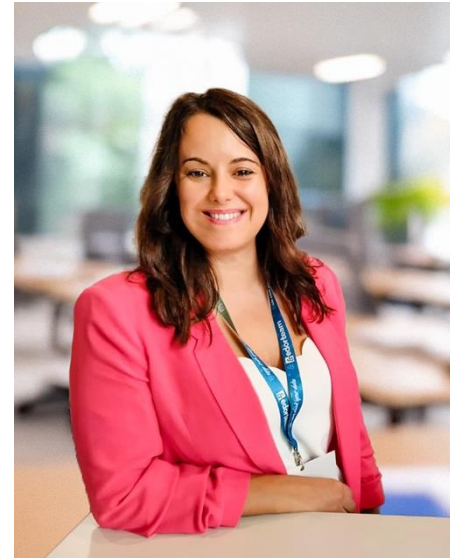


# Directiva NIS2: cómo afecta a tu empresa y por qué debes prepararte

# Índice

- Qué es la Directiva NIS2 y por qué es importante
- Sectores y empresas a las que afecta
- Sanciones por incumplimiento
- Cómo cumplir con los requisitos de la Directiva
- Aprovecha el Kit Consulting para adaptarte sin coste



Gemma Rufino, CMO de Edorteam

[gemma@edorteam.com](mailto:gemma@edorteam.com)



Edorteam

# ¿Qué es la Directiva NIS2 y por qué es importante?

# ¿Qué es la Directiva NIS2?

- Actualización de la **Directiva NIS** (en España RD 43/2021).
- Respuesta a las **crecientes amenazas** cibernéticas en sectores esenciales.
- Creada para **proteger la economía y sociedad** en la UE.
- Tras la pandemia, aumentaron los ciberataques y la **dependencia de las tecnologías de la información**.
- La NIS2 nace para **ampliar el alcance** de la normativa y las obligaciones.
- España aún debe **transponer la NIS2** a ley nacional.

# ¿Por qué es importante?

- Las empresas dependen de la tecnología y están **expuestas a riesgos** cibernéticos.
- Un ciberataque podría **paralizar servicios esenciales**, afectando a la sociedad y la economía.
- La NIS2 establece medidas de seguridad obligatorias para **proteger la operatividad y resiliencia** de estos servicios esenciales.



# Sectores y empresas a las que afecta la NIS2

# Alcance

## Sectores de alta criticidad



Energía



Banca e infraestructuras de mercados financieros



Sector sanitario



Transporte



Infraestructura digital



Aguas potables y residuales



Administración Pública



Proveedores de servicios TIC (B2B)



Espacio

## Otros sectores críticos



Investigación



Química



Alimentación



Servicios postales



Proveedores de servicios digitales



Fabricación



Gestión de residuos

# Sanciones por incumplimiento



# Consecuencias legales

- **Multas elevadas:** pueden alcanzar los 10 millones de euros o el 2% de la facturación anual de la empresa, si supone una cifra mayor.
- **Sanciones administrativas:** suspensión de actividad o imposición de medidas correctivas impuestas por las autoridades competentes.
- **Responsabilidad penal:** los directivos podrían ser responsables si no implementan las medidas adecuadas para proteger los datos y sistemas.

# Impacto en la actividad empresarial

- **Pérdida de productividad:** debido a las interrupciones en su operativa.
- **Costes de recuperación:** los costes derivados de un ataque, como la recuperación de datos, implementación de nuevos sistemas y contratación de expertos, pueden ser elevados.
- **Pérdida de competitividad:** las empresas que no se adaptan a la normativa pierden ventaja competitiva frente a aquellas que sí lo hacen.

# Impacto en la reputación

- **Pérdida de clientes:** pierden confianza en la capacidad de la empresa para proteger sus datos.
- **Impacto en las relaciones comerciales:** los socios pueden optar por trabajar con empresas mejor protegidas.
- **Reputación pública:** un ciberataque puede atraer la atención negativa de los medios y dañar la imagen pública de la empresa.

# Cómo cumplir con los requisitos de la Directiva

# Medidas a implementar

- **Informe con las medidas de seguridad** para la gestión de incidentes, control de acceso y protección de datos.
- Desarrollo y mantenimiento de **políticas de seguridad** de la información.
- Concienciación y **formación** al equipo profesional.
- Evaluación de **proveedores**.
- Creación de un **plan de respuesta y recuperación** a incidentes.
- Gestión y **notificación de incidentes** a autoridades en 24 horas.
- Realización de **auditorías periódicas**.
- **Actualización periódica** de políticas y procedimientos.

Aprovecha el Kit Consulting  
para adaptarte sin coste

# 7 claves del Kit Consulting



- Bono digital para invertir en **servicios de consultoría**.
- Para empresas de **10 a 249 empleados**.
- Bonos desde **12.000 € hasta 24.000 €** a fondo perdido.
- La empresa no adelanta la ayuda, tan solo **asume el IVA**.
- Los servicios deben ser contratados a **asesores digitales** adheridos al programa Kit Consulting.
- **Ayudas 100% compatibles** con el Kit Digital.
- Plazos de solicitud y fondos muy limitados (por orden de solicitud).

# Categorías de asesoramiento



Entre 10 y menos de 50 empleados	<b>12.000 €</b>
Entre 50 y menos de 100 empleados	<b>18.000 €</b>
Entre 100 y menos de 250 empleados	<b>24.000 €</b>

■ Cada categoría = 6.000 €



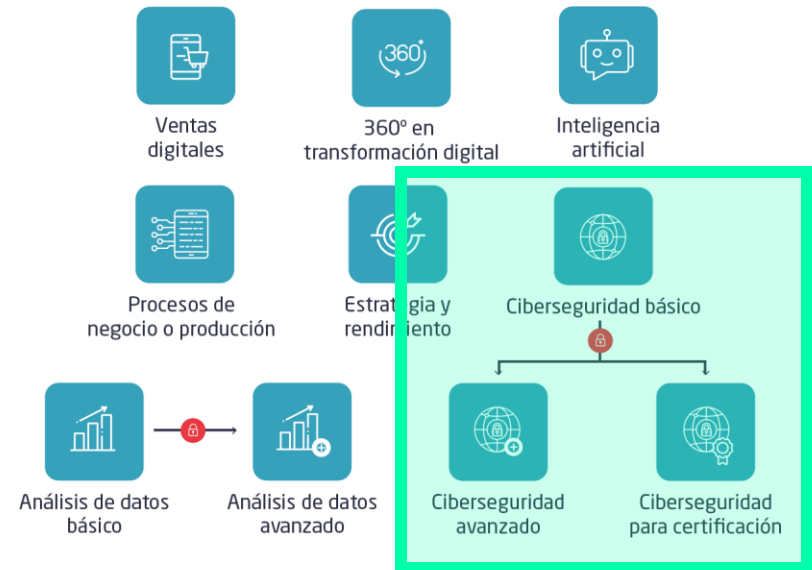


# Categorías de asesoramiento



Entre 10 y menos de 50 empleados	<b>12.000 €</b>
Entre 50 y menos de 100 empleados	<b>18.000 €</b>
Entre 100 y menos de 250 empleados	<b>24.000 €</b>

■ Cada categoría = 6.000 €



# Servicios de consultoría ciberseguridad



Kit Consulting establece tres niveles para el  
**Servicio de Asesoramiento en Ciberseguridad:**

- **Básico** (6.000 €)
- **Avanzado** (6.000 €)
- **Preparación para Certificación** (6.000 €)

**Realizar el nivel Básico es obligatorio para acceder a cualquiera de los otros dos niveles de Asesoramiento en Ciberseguridad.**

# Preparación para certificación



En la categoría Preparación para Certificación, se preparará toda la documentación para presentar tu SGSI a la certificación elegida\* (**ISO27001 o ENS media-alta**, según la Guía CCN-STIC 825).

- Revisión documental
- Roles y responsabilidades
- Formación al equipo profesional
- Documentación de procesos
- Análisis del entorno tecnológico y servicios

# ¿Cómo solicitar el Kit Consulting?



- **Solicitud online** en la sede electrónica de red.es.
- Es necesario acceder con el **certificado digital** de empresa.
- Para la solicitud no es necesario indicar **en qué vas a invertir el bono**.
- **Gestión rápida** y sin aportar documentación.
- Tras la concesión del bono, dispones de **3 meses** para firmar el primer acuerdo con el asesor digital que elijas.



Te ayudamos  
desde Edorteam

¿Alguna pregunta?



*Gracias*

Financiado por:

