MEGASTAR S.L.
Paula Montal Fornés nº 4, local - 50.018 – Zaragoza - **Tel:** 976 466 644 - www.megastar.es – megastar@megastar.es

RESUMEN DE LA DIRECTIVA NIS2

La Directiva NIS 2 entró en vigor el 16 de enero de 2023, y los Estados miembros disponen de 21 meses, hasta el 17 de octubre de 2024, para transponerla a la legislación nacional. Está destinada a garantizar un elevado nivel común de ciberseguridad en toda la Unión Europea y su objetivo es mejorar las medidas destinadas a garantizar un adecuado nivel común de ciberseguridad.

Sectores afectados:
Entidades esenciales, Sectores de Alta Criticidad (11 sectores):
energía, banca, infraestructuras de mercados financieros, sector sanitario, transporte, infraestructura digital, aguas potables, aguas residuales, administración pública (con exclusión del poder judicial, parlamentos y bancos centrales), gestión de servicios TIC (Business to Business) y espacio.

Entidades importantes, que serán todas aquellas entidades que pertenezcan a los sectores de alta criticidad o a otros sectores críticos que no pueden considerarse entidades esenciales.

También están obligadas a cumplir con la directiva NIS 2 **las empresas que suministran a las que están en alguno de los sectores mencionados**.

El flujo de notificación que propone la Directiva NIS 2 para los incidentes significativos es:

1. Notificación inicial:
   - Alerta temprana: **en un plazo de 24 horas** desde que se haya tenido constancia del incidente.
2. Notificación intermedia:
   - Actualización: **pasadas 72 horas** desde la detección del incidente, las entidades deberán actualizar el estado del incidente exponiendo una evaluación inicial.
3. Notificación final:
   - Presentación informe: a más tardar **un mes después** de la notificación del incidente, las entidades deberán presentar un informe final que recoja una descripción detallada del mismo (incluyendo gravedad, impacto, tipo de amenaza que haya provocado el incidente, medidas paliativas aplicadas y en curso y, si aplica, repercusiones transfronterizas).

La información detalla se encuentra en el Boletín Oficial del Estado (BOE) https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963

MEGASTAR S.L.
Paula Montal Fornés nº 4, local - 50.018 – Zaragoza - **Tel:** 976 466 644 - www.megastar.es – megastar@megastar.es

Resumen gráfico

DIRECTIVA | NIS 2

1. Qué es la Directiva NIS 2.

NIS 2 es una directiva de la Unión Europea con aplicación directa de tipo vertical.

Objetivo: elevar el nivel de ciberseguridad en la Unión Europea.

1. Estrategias nacionales, autoridades competentes, puntos de contacto únicos y equipos de respuesta (CSIRT).
2. Medidas para la **gestión de riesgos** de ciberseguridad.
3. Obligaciones de **notificación**.
4. Obligaciones de **intercambio de información**.
5. Obligaciones de **supervisión y ejecución**.

Entrada en vigor: 26 de enero de 2023.
Obligatoria en España*: 18 de octubre de 2024.

N I S
Network and Information Security

*La Directiva NIS debe ser transpuesta y esa ley será obligatoria en España.

esic University

3

DIRECTIVA | NIS 2

2. ¿Me afecta la Directiva NIS 2?

Están obligadas grandes empresas, e incluso muchas medianas y pequeñas que operan en servicios esenciales e importantes.

La Directiva NIS 2 se aplica a 18 sectores, divididos en:
- Sectores de Alta Criticidad.
- Otros Sectores Críticos.

La Directiva NIS 2 distingue dos tipos de entidades:
- Entidades esenciales.
- Entidades importantes.

Cumplirán NIS 2 las empresas de alguno de los 18 sectores con al menos 50 personas empleadas o cuyo volumen de negocios anual sea igual o superior a 10 millones de euros*.

* El artículo 2 de la Directiva NIS 2 concreta el detalle de las entidades que son sujetos obligados.

Aplica a servicios y redes de comunicaciones electrónicas.

Aplica a proveedores y demás sujetos de la cadena de suministro.

esic University

4

DIRECTIVA | NIS 2

3. Sectores con empresas obligadas al cumplimiento de la Directiva NIS 2.

También están obligadas a cumplir con la Directiva NIS 2 las empresas que suministran a las que están en alguno de los sectores.

Sectores:

- Energía
- Transporte
- Banca
- Mercados financieros
- Salud
- Agua potable
- Aguas residuales
- Infraestructura digital
- Gestión de servicios TIC B2B
- Administración Pública
- Espacio
- Servicios de correo y mensajería
- Gestión de residuos
- Fabricación, producción y distribución de químicos
- Producción, procesamiento y distribución de alimentos
- Fabricación
- Proveedores digitales
- Investigación

Administración local y centros de enseñanza podrían estar obligados.

17 de abril de 2025: existirá una lista de entidades esenciales e importantes.

5

DIRECTIVA | NIS 2

4. El equipo directivo está obligado a conocer sobre ciberseguridad.

Saber de ciberseguridad es requisito indispensable para poder mantenerse en un cargo del órgano de dirección.

Los miembros de los órganos de dirección están obligados a tener conocimientos prácticos suficientes en ciberseguridad:

- Formarse y demostrar conocimientos en ciberseguridad.
- Articular formaciones en ciberseguridad para su plantilla:
  - Conocimientos y destrezas suficientes.
  - Capacidades de detección de riesgos.
  - Evaluar prácticas de gestión del riesgo.
- Aprobar medidas para la gestión de riesgos.
- Supervisar la puesta en práctica de las medidas.
- Responder personalmente por el incumplimiento.

El órgano directivo es el primero que debe aprender ciberseguridad.

Las personas incompetentes con cargos directivos podrán ser cesadas.

6

5. Medidas para la gestión de riesgos de ciberseguridad.

Las medidas de seguridad se desplegarán sin demora indebida y se documentará su estado actual y su evolución.

Gestión de riesgos y prevención de repercusiones:

- **Políticas de seguridad** y análisis de riesgos.
- **Gestión de incidentes** y de comunicación de emergencias.
- **Continuidad:** gestión de *backup*, recuperación, crisis...
- Seguridad de la **cadena de suministro.**
- **Seguridad en adquisición,** desarrollo y mantenimiento de sistemas de redes y de información.
- Procedimientos de evaluación de la **eficacia de las medidas.**
- **Ciberhigiene** y formación en ciberseguridad.
- Uso de **criptografía** y, en su caso, de cifrado.
- Seguridad de RRHH, control de accesos y **gestión de activos.**
- **Autenticación multifactorial** o continua.

El uso de soluciones certificadas según esquemas UE será exigido.

Proporcionalidad: grado de exposición, tamaño, probabilidad, coste, gravedad.

7

6. Medidas de supervisión y ejecución para asegurar el cumplimiento.

Se establecerán medidas efectivas, proporcionadas y disuasorias teniendo en cuenta las circunstancias de cada caso individual.

Acciones de supervisión:

- Inspección *in situ* y supervisión a distancia
- Auditorías de seguridad (y *ad hoc* para entidades esenciales)
- Análisis de seguridad y evaluación del riesgo
- Requerimientos de información y acceso a datos
- Solicitudes de prueba de aplicación de las medidas

Acciones de ejecución:

- Apercibimiento y requerimiento de subsanación.
- Cese de la actividad infractora.
- Comunicación a los afectados o publicación de la brecha.
- Multa administrativa.

Los costes de las auditorías serán sufragados por la entidad auditada.

La persona con cargo directivo podrá ser suspendida en sus funciones o se le prohibirá ejercer en su cargo directivo.

8

MEGASTAR S.L.
Paula Montal Fornés nº 4, local - 50.018 – Zaragoza - **Tel:** 976 466 644 - www.megastar.es – megastar@megastar.es

DIRECTIVA | NIS 2

7. Notificación de incidentes.

Los incidentes que tengan un impacto significativo en la prestación de servicios tienen que notificarse al CSIRT.

Informe final de notificación de un incidente:
- Descripción detallada del incidente (gravedad e impacto).
- Tipo de amenaza y causa probable de la amenaza.
- Medidas paliativas aplicadas y en curso.
- Repercusiones transfronterizas.

CSIRT responderá con orientaciones y asesoramiento operativo.

Antes de 24 h.: alerta temprana.
Antes de 72 h.: notificación de incidente.
Antes de 1 mes: informe final (+ intermedio + posterior)

Notificar no eleva la responsabilidad ni hace surgir nuevas obligaciones.

Las entidades no obligadas también pueden notificar ciberamenazas, incidentes y cuasiincidentes.

esic University

9

DIRECTIVA | NIS 2

8. Multas administrativas por incumplimiento de la Directiva NIS 2 (a través de la norma local).

Las sanciones serán efectivas, proporcionadas y disuasorias.

Para la imposición de multas se tendrá en cuenta:
- Gravedad y duración del incumplimiento.
- La existencia de incumplimientos anteriores.
- Todo perjuicio material o inmaterial.
- Cualquier intencionalidad o negligencia.
- Medidas adoptadas para prevenir o mitigar.
- Adhesión a códigos de conducta y grado de cooperación.

Multas:
- Entidades esenciales: <10M € ~ <2% del negocio.
- Entidades importantes: <7M € ~ <1,4% del negocio.

Las multas por protección de datos se acumulan, pero no se duplican.

Los importes y porcentajes de las multas (eligiéndose la de mayor valor) podrán ser elevados por los Estados.

esic University

10

DIRECTIVA | NIS 2

9. Conclusiones sobre la Directiva NIS 2.

Se espera una actividad de responsabilidad proactiva para el cumplimiento con un enfoque en todo el riesgo.

Puntos clave de la Directiva NIS 2:

- El objetivo de NIS 2 es alcanzar un nivel adecuado de **seguridad completa** (lógica y física).
- La norma obliga a **documentar el cumplimiento** y ser capaz de probar la eficacia y eficiencia de las medidas de seguridad.
- El órgano directivo puede ser cesado si carece de conocimientos y **competencias prácticas** en ciberseguridad.
- La empresa debe estar en disposición de **notificar** inmediatamente al CSIRT los incidentes.
- Las **multas** podrán superar los 10 millones de euros o el 2% de la cifra anual de negocio.

NIS 2 busca elevar la seguridad

Estamos en tiempo de descuento para cumplir antes del 18 oct. 2024.

esic University

11