NIS2: Ciberseguridad más allá de la tecnología

Gobernanza, riesgo y cumplimiento normativo



Un nuevo nivel de exigencia en ciberseguridad

La Directiva NIS2 refuerza las obligaciones de las organizaciones en materia de **ciberseguridad, gestión de riesgos y gobernanza**, situando estas cuestiones más allá de una dimensión estrictamente tecnológica.

En España, la **transposición de la Directiva continúa en tramitación** a través del Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad. Este marco permite anticipar un refuerzo de las obligaciones de gestión de riesgos, supervisión, notificación de incidentes y responsabilidad de los órganos de dirección.

¿Está su organización dentro del ámbito de NIS2?

El ámbito previsto por la NIS2 comprende, con carácter general, a **medianas y grandes organizaciones** que operan en sectores de alta criticidad y otros sectores críticos, junto con determinadas entidades que pueden quedar sujetas con independencia de su tamaño.

La aplicabilidad debe analizarse caso por caso, atendiendo al **sector, tamaño, actividad desarrollada y naturaleza de los servicios prestados.**

Entre los sectores potencialmente afectados se encuentran:

- Energía, transporte y sanidad;
- Banca e infraestructuras de los mercados financieros;
- Agua potable y aguas residuales;
- Infraestructuras digitales y gestión de servicios TIC;
- Administración Pública, espacio e industria nuclear;
- Servicios postales, mensajería y gestión de residuos;
- Productos químicos, alimentación e industria manufacturera;
- Proveedores de servicios digitales;
- Investigación;
- Seguridad privada.

¿Qué se exigirá a las organizaciones?

Las organizaciones incluidas en el ámbito de NIS2 deberán adoptar medidas adecuadas y proporcionadas para gestionar sus riesgos de ciberseguridad, incluyendo, entre otras:

- Gestión y evaluación de riesgos de ciberseguridad;
- Gobernanza y supervisión por los órganos de dirección;
- Gestión y notificación de incidentes;
- Continuidad de negocio y gestión de crisis;
- Seguridad de la cadena de suministro y de terceros;
- Seguridad en la adquisición, desarrollo y mantenimiento de redes y sistemas;
- Políticas de control de acceso, autenticación y uso de criptografía;



- Formación y concienciación en ciberseguridad.

El Anteproyecto español prevé, además, la figura del Responsable de la Seguridad de la Información, con funciones de coordinación de la estrategia y las políticas de ciberseguridad y de supervisión de su cumplimiento.

¿Por qué es importante actuar?

La NIS2 refuerza significativamente tanto el régimen de supervisión como las consecuencias del incumplimiento. Para las entidades esenciales, la Directiva exige que los Estados miembros prevean multas administrativas máximas de, al menos, **10 millones de euros o el 2 % del volumen de negocios anual mundial**, aplicándose el importe superior. Para las entidades importantes, los umbrales son de **7 millones de euros o el 1,4 %.**

La Directiva atribuye asimismo a los **órganos de dirección** responsabilidades en la aprobación y supervisión de las medidas de gestión de riesgos, reforzando la dimensión de gobernanza y responsabilidad corporativa de la ciberseguridad.

De la evaluación a la implementación

La preparación para NIS2 debe comenzar por la identificación del encaje de la organización y evolucionar hacia una revisión concreta de su nivel de cumplimiento y de las medidas necesarias para adaptarse al nuevo marco.

1. Determinar la aplicabilidad y clasificación
Analizar el sector, tamaño, actividad y servicios prestados para determinar si la organización se encuentra dentro del ámbito de NIS2 y su posible clasificación como entidad esencial o importante.

2. Evaluar el nivel de cumplimiento
Revisar políticas, procedimientos, contratos, mecanismos de gobernanza, gestión de proveedores y procedimientos de respuesta a incidentes existentes.

3. Identificar brechas y prioridades
Detectar las principales brechas de cumplimiento y los riesgos asociados, y definir las medidas de mitigación y las prioridades de actuación.

4. Preparar la implementación
Adaptar documentación, contratos, procesos y mecanismos de gobernanza y coordinar las medidas técnicas necesarias para avanzar hacia el cumplimiento del nuevo marco.

Asesoramiento en cumplimiento NIS2

Andersen presta asesoramiento a las organizaciones en las distintas fases de preparación y cumplimiento de NIS2, desde la **evaluación de la aplicabilidad y clasificación** hasta la identificación de gaps, definición de prioridades y adaptación de las medidas jurídicas y de gobernanza necesarias.

El acompañamiento incluye, entre otros aspectos, la revisión de políticas, procedimientos y contratos, la gestión y notificación de incidentes, la seguridad de la cadena de suministro y la preparación ante posibles actuaciones de supervisión, con un enfoque adaptado a la actividad y nivel de exposición de cada organización.

Para más información puede contactar con:



Isabel Martínez Moriel
Socia | Privacy, IT & Digital Business
isabel.martinez@es.andersen.com



María Suárez
Socia | Privacy, IT & Digital Business
maria.suarez@es.andersen.com



Daniel Torres Gonçalves
Socio | Privacy, IT & Digital Business
daniel.goncalves@pt.andersen.com



João Sousa Guimarães
Socio | Privacy, IT & Digital Business
joao.guimaraes@pt.andersen.com



Gonçalo Gil Barreiros
Socio Local | Privacy, IT & Digital Business
goncalo.barreiros@pt.andersen.com



María Zarzalejos García
Counsel | Privacy, IT & Digital Business
maria.zarzalejos@es.andersen.com



Augusto Almeida Correia
Director | Privacy, IT & Digital Business
augusto.correira@pt.andersen.com