



EUROPEAN COMMISSION

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

Single Market Enforcement

Notification of Regulatory Barriers

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

Projeto de Decreto Real relativo à segurança e resiliência das redes e serviços de comunicações eletrónicas e determinadas infraestruturas digitais

Data de receção : 08/07/2026

Fim do período de statu quo : 09/10/2026

Message

Mensagem 001

Comunicação da Comissão - TRIS/(2026) 1822

Directiva (UE) 2015/1535

Notificação: 2026/0346/ES

Notificação de um projeto de texto de um Estado-Membro

Notification – Notificación – 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 - Καμία 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.PT

1. MSG 001 IND 2026 0346 ES PT 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 - Telecomunicações

5. Projeto de Decreto Real relativo à segurança e resiliência das redes e serviços de comunicações eletrónicas e determinadas infraestruturas digitais

6. Tem como objetivo reforçar a segurança, a resiliência e a continuidade das redes e serviços de comunicações eletrónicas, dos respetivos recursos conexos e de determinadas infraestruturas digitais na Espanha.

7.

8. O Decreto Real tem como objetivo garantir a segurança, a resiliência e a continuidade das redes e serviços de comunicações eletrónicas, dos respetivos recursos conexos e de determinadas infraestruturas digitais na Espanha. O objetivo consiste em assegurar a prestação de serviços essenciais em caso de incidentes de segurança, interrupções de serviço ou degradações significativas, bem como regular a obrigação de notificar tais incidentes às autoridades. As entidades obrigadas são os operadores de redes públicas de comunicações eletrónicas, os prestadores de serviços acessíveis ao público, os operadores de recursos conexos e infraestruturas digitais, tais como cabos submarinos, sistemas de satélite, centros de tratamento de dados (CPD), redes de distribuição de conteúdos (CDN) e pontos de troca de tráfego (PTT), bem como, em determinados aspetos, os centros de chamadas de emergência 112 e os sistemas de alerta público. O carácter essencial destas redes e infraestruturas em situações de emergência é igualmente reconhecido. Foi elaborado um «Plano Nacional de Segurança e Resiliência», que definirá a organização da resposta a situações de crise e os mecanismos de coordenação institucional. Estabelece ainda a obrigação de as entidades obrigadas elaborarem um «plano geral» por cada entidade obrigada e «planos específicos» por cada tipo de rede e serviço específico. Devem incluir análises de risco, a identificação das infraestruturas essenciais, medidas preventivas, mecanismos de recuperação e protocolos de ação para vários cenários, tais como cortes de energia, catástrofes naturais, incêndios, falhas informáticas ou ciberataques.

São introduzidas obrigações específicas para assegurar a continuidade dos serviços de telecomunicações. Os operadores devem tomar medidas para minimizar o impacto dos incidentes e assegurar o funcionamento dos serviços essenciais, nomeadamente das comunicações de emergência. Em circunstâncias excecionais, podem dar prioridade a determinados tipos de tráfego, tais como as comunicações de emergência ou os serviços de voz e SMS, respeitando sempre o princípio da neutralidade tecnológica. Além disso, são estabelecidos requisitos mínimos de autonomia energética para as infraestruturas essenciais e é imposta às redes móveis a obrigação de assegurar progressivamente um mínimo de quatro horas de energia de emergência para 75 % da população no prazo de três anos.

Inclui um sistema de notificação de incidentes significativos que não são considerados incidentes de cibersegurança, sendo estes últimos regulamentados pela Diretiva SRI 2 e pela Diretiva REC. Os operadores devem notificar a Secretaria de Estado de qualquer incidente significativo no prazo de uma hora após terem tomado conhecimento do mesmo e, posteriormente, devem fornecer atualizações regulares enquanto a interrupção se mantiver, seguidas de um relatório final assim que o serviço for restabelecido.

São estabelecidas medidas específicas para as comunicações de emergência através do número 112 e dos sistemas de alerta público. Tanto os centros de chamadas de emergência como os operadores devem pôr em prática medidas de redundância e de continuidade das atividades, elaborar planos de contingência específicos e notificar imediatamente qualquer perturbação destes serviços, que é automaticamente classificada como um incidente significativo.

O Decreto Real complementa as medidas e os mecanismos de coordenação com a legislação em matéria de cibersegurança e resiliência das entidades críticas (Diretiva SRI 2 e Diretiva REC), a criação de um Comité de Coordenação da Segurança e da Resiliência e a futura implantação de plataformas digitais para a gestão e notificação de incidentes. Em termos gerais, representa um reforço significativo das obrigações em matéria de segurança, continuidade e supervisão aplicáveis ao setor das telecomunicações e às infraestruturas digitais críticas.



EUROPEAN COMMISSION

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

9. A crescente digitalização da economia e dos serviços públicos aumentou significativamente a dependência das redes de comunicações eletrónicas e das infraestruturas digitais que as apoiam. Esta situação veio pôr em evidência a existência de vulnerabilidades e riscos que não se limitam exclusivamente ao domínio da cibersegurança, afetando igualmente a segurança física e a capacidade das infraestruturas para resistir a acontecimentos adversos e recuperar dos mesmos. Neste contexto, o ato regulamentar considera necessário reforçar a capacidade de prevenção, resposta e recuperação em caso de incidentes que possam comprometer a disponibilidade, a integridade ou o funcionamento das redes e serviços de comunicações eletrónicas.

A exposição de motivos do Decreto Real destaca uma série de acontecimentos recentes que demonstraram a necessidade de aumentar a resiliência destas infraestruturas. Entre estes, menciona fenómenos naturais como a erupção vulcânica em La Palma, em 2021, e a depressão isolada em níveis altos que afetou várias regiões da Espanha em 2024, bem como incidentes de origem não natural, tais como a recente falha de energia a nível nacional. Estes acontecimentos demonstraram que tanto os fenómenos naturais extremos como as falhas técnicas ou de energia podem causar perturbações significativas nas redes de comunicações e comprometer a continuidade dos serviços essenciais para o público e as autoridades públicas.

Além disso, a transformação digital está a alterar profundamente a arquitetura e o funcionamento das redes de telecomunicações. A integração de tecnologias como a Internet das Coisas (IdC), a Inteligência Artificial (IA), os megadados («Big Data»), a computação em nuvem e a virtualização de serviços permitiu melhorar a eficiência, a conectividade e o desenvolvimento económico, mas, ao mesmo tempo, aumentou a complexidade dos sistemas e gerou novos riscos operacionais e de segurança. Por conseguinte, considera-se essencial que o quadro regulamentar evolua por forma a antecipar estes riscos e a garantir níveis adequados de proteção e resiliência.

Do ponto de vista jurídico, a iniciativa baseia-se principalmente no artigo 63.º da Lei n.º 11/2022, a Lei Geral das Telecomunicações, no que diz respeito à integridade e segurança das redes e serviços de comunicações eletrónicas. Além disso, baseia-se na legislação em vigor em matéria de segurança das redes 5G, nomeadamente o Decreto-Lei Real n.º 7/2022, o Decreto-Lei Real n.º 12/2018 relativo à segurança das redes e sistemas de informação e o Decreto Real n.º 443/2024 que aprova o quadro nacional de segurança de redes e serviços 5G. Não obstante o que precede, embora estes atos regulamentares tenham conduzido a progressos significativos, é necessário desenvolver um quadro específico que aborde de forma abrangente a segurança e a resiliência de todas as redes e serviços de comunicações eletrónicas, bem como de determinadas infraestruturas digitais.

Por fim, o texto explica que o novo Decreto Real visa atuar de forma complementar à futura legislação espanhola em matéria de cibersegurança e resiliência das entidades críticas. Por conseguinte, as obrigações decorrentes dos atos regulamentares que transpõem a Diretiva SRI 2 e a Diretiva REC continuarão a ser plenamente aplicáveis aos incidentes de cibersegurança e aos incidentes que afetem redes, serviços e infraestruturas digitais e que não sejam expressamente regulados no presente Decreto Real. Deste modo, o objetivo consiste em assegurar a coerência entre os vários instrumentos regulamentares, evitar sobreposições regulamentares e estabelecer um sistema de proteção abrangente que reforce a segurança, a continuidade e a resiliência das telecomunicações e das infraestruturas digitais essenciais para o funcionamento da sociedade espanhola e da economia espanhola.

9-A. A medida é adequada para alcançar o objetivo pretendido de reforçar a segurança, a resiliência e a continuidade das redes e serviços de comunicações eletrónicas, bem como de determinadas infraestruturas digitais.

A experiência adquirida nos últimos anos demonstrou que as redes de telecomunicações são infraestruturas essenciais para o funcionamento da sociedade, tal como evidenciado durante a pandemia de COVID-19, bem como em situações de emergência decorrentes de fenómenos naturais extremos, cortes de energia ou incidentes de segurança que afetaram a disponibilidade dos serviços. Neste cenário, a adoção de um quadro regulamentar específico é adequada para reforçar a capacidade de prevenção, resposta e recuperação de incidentes que possam comprometer a continuidade das comunicações eletrónicas.

O ato regulamentar aplica as disposições constantes do artigo 63.º da Lei n.º 11/2022, a Lei Geral das Telecomunicações. Além disso, complementa o quadro regulamentar e adapta o mesmo aos avanços tecnológicos e aos novos riscos associados à digitalização, à virtualização de redes, à computação em nuvem, à inteligência artificial e à Internet das Coisas (IdC), cuja adoção crescente aumenta a exposição a vulnerabilidades tanto de carácter físico como digital. A este respeito, o Decreto Real é o instrumento adequado para especificar as obrigações setoriais que permitem uma abordagem global das especificidades técnicas e operacionais do setor das telecomunicações.

A adequação da medida reflete-se, em particular, na integração de mecanismos preventivos e de planeamento



EUROPEAN COMMISSION

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

destinados a melhorar a preparação dos operadores em situações de crise. A obrigação de elaborar «planos gerais» e «planos específicos» por rede ou serviço, juntamente com a elaboração de um «Plano Nacional de Segurança e Resiliência» e de um «Plano Nacional de Emergência Civil», permite estabelecer procedimentos específicos de identificação dos riscos, prevenção, resposta e recuperação.

Do mesmo modo, a atualização dos procedimentos de notificação de incidentes constitui uma medida adequada para melhorar a capacidade de monitorização e gestão de crises das autoridades competentes. A experiência tem demonstrado a necessidade de adaptar os critérios, os prazos e o conteúdo das notificações a uma realidade tecnológica e operacional mais complexa.

Além disso, a medida é adequada para reforçar a proteção de serviços particularmente sensíveis, como as comunicações de emergência através do número 112 e dos sistemas de alerta público, impondo obrigações específicas em matéria de continuidade, redundância e notificação tanto aos operadores como aos centros de chamadas de emergência. Tal contribui para garantir que estes serviços críticos sejam mantidos, mesmo em situações em que as infraestruturas de comunicações sejam gravemente afetadas.

O estabelecimento de mecanismos de cooperação entre as autoridades públicas e as autoridades nacionais e europeias, bem como a criação de um comité de coordenação permanente que envolva as várias partes interessadas, constituem um meio adequado para promover o intercâmbio de informações, a coordenação institucional e a adoção das melhores práticas no domínio da segurança e da resiliência.

Por último, a medida é coerente com o quadro regulamentar europeu decorrente da Diretiva SRI 2 e da Diretiva REC, assegurando uma coordenação adequada com a futura legislação nacional de transposição e evitando lacunas regulamentares num setor estratégico para a economia e a segurança nacional.

9-B. A adoção do Decreto Real dá resposta a uma necessidade real e comprovada de reforçar a capacidade de prevenção, proteção e recuperação das infraestruturas que se tornaram essenciais para o funcionamento da sociedade, da economia e dos serviços públicos.

A crescente digitalização das atividades económicas e sociais, aliada a uma dependência cada vez maior das redes e serviços de comunicações eletrónicas, bem como a acontecimentos como a erupção vulcânica em La Palma, a depressão isolada em níveis altos que afetou várias regiões do país ou a recente falha de energia, demonstraram que as redes e serviços de comunicações eletrónicas estão expostos a uma grande variedade de riscos que podem comprometer gravemente a prestação de serviços essenciais aos cidadãos, às empresas e às autoridades públicas. Estes incidentes vieram realçar a necessidade de reforçar a resiliência das infraestruturas digitais e de melhorar a capacidade de resposta a emergências e crises.

Esta medida é necessária para aplicar e dar execução ao artigo 63.º da Lei n.º 11/2022, a Lei Geral das Telecomunicações, que estabelece a obrigação dos operadores de gerir adequadamente os riscos de segurança e de assegurar a integridade das suas redes e serviços. É essencial elaborar atos regulamentares que definam de forma mais pormenorizada as obrigações em matéria de planeamento, prevenção, notificação de incidentes, coordenação institucional e supervisão que os operadores e outras partes envolvidas devem cumprir.

Do mesmo modo, a necessidade do ato regulamentar justifica-se pela obsolescência parcial do quadro regulamentar atualmente em vigor em matéria de notificação de incidentes. Os procedimentos existentes deixaram de responder adequadamente à complexidade dos incidentes que podem afetar atualmente redes, serviços e infraestruturas digitais. A atualização dos tipos de incidentes, dos procedimentos de comunicação e dos prazos de notificação é necessária para que as autoridades competentes disponham de informações suficientes e atualizadas, a fim de coordenarem uma resposta rápida e eficaz a situações de crise.

É igualmente necessário estabelecer mecanismos específicos para assegurar a continuidade de serviços particularmente críticos, tais como as comunicações de emergência através do número 112 e dos sistemas de alerta público. A experiência demonstra que qualquer interrupção destes serviços pode ter consequências diretas na proteção da vida, na integridade física das pessoas e na gestão de emergências. Por conseguinte, o ato regulamentar impõe obrigações específicas em matéria de planeamento, redundância e continuidade operacional tanto aos operadores como aos centros de chamadas de emergência.

Além disso, a medida é necessária para melhorar os mecanismos de cooperação nacional e europeia e para criar um comité de coordenação específico para facilitar o intercâmbio de informações, a partilha de experiências e o estabelecimento de procedimentos comuns de resposta a incidentes que, pela sua própria natureza, tendem a afetar simultaneamente vários operadores e infraestruturas.



EUROPEAN COMMISSION

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

Por último, é necessário assegurar a coerência do ordenamento jurídico espanhol com o novo quadro regulamentar europeu decorrente da Diretiva SRI 2 e da Diretiva REC. Estes instrumentos europeus reforçam as obrigações em matéria de segurança, gestão de riscos e resiliência das infraestruturas críticas, bem como exigem que os Estados-Membros desenvolvam mecanismos eficazes para a prevenção, deteção, resposta e recuperação em caso de incidentes.

9-C. A medida proposta não impõe um encargo excessivo ou desproporcionado em relação aos objetivos pretendidos, uma vez que as obrigações que introduz dão resposta à necessidade de garantir a segurança, a resiliência e a continuidade das infraestruturas essenciais para o funcionamento da sociedade, da economia e dos serviços públicos. A proporcionalidade da medida é evidente, em primeiro lugar, pelo facto de muitas das obrigações previstas já fazerem parte das práticas habituais de gestão de riscos e de continuidade das atividades dos operadores de telecomunicações e dos gestores de infraestruturas digitais. As análises de risco, os planos de contingência, os protocolos de recuperação e os mecanismos de supervisão são elementos normalizados na gestão das infraestruturas críticas e dos serviços essenciais. O Decreto Real não impõe a criação de estruturas completamente novas; pelo contrário, sistematiza e uniformiza determinadas obrigações, a fim de assegurar normas mínimas comuns a todas as entidades obrigadas. Além disso, as medidas previstas são adequadas à magnitude dos riscos que pretendem atenuar. Face a estes riscos, a exigência de dispor de planos de segurança e resiliência, mecanismos de apoio e procedimentos de notificação precoce constitui uma resposta razoável e necessária para minimizar os danos e acelerar a restauração dos serviços.

O ato regulamentar incorpora igualmente mecanismos que permitem adaptar as obrigações às circunstâncias de cada entidade obrigada. Os planos específicos devem ser elaborados tendo em conta as características de cada rede, serviço ou infraestrutura, permitindo que os operadores determinem as medidas técnicas e organizacionais mais adequadas em função dos seus riscos específicos. Esta flexibilidade evita a imposição de soluções uniformes ou rígidas suscetíveis de gerar custos desnecessários, bem como favorece uma abordagem baseada numa gestão eficaz dos riscos.

No que diz respeito à notificação de incidentes, as obrigações em causa justificam-se pela necessidade de dispor de informações atualizadas e fiáveis para coordenar a resposta a incidentes que possam afetar um grande número de utilizadores, operadores ou territórios. Além disso, as informações exigidas são aquelas que os operadores já são obrigados a recolher e gerir internamente, a fim de resolver incidentes e garantir a continuidade dos seus serviços; por conseguinte, não impõem encargos administrativos desproporcionados em relação aos benefícios que proporcionam em termos de coordenação e capacidade de resposta.

O Relatório de avaliação do impacto regulamentar conclui igualmente que o impacto económico resultante do ato regulamentar é exequível e proporcionado ao interesse público que protege. Embora o custo financeiro estimado para as entidades obrigadas se situe entre 45 milhões de EUR e 90 milhões de EUR, este custo está principalmente associado a investimentos destinados a reforçar a resiliência das infraestruturas e a assegurar a continuidade dos serviços essenciais. Os novos encargos administrativos são quantificados em cerca de 19 276 EUR, um valor baixo em comparação com o volume de atividade e a dimensão económica dos operadores em causa. Além disso, o ato regulamentar não implica quaisquer custos orçamentais para as autoridades públicas, nem tem qualquer impacto significativo na concorrência.

Por todos estes motivos, pode concluir-se que a medida não impõe encargos excessivos às entidades obrigadas; contudo, estabelece obrigações que são proporcionadas, razoáveis e necessárias para garantir um elevado nível de segurança e resiliência das redes e serviços de comunicações eletrónicas.

10. Referências aos textos de base:

11. Não

12.

13. Sim

Interesses Estratégicos do País

As redes e serviços de comunicações eletrónicas são infraestruturas essenciais para a segurança nacional, os serviços públicos, os serviços de emergência, a atividade económica e a coesão territorial.

14. Não



EUROPEAN COMMISSION

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

15. Sim

16.

Aspectos OTC: Não

Aspectos MSF: Não

Comissão Europeia

Contacto para obter informações de carácter general Directiva (UE) 2015/1535

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