



EUROPEAN COMMISSION

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

Single Market Enforcement

Notification of Regulatory Barriers

Anmälningsnummer : 2026/0346/ES (Spain)

Utkast till kungligt dekret om säkerhet och motståndskraft hos nät och tjänster för elektronisk kommunikation och viss digital infrastruktur.

Inkommet datum : 08/07/2026

Slut på frysning : 09/10/2026

Message

Meddelande 001

Meddelande från kommissionen - TRIS/(2026) 1822

Direktiv (EU) 2015/1535

Anmälan: 2026/0346/ES

Anmälan av ett utkast till text från en medlemsstat

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.SV

1. MSG 001 IND 2026 0346 ES SV 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
Calle Poeta Joan Maragall 41
28020 Madrid



EUROPEAN COMMISSION

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

+34 913462750

4. 2026/0346/ES - V00T - Telekommunikation

5. Utkast till kungligt dekret om säkerhet och motståndskraft hos nät och tjänster för elektronisk kommunikation och viss digital infrastruktur.

6. Syftet är att stärka säkerheten, motståndskraften och driftskontinuiteten hos nät och tjänster för elektronisk kommunikation, tillhörande anläggningar samt viss digital infrastruktur i Spanien.

7.

8. Syftet med det kungliga dekretet är att säkerställa säkerheten, motståndskraften och driftskontinuiteten hos nät och tjänster för elektronisk kommunikation, tillhörande anläggningar samt viss digital infrastruktur i Spanien.

Målet är att säkerställa tillhandahållandet av väsentliga tjänster i händelse av säkerhetsincidenter, driftstörningar eller väsentliga försämringar av tjänsterna, samt att reglera skyldigheterna att anmäla sådana incidenter till myndigheterna. De ansvariga enheterna är operatörer av allmänna elektroniska kommunikationsnät, leverantörer av allmänt tillgängliga tjänster, operatörer av tillhörande anläggningar och digital infrastruktur såsom undervattenskablar, satellitsystem, databehandlingscentraler, innehållsleveransnätverk och internetknutpunkter samt, i vissa avseenden, larmcentraler för larmnumret 112 och offentliga varningssystem. Nätverkens och infrastrukturens avgörande betydelse i nödsituationer lyfts också fram.

En "nationell plan för säkerhet och motståndskraft" har utarbetats för att fastställa hur krishantering och de institutionella samordningsmekanismerna ska organiseras. I dekretet fastställs även skyldigheten för ansvariga enheter att utarbeta en "allmän plan" för varje ansvarig part och "särskilda planer" för varje typ av nätverk och särskilda tjänster. De måste omfatta riskanalyser, identifiering av viktig infrastruktur, förebyggande åtgärder, återhämtningsmekanismer och åtgärdsprotokoll för olika scenarier, däribland strömbrott, naturkatastrofer, bränder, fel i it-systemen eller cyberattacker.

Särskilda skyldigheter införs för att säkerställa kontinuiteten i telekommunikationstjänsterna. Operatörerna ska vidta åtgärder för att minimera konsekvenserna av incidenter och säkerställa att samhällsviktiga tjänster fungerar, särskilt för nödkommunikation. Under exceptionella omständigheter får de prioritera vissa typer av trafik, till exempel nödkommunikation eller röst- och SMS-tjänster, men de måste alltid respektera principen om teknisk neutralitet.

Dessutom fastställs minimikrav på självförsörjning av energi för nödvändig infrastruktur, och en skyldighet införs för mobilnät att gradvis säkerställa minst fyra timmars reservkraft för 75 % av befolkningen inom tre år.

Detta omfattar ett system för rapportering av allvarliga händelser som inte betraktas som cybersäkerhetsincidenter, vilka regleras genom NIS2-direktivet och CER-direktivet. Operatörerna ska underrätta statssekretariatet om alla betydande incidenter inom en timme efter att ha fått kännedom om dem, för att därefter tillhandahålla regelbundna uppdateringar under den tid störningen varar och en slutrapport när tjänsten har återställts.

Särskilda åtgärder fastställs för nödkommunikation via larmnumret 112 och systemen för varning till allmänheten. Både larmcentraler och operatörer ska införa åtgärder för reservkapacitet och verksamhetskontinuitet, utarbeta specifika beredskapsplaner och omedelbart rapportera eventuella störningar i dessa tjänster, vilka automatiskt klassificeras som allvarliga incidenter.

I det kungliga dekretet fastställs åtgärder och mekanismer för samordningen med föreskrifterna om cybersäkerhet och motståndskraft för kritiska enheter (NIS2-direktivet och CER-direktivet), inrättandet av en samordningskommitté för säkerhet och motståndskraft samt den framtida utbyggnaden av digitala plattformar för incidenthantering och kommunikation. Sammantaget innebär detta en betydande utökning av de skyldigheter som gäller för säkerhet, kontinuitet och tillsyn inom telekommunikationssektorn och kritisk digital infrastruktur.

9. Den allt snabbare digitaliseringen av ekonomin och de offentliga tjänsterna har avsevärt ökat beroendet av elektroniska kommunikationsnät och den digitala infrastruktur som stöder dem. Denna situation har visat att det finns sårbarheter och risker som inte enbart är begränsade till cybersäkerhet, utan även påverkar den fysiska säkerheten och infrastrukturens förmåga att stå emot och återhämta sig efter allvarliga händelser. I detta sammanhang fastställs i



EUROPEAN COMMISSION

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

förordningen att det är nödvändigt att stärka kapaciteten för förebyggande åtgärder, insatser och återställning i händelse av incidenter som skulle kunna äventyra tillgängligheten, integriteten eller funktionen hos nät och tjänster för elektronisk kommunikation.

I motiveringen till det kungliga dekretet beskrivs ett antal händelser som inträffat på senare tid och som har visat på behovet av att stärka infrastrukturens motståndskraft. Bland dessa händelser anges naturfenom som vulkanutbrottet på La Palma 2021 och det lågtryckssystem som drabbade olika delar av Spanien 2024, liksom händelser av icke-naturligt ursprung, till exempel det landsomfattande strömavbrottet för en tid sedan. Dessa händelser visade att både extrema naturfenomen och tekniska fel eller strömavbrott kan orsaka betydande störningar i kommunikationsnäten och äventyra kontinuiteten i väsentliga tjänster för allmänheten och myndigheterna.

Den digitala omställningen förändrar dessutom telekommunikationsnätens utformning och funktion i grunden. Införandet av teknik som sakernas internet, artificiell intelligens (AI), stordata, molntjänster och virtualisering av tjänster har gjort det möjligt att förbättra effektiviteten, konnektiviteten och den ekonomiska utvecklingen, men har samtidigt ökat systemens komplexitet och skapat nya operativa och säkerhetsmässiga risker. Enligt dekretet är det därför av avgörande betydelse att utveckla regelverket för att förebygga dessa risker och säkerställa lämpliga nivåer av skydd och motståndskraft.

Ur rättslig synvinkel bygger initiativet främst på artikel 63 i lag 11/2022, den allmänna telekommunikationslagen, om integritet och säkerhet för elektroniska kommunikationsnät och kommunikationstjänster. Det bygger även på befintlig lagstiftning om säkerhet i 5G-nätet, särskilt kungligt lagdekret 7/2022, kungligt lagdekret 12/2018 om säkerhet i nät och informationssystem samt kungligt dekret 443/2024 om godkännande av den nationella säkerhetsramen för 5G-nät och 5G-tjänster. Även om dessa föreskrifter har lett till betydande framsteg är det nödvändigt att utarbeta ett särskilt regelverk som på ett heltäckande sätt garanterar säkerheten och motståndskraften hos alla elektroniska nät och tjänster för kommunikation, liksom hos viss digital infrastruktur.

Slutligen förklaras det i texten att det nya kungliga dekretet ska vara ett komplement till den framtida spanska lagstiftningen om cybersäkerhet och motståndskraft hos kritiska enheter. Följaktligen kommer de skyldigheter som följer av förordningarna om införlivande av NIS2- och CER-direktiven att fortsätta att gälla fullt ut för cybersäkerhetsincidenter och andra incidenter som påverkar digitala nätverk, tjänster och infrastruktur och som inte uttryckligen regleras i detta kungliga dekret. Syftet är således att säkerställa enhetligheten mellan de olika regleringsinstrumenten, att undvika överlappningar i regelverket och att inrätta ett heltäckande skyddssystem som ökar säkerheten, kontinuiteten och motståndskraften hos de telekommunikationsnät och den digitala infrastruktur som är avgörande för att det spanska samhället och den spanska ekonomin ska fungera.

9a. Åtgärden är lämplig för att uppnå det eftersträlvade målet att öka säkerheten, motståndskraften och kontinuiteten hos nät och tjänster för elektronisk kommunikation och viss digital infrastruktur.

De senaste årens erfarenheter har visat att telekommunikationsnät är en väsentlig infrastruktur för att samhället ska fungera, vilket blev särskilt tydligt under covid-19-pandemin och i samband med andra nödsituationer till följd av extrema naturkatastrofer, strömavbrott eller säkerhetsincidenter som påverkat tjänsternas tillgänglighet. I detta scenario är det lämpligt att anta ett särskilt regelverk för att stärka kapaciteten att förebygga, hantera och återuppta verksamheten efter incidenter som kan äventyra kontinuiteten i den elektroniska kommunikationen.

Genom förordningen genomförs bestämmelserna i artikel 63 i lag 11/2022, den allmänna telekommunikationslagen. Den innebär även att regelverket kompletteras och anpassas till den tekniska utvecklingen och de nya riskerna i samband med digitalisering, virtualisering av nätverk, molntjänster, artificiell intelligens och sakernas internet, vars alltmer utbredda användning ökar utsattheten för sårbarheter av både fysisk och digital karaktär. I detta avseende är det kungliga dekretet ett lämpligt instrument för att fastställa sektorsspecifika skyldigheter som möjliggör en helhetssyn på de tekniska och operativa särdragen inom telekommunikationssektorn.

Åtgärdens lämplighet återspeglas särskilt i införandet av förebyggande åtgärder och planeringsmekanismer som syftar till att förbättra operatörernas beredskap i krissituationer. Skyldigheten att utarbeta "allmänna planer" och "särskilda planer" för varje nätverk eller tjänst, i kombination med en "nationell plan för säkerhet och motståndskraft" och en "nationell civil beredskapsplan", gör det möjligt att fastställa specifika förfaranden för riskidentifiering, förebyggande åtgärder, insatser och återuppbyggnad.

På samma sätt är uppdateringen av förfarandena för incidentrapportering en lämplig åtgärd för att förbättra de behöriga myndigheternas förmåga till övervakning och krishantering. Erfarenheten har visat att kriterierna, tidsfristerna och innehållet i anmälningarna måste anpassas till en mer komplex teknisk och operativ verklighet.



EUROPEAN COMMISSION

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

Åtgärden är dessutom väl lämpad för att stärka skyddet av särskilt känsliga tjänster, däribland nödkommunikation via 112-numret och systemet för allmän varning, genom att ålägga både operatörer och larmcentraler särskilda skyldigheter avseende driftskontinuitet, reservkapacitet och anmälningar. Detta bidrar till att säkerställa att dessa kritiska tjänster upprätthålls även i situationer där kommunikationsinfrastrukturen har utsatts för allvarliga störningar.

Inrättandet av samarbetsmekanismer mellan offentliga myndigheter på nationell och europeisk nivå, liksom skapandet av en permanent samordningskommitté med de olika berörda parterna, är ett lämpligt sätt att främja informationsutbyte, institutionell samordning och tillämpning av bästa praxis inom området för säkerhet och motståndskraft.

Slutligen är åtgärden förenlig med det europeiska regelverk som följer av NIS2- och CER-direktiven, vilket säkerställer en lämplig samordning med framtida nationell lagstiftning om införlivande och förebygger luckor i lagstiftningen inom en sektor som är strategisk för ekonomin och den nationella säkerheten.

9b. Det kungliga dekretet antas som ett svar på ett reellt och påvisat behov av att stärka förmågan till förebyggande, skydd och återställande av en infrastruktur som har blivit avgörande för att samhället, ekonomin och de offentliga tjänsterna ska fungera.

Den ökande digitaliseringen av ekonomiska och sociala verksamheter och det växande beroendet av nätverk och tjänster för elektronisk kommunikation, i kombination med händelser som vulkanutbrottet på La Palma, det lågtryckssystem som påverkade olika delar av landet eller det senaste strömavbrottet, har visat att nätverk och tjänster för elektronisk kommunikation är utsatta för en rad olika risker som skulle kunna äventyra tillhandahållandet av samhällsviktiga tjänster för medborgare, företag och offentliga myndigheter. Dessa händelser har visat att det är nödvändigt att stärka den digitala infrastrukturens motståndskraft och förbättra förmågan att hantera nödsituationer och kriser.

Denna åtgärd är nödvändig för att genomföra och tillämpa artikel 63 i lag 11/2022, den allmänna telekommunikationslagen, vilken föreskriver att operatörerna är skyldiga att hantera säkerhetsrisker på ett lämpligt sätt och säkerställa integriteten hos sina nät och tjänster. Det är helt avgörande att utarbeta föreskrifter som mer ingående fastställer de skyldigheter avseende planering, förebyggande åtgärder, rapportering av incidenter, samordning mellan olika instanser och tillsyn som verksamhetsutövare och andra berörda parter måste uppfylla.

Behovet av nya föreskrifter motiveras även av att det gällande regelverket för rapportering av incidenter delvis är föråldrat. De nuvarande förfarandena är inte längre tillräckliga för att hantera de komplicerade incidenter som idag kan drabba digitala nätverk, tjänster och infrastrukturer. En uppdatering av typerna av incidenter, kommunikationsförfarandena och tidsfristerna för rapportering är nödvändig för att de behöriga myndigheterna ska ha tillräcklig och aktuell information så att de kan samordna snabba och effektiva insatser i krissituationer.

Det är även nödvändigt att inrätta särskilda mekanismer för att säkerställa kontinuiteten hos särskilt kritiska tjänster, däribland nödkommunikation via 112-numret och systemen för varning till allmänheten. Erfarenheten har visat att varje avbrott i dessa tjänster kan få direkta konsekvenser för skyddet av människors liv och hälsa och för krishanteringen. Följaktligen omfattar förordningen särskilda skyldigheter för både operatörer och larmcentraler i fråga om planering, reservkapacitet och driftskontinuitet.

Åtgärden är även nödvändig för att förbättra de nationella och europeiska samarbetsmekanismerna och för att inrätta en särskild samordningskommitté som ska underlätta utbytet av information och erfarenheter och fastställandet av gemensamma förfaranden för hantering av incidenter som, på grund av sin natur, ofta drabbar flera operatörer och infrastrukturer samtidigt.

Slutligen är det nödvändigt att säkerställa att det spanska rättssystemet är förenligt med det nya europeiska regelverk som härrör från NIS2- och CER-direktiven. Dessa europeiska rättsakter skärper kraven på säkerhet, riskhantering och motståndskraft när det gäller kritisk infrastruktur och ålägger medlemsstaterna att utarbeta effektiva mekanismer för att förebygga, upptäcka, reagera på och återhämta sig från incidenter.

9c. Den föreslagna åtgärden medför inte någon överdriven eller oproportionerlig börda i förhållande till de eftersträlvade målen, eftersom de skyldigheter som införs svarar mot behovet av att garantera säkerheten, motståndskraften och kontinuiteten hos infrastruktur som är avgörande för att samhället, ekonomin och de offentliga tjänsterna ska fungera. Åtgärdens proportionalitet framgår framför allt av det faktum att många av skyldigheterna redan ingår i de sedvanliga rutinerna för riskhantering och kontinuitetsplanering för telekomoperatörer och förvaltare av digital infrastruktur. Riskanalyser, beredskapsplaner, återhämtningsprotokoll och tillsynsmekanismer är vanliga inslag i förvaltningen av kritisk infrastruktur och samhällsviktiga tjänster. Det kungliga dekretet föreskriver inte att helt nya strukturer ska



EUROPEAN COMMISSION

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

inrättas, utan systematiserar och homogeniserar vissa skyldigheter för att säkerställa att minimistandarderna är gemensamma för alla ansvariga enheter.

De planerade åtgärderna står även i proportion till omfattningen av de risker som de är avsedda att minska. Mot bakgrund av dessa risker är kravet att införa säkerhets- och kontinuitetsplaner, reservlösningar och rutiner för tidig varning en rimlig och nödvändig åtgärd för att minimera skadorna och påskynda återställningen av tjänsterna. Förordningen omfattar även mekanismer som gör det möjligt att anpassa skyldigheterna efter de specifika omständigheter för varje reglerad enhet. De specifika planerna bör utarbetas med hänsyn till särdragen hos varje nätverk, tjänst eller infrastruktur, så att operatörerna kan fastställa de lämpligaste tekniska och organisatoriska åtgärderna utifrån sina specifika risker. Denna flexibilitet innebär att det går att undvika enhetliga eller rigida lösningar som skulle kunna medföra onödiga kostnader, för att i stället främja en strategi som bygger på effektiv riskhantering. Vad gäller rapporteringen av incidenter motiveras dessa skyldigheter av behovet av aktuell och tillförlitlig information för att kunna samordna insatserna vid incidenter som kan påverka ett stort antal användare, operatörer eller områden. Dessutom är operatörerna redan skyldiga att samla in de uppgifter som krävs och att hantera dem internt för att kunna lösa incidenter och säkerställa kontinuiteten i sina tjänster. Åtgärden medför därför inte någon oproportionerlig administrativ börda i förhållande till de fördelar den ger när det gäller samordning och insatsförmåga.

I rapporten om konsekvensbedömning av regelverket dras slutsatsen att de ekonomiska konsekvenserna av föreskrifterna är hanterbara och står i rimlig proportion till det allmänintresse som de ska skydda. Även om den beräknade kostnaden för reglerade enheter uppgår till mellan 45 miljoner och 90 miljoner euro är denna kostnad främst kopplad till investeringar som syftar till att stärka infrastrukturens motståndskraft och kontinuiteten i samhällsviktiga tjänster. De nya administrativa bördorna beräknas uppgå till omkring 19 276 euro, vilket är en låg siffra jämfört med de berörda aktörernas verksamhet och ekonomiska storlek. Dessutom medför förordningen inte några budgetkostnader för de offentliga myndigheterna, och den har inte heller någon betydande inverkan på konkurrensen.

Av alla dessa skäl kan slutsatsen dras att åtgärden inte medför någon orimlig börda för de parter som omfattas av den, utan snarare fastställer skyldigheter som är proportionerliga, rimliga och nödvändiga för att säkerställa en hög nivå av säkerhet och motståndskraft hos nätverk och tjänster för elektronisk kommunikation.

10. Hänvisning till grundtexter:

11. Nej

12.

13. Ja

Landets strategiska intressen

Nätverk och tjänster för elektronisk kommunikation utgör en nödvändig infrastruktur för nationell säkerhet, offentliga tjänster, räddningstjänster, ekonomisk verksamhet och territoriell sammanhållning.

14. Nej

15. Ja

16.

TBT-aspekt: Nej

SPS-aspekt: Nej

Europeiska kommissionen

Kontaktadress Direktiv (EU) 2015/1535

e-post: grow-dir2015-1535-central@ec.europa.eu