



EUROPEAN COMMISSION

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

Single Market Enforcement

Notification of Regulatory Barriers

Kennisgevingsnumme : 2026/0346/ES (Spain)

Ontwerp van koninklijk besluit betreffende de veiligheid en veerkracht van elektronische communicatienetwerken en -diensten en bepaalde digitale infrastructuren.

Datum van ontvangst : 08/07/2026

Einde van de status-quoperiode : 09/10/2026

Message

Bericht 001

Mededeling van de Commissie - TRIS/(2026) 1822

Richtlijn (EU) 2015/1535

Kennisgeving: 2026/0346/ES

Kennisgeving van een ontwerptekst van een lidstaat

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.NL

1. MSG 001 IND 2026 0346 ES NL 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 - Telecommunicatie

5. Ontwerp van koninklijk besluit betreffende de veiligheid en veerkracht van elektronische communicatienetwerken en -diensten en bepaalde digitale infrastructuren.

6. Het heeft tot doel de veiligheid, veerkracht en continuïteit van elektronische communicatienetwerken en -diensten, bijbehorende faciliteiten en bepaalde digitale infrastructuren in Spanje te versterken.

7.

8. Het koninklijk besluit heeft tot doel de veiligheid, veerkracht en continuïteit van elektronische communicatienetwerken en -diensten, bijbehorende faciliteiten en bepaalde digitale infrastructuren in Spanje te waarborgen.

De doelstelling is enerzijds ervoor zorgen dat essentiële diensten in het geval van veiligheidsincidenten, dienstonderbrekingen of aanzienlijke storingen blijven functioneren en anderzijds de verplichtingen vastleggen met betrekking tot het melden van dergelijke incidenten aan de autoriteiten.

De verplichte entiteiten zijn exploitanten van openbare elektronische communicatienetwerken, aanbieders van openbaar beschikbare diensten, exploitanten van bijbehorende faciliteiten en digitale infrastructuren zoals onderzeese kabels, satellietssystemen, dataverwerkingscentra (DPC's), content delivery networks (CDN's) en internetknooppunten (IXP's), alsmede in bepaalde opzichten 112-noodoproepcentrales en openbare waarschuwingssystemen. Ook wordt erkend dat deze netwerken en infrastructuren van essentieel belang zijn in noodsituaties.

Er is een "Nationaal Veiligheids- en Veerkrachtplan" opgesteld waarin de organisatie van de crisisrespons en de institutionele coördinatiemechanismen worden vastgelegd. Het legt ook de verplichting vast voor verplichte entiteiten om een "algemeen plan" op te stellen voor elke verplichte partij en "specifieke plannen" voor elk type netwerk en specifieke diensten. Ze moeten bestaan uit risicoanalyses, de identificatie van essentiële infrastructuur, preventieve maatregelen, herstelmechanismen en actieprotocollen voor verschillende scenario's, zoals stroomuitval, natuurrampen, branden, IT-storingen of cyberaanvallen.

Er worden specifieke verplichtingen ingevoerd om de continuïteit van telecommunicatiediensten te waarborgen. Exploitanten moeten maatregelen treffen om de gevolgen van incidenten tot een minimum te beperken en om de werking van essentiële diensten, met name noodcommunicatie, te waarborgen. In uitzonderlijke omstandigheden kunnen zij voorrang geven aan bepaalde soorten verkeer, zoals noodcommunicatie of spraak- en sms-diensten, met inachtneming van het beginsel inzake technologische neutraliteit. Daarnaast worden minimale vereisten inzake energieautonomie vastgelegd voor essentiële infrastructuur en wordt aan mobiele netwerken een verplichting opgelegd om binnen drie jaar stapsgewijs te zorgen voor minimaal vier uur noodstroomvoorziening voor 75 % van de bevolking. Dit omvat een systeem voor het melden van ernstige incidenten die niet als cyberveiligheidsincidenten worden beschouwd; deze laatste worden geregeld in de NIS2-richtlijn en de CER-richtlijn. Nadat exploitanten kennis hebben genomen van een ernstig incident moeten zij dit binnen één uur melden aan het Staatssecretariaat en vervolgens gedurende de verstoring regelmatig updates verstrekken, gevolgd door een eindverslag zodra de dienstverlening is hersteld.

Er worden specifieke maatregelen vastgesteld voor noodcommunicatie via het nummer 112 en voor openbare waarschuwingssystemen. Zowel noodoproepcentrales als exploitanten moeten redundantie- en bedrijfscontinuïteitsmaatregelen treffen, specifieke noodplannen opstellen en onmiddellijk elke verstoring melden van deze diensten die automatisch worden aangemerkt als ernstige incidenten.

Het koninklijk besluit stelt maatregelen en mechanismen vast voor coördinatie met de regelgeving inzake cyberveiligheid en veerkracht voor kritieke entiteiten (de NIS2-richtlijn en de CER-richtlijn), de oprichting van een Veiligheids- en veerkrachtcoördinatiecomité en de toekomstige uitrol van digitale platforms voor incidentenbeheer en communicatie. In het algemeen vormt dit een aanzienlijke aanscherping van de veiligheids-, continuïteits- en toezichtverplichtingen die gelden voor de telecommunicatiesector en kritieke digitale infrastructuren.



EUROPEAN COMMISSION

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

9. De toenemende digitalisering van de economie en overheidsdiensten leidde tot een aanzienlijke toename van de afhankelijkheid van elektronische communicatienetwerken en de digitale infrastructuur die deze ondersteunen. Deze situatie heeft kwetsbaarheden en risico's aan het licht gebracht die niet enkel betrekking hebben op cyberveiligheid maar ook van invloed zijn op de fysieke veiligheid en het vermogen van infrastructuur om het hoofd te bieden aan ongunstige gebeurtenissen en hiervan te herstellen. In het kader hiervan acht de regelgeving het noodzakelijk om de capaciteit voor preventie, respons en herstel te versterken in het geval van incidenten die de beschikbaarheid, integriteit of werking van elektronische communicatienetwerken en -diensten in gevaar kunnen brengen.

In de toelichting bij het koninklijk besluit wordt gewezen op een aantal recente gebeurtenissen die hebben aangetoond dat het noodzakelijk is om de veerkracht van deze infrastructuur te vergroten. Daarbij wordt onder meer verwezen naar natuurrampen, zoals de vulkaanuitbarsting op La Palma in 2021 en het koude lagedruksysteem dat in 2024 verschillende delen van Spanje trof maar ook incidenten van niet-natuurlijke oorsprong, zoals de recente nationale stroomuitval. Uit deze gebeurtenissen is gebleken dat zowel extreme natuurverschijnselen als technische storingen of stroomuitval kunnen zorgen voor ernstige verstoringen van communicatienetwerken en de continuïteit van essentiële diensten voor het publiek en overheidsinstanties in gevaar kunnen brengen.

Bovendien zorgt de digitale transformatie voor ingrijpende veranderingen van de architectuur en werking van telecommunicatienetwerken. Door de integratie van technologieën zoals het internet der dingen (IoT), kunstmatige intelligentie (AI), big data, cloud computing en servicevirtualisatie is het mogelijk om de efficiëntie, connectiviteit en economische ontwikkeling te verbeteren maar tegelijkertijd is de complexiteit van de systemen toegenomen en zijn er nieuwe operationele en veiligheidsrisico's ontstaan. Het is dan ook essentieel dat het regelgevingskader wordt aangepast om in te spelen op deze risico's en te zorgen voor passende beschermings- en veerkrachtniveaus.

Vanuit wettelijk oogpunt is het initiatief voornamelijk gebaseerd op artikel 63 van wet 11/2022, de algemene telecommunicatiewet, inzake de integriteit en veiligheid van elektronische communicatienetwerken en -diensten.

Bovendien bouwt dit voort op bestaande wetgeving inzake de veiligheid van 5G-netwerken, met name koninklijk besluit-wet 7/2022, koninklijk besluit-wet 12/2018 inzake de veiligheid van netwerken en informatiesystemen en koninklijk besluit 443/2024 tot goedkeuring van het nationaal veiligheidskader voor 5G-netwerken en -diensten. Niettegenstaande het bovenstaande, hoewel deze regelgeving tot aanzienlijke vooruitgang heeft geleid, is het noodzakelijk om een specifiek kader te ontwikkelen dat volledig is gericht op de veiligheid en veerkracht van alle elektronische communicatienetwerken en -diensten, alsmede bepaalde digitale infrastructuur.

Tot slot wordt in de tekst uitgelegd dat het nieuwe koninklijk besluit bedoeld is als aanvulling op de toekomstige Spaanse wetgeving inzake cyberveiligheid en veerkracht van kritieke entiteiten. Bijgevolg blijven de verplichtingen die voortvloeien uit de regelgeving die NIS2 en CER omzet volledig van toepassing op cyberveiligheidsincidenten en incidenten die gevolgen hebben voor digitale netwerken, diensten en infrastructuur en die niet uitdrukkelijk in dit koninklijk besluit zijn geregeld. Het doel is dan ook om de samenhang tussen de verschillende regelgevingsinstrumenten te waarborgen, overlappingen in de regelgeving te voorkomen en een alomvattend beschermingssysteem op te zetten dat zorgt voor een betere veiligheid, continuïteit en veerkracht van de telecommunicatie- en digitale infrastructuur die essentieel is voor de werking van de Spaanse maatschappij en de Spaanse economie.

9a. De maatregel is geschikt voor het behalen van de beoogde doelstelling, namelijk het versterken van de veiligheid, veerkracht en continuïteit van elektronische communicatienetwerken en -diensten en van bepaalde digitale infrastructuur.

Uit de ervaring van de afgelopen jaren is gebleken dat telecommunicatienetwerken essentiële infrastructuur zijn voor de werking van de maatschappij, zoals is gebleken tijdens de COVID-19-pandemie maar ook in noodsituaties die het gevolg zijn van extreme natuurverschijnselen, stroomstoringen of veiligheidsincidenten die de beschikbaarheid van diensten beïnvloeden. In dit scenario is de goedkeuring van een specifiek regelgevingskader passend voor het versterken van de capaciteit om incidenten die de continuïteit van elektronische communicatie in gevaar kunnen brengen, te voorkomen, erop te reageren en ervan te herstellen.

De regelgeving legt de bepalingen ten uitvoer van artikel 63 van wet nr. 11/2022, de algemene telecommunicatiewet. Het vult het regelgevingskader ook aan en past dit aan aan technologische ontwikkelingen en de nieuwe risico's die gepaard gaan met digitalisering, netwerkvirtualisatie, cloud computing, kunstmatige intelligentie en het internet der dingen, waarvan het toenemende gebruik de blootstelling aan kwetsbaarheden van zowel fysieke als digitale aard vergroot. In dit opzicht is het koninklijk besluit het geschikte instrument voor het vastleggen van sectorale verplichtingen die een alomvattende benadering van de technische en operationele kenmerken van de telecommunicatiesector mogelijk



EUROPEAN COMMISSION

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

maken.

De geschiktheid van de maatregel wordt met name weerspiegeld in de integratie van preventie- en planningsmechanismen die zijn gericht op het verbeteren van de paraatheid van exploitanten in crisissituaties. De verplichting inzake het opstellen van “algemene plannen” en “specifieke plannen” per netwerk of dienst, samen met de opstelling van een “Nationaal Veiligheids- en Veerkrachtplan” en een “Nationaal Civiel Noodplan” maakt het mogelijk om specifieke procedures vast te stellen voor risico-identificatie, preventie, respons en herstel.

Ook vormt het bijwerken van procedures voor het melden van incidenten een geschikte maatregel om de monitoring- en crisisbeheercapaciteit van de bevoegde instanties te verbeteren. Uit ervaring blijkt de noodzaak om de criteria, termijnen en inhoud van kennisgevingen aan te passen aan een complexere technologische en operationele realiteit.

Bovendien is de maatregel bij uitstek geschikt voor het versterken van de bescherming van bijzonder gevoelige diensten, zoals noodcommunicatie via het nummer 112 en openbare waarschuwingssystemen, door specifieke verplichtingen inzake continuïteit, redundantie en kennisgeving op te leggen aan zowel exploitanten als noodoproepcentrales. Dit helpt ervoor te zorgen dat deze kritieke diensten behouden blijven, zelfs in situaties waarin de communicatie-infrastructuur ernstig is verstoord.

Het opzetten van samenwerkingsmechanismen tussen overheidsinstanties en nationale en Europese autoriteiten, evenals het oprichten van een permanent coördinatiecomité met de verschillende belanghebbenden, vormt een geschikt middel om de informatie-uitwisseling, institutionele coördinatie en de toepassing van beste praktijken op het gebied van veiligheid en veerkracht te bevorderen.

Tot slot sluit de maatregel aan bij het Europese regelgevingskader dat voortvloeit uit de NIS2- en CER-richtlijnen. Dit waarborgt een goede coördinatie met toekomstige nationale omzettingswetgeving en voorkomt regelgevingslacunes in een sector die van strategisch belang is voor de economie en nationale veiligheid.

9b. De goedkeuring van het koninklijk besluit beantwoordt aan een reële en bewezen behoefte om de preventie-, beschermings- en herstelcapaciteit te versterken van infrastructuren die essentieel zijn geworden voor de werking van de maatschappij, economie en openbare diensten.

De toenemende digitalisering van economische en maatschappelijke activiteiten, in combinatie met een groeiende afhankelijkheid van elektronische communicatienetwerken en -diensten, alsook gebeurtenissen zoals de vulkaanuitbarsting op La Palma, het koude lagedruksysteem dat verschillende delen van het land trof of de recente stroomstoring, hebben aangetoond dat elektronische communicatienetwerken en -diensten worden blootgesteld aan heel wat risico's die de verlening van essentiële diensten aan burgers, bedrijven en overheidsinstanties ernstig in gevaar kunnen brengen. Uit deze incidenten is gebleken dat de veerkracht van de digitale infrastructuur moet worden versterkt en dat het reactievermogen in noodsituaties en crises moet worden verbeterd.

Deze maatregel is noodzakelijk om artikel 63 van wet 11/2022, de algemene telecomunicatiewet, ten uitvoer te leggen en kracht bij te zetten; dit artikel legt aan exploitanten de verplichting op om veiligheidsrisico's op passende wijze te beheren en de integriteit van hun netwerken en diensten te waarborgen. Het is van essentieel belang om regelgeving op te stellen die een gedetailleerdere omschrijving bevat van de verplichtingen inzake planning, preventie, melding van incidenten, institutionele coördinatie en toezicht waaraan exploitanten en andere betrokken partijen moeten voldoen.

De behoefte aan de regelgeving wordt tevens gerechtvaardigd door de gedeeltelijke veroudering van het huidige regelgevingskader voor het melden van incidenten. De bestaande procedures beantwoorden niet langer op gepaste wijze aan de complexiteit van de incidenten die tegenwoordig digitale netwerken, diensten en infrastructuren kunnen treffen.

Het bijwerken van de soorten incidenten, communicatieprocedures en meldingstermijnen is noodzakelijk opdat de bevoegde instanties over voldoende en actuele informatie beschikken om een snelle en doeltreffende respons op crisissituaties te coördineren.

Bovendien is het nodig om specifieke mechanismen op te stellen om de continuïteit van bijzonder cruciale diensten te waarborgen, zoals noodcommunicatie via het nummer 112 en openbare waarschuwingssystemen. Uit ervaring blijkt dat elke onderbreking van deze diensten directe gevolgen kan hebben voor de bescherming van het leven en de lichamelijke integriteit van mensen, alsook voor het beheer van noodsituaties. Bijgevolg legt de regelgeving specifieke verplichtingen inzake planning, redundantie en operationele continuïteit op aan zowel exploitanten als noodoproepcentrales.

Bovendien is de maatregel noodzakelijk om de nationale en Europese samenwerkingsmechanismen te verbeteren en een speciaal coördinatiecomité op te richten dat de uitwisseling van informatie en ervaringen bevordert en gemeenschappelijke procedures vaststelt voor de respons op incidenten die door hun aard vaak meerdere exploitanten en infrastructuren tegelijk treffen.



EUROPEAN COMMISSION

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

Tot slot moet ervoor worden gezorgd dat het Spaanse rechtsstelsel in overeenstemming is met het nieuwe Europese regelgevingskader dat voortvloeit uit de NIS2- en CER-richtlijnen. Deze Europese instrumenten versterken de verplichtingen inzake veiligheid, risicobeheer en veerkracht van kritieke infrastructuur en verplichten de lidstaten om doeltreffende mechanismen te ontwikkelen voor de preventie en detectie van, de respons op en het herstel van incidenten.

9c. De voorgestelde maatregel legt geen buitensporige of onevenredige last op met betrekking tot de beoogde doelstellingen omdat de ingevoerde verplichtingen beantwoorden aan de noodzaak om de veiligheid, veerkracht en continuïteit te waarborgen van infrastructuren die essentieel zijn voor de werking van de maatschappij, economie en openbare diensten.

De maatregel is evenredig en dit blijkt in de eerste plaats uit het feit dat veel van de vastgelegde verplichtingen al deel uitmaken van de standaardpraktijken op het gebied van risicobeheer en bedrijfscontinuïteit bij telecommunicatie-exploitanten en beheerders van digitale infrastructuur. Risicoanalyses, noodplannen, herstelprotocollen en toezichtmechanismen zijn standaardelementen bij het beheer van kritieke infrastructuur en essentiële diensten. Het koninklijk besluit legt geen verplichting op inzake de creatie van volledig nieuwe structuren maar systematiseert en homogeniseert bepaalde verplichtingen om te zorgen voor gemeenschappelijke minimumnormen voor alle verplichte entiteiten.

Daarnaast zijn de beoogde maatregelen afgestemd op de omvang van de risico's die zij beogen te beperken. Gezien deze risico's is de verplichting om te beschikken over veiligheids- en veerkrachtplannen, back-upmechanismen en procedures voor vroegtijdige melding een redelijke en noodzakelijke respons om de schade tot een minimum te beperken en het herstel van de diensten te bespoedigen.

De regelgeving integreert ook mechanismen waarmee de verplichtingen kunnen worden afgestemd op de omstandigheden van elke gereguleerde entiteit. De specifieke plannen moeten worden opgesteld door rekening te houden met de kenmerken van elk netwerk, elke dienst of elke infrastructuur zodat exploitanten kunnen bepalen welke technische en organisatorische maatregelen het meest geschikt zijn op basis van hun specifieke risico's. Deze flexibiliteit voorkomt dat uniforme of rigide oplossingen worden opgelegd die onnodige kosten met zich mee kunnen brengen en bevordert een aanpak op basis van doeltreffend risicobeheer.

Wat de melding van incidenten betreft, worden deze verplichtingen gerechtvaardigd door de noodzaak om te beschikken over actuele en betrouwbare informatie voor het coördineren van de respons op incidenten die gevolgen kunnen hebben voor een groot aantal gebruikers, exploitanten of gebieden. Bovendien gaat het om informatie die exploitanten nu al verplicht moeten verzamelen en intern beheren om incidenten op te lossen en de continuïteit van hun diensten te waarborgen; er wordt dan ook geen onevenredige administratieve last opgelegd met betrekking tot de voordelen die dit oplevert op het gebied van coördinatie en reactievermogen.

In het verslag inzake de effectbeoordeling van de regelgeving wordt ook geconcludeerd dat de economische gevolgen van de regelgeving beheersbaar zijn en in verhouding staan tot het algemeen belang dat ermee wordt beschermd.

Hoewel de geraamde financiële kosten voor gereguleerde entiteiten tussen 45 miljoen EUR en 90 miljoen EUR liggen, hebben deze kosten voornamelijk betrekking op investeringen die zijn gericht op het versterken van de veerkracht van infrastructuur en het waarborgen van de continuïteit van essentiële diensten. Daarnaast worden de nieuwe administratieve lasten geraamd op ongeveer 19 276 EUR, een laag bedrag in vergelijking met het activiteitenvolume en de economische omvang van de betrokken exploitanten. Bovendien brengt de regelgeving geen begrotingskosten met zich mee voor overheidsinstanties en heeft geen noemenswaardige gevolgen voor concurrentie.

Om al deze redenen kan worden geconcludeerd dat de maatregel geen buitensporige lasten met zich meebrengt voor de partijen die eraan onderworpen zijn maar eerder verplichtingen bevat die evenredig, redelijk en noodzakelijk zijn om een hoog niveau van veiligheid en veerkracht van elektronische communicatienetwerken en -diensten te waarborgen.

10. Verwijzingen naar de basisteksten:

11. Nee

12.

13. Ja



EUROPEAN COMMISSION

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

Strategische belangen van het land

Elektronische communicatienetwerken en -diensten vormen een essentiële infrastructuur voor de nationale veiligheid, openbare diensten, nooddiensten, economische activiteit en territoriale cohesie.

14. Nee

15. Ja

16.

TBT-aspect: Nee

SPS-aspect: Nee

Europese Commissie

Contactpunt Richtlijn (EU) 2015/1535

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