



EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs

Single Market Enforcement

Notification of Regulatory Barriers

Número de notificación : 2026/0346/ES (Spain)

Proyecto de Real Decreto sobre Seguridad y Resiliencia de las Redes y Servicios de Comunicaciones Electrónicas y determinadas Infraestructuras Digitales.

Fecha de recepción : 08/07/2026

Final del periodo de statu quo : 09/10/2026

Message

Mensaje 001

Comunicación de la Comisión - TRIS/(2026) 1822

Directiva (UE) 2015/1535

Notificación: 2026/0346/ES

Notificación de un proyecto de texto de un Estado miembro

Notification – Notifikation – Notifizierung – Нотификация – Oznámení – Notifikation – Γνωστοποίηση – Notificación – Teavitamine – Ilmoitus – Obavijest – Bejelentés – Notifica – Pranešimas – Paziņojums – Notifika – Kennisgeving – Zawiadomienie – Notificação – Notificare – Oznámenie – Obvestilo – Anmälan – Fógra a thabhairt

Does not open the delays - N'ouvre pas de délai - Kein Fristbeginn - Не се предвижда период на прекъсване - Nezahajuje prodlení - Fristerne indledes ikke - Καμμία έναρξη προθεσμίας - No abre el plazo - Viivituste perioodi ei avata - Määräaika ei ala tästä - Ne otvara razdoblje kašnjenja - Nem nyitja meg a késéset - Non fa decorrere la mora - Atidējimai nepradedami - Atlikšanas laikposms nesākas - Ma jiftaħ il-perijodi ta' dewmien - Geen termijnbegin - Nie otwiera opóźnień - Não inicia o prazo - Nu deschide perioadele de stagnare - Nezačína oneskorenia - Ne uvaja zamud - Inleder ingen frist - Ní osclaíonn sé na moilleanna

MSG: 20261822.ES

1. MSG 001 IND 2026 0346 ES ES 08-07-2026 ES NOTIF

2. Spain

3A. Subdirección General de Ordenación de las Telecomunicaciones.

Secretaría General de Telecomunicaciones, Infraestructuras Digitales y Seguridad Digital.

Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

Ministerio para la Transformación Digital y de la Función Pública

Calle Poeta Joan Maragall 41

28020 Madrid

+34 913462750

3B. Subdirección General de Ordenación de las Telecomunicaciones.

Secretaría General de Telecomunicaciones, Infraestructuras Digitales y Seguridad Digital.

Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

Ministerio para la Transformación Digital y de la Función Pública



EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Single Market Enforcement
Notification of Regulatory Barriers

Calle Poeta Joan Maragall 41
28020 Madrid
+34 913462750

4. 2026/0346/ES - V00T - Telecomunicaciones

5. Proyecto de Real Decreto sobre Seguridad y Resiliencia de las Redes y Servicios de Comunicaciones Electrónicas y determinadas Infraestructuras Digitales.

6. Tiene como objeto reforzar la seguridad, resiliencia y continuidad de las redes y servicios de comunicaciones electrónicas, sus recursos asociados y determinadas infraestructuras digitales en España.

7.

8. El RD busca garantizar la seguridad, resiliencia y continuidad de las redes y servicios de comunicaciones electrónicas, sus recursos asociados y determinadas infraestructuras digitales en España.

El objetivo es garantizar la prestación de servicios esenciales ante incidentes de seguridad, interrupciones del servicio o degradaciones significativas, así como regular las obligaciones de notificación de dichos incidentes a la Administración. Los sujetos obligados son los operadores de redes públicas de comunicaciones electrónicas, prestadores de servicios disponibles al público, gestores de recursos asociados e infraestructuras digitales como cables submarinos, sistemas satelitales, centros de procesamiento de datos (CPD), redes de distribución de contenidos (CDN) y puntos de intercambio de Internet (IXP), así como, en determinados aspectos, a los centros de recepción de emergencias 112 y sistemas de alertas públicas. Se reconoce además el carácter esencial de estas redes e infraestructuras en situaciones de emergencia.

Se establece la elaboración de un “Plan Nacional de Seguridad y Resiliencia”, que definirá la organización de la respuesta ante crisis y los mecanismos de coordinación institucional. También establece la obligación de los sujetos obligados de elaborar, un “Planes general” por sujeto obligado y “Planes específicos” por tipo de red y servicios concretos. Deberán incluir análisis de riesgos, identificación de infraestructuras esenciales, medidas preventivas, mecanismos de recuperación y protocolos de actuación ante distintos escenarios, como interrupciones eléctricas, fenómenos naturales, incendios, fallos informáticos o ciberataques.

Se introducen obligaciones específicas para garantizar la continuidad de los servicios de telecomunicaciones. Los operadores deberán adoptar medidas para minimizar el impacto de los incidentes y asegurar el funcionamiento de servicios esenciales, especialmente las comunicaciones de emergencia. En situaciones excepcionales podrán priorizar determinados tipos de tráfico, como las comunicaciones de emergencia o los servicios de voz y SMS, siempre respetando el principio de neutralidad tecnológica. Además, se fijan requisitos mínimos de autonomía energética para infraestructuras esenciales y se impone a las redes móviles la obligación de garantizar progresivamente una autonomía mínima de 4 horas para un porcentaje del 75% de la población en un plazo de tres años.

Incluye un sistema de notificación de incidentes significativos que no son considerados de ciberseguridad, estos últimos regulados en la Directiva NIS2 y Directiva CER. Los operadores comunicarán a la Secretaría de Estado cualquier incidente significativo en un plazo máximo de una hora desde que tengan conocimiento de ella, remitiendo posteriormente actualizaciones periódicas mientras dure la afectación un informe final una vez restablecido el servicio.

Se establecen medidas concretas para las comunicaciones de emergencia a través del número 112 y los sistemas de alertas públicas. Tanto los centros de recepción de emergencias como los operadores deberán implantar medidas de redundancia y continuidad, elaborar planes específicos de actuación y notificar de forma inmediata cualquier interrupción de estos servicios, considerados automáticamente incidentes significativos.

El Real Decreto completa medidas y mecanismos de coordinación con la normativa de ciberseguridad y resiliencia de entidades críticas (Directiva NIS2 y Directiva CER), la creación de una Mesa de Coordinación de Seguridad y Resiliencia y la futura implantación de plataformas telemáticas para la gestión y comunicación de incidentes. En conjunto, supone un importante refuerzo de las obligaciones de seguridad, continuidad y supervisión aplicables al sector de las telecomunicaciones y a las infraestructuras digitales críticas.



EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Single Market Enforcement
Notification of Regulatory Barriers

9. La creciente digitalización de la economía y de los servicios públicos ha incrementado notablemente la dependencia de las redes de comunicaciones electrónicas y de las infraestructuras digitales que las soportan. Esta situación ha puesto de relieve la existencia de vulnerabilidades y riesgos que no se limitan exclusivamente al ámbito de la ciberseguridad, sino que también afectan a la seguridad física y a la capacidad de las infraestructuras para resistir y recuperarse de acontecimientos adversos. En este contexto, la norma considera necesario reforzar la capacidad de prevención, respuesta y recuperación frente a incidentes que puedan comprometer la disponibilidad, integridad o funcionamiento de las redes y servicios de comunicaciones electrónicas.

La exposición de motivos del Real Decreto pone de manifiesto diversos acontecimientos recientes que han demostrado la necesidad de incrementar la resiliencia de estas infraestructuras. Entre ellos menciona fenómenos naturales como la erupción volcánica de La Palma en 2021 o la DANA que afectó a distintas zonas de España en 2024, así como incidentes de origen no natural, como el reciente apagón eléctrico que afectó al territorio nacional. Estos sucesos evidenciaron que tanto los fenómenos naturales extremos como las fallas técnicas o energéticas pueden provocar alteraciones significativas en las redes de comunicaciones y poner en riesgo la continuidad de servicios esenciales para la ciudadanía y las administraciones públicas.

Por otro lado, transformación digital está modificando profundamente la arquitectura y el funcionamiento de las redes de telecomunicaciones. La incorporación de tecnologías como el Internet de las Cosas (IoT), la Inteligencia Artificial (IA), el Big Data, la computación en la nube y la virtualización de servicios ha permitido mejorar la eficiencia, la conectividad y el desarrollo económico, pero al mismo tiempo ha incrementado la complejidad de los sistemas y ha generado nuevos riesgos operativos y de seguridad. Por ello, considera imprescindible que el marco regulatorio evolucione para anticiparse a estos riesgos y garantizar niveles adecuados de protección y resiliencia.

Desde el punto de vista jurídico, la iniciativa se fundamenta principalmente en el artículo 63 de la Ley 11/2022, General de Telecomunicaciones, relativo a la integridad y seguridad de las redes y servicios de comunicaciones electrónicas. Además, se apoya en la normativa ya existente en materia de seguridad de redes 5G, en particular el Real Decreto-ley 7/2022, el Real Decreto-ley 12/2018 sobre seguridad de las redes y sistemas de información y el Real Decreto 443/2024 por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G. Sin perjuicio de lo anterior, aunque estas normas han supuesto avances importantes, resulta necesario desarrollar un marco específico que aborde de forma integral la seguridad y resiliencia del conjunto de las redes y servicios de comunicaciones electrónicas y de determinadas infraestructuras digitales.

Finalmente, el texto explica que el nuevo Real Decreto pretende actuar de forma complementaria a la futura normativa española de ciberseguridad y resiliencia de entidades críticas. En consecuencia, las obligaciones derivadas de la normativa de transposición de NIS2 y CER seguirán siendo plenamente aplicables a los incidentes de ciberseguridad y a aquellos incidentes que afecten a redes, servicios e infraestructuras digitales y que no estén expresamente regulados en este Real Decreto. De este modo, se busca garantizar la coherencia entre los distintos instrumentos normativos, evitar solapamientos regulatorios y configurar un sistema integral de protección que refuerce la seguridad, continuidad y resiliencia de las telecomunicaciones y de las infraestructuras digitales esenciales para el funcionamiento de la sociedad y la economía españolas.

9a. La medida es idónea para alcanzar el objetivo perseguido de reforzar la seguridad, resiliencia y continuidad de las redes y servicios de comunicaciones electrónicas y de determinadas infraestructuras digitales.

La experiencia acumulada durante los últimos años ha puesto de manifiesto que las redes de telecomunicaciones constituyen infraestructuras esenciales para el funcionamiento de la sociedad, como quedó evidenciado durante la pandemia de COVID-19, así como en situaciones de emergencia derivadas de fenómenos naturales extremos, interrupciones del suministro eléctrico o incidentes de seguridad que han afectado a la disponibilidad de los servicios. En este escenario, la adopción de un marco normativo específico resulta adecuada para reforzar la capacidad de prevención, respuesta y recuperación frente a incidentes que puedan comprometer la continuidad de las comunicaciones electrónicas.

La norma desarrolla las previsiones contenidas en el artículo 63 de la Ley 11/2022, General de Telecomunicaciones. También complementa y adapta el marco regulatorio a la evolución tecnológica y a los nuevos riesgos asociados a la digitalización, la virtualización de redes, la computación en la nube, la inteligencia artificial o el IoT, cuya creciente implantación incrementa la exposición a vulnerabilidades tanto de naturaleza física como digital. En este sentido, el Real Decreto constituye el instrumento adecuado para concretar obligaciones sectoriales específicas que permitan abordar de forma integral las particularidades técnicas y operativas del sector de las telecomunicaciones.



EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Single Market Enforcement
Notification of Regulatory Barriers

La idoneidad de la medida se refleja especialmente en la incorporación de mecanismos preventivos y de planificación orientados a mejorar la preparación de los operadores ante situaciones de crisis. La obligación de elaborar “Planes generales” y “Planes específicos” por red o servicio, junto con la elaboración de un “Plan Nacional de Seguridad y Resiliencia” y de un “Plan Nacional Civil de Emergencias”, permite establecer procedimientos específicos de identificación de riesgos, prevención, respuesta y recuperación.

Igualmente, la actualización de los procedimientos de notificación de incidentes constituye una medida adecuada para mejorar la capacidad de supervisión y gestión de crisis por parte de las autoridades competentes. La experiencia acumulada ha puesto de manifiesto la necesidad de adaptar los criterios, plazos y contenidos de las notificaciones a una realidad tecnológica y operativa más compleja.

Asimismo, la medida resulta idónea para reforzar la protección de servicios especialmente sensibles, como las comunicaciones de emergencia a través del número 112 y los sistemas de alertas públicas, al imponer obligaciones específicas de continuidad, redundancia y notificación tanto a los operadores como a los centros de recepción de emergencias. Ello contribuye a garantizar el mantenimiento de estos servicios críticos incluso en escenarios de grave afectación de las infraestructuras de comunicaciones.

La creación de mecanismos de cooperación entre administraciones públicas, autoridades nacionales y europeas, así como la constitución de una mesa de coordinación permanente con participación de los distintos agentes implicados, constituye una herramienta adecuada para favorecer el intercambio de información, la coordinación institucional y la adopción de buenas prácticas en materia de seguridad y resiliencia.

Finalmente, la medida es coherente con el marco normativo europeo derivado de las Directivas NIS2 y CER, garantizando una adecuada coordinación con las futuras normas nacionales de transposición y evitando vacíos regulatorios en un sector estratégico para la economía y la seguridad nacional.

9b. La aprobación del Real Decreto responde a una necesidad real y acreditada de reforzar la capacidad de prevención, protección y recuperación de unas infraestructuras que se han convertido en esenciales para el funcionamiento de la sociedad, la economía y los servicios públicos.

La creciente digitalización de las actividades económicas y sociales, junto con la dependencia cada vez mayor de las redes y servicios de comunicaciones electrónicas, así como los acontecimientos como la erupción volcánica de La Palma, la DANA que afectó a distintas zonas del territorio nacional o el reciente apagón eléctrico han demostrado que las redes y servicios de comunicaciones electrónicas están expuestos a riesgos de naturaleza muy diversa que pueden comprometer gravemente la prestación de servicios esenciales para ciudadanos, empresas y administraciones públicas. Estos episodios han evidenciado la necesidad de fortalecer la resiliencia de las infraestructuras digitales y mejorar la capacidad de respuesta ante situaciones de emergencia y crisis.

Esta medida resulta necesaria para desarrollar y concretar el artículo 63 de la Ley 11/2022, General de Telecomunicaciones, que establece la obligación de los operadores de gestionar adecuadamente los riesgos de seguridad y garantizar la integridad de sus redes y servicios. Resulta imprescindible un desarrollo reglamentario que determine con mayor precisión las obligaciones de planificación, prevención, notificación de incidentes, coordinación institucional y supervisión que deben asumir los operadores y demás sujetos afectados.

Asimismo, la necesidad de la norma se justifica por la obsolescencia parcial del marco regulatorio actualmente vigente en materia de notificación de incidentes. Los procedimientos previstos ya no responden adecuadamente a la complejidad de los incidentes que pueden afectar hoy a las redes, servicios e infraestructuras digitales. La actualización de las tipologías de incidentes, de los procedimientos de comunicación y de los plazos de notificación resulta necesaria para que las autoridades competentes dispongan de información suficiente y actualizada que permita coordinar una respuesta rápida y eficaz ante situaciones de crisis.

También es necesario establecer mecanismos específicos para garantizar la continuidad de servicios especialmente críticos, como las comunicaciones de emergencia a través del número 112 y los sistemas de alertas públicas. La experiencia demuestra que cualquier interrupción de estos servicios puede tener consecuencias directas sobre la protección de la vida, la integridad física de las personas y la gestión de emergencias. Por ello, la norma impone obligaciones específicas de planificación, redundancia y continuidad operativa tanto a los operadores como a los centros de recepción de emergencias.

Por otra parte, la medida resulta necesaria para mejorar los mecanismos de cooperación nacional y europea, la creación de una mesa de coordinación específica que facilite el intercambio de información, compartir experiencias y establecer procedimientos comunes de actuación ante incidentes que, por su naturaleza, suelen afectar simultáneamente a



EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Single Market Enforcement
Notification of Regulatory Barriers

múltiples operadores e infraestructuras.

Finalmente, resulta necesario para garantizar la coherencia del ordenamiento jurídico español con el nuevo marco regulatorio europeo derivado de las Directivas NIS2 y CER. Estas normas europeas refuerzan las obligaciones de seguridad, gestión de riesgos y resiliencia de las infraestructuras críticas y exigen a los Estados miembros desarrollar mecanismos eficaces de prevención, detección, respuesta y recuperación frente a incidentes.

9c. La medida propuesta no supone una carga excesiva ni desproporcionada en relación con los objetivos perseguidos, ya que las obligaciones que introduce responden a la necesidad de garantizar la seguridad, resiliencia y continuidad de unas infraestructuras que tienen carácter esencial para el funcionamiento de la sociedad, la economía y los servicios públicos.

La proporcionalidad de la medida se manifiesta, en primer lugar, en que muchas de las obligaciones previstas ya forman parte de las prácticas habituales de gestión de riesgos y continuidad de negocio de los operadores de telecomunicaciones y de los gestores de infraestructuras digitales. La elaboración de análisis de riesgos, planes de contingencia, protocolos de recuperación o mecanismos de supervisión constituyen elementos habituales en la gestión de infraestructuras críticas y servicios esenciales. El Real Decreto no impone la creación de estructuras completamente nuevas, sino que sistematiza y homogeneiza determinadas obligaciones con el fin de garantizar unos estándares mínimos comunes para todos los sujetos obligados.

Asimismo, las medidas previstas resultan adecuadas a la magnitud de los riesgos que pretenden mitigar. Frente a estos riesgos, la exigencia de disponer de planes de seguridad y resiliencia, mecanismos de respaldo y procedimientos de notificación temprana constituye una respuesta razonable y necesaria para minimizar los daños y acelerar la recuperación de los servicios.

La norma también incorpora mecanismos que permiten adaptar las obligaciones a la realidad de cada sujeto obligado. Los planes específicos deben elaborarse teniendo en cuenta las características de cada red, servicio o infraestructura, permitiendo a los operadores determinar las medidas técnicas y organizativas más adecuadas en función de sus riesgos concretos. Esta flexibilidad evita imponer soluciones uniformes o rígidas que pudieran generar costes innecesarios y favorece un enfoque basado en la gestión efectiva del riesgo.

En materia de notificación de incidentes, estas obligaciones se justifican por la necesidad de disponer de información actualizada y fiable que permita coordinar la respuesta ante incidentes que pueden afectar a un gran número de usuarios, operadores o territorios. Además, la información requerida es aquella que los operadores ya deben recopilar y gestionar internamente para resolver las incidencias y garantizar la continuidad de sus servicios, por lo que no supone una carga administrativa desproporcionada respecto del beneficio que genera en términos de coordinación y capacidad de respuesta.

La Memoria de Análisis de Impacto Normativo concluye igualmente que el impacto económico derivado de la norma es asumible y proporcionado al interés general protegido. Aunque se estima un coste económico para los sujetos obligados de entre 45 y 90 M€, dicho coste se encuentra vinculado principalmente a inversiones destinadas a reforzar la resiliencia de las infraestructuras y garantizar la continuidad de servicios esenciales. Asimismo, las nuevas cargas administrativas se cuantifican en aproximadamente 19.276€ una cifra reducida en comparación con el volumen de actividad y la dimensión económica de los operadores afectados. Por otro lado, la norma no implica costes presupuestarios para las administraciones públicas ni genera impactos significativos sobre la competencia.

Por todo ello, puede concluirse que la medida no impone cargas excesivas a los sujetos obligados, sino que establece obligaciones proporcionadas, razonables y necesarias para garantizar un elevado nivel de seguridad y resiliencia de las redes y servicios de comunicaciones electrónicas.

10. Referencias de los textos de base:

11. No

12.

13. Sí

Strategic Interests of the Country

Las redes y servicios de comunicaciones electrónicas son infraestructuras esenciales para la seguridad nacional, los



EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs

Single Market Enforcement

Notification of Regulatory Barriers

servicios públicos, servicios de emergencia, la actividad económica, cohesión territorial.

14. No

15. Sí

16.

Aspecto TBT: No

Aspecto SPS: No

Comisión Europea

Punto de contacto Directiva (UE) 2015/1535

email: grow-dir2015-1535-central@ec.europa.eu