Borrador de la Transposición Directiva NIS2 en España

ISMS Forum
Handbook

isms forum

ÍNDICE

Transposición de la directiva NIS2 en España: claves y novedades

La **Directiva NIS2 (UE 2022/2555)** refuerza la seguridad de las redes y sistemas de información en la Unión Europea, estableciendo un marco común para mejorar la resiliencia digital. España ha traspuesto la Directiva en la ley llamada de **Gobernanza y Coordinación de la ciberseguridad** en sectores clave.

¿Qué cambia con NIS2?

La nueva Directiva introduce *obligaciones más estrictas* y amplía su alcance para abordar las crecientes amenazas cibernéticas. Las principales novedades incluyen:

- **Mayor cobertura:** Se amplía el número de sectores regulados y se diferencian en *entidades esenciales e importantes* según su tamaño e impacto.
- **Normas más estrictas de notificación de incidentes:** Se establecen plazos más cortos y procedimientos más claros para informar sobre ciberincidentes.
- **Exigencia de acreditación del personal de seguridad.** Para las entidades esenciales, el responsable de seguridad de la información y para entidades críticas, el responsable de seguridad de la información y su personal.
- **Requisitos de gestión de riesgos más detallados:** Por ejemplo, medidas obligatorias para la seguridad en la cadena de suministro, que incluyen el punto de contacto de seguridad principal para cada uno de los proveedores
- **Supervisión y cumplimiento reforzado:** Las autoridades nacionales podrán realizar auditorías, imponer sanciones y exigir medidas correctivas.
- **Mayor armonización y cooperación** entre Estados Miembros para responder a incidentes transfronterizos.

¿Quiénes están obligados?

Las entidades afectadas por la **transposición de la NIS2** en España se dividen en **dos categorías:**

Entidades Esenciales

- Empresas grandes (**≥250 empleados o >50M€** de facturación anual).
- Energía, transporte, agua, sanidad, telecomunicaciones, Espacio, industria nuclear, servicios financieros, tecnologías digitales (nube, centros de datos y plataformas digitales).
- Administraciones públicas

Entidades Importantes

- Empresas medianas (**50-249 empleados o >10M€** de facturación anual).
- Sectores industriales clave (fabricación, postales y mensajería, alimentación, fabricación, residuos, químico, etc.).
- Investigación y seguridad privada

Inclusión de entidades transfronterizas con impacto significativo en la seguridad de la UE.

Sobre estas reglas generales, las autoridades pueden incluir excepcionalmente a otras empresas como sujetos obligados.

La cadena de suministro no está incluido en la ley como sujeto obligado, pero sus obligaciones con las entidades deben ser supervisadas por éstas.

Claves de la transposición en España

El anteproyecto de ley define un marco de gobernanza, supervisión y ejecución basado en:

1. **Creación del Centro Nacional de Ciberseguridad (CNC)** como autoridad única encargada de la gestión y coordinación de la ciberseguridad en España.

2. **Obligaciones de seguridad y gestión de riesgos** para entidades esenciales e importantes, alineadas con el **Esquema Nacional de Seguridad (ENS)** y normativas europeas.

3. **Notificación obligatoria de incidentes** a través de la **Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes** y los CSIRTs nacionales (CCN-CERT, INCIBE-CERT, ESPDEF-CERT).

4. **Supervisión y auditoría por autoridades de control** según el sector (Ministerio del Interior, Defensa, Transformación Digital).

5. **Sanciones más severas** por incumplimiento, con multas de hasta **10 millones de euros o el 2% del volumen de negocio global** para entidades esenciales.

6. **Refuerzo de las funciones** del Responsable de Seguridad de la Información.

Responsabilidades y obligaciones para empresas

Las organizaciones afectadas por la transposición deben adoptar un **enfoque proactivo** en ciberseguridad, con las siguientes medidas clave:

1. Responsabilidad
solidaria de los órganos de dirección, así como la designación de un Responsable de Seguridad de la Información, CISO, con acreditación específica.

2. Implementación
de medidas de seguridad avanzadas en redes y sistemas críticos.

3. Gestión
de riesgos en la cadena de suinistro, asegurando la seguridad de proveedores y servicios TIC externos.

4. Notificación
rápida de incidentes a través de la plataforma nacional de ciberincidentes.

5. Auditorías y controles
periódicos para garantizar el cumplimiento de la normativa.

6. Formación y concienciación
en ciberseguridad para órganos de dirección y empleados.

Novedad

Los directivos de las entidades esenciales serán responsables directos de la implementación de la ciberseguridad en sus organizaciones y deberán demostrar formación continua en la materia.

Obligaciones de los órganos de dirección

Aprobar las medidas para la gestión de riesgos de ciberseguridad incluidas en esta ley.

Supervisar su implan - tación y responder por su incumplimiento

Asumir la responsabilidad por su incumplimiento.

Los miembros de los órganos de dirección deben recibir formación adecuada de forma periódica para detectar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su repercusión en los servicios proporcionados por la entidad.

Los órganos de dirección deberán organizar periódicamente formaciones similares para sus empleados.

Responsable de Seguridad de la Información

Gestión y Estrategia

- Diseñar y someter a aparobación la estrategia de ciberseguridad y políticas de seguridad.
- Supervisar la implementación y efectividad de las políticas de seguridad.
- Asegurar el cumplimiento normativo en seguridad de redes y sistemas.

Supervisión y Capacitación

- Actuar como capacitador en buenas prácticas de ciberseguridad.
- Realizar controles periódicos para evaluar riesgos y vulnerabilidades.
- Garantizar el seguimiento y control de las políticas de seguridad implementadas.

Gestión de Incidentes y Notificación

- Gestionar ciberincidentes conforme al marco legal.
- Notificar sin demora a las autoridades de control y CSIRTs sobre incidentes y vulnerabilidades.

Interacción con Autoridades

- Implementar las instrucciones y guías de la autoridad de control.
- Recopilar y suministrar información relevante sobre seguridad.

Supervisión de Proveedores

- Garantizar que empresas externas y proveedores cumplan con los estándares de seguridad de la entidad.

Participación Activa en Ciberseguridad

- Involucrarse en todas las decisiones y aspectos relacionados con la ciberseguridad.

Independencia y Reporte Estratégico

- Informar a la alta dirección sobre riesgos y vulnerabilidades críticas.
- Facilitar la toma de decisiones estratégicas y operativas en ciberseguridad.

Diferencias en las obligaciones según el grado de la entidad

1. Medidas de Seguridad

- **Esenciales: Certificación obligatoria** de conformidad.
- **Importantes:** Pueden optar por certificación o autoevaluación de seguridad.
- **Esenciales e importante** bajo el ámbito de aplicación del RD 311/2022: la certificación de conformidad en el ENS

2. Supervisión y Ejecución

- **Esenciales: Controles más estrictos,** inspecciones presenciales y remotas, acceso a datos y medidas correctivas severas.
- **Importantes:** Supervisión a posteriori, con auditorías y sanciones solo en caso de incumplimiento probado.

3. Régimen Sancionador

- **Esenciales:** Multas de hasta **10M€ o el 2% del volumen de negocio global.**
- **Importantes:** Multas de hasta **7M€ o el 1.4% del volumen de negocio global.**

4. Responsable de Seguridad de la Información, CISO, y su personal:

- **Esenciales e importantes: Acreditación obligatoria** del Ministerio del Interior.
- **Críticos:** Acreditación también obligatoria **para todo el personal de ciberseguridad.**

Régimen de supervisión y sanciones

La transposición de la NIS2 establece un **modelo de supervisión y sanción más estricto:**

Supervisión Proactiva

- **Auditorías e inspecciones por parte de las autoridades de control.**
- **Evaluación periódica del cumplimiento de medidas de seguridad.**

Régimen Sancionador

Las sanciones varían según la gravedad de la infracción:

Entidades Esenciales

- **Multas de hasta 10M€ o el 2% del volumen de negocio global (la mayor de ambas).**

Entidades Esenciales

- **Multas de hasta 7M€ o el 1.4% del volumen de negocio global.**

Novedad

Incumplimientos graves pueden llevar a la suspensión temporal de directivos y restricciones en la actividad empresarial.

Cooperación y coordinación nacional e internacional

- **Fortalecimiento de la colaboración público-privada** en la respuesta a ciberincidentes.
- **Intercambio de información entre entidades** sobre amenazas, vulnerabilidades y mejores prácticas.
- **Mayor coordinación a nivel europeo** para incidentes transfronterizos.

Novedad

Se fomenta la notificación voluntaria de ciberamenazas menores para mejorar la respuesta global ante ataques.

AUTORES

Participantes Francisco Lázaro
Beatriz García

Diseño y maquetación Lydia García

CONTACTA CON NOSOTROS

Si estás interesado/a en colaborar con nosotros o necesitas más información sobre nuestros proyectos, escríbenos a: **proyectos@ismsforum.es**

isms forum