



## RESPUESTA DEL GOBIERNO

### (184) PREGUNTA ESCRITA CONGRESO

184/20883

04/03/2025

59262

**AUTOR/A: FERNÁNDEZ HERNÁNDEZ, Pedro (GVOX); MEJÍAS SÁNCHEZ, Carina (GVOX); RODRÍGUEZ ALMEIDA, Andrés Alberto (GVOX)**

#### RESPUESTA:

El Gobierno de España ha adoptado una postura firme y proactiva para garantizar la seguridad de las redes de telecomunicaciones 5G, en línea con la normativa europea. Esta postura se refleja en la aprobación del Real Decreto-ley 7/2022, de 29 de marzo, sobre los requisitos de seguridad de las redes 5G, así como en el Real Decreto 443/2024, de 30 de abril, que establece el Esquema Nacional de Seguridad para estas redes.

En este marco normativo, España ha habilitado mecanismos para identificar y controlar los riesgos asociados a los suministradores de tecnología 5G. En concreto, la ley permite declarar a determinados proveedores como "suministradores de alto riesgo", tomando en cuenta tanto factores técnicos como la posible exposición a injerencias externas. Esta declaración puede realizarse en cualquier momento, de forma preventiva, y conlleva la posibilidad de restringir o vetar su acceso a la red.

Además, cabe señalar que, en las zonas consideradas críticas por razones de seguridad nacional -determinadas por el Consejo de Seguridad Nacional el 19 de marzo de 2024- el Ministerio para la Transformación Digital y de la Función Pública podrá excluir la instalación de equipos 5G de cualquier proveedor, sin necesidad de que previamente haya sido declarado de alto riesgo. Esta medida se aplica caso por caso, con el fin de salvaguardar los intereses estratégicos de España.

Por otra parte, España ya está aplicando la normativa de la Unión Europea (UE) en materia de ciberseguridad de las redes de telecomunicaciones 5G, en especial a través de la plena implementación de la *Cybersecurity Toolbox 5G* aprobada por la Comisión Europea. Este marco incluye medidas estratégicas y técnicas destinadas a mitigar los riesgos para la seguridad de las redes 5G y posteriores.



En cumplimiento de esta normativa, España ha alcanzado los siguientes hitos clave en las siguientes materias:

- **Legislación específica:** La adopción del Real Decreto-ley 7/2022, conocida como la Ley de Ciberseguridad 5G, y el Real Decreto 443/2024, que establece el Esquema Nacional de Seguridad para estas redes, que transponen las disposiciones de la *toolbox* de la UE a la normativa española.
- **Clasificación de ubicaciones críticas:** el Consejo de Seguridad Nacional, el 19 de marzo de 2024, identificó las áreas y centros estratégicos donde la red de acceso radio 5G será considerada elemento crítico (así como el Core y los elementos de gestión, que lo son, en cualquier caso), reforzando así las medidas de control.
- **Control de proveedores:** la legislación establece la posibilidad de declarar como "suministradores de alto riesgo" a aquellos operadores que presenten un perfil de riesgo elevado, con base en la evaluación de factores técnicos y externos.
- **Diversificación de proveedores y análisis de riesgos:** las empresas operadoras deben presentar anualmente sus estrategias de diversificación, así como sus análisis de riesgos, que están sujetas a revisión por parte del Ministerio para la Transformación Digital y de la Función Pública. Este control permite evitar una dependencia excesiva de un solo proveedor y garantizar la resiliencia de la red.

Por lo tanto, España ya ha comenzado a aplicar de forma efectiva la normativa de la UE para controlar el acceso de empresas extranjeras a las redes de telecomunicaciones, especialmente a las 5G. La normativa actual no solo está en vigor, sino que se aplica mediante un enfoque preventivo, flexible y adaptado a las necesidades de seguridad nacional.

Asimismo, cabe destacar también que el Gobierno está trabajando en diferentes ámbitos como el refuerzo de capacidades y del marco legal mediante la transposición de la Directiva NIS 2 a través del anteproyecto de ley de Coordinación y Gobernanza de la Ciberseguridad, una iniciativa clave para reforzar la protección de redes y sistemas de información y que crea el Centro Nacional de Ciberseguridad.

Por último, cabe mencionar que la normativa actual en materia de prevención de conflictos de intereses garantiza la objetividad y la independencia de las actuaciones de los altos cargos, así como la transparencia de las mismas.





Madrid, 09 de abril de 2025