NIS 2

¿QUÉ ES Y QUÉ IMPACTO TENDRÁ LA NUEVA DIRECTIVA EN LA ESTRATEGIA DE CIBERSEGURIDAD DE SU EMPRESA?

cylsolar
Cluster de Energías Renovables y Soluciones Energéticas en Castilla y León

icecyl

Junta de Castilla y León

DIPUTACIÓN DE ÁVILA

Ayuntamiento de Ávila

NUEVOS REQUERIMIENTOS EN CIBERSEGURIDAD PARA EL SECTOR ENERGÉTICO Y AGROALIMENTARIO NIS 2

Jorge Herráez

CLICKDEFENSE

ÍNDICE DE CONOCIMIENTOS SOBRE LA DIRECTIVA NIS 2

La Directiva NIS 2, un paso más hacia la ciberseguridad en la Unión Europea

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 el territorio de la Unión Europea.

¿Qué integra?

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

N I S
Network and **I**nformation **S**ecurity

Entrada en vigor de la directiva: 26 de enero de 2023.
Transposición y ley obligatoria en España: 18 de octubre de 2024.

2. ¿PUEDO VERME AFECTADO POR LA DIRECTIVA NIS 2?

La Directiva NIS 2 es aplicable tanto a grandes empresas como a medianas y pequeñas empresas que operen 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.

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

Es de **obligado cumplimiento para empresas que pertenezcan a alguno de los 18 sectores con, al menos, 50 empleados o cuyo volumen de facturación anual sea igual o superior a 10 millones de euros*.**

* El Artículo 2 de la Directiva NIS 2, concreta las entidades que son sujetos obligados

3. SECTORES CON EMPRESAS OBLIGADAS AL CUMPLIMIENTO DE LA DIRECTIVA NIS 2

También se encuentran obligadas al cumplimiento de la Directiva NIS 2 las empresas que suministran a aquéllas que se encuentran en alguno de los siguientes 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.

La Administración Local y los centros de enseñanza, podrían verse obligados.

A partir del **17/04/25** existirá una lista de entidades esenciales e importantes.

4. ¿EL EQUIPO DIRECTIVO ESTÁ OBLIGADO A TENER CONOCIMIENTOS SOBRE CIBERSEGURIDAD?

Es indispensable disponer de conocimientos de ciberseguridad para poder mantenerse en un cargo del órgano de dirección.

- Deben de formarse y demostrar los conocimientos en ciberseguridad.
- Facilitar formaciones para el resto de miembros de la plantilla:
  - Conocimientos y destrezas.
  - Capacidades de detección de riesgos.
  - Evaluar prácticas de gestión del riesgo.
- Aprobar medidas para la gestión de riesgos.
- Supervisar la puesta en marcha de las medidas.
- Responder personalmente ante el incumplimiento.

Los cargos directivos tendrán responsabilidad personal.

5. MEDIDAS PARA LA GESTIÓN DE RIESGOS DE CIBERSEGURIDAD

Gestión de riesgos y prevención de consecuencias:

- **Políticas de seguridad** y análisis de riesgos.
- **Gestión de incidentes** y de comunicación de emergencias.
- **Continuidad:** gestión de backup, repercusión, dificultades…
- Seguridad de la **cadena de suministro**.
- Seguridad en la adquisición, desarrollo y mantenimiento de sistemas de redes y de información.
- Procesamientos de evaluación de la **eficacia de medidas**.
- **Ciberhigiene** y formación en ciberseguridad.
- Uso de **criptografía** y 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.

6. MEDIDAS DE EJECUCIÓN Y SUPERVISIÓN PARA ASEGURAR EL CUMPLIMIENTO

Será necesario establecer medidas para asegurar el cumplimiento, teniendo en cuenta cada caso de manera individual.

- **Acciones de supervisión:**
  - Inspección in situ y supervisión a distancia.
  - Adquisición 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:**
  - Advertencia 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 asumidos por las entidades auditoras.

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

7. NOTIFICACIÓN DE INCIDENTES

Los incidentes con impacto significativo, tienen que ser notificados al CSIRT. Notificar, no eleva la responsabilidad ni crea nuevas obligaciones.

El informe final de notificación de incidentes debe contener:

- Descripción detallada del incidente (gravedad e impacto).
- Tipo de amenaza y posible causa.
- Medidas aplicables y en curso.
- Repercusiones transfronterizas.

CSIRT debe responder con orientaciones y asesoramiento operativo:

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

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

8. MULTAS ADMINISTRATIVAS POR EL INCUMPLIMIENTO DE LA DIRECTIVA NIS (MEDIANTE LA NORMA LOCAL)

Las sanciones serán efectivas, proporcionadas y convincentes.

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 adaptadas para prevenir o mitigar.
- Adhesión o códigos de conducta y grados de cooperación.

Multas:

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

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

Los importes y los porcentajes de las multas (eligiendo el de más valor), pueden ser elevados por los Estados.

9. CONCLUSIONES SOBRE LA DIRECTIVA NIS 2

NIS 2 pretende elevar la seguridad, de este modo, se espera así una actividad responsable y proactiva par el cumplimiento con un enfoque en todo el riesgo.

Puntos clave a tener en cuenta:

- El objetivo principal es conseguir **una seguridad completa** (lógica y física).
- La norma obliga a **documentar el cumplimiento** y ser capaz de probar la eficacia y la eficiencia de los medios de seguridad.
- El órgano directivo puede ser cesado si carece de conocimientos y **competencias prácticas** en ciberseguridad.
- La empresa debe de notificar a CSIRT los incidentes.
- Las **multas** impuestas podrán superar los 10 millones de euros o el 2% de la cifra anual de negocio.

Estamos en el tiempo de descuento para cumplir antes del 18/10/24.

¡GRACIAS!

https://www.linkedin.com/in/jorgeherraez/

SCAN ME