



EUROPEAN COMMISSION

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

Single Market Enforcement

Notification of Regulatory Barriers

Numero di notifica : 2026/0346/ES (Spain)

Progetto di regio decreto sulla sicurezza e la resilienza delle reti e dei servizi di comunicazione elettronica e di talune infrastrutture digitali.

Data di ricezione : 08/07/2026

Termine dello status quo : 09/10/2026

Message

Messaggio 001

Comunicazione della Commissione - TRIS/(2026) 1822

Direttiva (UE) 2015/1535

Notifica: 2026/0346/ES

Notifica di un progetto di testo da parte di uno Stato membro

Notification – Notification – 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.IT

1. MSG 001 IND 2026 0346 ES IT 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 - Telecomunicazioni

5. Progetto di regio decreto sulla sicurezza e la resilienza delle reti e dei servizi di comunicazione elettronica e di talune infrastrutture digitali.

6. Mira a rafforzare la sicurezza, la resilienza e la continuità delle reti e dei servizi di comunicazione elettronica, delle relative risorse e di talune infrastrutture digitali in Spagna.

7.

8. Il regio decreto mira a garantire la sicurezza, la resilienza e la continuità delle reti e dei servizi di comunicazione elettronica, delle relative risorse e di talune infrastrutture digitali in Spagna.

L'obiettivo è garantire la fornitura dei servizi essenziali in caso di incidenti di sicurezza, interruzioni del servizio o significativi cali di qualità, oltre a disciplinare gli obblighi di segnalazione alle autorità di incidenti di questo genere.

I soggetti obbligati sono gli operatori di reti pubbliche di comunicazioni elettroniche, i fornitori di servizi accessibili al pubblico, gli operatori di strutture associate e infrastrutture digitali quali cavi sottomarini, sistemi satellitari, centri di elaborazione dati (DPC), reti di distribuzione dei contenuti (CDN) e punti di interscambio Internet (IXP), nonché, sotto determinati aspetti, i centri di chiamata di emergenza 112 e i sistemi di allerta pubblica. Viene inoltre riconosciuta la natura essenziale di tali reti e infrastrutture in situazioni di emergenza.

È stato elaborato un «Piano di sicurezza e resilienza nazionale» che definirà l'organizzazione della risposta alle crisi e i meccanismi di coordinamento istituzionale. Esso stabilisce inoltre l'obbligo per i soggetti obbligati di elaborare un «piano generale» per ciascun soggetto obbligato e «piani specifici» per ciascun tipo di rete e di servizi specifici. Devono essere presenti analisi dei rischi, l'individuazione delle infrastrutture essenziali, misure preventive, meccanismi di ripristino e protocolli d'azione per vari scenari, quali interruzioni di corrente, catastrofi naturali, incendi, guasti informatici o attacchi informatici.

Sono introdotti obblighi specifici per garantire la continuità dei servizi di telecomunicazione. Gli operatori devono adottare misure volte a ridurre al minimo l'impatto degli incidenti e a garantire il funzionamento dei servizi essenziali, in particolare delle comunicazioni di emergenza. In circostanze eccezionali, possono dare priorità a determinati tipi di traffico, quali le comunicazioni di emergenza o i servizi vocali e SMS, nel rispetto costante del principio di neutralità tecnologica. Inoltre, sono stabiliti requisiti minimi di autonomia energetica per le infrastrutture essenziali e viene imposto alle reti mobili l'obbligo di assicurare progressivamente un minimo di quattro ore di alimentazione di riserva per una percentuale del 75 % della popolazione entro tre anni.

Prevede un sistema di segnalazione degli incidenti significativi che non sono considerati incidenti di sicurezza informatica, questi ultimi essendo disciplinati dalla direttiva NIS2 e dalla direttiva CER. Gli operatori sono tenuti a segnalare alla Segreteria di Stato qualsiasi incidente rilevante entro un'ora dal momento in cui ne vengono a conoscenza e a fornire successivamente aggiornamenti periodici per tutta la durata dell'interruzione, e successivamente a inviare una relazione finale una volta ripristinato il servizio.

Sono stabilite misure specifiche per le comunicazioni di emergenza attraverso il numero 112 e i sistemi di allerta pubblica. Sia i centri di chiamata di emergenza che gli operatori devono adottare misure di ridondanza e di continuità operativa, elaborare piani di emergenza specifici e segnalare immediatamente qualsiasi interruzione di tali servizi, classificate automaticamente come incidenti significativi.

Il regio decreto definisce le misure e i meccanismi di coordinamento con le normative in materia di sicurezza informatica e resilienza per gli enti critici (la direttiva NIS2 e la direttiva CER), l'istituzione di un comitato di coordinamento per la sicurezza e la resilienza e la futura implementazione di piattaforme digitali per la gestione degli incidenti e la comunicazione. Nel complesso, ciò rappresenta un significativo rafforzamento degli obblighi in materia di sicurezza, continuità e sorveglianza applicabili al settore delle telecomunicazioni e alle infrastrutture digitali critiche.

9. La crescente digitalizzazione dell'economia e dei servizi pubblici ha aumentato significativamente la dipendenza dalle reti di comunicazione elettronica e dalle infrastrutture digitali su cui si fondano. Questa situazione ha messo in luce



EUROPEAN COMMISSION

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

l'esistenza di vulnerabilità e rischi non limitati esclusivamente al settore della sicurezza informatica, ma che incidono anche sulla sicurezza fisica e sulla capacità delle infrastrutture di resistere agli eventi avversi e di ripristino. In tale contesto, il regolamento ritiene necessario rafforzare la capacità di prevenzione, risposta e ripristino in caso di incidenti che potrebbero compromettere la disponibilità, l'integrità o il funzionamento delle reti e dei servizi di comunicazione elettronica.

La relazione illustrativa del regio decreto evidenzia una serie di eventi recenti che hanno dimostrato la necessità di rafforzare la resilienza di tali infrastrutture. Tra questi, si citano fenomeni naturali quali l'eruzione vulcanica a La Palma nel 2021 e il sistema di bassa pressione fredda che ha colpito diverse zone della Spagna nel 2024, nonché eventi di origine non naturale, come la recente interruzione di corrente che ha interessato l'intero Paese. Questi eventi hanno dimostrato che sia i fenomeni naturali estremi sia i guasti tecnici o le interruzioni di corrente possono causare gravi malfunzionamenti delle reti di comunicazione e compromettere la continuità dei servizi essenziali per i cittadini e le autorità pubbliche.

Inoltre, la trasformazione digitale sta cambiando profondamente l'architettura e il funzionamento delle reti di telecomunicazioni. L'integrazione di tecnologie quali l'Internet delle cose (IoT), l'intelligenza artificiale (IA), i big data, il cloud computing e la virtualizzazione dei servizi ha consentito di migliorare l'efficienza, la connettività e lo sviluppo economico, ma allo stesso tempo ha accresciuto la complessità dei sistemi e ha generato nuovi rischi operativi e di sicurezza. Ritiene pertanto essenziale un'evoluzione del quadro normativo per anticipare tali rischi e garantire livelli adeguati di protezione e resilienza.

Dal punto di vista giuridico, l'iniziativa si basa principalmente sull'articolo 63 della Legge n. 11/2022, la Legge generale sulle telecomunicazioni, in materia di integrità e sicurezza delle reti e dei servizi di comunicazione elettronica. Si basa inoltre sulla legislazione vigente in materia di sicurezza delle reti 5G, in particolare il regio decreto-legge 7/2022, il regio decreto-legge 12/2018 sulla sicurezza delle reti e dei sistemi informativi e il regio decreto 443/2024 che approva il quadro di sicurezza nazionale per le reti e i servizi 5G. Fatto salvo quanto precede, sebbene tali normative abbiano portato a progressi significativi, è necessario sviluppare un quadro normativo specifico che affronti in modo esaustivo la sicurezza e la resilienza di tutte le reti e i servizi di comunicazione elettronica, nonché di talune infrastrutture digitali. Infine, il testo spiega che il nuovo regio decreto mira a integrare la futura legislazione spagnola in materia di sicurezza informatica e resilienza dei soggetti critici. Pertanto, gli obblighi derivanti dai regolamenti di recepimento della direttiva NIS2 e del regolamento CER continueranno ad essere pienamente applicabili agli incidenti di sicurezza informatica e a quegli incidenti che interessano le reti, i servizi e le infrastrutture digitali, e non sono espressamente disciplinati dal presente regio decreto. L'obiettivo è quindi garantire la coerenza tra i vari strumenti normativi, evitare sovrapposizioni normative e istituire un sistema di protezione globale che rafforzi la sicurezza, la continuità e la resilienza delle infrastrutture digitali e di telecomunicazione essenziali per il funzionamento della società e dell'economia spagnole.

9 bis. La misura è idonea a conseguire l'obiettivo perseguito di rafforzare la sicurezza, la resilienza e la continuità delle reti e dei servizi di comunicazione elettronica, nonché di talune infrastrutture digitali.

L'esperienza maturata negli ultimi anni ha dimostrato che le reti di telecomunicazioni sono infrastrutture essenziali per il funzionamento della società, come è emerso chiaramente durante la pandemia di COVID-19, nonché in situazioni di emergenza causate da eventi naturali estremi, interruzioni di corrente o incidenti di sicurezza che hanno compromesso la disponibilità dei servizi. In questo scenario, l'adozione di un quadro normativo specifico è appropriata per rafforzare la capacità di prevenzione, risposta e ripristino in caso di incidenti che possono compromettere la continuità delle comunicazioni elettroniche.

La normativa in questione attua le disposizioni contenute nell'articolo 63 della legge generale 11/2022, la legge generale sulle telecomunicazioni. Inoltre, integra il quadro normativo e lo adegua agli sviluppi tecnologici e ai nuovi rischi associati alla digitalizzazione, alla virtualizzazione delle reti, al cloud computing, all'intelligenza artificiale e all'Internet delle cose (IoT), la cui crescente diffusione aumenta l'esposizione a vulnerabilità sia di natura fisica che digitale. A tale riguardo, il regio decreto è lo strumento appropriato per specificare obblighi settoriali che consentono un approccio complessivo alle particolarità tecniche e operative del settore delle telecomunicazioni.

L'adeguatezza della misura si riflette in particolare nell'integrazione di meccanismi di prevenzione e pianificazione volti a migliorare la preparazione degli operatori in situazioni di crisi. L'obbligo di elaborare «Piani generali» e «Piani specifici» per ciascuna rete o servizio, unitamente all'elaborazione di un «Piano nazionale di sicurezza e resilienza» e di un «Piano nazionale di emergenza civile», consente di definire procedure specifiche per l'identificazione dei rischi, la prevenzione, la risposta e il ripristino.



EUROPEAN COMMISSION

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

Allo stesso modo, l'aggiornamento delle procedure di segnalazione degli incidenti costituisce una misura adeguata per migliorare la capacità di monitoraggio e di gestione delle crisi delle autorità competenti. L'esperienza ha dimostrato la necessità di adattare i criteri, le scadenze e il contenuto delle notifiche a una realtà tecnologica e operativa più complessa.

Inoltre, la misura è particolarmente indicata per rafforzare la protezione di servizi particolarmente sensibili, quali le comunicazioni di emergenza tramite il numero 112 e i sistemi di allerta pubblica, imponendo obblighi specifici in materia di continuità, ridondanza e notifica sia agli operatori che ai centri di chiamata di emergenza. Ciò contribuisce a garantire che questi servizi essenziali continuino a funzionare anche in situazioni in cui le infrastrutture di comunicazione subiscano gravi interruzioni.

L'istituzione di meccanismi di cooperazione tra le autorità pubbliche e le autorità nazionali ed europee, così come la creazione di un comitato di coordinamento permanente che coinvolga le varie parti interessate, è uno strumento adeguato per promuovere lo scambio di informazioni, il coordinamento istituzionale e l'adozione delle migliori pratiche nel settore della sicurezza e della resilienza.

Infine, la misura è coerente con il quadro normativo europeo derivante dalle direttive NIS2 e CER, garantendo un adeguato coordinamento con la futura normativa nazionale di recepimento e prevenendo lacune normative in un settore strategico per l'economia e la sicurezza nazionale.

9 ter. L'adozione del regio decreto risponde a una necessità reale e comprovata di rafforzare la capacità di prevenzione, protezione e recupero delle infrastrutture che sono diventate essenziali per il funzionamento della società, dell'economia e dei servizi pubblici.

La crescente digitalizzazione delle attività economiche e sociali, unita alla crescente dipendenza dalle reti e dai servizi di comunicazione elettronica, nonché eventi quali l'eruzione vulcanica a La Palma, il sistema di bassa pressione fredda che ha colpito varie parti del Paese o la recente interruzione di corrente, hanno dimostrato che le reti e i servizi di comunicazione elettronica sono esposti a un'ampia gamma di rischi che potrebbero compromettere gravemente la fornitura di servizi essenziali ai cittadini, alle imprese e alle autorità pubbliche. Questi incidenti hanno evidenziato la necessità di rafforzare la resilienza delle infrastrutture digitali e di migliorare la capacità di risposta alle emergenze e alle crisi.

Questa misura è necessaria per attuare l'articolo 63 della legge 11/2022, la legge generale sulle telecomunicazioni, che stabilisce l'obbligo per gli operatori di gestire adeguatamente i rischi per la sicurezza e di garantire l'integrità delle loro reti e dei loro servizi. È essenziale elaborare regolamentazioni che stabiliscano in modo più dettagliato gli obblighi in materia di pianificazione, prevenzione, segnalazione degli incidenti, coordinamento istituzionale e supervisione che gli operatori e le altre parti interessate devono rispettare.

Analogamente, l'esigenza di questa normativa è giustificata dall'obsolescenza parziale del quadro normativo attualmente in vigore per la segnalazione degli incidenti. Le attuali procedure non rispondono più adeguatamente alla complessità degli incidenti che oggi possono interessare le reti, i servizi e le infrastrutture digitali. L'aggiornamento delle tipologie di incidenti, delle procedure di comunicazione e dei termini di segnalazione è necessario affinché le autorità competenti dispongano di informazioni sufficienti e aggiornate per coordinare una risposta rapida ed efficace alle situazioni di crisi. È inoltre necessario stabilire meccanismi specifici per garantire la continuità dei servizi particolarmente critici, come le comunicazioni di emergenza attraverso il numero 112 e i sistemi di allerta pubblica. L'esperienza dimostra che qualsiasi interruzione di questi servizi può avere conseguenze dirette sui rischi per la vita e l'integrità fisica delle persone e sulla gestione delle emergenze. Di conseguenza, la normativa impone obblighi specifici in materia di pianificazione, ridondanza e continuità operativa sia per gli operatori che per i centri di chiamate di emergenza.

Inoltre, tale misura è necessaria per migliorare i meccanismi di cooperazione a livello nazionale ed europeo e per istituire un comitato di coordinamento dedicato, al fine di agevolare lo scambio di informazioni, la condivisione di esperienze e la definizione di procedure comuni per la gestione degli incidenti che, per loro stessa natura, tendono a coinvolgere contemporaneamente più operatori e infrastrutture.

Infine, è necessario garantire la coerenza del sistema giuridico spagnolo con il nuovo quadro normativo europeo derivato dalle direttive NIS2 e CER. Questi strumenti europei rafforzano gli obblighi in materia di sicurezza, gestione dei rischi e resilienza delle infrastrutture critiche e impongono agli Stati membri di mettere a punto meccanismi efficaci per la prevenzione, l'individuazione, la risposta e il ripristino a seguito di incidenti.

9 quater. La misura proposta non impone un onere eccessivo o sproporzionato rispetto agli obiettivi perseguiti, in quanto



EUROPEAN COMMISSION

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

gli obblighi che introduce rispondono alla necessità di garantire la sicurezza, la resilienza e la continuità delle infrastrutture essenziali per il funzionamento della società, dell'economia e dei servizi pubblici.

La proporzionalità della misura è evidente, in primo luogo, nel fatto che molti degli obblighi previsti sono già previsti da pratiche standard di gestione del rischio e di continuità operativa adottate dagli operatori delle telecomunicazioni e dai gestori delle infrastrutture digitali. Le analisi dei rischi, i piani di emergenza, i protocolli di ripristino e i meccanismi di sorveglianza sono elementi standard nella gestione delle infrastrutture critiche e dei servizi essenziali. Il regio decreto non impone la creazione di strutture completamente nuove, ma sistematizza e uniforma determinati obblighi al fine di garantire standard minimi comuni a tutti i soggetti obbligati.

Inoltre, le misure previste sono adeguate all'entità dei rischi che intendono attenuare. Di fronte a tali rischi, l'obbligo di disporre di piani di sicurezza e resilienza, meccanismi di backup e procedure di notifica tempestiva costituisce una risposta ragionevole e necessaria per ridurre al minimo i danni e accelerare il ripristino dei servizi.

La normativa prevede inoltre meccanismi che consentono di adattare gli obblighi alle circostanze specifiche di ciascun soggetto regolamentato. I piani specifici dovrebbero essere elaborati tenendo conto delle caratteristiche di ciascuna rete, servizio o infrastruttura, consentendo agli operatori di individuare le misure tecniche e organizzative più adeguate in funzione dei rischi specifici a cui sono esposti. Questa flessibilità evita di imporre soluzioni indifferenziate o rigide, che potrebbero generare costi inutili, e favorisce un approccio basato su un'efficace gestione dei rischi.

Per quanto riguarda la segnalazione degli incidenti, tali obblighi sono giustificati dalla necessità di disporre di informazioni aggiornate e affidabili per coordinare la risposta agli incidenti che possono riguardare un gran numero di utenti, operatori o territori. Inoltre, le informazioni richieste sono quelle che gli operatori sono già tenuti a raccogliere e gestire internamente al fine di risolvere gli incidenti e garantire la continuità dei loro servizi; pertanto, esse non impongono un onere amministrativo sproporzionato rispetto ai benefici che apportano in termini di coordinamento e reattività.

Anche la relazione sulla valutazione dell'impatto normativo giunge alla conclusione che l'impatto economico derivante dal regolamento è gestibile e proporzionato all'interesse pubblico che tutela. Sebbene il costo finanziario stimato per i soggetti regolamentati sia compreso tra i 45 e i 90 milioni di euro, esso è legato principalmente agli investimenti volti a rafforzare la resilienza delle infrastrutture e a garantire la continuità dei servizi essenziali. Inoltre, i nuovi oneri amministrativi sono quantificati in circa 19 276 EUR, un valore basso rispetto al volume di attività e alle dimensioni economiche degli operatori interessati. Inoltre, il regolamento non comporta costi di bilancio per le autorità pubbliche, e non ha un impatto significativo sulla concorrenza.

Per tutti questi motivi, si può concludere che la misura non impone oneri eccessivi alle parti soggette ad essa, ma stabilisce piuttosto obblighi proporzionati, ragionevoli e necessari per garantire un elevato livello di sicurezza e resilienza delle reti e dei servizi di comunicazione elettronica.

10. Riferimenti ai testi di base:

11. No

12.

13. Sì

Interessi strategici del paese

Le reti e i servizi di comunicazione elettronica costituiscono un'infrastruttura essenziale per la sicurezza nazionale, i servizi pubblici, i servizi di emergenza, l'attività economica e la coesione territoriale.

14. No

15. Sì

16.

Aspetto OTC: No

Aspetto SPS: No



EUROPEAN COMMISSION

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

Single Market Enforcement

Notification of Regulatory Barriers

Commissione europea

Punto di contatto Direttiva (UE) 2015/1535

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