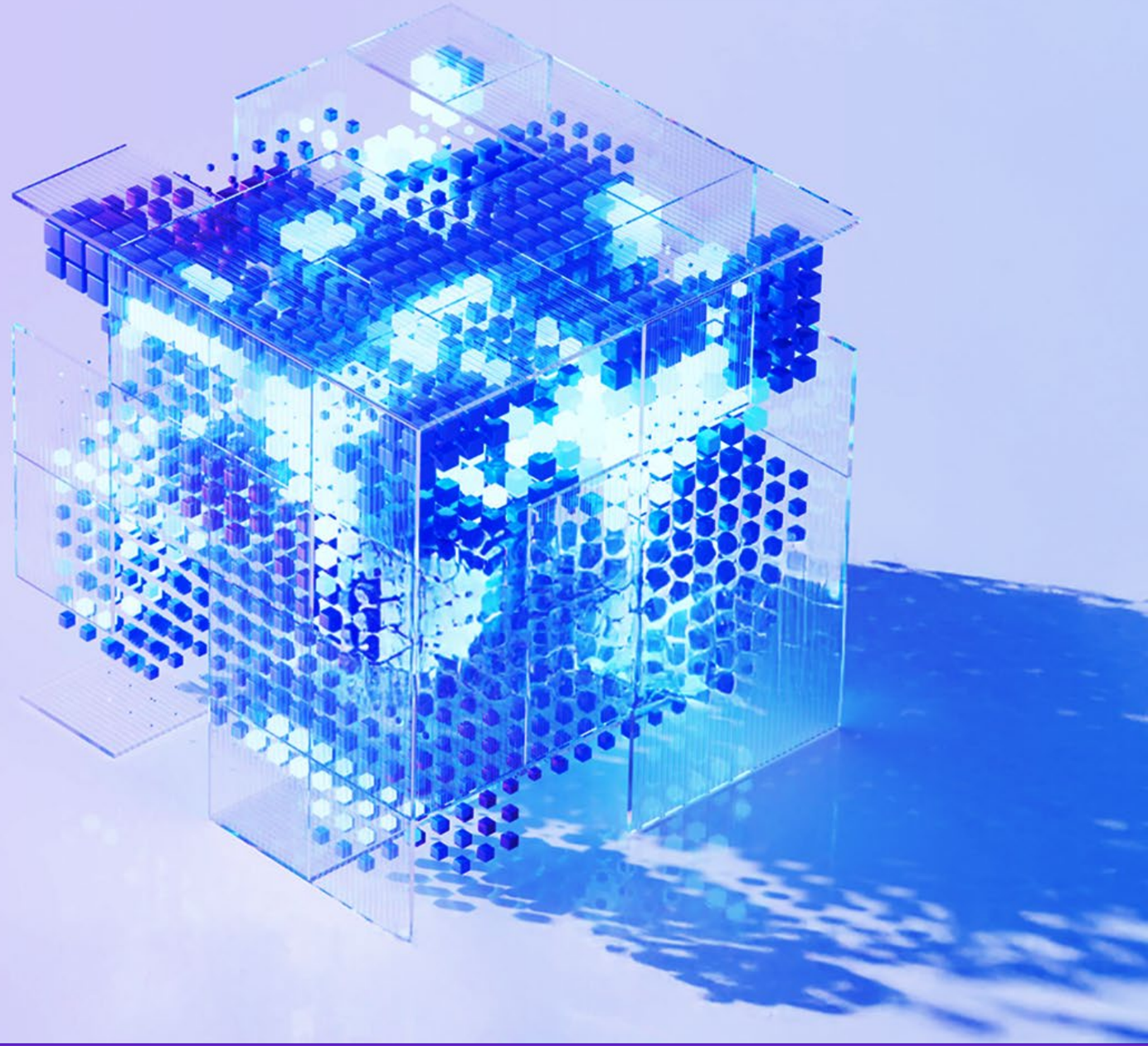
Claves para cumplir con la Directiva NIS2



KPMG. Make the Difference.

Octubre 2025

kpmg.es

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

El **90%**

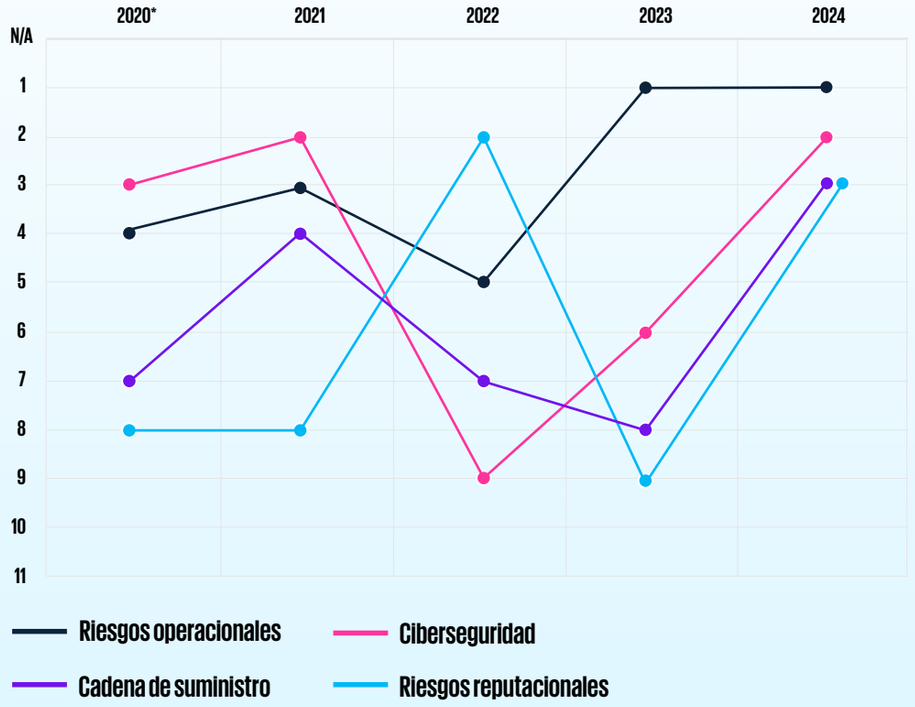
de las empresas prevé un aumento de ciberataques, por lo que han aumentado su presupuesto en ciberseguridad (el gasto medio en TI por organización aumentó a 15 millones de euros en 2023, **duplicándose el presupuesto en ciberseguridad).** ENISA (European Union Agency for Cybersecurity) en su Informe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

En **2025**

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.

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

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 nacional claro que les permita adaptarse.** La razón es que el anteproyecto de ley publicado en enero de 2025 sigue sin aprobación oficial y, a pesar de establecer ciertas directrices, siguen quedando dudas sobre la definición de varias cuestiones relacionadas con esta normativa.

Ante lo cual surgen interrogantes, que esclarecemos a continuación:

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

LLa respuesta recae en el Anteproyecto de ley publicado en enero de 2025.

Tres meses después de la fecha límite de transposición a la normativa nacional de cada Estado miembro, España publica el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, que, si bien todavía está en fase de aprobación, ofrece un marco más claro y detallado sobre cómo se implementarán las obligaciones derivadas de la Directiva en nuestro país. Analizamos cuáles son las principales novedades:

Hasta la llegada de la transposición, el Anteproyecto de ley aprobado en enero de 2025 deberá tomarse como punto de partida para que cualquier organización pueda prepararse para cumplir con la NIS2.

Objetivos

- Crear una **Autoridad Nacional Competente** única.
- Establecer **criterios uniformes** para clasificar entidades esenciales e importantes.
- Definir la figura del **responsable de seguridad de la información**.
- Crear un marco institucional de **coordinación entre autoridades competentes**.

Alcance

Se incluyen los sectores de **Industria nuclear** y las empresas de **Seguridad Privada**.

Marco nacional, estratégico e institucional

Autoridad Competente

Centro Nacional de ciberseguridad
(creación pendiente)

Tareas:

- Es la **Autoridad nacional de gestión de crisis y punto de contacto único**, enlace con la ENISA y otros EEMM.
- Asume la **superior dirección y coordinación de las autoridades de control** y puntos de contacto sectoriales y de los CSIRT nacionales de referencia.

Autoridades de control

Autoridad	Entidades que surpervisa
Ministerio de Defensa (Centro Criptológico Nacional)	› Entidades públicas esenciales e importantes, no siendo entidades críticas pertenezcan al Sector Público.
Ministerio de Transformación Digital a través de SETELECO y SEDIA	› Entidades esenciales e importantes, no críticas, de los sectores de Infraestructura digital y Proveedores de servicios digitales › Entidades importantes, no críticas, del resto de sectores
Ministerio del Interior (Oficina de Coordinación de Ciberseguridad)	› Entidades críticas de cualquier sector › Entidades esenciales, no críticas de cualquier sector › Entidades esenciales e importantes del sector de seguridad privada

Tareas:

- **Reporte de información** de entidades esenciales/importantes a autoridad competente
- **Supervisión y ejecución** de las entidades

Certificación y autoevaluación de entidades

- Las **entidades esenciales** demostrarán su cumplimiento mediante la **obtención y mantenimiento** de una **certificación de conformidad.**
- Las **entidades importantes no están obligadas** a obtener tal certificación, sino que pueden optar a la misma de **forma voluntaria** o demostrar su cumplimiento **mediante una autoevaluación**.

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	

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.

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.

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

- 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
- 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?

Autoridades competentes vs Autoridades de control

Autoridad Competente	Autoridades de control
Centro Nacional de Ciberseguridad (creación pendiente)	**Ministerio de Defensa (Centro Criptológico Nacional)**
	Ministerio de Defensa (Centro Criptológico Nacional)
	Ministerio del Interior (Oficina de Coordinación de Ciberseguridad)

Tareas:

- Es la **Autoridad nacional de gestión de crisis y punto de contacto único**, enlace con la ENISA y otros EEMM.
- Asume la **superior dirección y coordinación de las autoridades de control** y puntos de contacto sectoriales y de los CSIRT nacionales de referencia.

Tareas:

- **Reporte de información** de entidades esenciales/ importantes a autoridad competente.
- **Supervisión y ejecución** de las entidades.

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:

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 estado actual de nuestra organización respecto a los requerimientos de la directiva y el anteproyecto de ley y, para las obligaciones concretas en materias de seguridad, según ha dispuesto el CCN en una nota publicada el 3 de octubre de 2025, el ENS y los perfiles específicos serán claves en la futura transposición española. Es por ello, que podemos ir dando pasos usando como base bien el ENS o el Reglamento de ejecución publicado el año pasado.

En relación con lo mencionado anteriormente, actualmente en España no se ha llevado a cabo la transposición. Sin embargo, tenemos información suficiente, tanto por el anteproyecto de ley, como por diferentes publicaciones del CCN, donde se indica que, para el aterrizaje de las medidas de seguridad, el Esquema Nacional de Seguridad, y sus futuros perfiles de cumplimiento específico por sectores, serán claves para adaptarnos a la normativa NIS2. Esta normativa, modificada en 2022 y de amplia adopción tanto de parte del sector público como el privado, nos ayuda a tener bastante certeza respecto de hacia donde se dirige la normativa española.

El Esquema Nacional de Seguridad, y sus futuros perfiles de cumplimiento específico por sectores, serán claves para adaptarnos a la normativa NIS2.

1. Marco Organizativo

Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.

- Política de seguridad
- Normas de seguridad
- Procedimientos de seguridad
- Proceso de autorización

2. Marco Operacional

Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

- Planificación
- Control de acceso
- Explotación
- Servicios externos
- Servicio en la nube
- Continuidad del servicio
- Monitorización del sistema

3. Medidas de protección

Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones actuales.

- Instalaciones e infraestructuras
- Gestión del personal
- Protección de los equipos
- Protección de las comunicaciones
- Protección de los soportes de información
- Protección de aplicaciones informáticas
- Otras

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.

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.

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.**

Enero 2025

Anteproyecto de ley de transposición española.

2025 - 2026

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

2025 - 2026

Aprobación del anteproyecto de transposición y entrada en vigor de la futura Ley.

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.

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.

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.

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.

Javier Aznar
Socio de Technology Risk Ciberseguridad y Privacidad de KPMG en España
E: 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
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
T: +34 606 67 04 28

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

Descubre cómo

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.

kpmg.es