Nº 12 marzo 2026

La Nueva Ley de Resiliencia y su impacto en la normativa española de infraestructuras críticas

Hacia un modelo integral basado en la continuidad de funciones esenciales

La evolución del entorno de riesgos, caracterizado por amenazas híbridas, interdependencias críticas y alta digitalización, ha impulsado un cambio profundo en el marco regulatorio europeo y nacional. La nueva legislación en materia de resiliencia -inspirada en la Directiva CER- introduce un cambio de paradigma en la protección de infraestructuras críticas.

En España, el Gobierno ha aprobado, a propuesta del Ministerio del Interior, el proyecto de Ley de Protección y Resiliencia de Entidades Críticas, que incorpora al ordenamiento jurídico nacional la más reciente directiva europea sobre la salvaguarda de aquellas instituciones y empresas que prestan servicios esenciales en sectores estratégicos indispensables para mantener las funciones sociales o las actividades económicas vitales en el ámbito nacional y la Unión Europea.

Este cambio supone la transición desde el modelo tradicional de protección de activos hacia un enfoque centrado en la resiliencia de las entidades críticas, donde el objetivo principal es garantizar la continuidad de los servicios esenciales.

1 Introducción: del modelo PIC a la resiliencia

El modelo español de protección de infraestructuras críticas, basado en la Ley 8/2011 y su desarrollo reglamentario, ha sido durante años un referente en la gestión de la seguridad estratégica.

Sin embargo, el contexto actual ha evolucionado significativamente hacia: Mayor exposición a riesgos complejos; Interdependencia entre sistemas físicos y digitales; Incremento de amenazas híbridas.

En este escenario, el enfoque tradicional -centrado en la protección de infraestructuras- resulta insuficiente. La nueva normativa impulsa un cambio hacia la resiliencia, entendida como la capacidad de las organizaciones para anticipar, resistir, responder y recuperarse ante cualquier tipo de incidente.

2 Origen del cambio: el marco europeo

La transformación normativa tiene su origen en el marco europeo, especialmente en la Directiva de Resiliencia de Entidades Críticas (CER).

Esta normativa introduce tres elementos clave:

- Ampliación del alcance: más sectores y servicios esenciales
- Enfoque "all hazards": consideración de todo tipo de amenazas
- Orientación a funciones críticas: más allá del activo físico

Además, la Directiva CER se complementa con otras regulaciones como NIS2, consolidando un modelo donde la **seguridad física y la ciberseguridad convergen**.

3 Transformación del modelo español

La adaptación de la normativa española implica una evolución significativa del modelo actual.

- **De infraestructura crítica a entidad crítica**

El foco se desplaza: De la infraestructura al servicio que presta; Del activo a la función esencial.

- **De protección a resiliencia**

Se pasa de: Proteger a garantizar continuidad; Reaccionar a anticipar

- **De cumplimiento a gestión activa**

La seguridad deja de ser un ejercicio de cumplimiento normativo para convertirse en un proceso continuo de gestión del riesgo.

4 Un nuevo modelo de gestión de riesgos

La nueva normativa introduce un enfoque más avanzado y dinámico:

Evaluación integral: Inclusión de riesgos físicos, digitales, naturales e híbridos; Análisis de interdependencias

Enfoque basado en escenarios: Eventos extremos; Crisis complejas; Impactos en cascada

Evaluación continua: Revisión periódica de riesgos; Adaptación a cambios del entorno

5 Nuevas obligaciones para operadores críticos

El nuevo marco normativo establece exigencias más amplias y profundas para los operadores.

- **Planes de resiliencia**

Evolución de los tradicionales: Planes de Seguridad del Operador (PSO); Planes de Protección Específicos (PPE)

Hacia modelos integrados que incluyen: Continuidad de negocio; Gestión de crisis; Recuperación operativa

- **Gobernanza y organización**

Designación de responsables de resiliencia; Integración en la alta dirección; Estructuras de coordinación interna

- **Gestión de incidentes**

Notificación obligatoria; Coordinación con autoridades; Evaluación posterior

- **Continuidad operativa**

Planes de continuidad robustos; Redundancia de sistemas; Capacidades de recuperación

6 Refuerzo de la colaboración público–privada

Uno de los pilares del nuevo modelo es la intensificación de la cooperación entre sector público y privado.

Elementos clave: Intercambio de información; Sistemas de alerta temprana; Coordinación en la gestión de crisis

Las autoridades asumen un rol más activo en: Supervisión: Apoyo operativo; Evaluación de resiliencia

7 Convergencia con la ciberseguridad

La integración con la normativa de ciberseguridad, especialmente NIS2, es uno de los aspectos más relevantes.

Características del nuevo enfoque: Gestión unificada de riesgos físicos y digitales; Protección de sistemas OT e IT; Enfoque integral "all hazards"

Esto obliga a las organizaciones a romper definitivamente la separación entre seguridad física y ciberseguridad.

8 Impacto en la gobernanza empresarial

La resiliencia se eleva al máximo nivel de decisión.

Implicaciones: Participación del consejo de administración; Responsabilidad directa de la alta dirección; Integración en la estrategia corporativa.

Nuevos roles: Chief Security Officer (CSO); Responsable de resiliencia; Coordinación con CISO.

9 Tecnología como habilitador de resiliencia

La transformación regulatoria impulsa la adopción de tecnologías avanzadas: Monitorización continua; Sistemas de detección temprana; Analítica de datos; Plataformas integradas de seguridad

No obstante, la tecnología debe estar alineada con una estrategia de gestión del riesgo, evitando enfoques puramente tecnológicos.

10 Supervisión, auditoría y cumplimiento

El nuevo marco introduce mecanismos más exigentes: Auditorías periódicas de resiliencia; Evaluación de capacidades operativas; Definición de indicadores (KPIs); Medición de tiempos de recuperación

11 Retos y oportunidades

Retos: Adaptación del marco normativo actual; Integración real de seguridad física y ciberseguridad; Desarrollo de cultura de resiliencia; Diferentes niveles de madurez entre sectores

Oportunidades: Modernización del modelo de seguridad; Mejora de la coordinación institucional; Incremento de la resiliencia nacional; Ventaja competitiva para organizaciones avanzadas

Conclusión

La nueva Ley de Resiliencia representa un **cambio estructural en la protección de infraestructuras críticas en España.**

El foco se desplaza desde la protección de activos hacia la garantía de continuidad de funciones esenciales, integrando seguridad, tecnología y gobernanza en un modelo único.

En este contexto, la resiliencia deja de ser un concepto teórico para convertirse en una **capacidad estratégica imprescindible.**

No se trata solo de evitar fallos, sino de garantizar que, cuando estos ocurran, el sistema siga funcionando y pueda recuperarse con rapidez y eficacia.

Manuel Sánchez Gómez-Merelo
Vocal de la Junta Directiva de AES