

**BLOG**  
**OPINIÓN**

## NIS2: la ciberseguridad pasa a ser obligatoria en la UE

JULIO CÉSAR MIGUEL

Imagínese que abre el grifo de su casa y no sale agua. Y no solo le pasa a usted, sino a toda la ciudad. ¿En cuanto tiempo se generaría un caos? Esto realmente puede pasar, ya que los equipos que controlan las bombas que impulsan el agua están conectados a Internet y pueden sufrir ciberataques que los bloqueen.

La Directiva NIS2 (Network and Information Security Directive 2) es la nueva normativa de la Unión Europea destinada

a reforzar la ciberseguridad en los Estados miembros y su aplicación es inminente.

Los sectores afectados por la NIS2 se dividen en dos categorías:

1. Sectores esenciales: Deben cumplir con estrictos requisitos de seguridad y estarán sujetos a una supervisión rigurosa. Incluyen: energía, transporte, banca y mercados financieros, agua potable y aguas residuales, salud, infraestructuras digitales y administración pública.

2. Sectores importantes: También deben aplicar medidas de seguridad y estarán sujetos a una supervisión más flexible. Incluyen: servicios postales y de mensajería, fabricación de productos esenciales (como farmacéuticos y equipos electrónicos), fabricación de vehículos de motor y empresas de producción y distribución de alimentos.

La NIS2 establece una serie de requisitos de seguridad y gestión del riesgo para las empresas y organismos afectados. Algunas de las medidas más destacadas incluyen:

**Gobernanza y responsabilidad:** Se exige la implicación de la alta dirección en la ciberseguridad.

**Evaluación de riesgos:** Las empresas deben realizar análisis de riesgos periódicos para identificar y mitigar vulnerabilidades en sus sistemas.

**Medidas técnicas y organizativas:** Se requieren controles de seguridad robustos, como autenticación multifactor, cifrado, segmentación de redes y gestión de accesos.

**Gestión de incidentes:** Las entidades deben contar con procedimientos para la detección, gestión y notificación de incidentes de ciberseguridad en un plazo de 24 horas.

**Continuidad del negocio:** Implementación de planes de recuperación ante desastres y pruebas periódicas para garantizar la disponibilidad de los servicios.

**Supervisión y auditorías:** Se establece la obligación de realizar auditorías periódicas.

El incumplimiento de la NIS2 conlleva sanciones significativas, que pueden alcanzar hasta 10M o el 2% del volumen de negocio global anual de la empresa, dependiendo de cuál sea mayor.

Y tu, querido empresario, ¿estás preparado para la NIS2?

Juño César Miguel es experto en ciberseguridad y privacidad, CEO de Grupo CFI, vicepresidente de CyberLur y presidente de AETICAL grupocfi.es