadena de suministro**, siendo necesaria la implementación y aplicación de una política de seguridad que, entre otras, recoja:



**Las prácticas de ciberseguridad de los proveedores y prestadores de servicio,** incluidos sus procedimientos de desarrollo seguro;



**La capacidad de cumplir las especificaciones de ciberseguridad pertinentes,** así como la calidad y resiliencia de los productos/servicios prestados;



**La capacidad de diversificar las fuentes de suministro** limitando la dependencia de proveedores.

# 9. ¿Cuáles son los próximos pasos que puedo dar?



Aunque todavía no exista una normativa de transposición, **estos meses son clave para identificar si mi organización es o no sujeto obligado al cumplimiento de la Directiva**, y, en su caso, entender el punto de partida para garantizar su cumplimiento, partiendo del Reglamento de Ejecución, y de los estándares de ciberseguridad más consolidados (ISO 27001, ENS o NIST-CSF).

- Análisis para **evaluar el estado actual e implantar acciones** para alcanzar el nivel de cumplimiento.

En relación con lo mencionado anteriormente, actualmente en España no se ha llevado a cabo la transposición. No obstante, el Reglamento de Ejecución publicado por la Comisión Europea el 17 de octubre de 2024 es aplicable a todas las entidades que se mencionan en su contenido. En caso de que una organización no se encuentre entre estas entidades, **sería recomendable realizar un análisis detallado de las implicaciones, solicitudes y especificaciones del Reglamento**. Esto permitirá evaluar el nivel de cumplimiento de la organización, ya que, desde una perspectiva legal, se espera que la futura transposición se ajuste a dicha documentación.

Para aquellos sectores aplicables, el Reglamento de Ejecución publicado el 17 de octubre, incluye requisitos específicos de aplicación de la Directiva NIS2.

13 dominios

94 controles



# 10. ¿Cuáles son las fechas clave?

## Enero 2023

El 17 de enero de 2023 empezó el **periodo de trasposición** de la Directiva NIS2 por parte de los estados miembros.

## Noviembre 2024

La Comisión pide a veintitrés Estados miembros que transpongan plenamente la Directiva SRI 2, **disponiendo de dos meses para responder, completar la transposición y notificar las medidas a la Comisión.**

## 2025

Los estados miembros determinarán qué **entidades** se consideran **esenciales e importantes.**

## 2027

A continuación, la Comisión deberá revisar **periódicamente el funcionamiento de la Directiva** e informar sobre ella por primera vez antes del 17 de octubre de 2027 al Parlamento y al Consejo.

## Octubre 2024

No se logra la transposición a fecha de 17 de Octubre en España.

La Comisión Europea publica el **Reglamento de Ejecución, aplicable a determinadas entidades importantes**, en cuyo Anexo describe acciones específicas.

## Enero 2025

Los Estados miembros comunicarán a la Comisión Europea el **régimen sancionador aplicable.**

## Abril 2025

Los Estados miembros deben elaborar una **lista de entidades esenciales e importantes**, así como de entidades que prestan servicios de registro de nombres de dominio.

Las organizaciones no deben entender esta regulación como algo aislado, ya que estará **vinculada a otras regulaciones a nivel europeo**, que forman parte de la **estrategia de seguridad de la UE** (Estrategia Europea de Ciberseguridad, el **Reglamento DORA**, el Reglamento de Ciberseguridad y sus esquemas de certificación, o el Reglamento de Ciberresiliencia). **Aumentar el nivel de resiliencia** de la Unión para hacer frente a amenazas crecientes y cada vez más complejas es el objetivo común de todos estos reglamentos.

# 11. ¿Somos el único país aún por trasponer la NIS2?



A pesar de que la fecha de transposición a la normativa nacional de cada Estado miembro finalizó **el 17 de octubre**, actualmente la mayoría de países todavía no han publicado esta Ley en su marco regulatorio nacional.

Si bien solo **5 países** han publicado la Ley sobre la que incluimos un poco más de detalle en esta slide, en **los 13 países** en los que se ha publicado un borrador, ya se puede identificar que existe alineamiento en los estándares de referencia que se han usado, al estar en su mayoría enfocados a algunos tan consolidados como la ISO 27001, NIST CSF, NIST 800 – 53 o guías CERT.

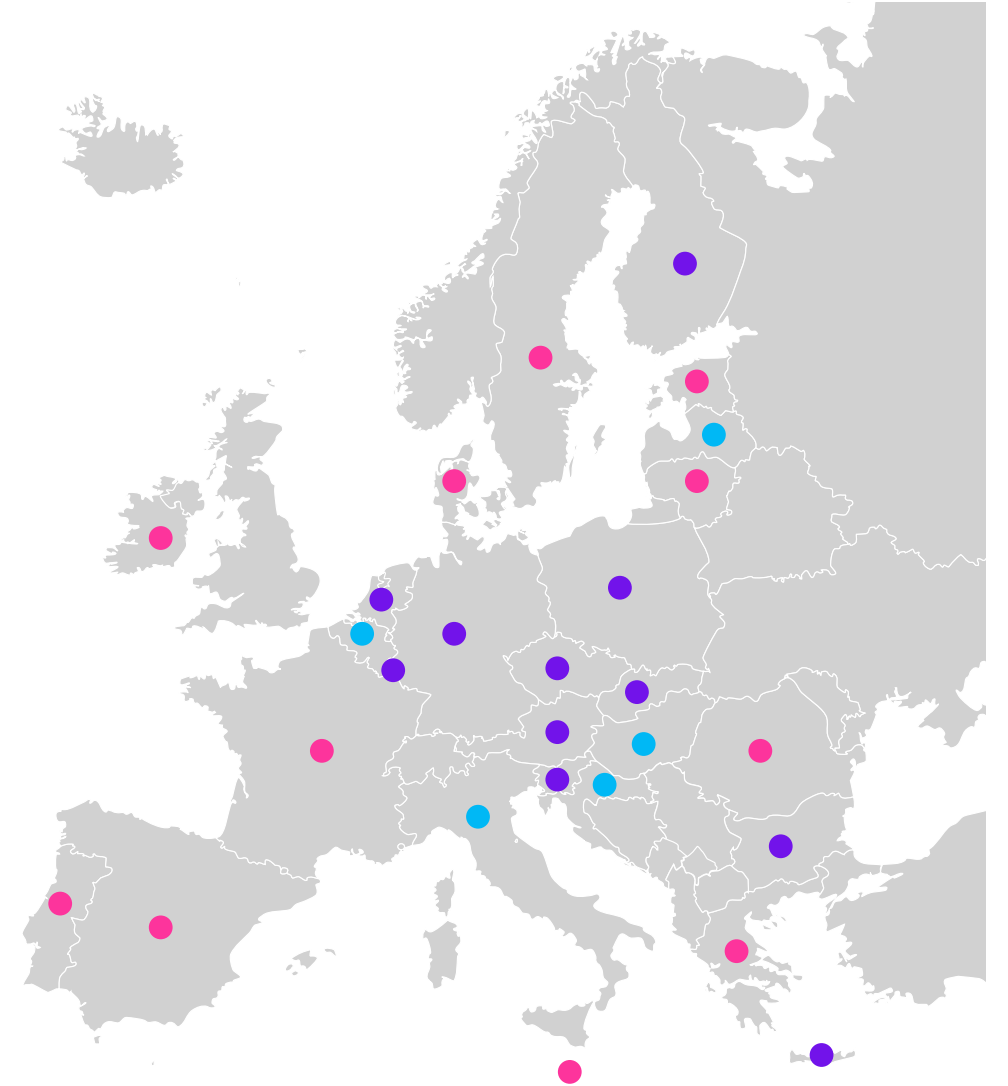
## País Transposición

<b>Bélgica</b>	—	Publicada en Abril 2024
<b>Croacia</b>	—	Publicada en Febrero de 2024
<b>Hungría</b>	—	Publicada en Octubre de 2024
<b>Italia</b>	—	Publicada en Octubre de 2024
<b>Letonia</b>	—	Publicada en Septiembre de 2024

● No existe borrador ● Borrador publicado ● Ley publicada



El Reglamento de Ejecución publicado el 17 de octubre, incluye requisitos específicos de aplicación de la Directiva NIS2 que deberán cumplir las entidades pertinentes, pertenecientes a los sectores que implica el propio Reglamento. Estos requisitos se aplicarán en todos los estados miembros de una manera directa.



# Cómo te podemos ayudar desde KPMG

En el entorno actual, la confianza es la base sobre la que vertebrar la ciberseguridad.

Desde KPMG, nuestra misión y nuestro foco se centran en ofrecer a nuestros clientes **las mejores soluciones y enfoques para su realidad**, ya venga marcada por imperativo interno, por regulaciones (locales, globales o sectoriales) o fruto de sus procesos de transformación digital.



**Javier Aznar**

**Socio de Technology Risk  
Ciberseguridad y Privacidad  
de KPMG en España**

**E:** [jaznar@kpmg.es](mailto:jaznar@kpmg.es)

**T:** +34 699 35 00 29



**Juan Ignacio Ríos**

**Director de Technology Risk  
Ciberseguridad y Privacidad  
de KPMG en España**

**E:** [juanignaciorios@kpmg.es](mailto:juanignaciorios@kpmg.es)

**T:** +34 683 66 38 39



**Pedro García Köllmer**

**Senior Manager de Technology  
Risk Ciberseguridad y Privacidad  
de KPMG en España**

**E:** [pedrogarcia1@kpmg.es](mailto:pedrogarcia1@kpmg.es)

**T:** +34 606 67 04 28

La ciberseguridad, la privacidad y la protección de la información, sea cual sea el perímetro de trabajo, se presentan como **pilares de confianza** para un negocio que, fruto de la recolección y analítica de datos, la cada vez mayor dependencia tecnológica o el aumento de vectores de exposición, **necesita evolucionar y recorrer este proceso con garantías**, de manera estratégica y transversal a toda la compañía.

**Te ayudamos a adaptarte a la nueva  
normativa en materia de ciberseguridad**



# La transformación nunca para. Nosotros tampoco.

En KPMG creemos que la transformación es una oportunidad que no se puede dejar pasar. Integrando la mejor tecnología, con los procesos adecuados y las capacidades y visión necesarias, la transformación será un éxito. Por esa razón, hemos trabajado durante décadas en el corazón de las empresas, ayudando a nuestros clientes a maximizar el potencial de sus personas y de su tecnología, trabajando junto para alcanzar resultados reales. Porque cuando personas y tecnologías se unen, el resultado es insuperable.

## **Construyendo un mundo diferente:**

Los profesionales de KPMG marcan la diferencia en la transformación tecnológica de tu organización. Juntos, te ayudamos a orientar tu negocio al cliente, optimizar funciones para afrontar nuevos retos, gestionar los riesgos y la regulación, alcanzar nuevas cotas de generación de valor y crear un entorno para adaptarse a los cambios.

**KPMG. Make the Difference.**





La información aquí contenida es de carácter general y no va dirigida a facilitar los datos o circunstancias concretas de personas o entidades. Si bien procuramos que la información que ofrecemos sea exacta y actual, no podemos garantizar que siga siéndolo en el futuro o en el momento en que se tenga acceso a la misma. Por tal motivo, cualquier iniciativa que pueda tomarse utilizando tal información como referencia, debe ir precedida de una exhaustiva verificación de su realidad y exactitud, así como del pertinente asesoramiento profesional.

© 2024 KPMG, S.A., sociedad anónima española y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

KPMG y el logotipo de KPMG son marcas registradas de KPMG International Limited, sociedad inglesa limitada por garantía.