



MINISTRY FOR DIGITAL
TRANSFORMATION AND THE
CIVIL SERVICE

SECRETARY OF STATE FOR TELECOMMUNICATIONS AND DIGITAL
INFRASTRUCTURE

General Secretariat for Telecommunications, Digital Infrastructure and
Digital Security

**REPORT ON THE REGULATORY IMPACT ASSESSMENT OF
THE DRAFT ROYAL DECREE ON THE SECURITY AND
RESILIENCE OF ELECTRONIC COMMUNICATIONS
NETWORKS AND SERVICES AND CERTAIN DIGITAL
INFRASTRUCTURES**



EXECUTIVE SUMMARY

Ministry	Ministry for Digital Transformation and the Civil Service	Date	05/05/2026
Proposing body	Secretary of State for Telecommunications and Digital Infrastructure		
Title of the regulation	DRAFT ROYAL DECREE ON THE SECURITY AND RESILIENCE OF ELECTRONIC COMMUNICATIONS NETWORKS AND SERVICES AND CERTAIN DIGITAL INFRASTRUCTURES		
Type of report	Normal ☒ Abbreviated ☐		
TIMELINESS OF THE PROPOSAL			
Subject	The purpose of this Royal Decree is to establish a national legal framework to ensure the security and resilience of electronic communications networks and services, their associated resources, and certain digital infrastructures against security incidents that could cause service interruption or a significant degradation in the quality of service, in accordance with Article 63 of Law 11/2022 of 28 June on General Telecommunications and Royal Decree-Law 12/2018 of 7 September on the security of networks and information systems, or any legislation replacing them. To this end, the regulation specifies the obliged entities and the requirements regarding risk management and the reporting of significant incidents. It also imposes on these obliged entities and on the centres receiving emergency calls via the 112 emergency number and public warning service the obligation to ensure security and to adopt the necessary measures to enable the routing of emergency communications and public warnings. Finally, the framework for supervision, inspection and sanctions is established, in line with national and European legislation on the coordination and governance of cybersecurity and on the resilience of critical infrastructure operators.		



Objectives pursued	The aim of this regulation is to safeguard the integrity and security of electronic communications networks and services, in order to ensure an adequate level of security and to prevent or minimise the impact of security incidents on users and on the continuity of electronic communications services.
Main alternatives considered	During the drafting of this Royal Decree, various regulatory options were analysed in accordance with the principles of necessity, proportionality, efficiency and legal certainty. As a result of this assessment, it has been concluded that the adoption of a Royal Decree constitutes the most appropriate legal instrument for implementing Article 63 of Law 11/2022 of 28 June, in coordination with Royal Decree–Law 12/2018 of 7 September. This option makes it possible to establish clear, proportionate and balanced obligations, in line with the practical experience of operators, whilst ensuring institutional coordination and providing for effective supervision and sanctioning mechanisms. This is also articulated in a manner consistent with the provisions of Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (hereinafter the NIS2 Directive), as well as Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities (hereinafter the CER Directive). These directives strengthen the obligations imposed on operators and organisations to prevent, detect, respond to and recover from certain security incidents that may compromise the availability and reliability of digital infrastructures and electronic communications networks and services, avoiding regulatory overlaps and strengthening legal certainty.
CONTENT AND LEGAL ANALYSIS	
Type of regulation	Royal Decree.
Structure of the regulation	The draft comprises an explanatory section and a substantive section, divided into seven chapters, containing 37 articles, five additional provisions, a single repealing provision and three final provisions.



Reports to be collected	• Report of the National Commission on Markets and Competition, in accordance with Article 5(2)(a) of Law 3/2013 of 4 June establishing the National Commission on Markets and Competition. • Report of the Technical General Secretariat of the Ministry of Digital Transformation and the Civil Service, in accordance with the provisions of Article 26(5), fourth paragraph, of Law 50/1997 of 27 November on the Government. • Reports from the Ministry of the Interior, Ministry of Defence, Ministry of Finance, Ministry of Territorial Policy and Democratic Memory, and the National Security Department of the Presidency of the Government, in accordance with the first paragraph of Article 26(5) of Law 50/1997 of 27 November on the Government. • Report of the Ministry of Territorial Policy and Democratic Memory in accordance with Article 26(5), sixth subparagraph, of Law 50/1997 of 27 November on the Government. • Report of the Office of Coordination and Regulatory Quality of the Ministry of the Presidency, Justice and Relations with the Courts in accordance with the provisions of Article 26(9) of Law 50/1997 of 27 November on the Government. • Opinion of the Council of State, in accordance with the provisions of Articles 19(1) and 22(3) of Organic Law 3/1980 of 22 April on the Council of State.
Prior public consultation	On 19 September 2025, the public consultation provided for in Article 133(1) of Law 39/2015 of 1 October on the Common Administrative Procedure of the Public Administrations took place.
Public hearing and information	In accordance with the provisions of Article 26(6) of Law 50/1997 of 27 November on the Government, the initial public consultation and hearing procedure was carried out. The deadline for submissions was 16 January 2026.



IMPACT ANALYSIS		
Compliance with the distribution of powers	This Royal Decree is issued pursuant to the State's exclusive competence in the field of telecommunications, as recognised in Article 149(1)(21) of the Spanish Constitution, which confers upon the State the power to regulate the framework and general coordination of economic activity, as well as exclusive competence in the field of telecommunications.	
Economic and Budgetary Impact	Economic impact for the obliged parties	☐ Entails a reduction in economic costs for the obliged parties ☒ Entails an economic cost for the obliged parties. Estimated cost: between €45 million and €90 million ☐ Does not affect administrative burdens
	With respect to administrative burdens	☐ Entails a reduction in administrative burdens. Estimated cost € _____ ☒ Incorporates new administrative burdens. Estimated cost: EUR 19,276
	With regard to budgets, the regulation	☐ Affects the budgets of the General State Administration ☐ Affects the budgets of other Regional Administrations ☒ Does not entail an expenditure ☐ Entails a revenue



Gender impact	The regulation has the following gender impact:	Negative ☐ None ☒ Positive ☐
Impact on Competition		☒ The regulation has no significant impact on competition. ☐ The regulation has positive effects on competition. ☐ The regulation has negative effects on competition.
Impact on data protection	The effects are set out in the report	No impact on data protection
Other impacts considered	- Impact on childhood and adolescence: negative - Impact on the family: negative - Impact on equal opportunities, non-discrimination and universal accessibility for persons with disabilities: negative - Environmental and climate change impact: the non-significant environmental impact caused by the installation of batteries is justified by the objective of ensuring the security and resilience of electronic communications networks and services. - Impact on health: negative.	
Other considerations	Data Protection Impact Assessment	



CONTENTS OF THE REPORT

I.- TIMELINESS OF THE PROPOSAL

1. Rationale
2. Objectives.
3. Compliance with the principles of good regulation
4. Alternatives.
5. Inclusion in the Annual Regulatory Plan and Ex-Post Evaluation.

II.- CONTENT AND LEGAL ANALYSIS

1. Content.
2. Legal analysis

III.- DESCRIPTION OF THE PROCEDURE

1. Description of the procedures carried out.
2. Pending procedures.

IV.- ADAPTATION OF THE REGULATION TO THE DISTRIBUTION OF POWERS

V.- IMPACT ANALYSIS

1. Economic impact
2. Budgetary impact
3. Impact on the single market
4. Analysis of administrative burdens
5. Gender impact
6. Impact on childhood and adolescence
7. Impact on family
8. Impact on the environment and as a result of climate change
9. Impact on equal opportunities, non-discrimination and universal accessibility for persons with disabilities
10. Impact on health
11. Impact on data protection

I.- TIMELINESS OF THE PROPOSAL



I.1.- RATIONALE

The COVID-19 pandemic powerfully demonstrated the essential role played by electronic communications networks and services. Millions of people relied on them to continue their work activities, access health services and maintain their social relationships, among many other activities, during a period of lockdowns and restrictions.

In societies and economies that are becoming increasingly technology-driven and reliant on the growing and intensive use of electronic communications networks and services, this dependence has highlighted a number of critical vulnerabilities relating to the security and integrity of electronic communications networks and services and digital infrastructures. This has created an urgent need to strengthen and enhance the security and resilience of electronic communications networks and services, their associated resources and certain digital infrastructures against potential future incidents, not only in terms of cybersecurity but also in the physical environment. Accordingly, in recent years there have been a series of incidents that have tested the security and resilience of electronic communications networks and services, some of a natural origin, such as the volcanic eruption on the island of La Palma on 19 September 2021, or the Isolated Upper-Level Low-Pressure System (DANA), which hit the Iberian Peninsula and the Balearic Islands, with the greatest intensity on the Mediterranean coast last October 2024, and others of non-natural origin, such as the recent nationwide power outage suffered by Spain.

The digital transformation driven by technological advances in the digitisation and virtualisation of services through the Internet of Things (IoT), Artificial Intelligence (AI), Big Data, and Cloud Computing has radically transformed traditional telecommunications networks and electronic communications services. While these developments offer significant opportunities in terms of efficiency, connectivity, and economic and social development, they also introduce significant risks and vulnerabilities to digital infrastructures, for which regulation must anticipate and be prepared.

The integrity and security of electronic communications networks and services are set out in Article 63 of Law 11/2022 of 28 June, the General Telecommunications Law (hereinafter, the "General Telecommunications Act"). This article is supplemented by regulations on the security of fifth-generation electronic communications networks and services, set out in Royal Decree-Law 7/2022 of 29 March on requirements to ensure the security of fifth-generation electronic communications networks and services, Royal Decree-Law 12/2018 of 7 September on the security of networks and information systems, and Royal Decree 443/2024 of 30 April, approving the National Security Framework for 5G networks and services.

At European level, the integrity and security of digital infrastructure—including electronic communications networks and services—have also been regulated by Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (hereinafter the NIS2 Directive), as well as by Directive (EU) 2022/2557 of 14 December on the resilience of critical entities (hereinafter the CER Directive). These directives strengthen the obligations imposed on operators



and organisations to prevent, detect, respond to and recover from certain security incidents that may compromise the availability and reliability of digital infrastructures and electronic communications networks and services.

The NIS2 Directive establishes new regulations to ensure a high, common level of cybersecurity across the European Union. In line with and in coordination with the forthcoming legislation on cybersecurity and critical infrastructures transposing the NIS2 and CER Directives, it is considered necessary to adopt a Royal Decree establishing, for the electronic communications networks and services sector and certain digital infrastructures, specific security and resilience obligations in coordination with and consistent with the legislation on cybersecurity and critical infrastructure, in accordance with Royal Decree-Law 12/2018 of 7 September and Article 63 of Law 11/2022 of 29 June.

To ensure that this Royal Decree is consistent and coherent with the national and European legislation in force as well as with the regulatory texts that modify them or derive from the transposition of the existing preliminary draft regulations in relation to the NIS2 Directives and the CER Directive, the obligations contained in the aforementioned Directives shall apply, in any case, to cybersecurity incidents and to those incidents that occur in the sector of networks, electronic communications services and digital infrastructures that are not provided for in this Royal Decree.

I.2. OBJECTIVES

The purpose of this Royal Decree is to establish a national regulatory framework to ensure the security and resilience of networks, electronic communications services, their associated resources and certain digital infrastructures against significant security incidents that may affect those networks or infrastructures, or cause a substantial degradation in the quality of the services provided. To this end, the regulation incorporates specific obligations regarding security and resilience applicable to the sector of networks, electronic communications services, their associated resources, and certain digital infrastructures, thereby implementing the provisions of Article 63 of Law 11/2022 of 28 June, the General Telecommunications Act, and Royal Decree-Law 12/2018 of 7 September, whilst being structured in a manner that is consistent and coordinated with the provisions set out in the NIS2 and CER Directives.

Article 63 of Law 11/2022 of 28 June establishes the need to ensure the integrity and security of electronic communications networks and services. Paragraph 1 stipulates that operators of public electronic communications networks and publicly available electronic communications services must manage security risks that may affect their networks and services, in order to ensure an adequate level of security and to prevent or minimise the impact of security incidents on users. To this end, they must adopt the appropriate technical and organisational measures they deem necessary. Paragraph 2, in turn, also includes the obligation of operators to ensure the integrity of telecommunications networks in order to safeguard the continuity of electronic communications services.



In line with the above, Chapter I of this Royal Decree defines its purpose and identifies the entities subject to the obligations laid down therein. Chapter 2, in turn, sets out the various plans that obliged entities must prepare—namely, a general operator-level plan and specific plans for particular services and categories of incidents—in order to ensure the security and resilience of networks, electronic communications services, associated resources and certain digital infrastructures.

Article 63(3) of the General Telecommunications Act requires operators providing public networks or electronic communications services available to the public to notify the current Ministry for Digital Transformation and the Civil Service of any security incidents that have had a significant impact on the provision of those networks or services. In this regard, Articles 20 to 23 of Order IET/1090/2014 of 16 June, regulating the conditions relating to service quality in the provision of electronic communications services (hereinafter the "Quality Order"), had already set out the criteria for determining what should be classified as a significant incident, whilst also establishing the notification obligations, and their deadlines, in relation to such incidents. However, technological developments, climate change and certain circumstances that have arisen in recent years have demonstrated that this Quality Order, has become obsolete in this area. It is therefore now appropriate to update the categories of incidents that must be taken into account in order to ensure the detection of risks and to plan appropriate response measures for events that test the integrity and security of electronic communications networks and services.

The Quality Order also sets out the deadlines and notification procedures for each type of incident. For the same reason mentioned above, it is considered that these deadlines and procedures should be updated and adapted to the new reality. Thus, on the one hand, the availability and handling—by both operators and the competent public bodies—of reliable and as up-to-date information as possible; and, on the other hand, an appropriate response to the management of the consequences arising from each incident, enabling the rapid restoration of the functionality of electronic communications networks, the continuity of service provision and the operational readiness of digital infrastructure, are not separate issues, but are clearly intertwined. They must therefore be addressed through a clear strengthening of time limits and the handling of structured and more detailed information whenever an incident occurs that affects network security or the normal functioning of electronic communications services, in order to facilitate the rapid recovery of networks, associated resources and services. Accordingly, Chapter III of this Royal Decree therefore sets out the new time limits and procedures for reporting security incidents affecting networks, electronic communications services, their associated resources, and certain digital infrastructures.

Similarly, paragraph 3 of the aforementioned Article 63 provides for the need to establish a mechanism for cooperation and information-sharing between the Ministry for Digital Transformation and the Civil Service and other competent national authorities in other Member States, as well as with the European Network and Information Security Agency (ENISA). It also provides that the Ministry may inform the public or require operators to do so, if it considers that disclosure of the



security incident is in the public interest. In accordance with this legal provision, Articles 24, 25 and 26 of Chapter VI of this Royal Decree set out the mechanisms for cooperation between the Ministry for Digital Transformation and the Civil Service and the competent national and European authorities in matters relating to security.

With a view to strengthening cooperation and coordination among all stakeholders and promoting the essential public-private collaboration in the planning, risk identification and joint management of incidents affecting an area of common interest, namely the security and resilience of electronic communications networks and services, the second additional provision establishes a coordination committee involving a wide range of stakeholders, to serve as a forum for dialogue, for sharing experiences and needs, and for establishing protocols and best practices in the event of future incidents such as those that have occurred in recent years, affecting the security of electronic communications networks and services and certain digital infrastructures.

Article 63(4) provides for a mechanism for informing users in the event of a security incident affecting the electronic communications services provided. This provision is further developed and specified in Article 15 of this Royal Decree. In particular, it establishes the obligation for obliged entities to ensure that natural and legal persons who are recipients of electronic communications services are properly informed, through customer service channels and support services, of any interruption affecting those services when they make contact as a result of an incident affecting the provision of electronic communications services, as well as of the measures or solutions adopted to resolve the incident promptly.

Article 63(5) sets out the inspection procedure and sanctioning regime, as well as the possibility to adopt additional measures to those identified in relation to the integrity and security of electronic communications networks and services. This section is set out in Chapter VII of this Royal Decree, as well as in Article 13, which empowers the Secretary of State for Telecommunications and Digital Infrastructures to issue recommendations, guidance or operational advice to obliged entities on the implementation of possible mitigating measures in relation to the contingency measures adopted during notified incidents or to reduce the risk of such incidents recurring.

For its part, the obligation set out in the General Telecommunications Act to provide the information necessary to assess the security and integrity of their services and networks—including documents on security policies—and the obligation to undergo a security audit carried out by an independent body, at the obliged entity's own expense, and to make the results available to the Ministry for Digital Transformation and the Civil Service, are provided for in Article 23 of this Royal Decree.

Chapter IV sets out the obligations of centres receiving emergency calls via the 112 emergency number and public warning systems to ensure safety and to take measures to enable the routing of emergency calls and public warnings. To this end, they may implement such technical measures, specific plans, strategies, redundancies or alternative service arrangements as they consider appropriate,



either through the operator providing the emergency call routing service itself or through one or more other service providers, in accordance with Article 63(6).

Chapter V of this Royal Decree regulates and implements the measures adopted in Article 4(6) of Law 11/2022 of 28 June in relation to the assumption by the General State Administration of the direct management of certain publicly available electronic communications services, to ensure public security and national security or the fulfilment of public service obligations in accordance with Article 63(7).

Article 63(8) concerning the protection of personal data and the safeguarding of digital rights, and its implementing regulations, are set out in Chapter VI, Articles 27 and 28 of this Royal Decree.

I.3. COMPLIANCE WITH THE PRINCIPLES OF GOOD REGULATION.

This Royal Decree has been drafted and processed according to the principles for good regulation set out in Article 129 of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations.

a) Principle of necessity.

It is considered necessary to adopt a series of measures to strengthen the security and resilience of telecommunications networks, electronic communications services, their associated resources, and certain digital infrastructures, thereby implementing the provisions of Article 63 of Law 11/2022 of 28 June on General Telecommunications and Royal Decree-Law 12/2018 of 7 September on the security of networks and information systems. These measures must be implemented in a coherent and coordinated manner in line with the provisions of the NIS2 Directive and the CER Directive, ensuring effective regulatory integration that is aligned with the European objectives regarding cybersecurity and the protection of critical infrastructure.

The aforementioned Directives set out obligations relating to cybersecurity and resilience from a cross-cutting, multi-sectoral perspective, which makes it difficult to address in sufficient depth the technical, operational and strategic specificities of the networks sector, electronic communications services, their associated resources and certain digital infrastructures. Consequently, it is considered necessary to introduce national legislation which, in full accordance with the aforementioned regulations, will enable a comprehensive approach to the security and resilience of these strategic sectors, taking into account their specific characteristics and strengthening their capacity to respond to security incidents.

In this regard, the Royal Decree recognises electronic communications networks, electronic communications services, their associated facilities, and certain digital infrastructures as “essential” services and infrastructure in emergency situations. It also provides for the development of a National Security and Resilience Plan for these types of networks and services. This plan will develop and coordinate a response and recovery plan for security incidents, setting out the objectives and measures for managing each type of incident. Furthermore, it includes the



obligation for obliged entities to have a General Action Plan for each obliged entity and a Specific Plan for each network, service, associated resource or infrastructure, which sets out the measures adopted for the prevention, detection, and response to security incidents and risks, prepared by each obliged entity in the event of a significant incident, with the aim of restoring services as soon as possible. Finally, the plan includes the development of a National Civil Emergency Plan with the aim of devising a strategy to mobilise resources and assets relating to networks, electronic communications services and digital infrastructures, thereby helping to restore normal conditions as quickly as possible.

Furthermore, it is considered necessary to update and regulate in detail the “content and deadlines for notifications” that obliged entities must submit to the Secretary of State for Telecommunications and Digital Infrastructure when a significant incident occurs that affects the integrity of networks, certain digital infrastructures and/or the continuity of telecommunications services.

Similarly, it is considered necessary to include the “obligation of centres receiving emergency communications via the 112 number and public warnings” to adopt the technical measures they deem necessary to enable the correct routing of emergency communications and public warnings. To this end, they shall adopt the technical measures they deem appropriate, including specific plans, strategies, redundancies and alternative service arrangements, either through the operator providing the routing service or through one or more other service providers. The measures adopted must be communicated to the Secretary of State for Telecommunications and Digital Infrastructure within a maximum period of 6 months from the entry into force of this Royal Decree. Similarly, it is considered necessary to establish a mechanism for notifying the Secretary of State for Telecommunications and Digital Infrastructure in the event of an interruption to the emergency communications service, so that both emergency services and policy-makers have, from the very outset, clear, reliable and as accurate as possible information on the status of telecommunications networks, the provision of electronic communications services, their associated resources and certain digital infrastructures, so that they may adopt, as quickly as possible, the decisions that are necessary at any given time.

Similarly, it is considered necessary to establish an “implementation and coordination procedure” with other national authorities, the Autonomous Communities and the relevant European bodies, as well as an “inspection and penalty regime” in the event of non-compliance with the obligations set out in this Royal Decree, in a manner that is coordinated and consistent with national legislation on cybersecurity and the security of critical infrastructure, and with the NIS2 Directive and the CER Directive, which establish a cross-cutting and multi-sectoral approach to obligations regarding cybersecurity and resilience.

As regards coordination and cooperation, it is considered necessary to set up a “coordination committee” involving a plurality of agents to serve as a forum for dialogue, for sharing experiences and needs, and for establishing protocols and best practices in the event of future incidents such as those that have occurred in recent years affecting the security of electronic communications networks and services and certain digital infrastructures.



Finally, it includes the possibility of modifying the contracts signed between operators that provide public networks or publicly available electronic communications services and the owners or operators of their associated resources and electronic communications networks that provide wholesale services, and certain digital infrastructures in order to comply with the obligations established in this Royal Decree, whose competence is attributed to the National Commission on Markets and Competition in order to resolve possible conflicts that may arise in relation to technical, economic and/or operational terms. In particular, any conflicts that may arise in relation to the allocation of costs arising from compliance with the obligations set out in Article 7(4) concerning electricity supply infrastructure, designed to guarantee the operational readiness and continuity of electronic communications services. The appropriate measures will be established to ensure that this allocation of costs is fair, reasonable, and proportionate.

It also incorporates the possibility for the National Commission on Markets and Competition to modify, if necessary, within one year from the moment the regulated operator informs the aforementioned committee of the need to modify and adapt ex ante regulation in order to comply with the obligations contained in this Royal Decree.

B) Principle of proportionality.

The obligations set out in this Royal Decree are considered proportionate and balanced, as they do not place an excessive burden on the parties subject to them, either from an economic or an administrative point of view.

The obligation to draw up a “General Plan for each obliged entity” and “Specific Plans” is nothing new for obliged entities. The requirement for these plans is in line with the previous experience of operators who have already been drawing up similar plans in the ordinary course of their duties, which demonstrates that they can count on the work already carried out and possess the technical and organisational capacity to fulfil this obligation.

Under the “Specific Plans”, it is stipulated that, in the event of a power supply interruption at facilities deemed essential due to their importance and impact on maintaining the service’s operability and functioning, the obliged parties must ensure that such facilities remain operational for at least 24 hours; essential intermediate-level installations or infrastructures for at least 12 hours; and all other installations and infrastructures must guarantee their operability for at least 4 hours. In the specific case of the access network of a mobile communications network through which publicly available electronic communications services are provided in harmonised European bands, this access network must be designed and equipped with its own generating equipment and electrical supply elements to ensure its operability and continuity of service as the ultimate objective for at least 4 hours for at least 75% of the population in Spain.

This ultimate objective must be achieved within three years of the entry into force of this Royal Decree and maintained thereafter. In order to achieve this ultimate objective, the access network must be designed and equipped with the appropriate



power supply equipment to ensure operational capability and continuity of service for at least 4 hours for at least 50% of the population in Spain before the end of the first year of this Royal Decree's entry into force, and for at least 4 hours for at least 65% of the population in Spain before the end of the second year of this Royal Decree's entry into force.

In the design, planning and implementation of this strategy to maintain the operational readiness of infrastructures and facilities and to ensure the continuity of service provision, the operator may use all base stations, whether fixed or portable, frequency bands and technologies it deems appropriate, and may prioritise all locations, centres and facilities it considers appropriate based on their connection to the provision of public services and services of economic and social importance.

In this regard, it is considered that the obligation to draw up these plans is proportionate and balanced and does not impose an excessive financial or administrative burden on the obliged parties.

As regards the obligation of "security incident reporting" by the obliged parties, it is also considered proportionate and balanced since, currently, telecommunications operators have also been making notifications similar to those identified in this Royal Decree. Whilst the reporting obligation may entail some additional administrative burden on top of those currently incurred, these burdens are proportionate, balanced and justified in light of the intended objective, since obtaining timely and well-organised information on security incidents enables the necessary decisions to be taken in the best possible way to prioritise the management of public resources and services in particularly critical situations.

The growing diversity of electronic communications networks and services—including fixed, mobile and audiovisual networks and services—together with the multitude of incidents of a multifactorial nature that have been occurring in quick succession in recent years, means that the measure included to empower the Secretary of State for Telecommunications and Digital Infrastructure to issue instructions and guidelines to amend both the General Action Plan and any of the Specific Plans submitted by each obliged entity, with the aim of ensuring the security of electronic communications networks and services, their associated resources and certain digital infrastructures, is proportionate. Without prejudice to the foregoing, any instructions and guidelines adopted must be proportionate and justified, and must take into account the costs associated with the various measures and solutions that may be imposed, having regard to the economic situation of the obliged party and the configuration of the network, service or infrastructure.

This authorisation is justified on the basis of the principle of regulatory flexibility, as it is essential for adapting the plans to technological developments and emerging risks that affect the continuity and quality of the services provided. Furthermore, this mechanism ensures a proportionate and appropriate response to unforeseen situations, strengthening the government's capacity to act in a dynamic and complex environment such as that of digital services and infrastructure.



C) Principle of legal certainty.

The measures adopted in this Royal Decree comply with the principle of legal certainty by setting out the details of Article 63 of Law 11/2022 of 28 June, the General Telecommunications Act, and Royal Decree-Law 12/2018 of 7 September on the security of networks and information systems, and are adopted in a manner consistent with and coordinated with the NIS2 Directive and the CER Directive.

As previously mentioned, these Directives set out obligations relating to cybersecurity and resilience, adopting a cross-cutting and multi-sectoral approach which does not allow for a sufficiently in-depth examination of the technical, operational and strategic specificities of the sector comprising networks, electronic communications services and certain digital infrastructures.

It is therefore necessary to establish national legislation which, in a manner that is consistent with and coordinated alongside the aforementioned legislation, holistically regulates the security and resilience of networks, electronic communications services, their associated resources and certain digital infrastructures in the event of a security incident resulting in service interruption or a significant degradation in service quality.

D) Transparency principle.

The principle of transparency has been complied with, as the public consultation and information procedures provided for in Article 133 of Law 39/2015 of 1 October have been carried out.

E) Principle of efficiency.

The adoption of this Royal Decree is considered efficient as it brings together, in a single regulatory text and in a comprehensive and structured manner, the provisions of Article 63 of Law 11/2022 of 28 June on General Telecommunications, Royal Decree-Law 12/2018 of 7 September on the security of networks and information systems, and the Quality Order which currently regulates the content and deadlines for the notifications that telecommunications operators are required to submit to the Secretary of State for Telecommunications and Digital Infrastructure when significant incidents occur that seriously affect the integrity of networks and the continuity of services provided via digital infrastructures.

I.4.- ALTERNATIVES.

During the drafting of the Royal Decree, various regulatory alternatives were considered, taking into account the principles of necessity, proportionality, efficiency and legal certainty. It was concluded that a Royal Decree is the most appropriate legal instrument for regulating the objectives set out in I.2.



The following alternatives have been analysed:

A) Maintaining the existing regulatory framework without further regulatory development.

The first alternative was not to adopt implementing regulations giving effect to Article 63 of Law 11/2022 of 28 June, the General Telecommunications Act, and to the provisions of Royal Decree 12/2018 of 7 September on the security of networks and information systems.

At European level, the integrity and security of digital infrastructures—including electronic communications networks and services—have also been regulated by Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (hereinafter the NIS2 Directive), as well as in Directive (EU) 2022/2557 of 14 December on the resilience of critical entities (hereinafter the CER Directive). These directives strengthen the obligations imposed on operators and organisations to prevent, detect, respond to and recover from certain security incidents that may compromise the availability and reliability of digital infrastructure, as well as electronic communications networks and services and their associated resources.

The NIS2 Directive establishes new regulations to ensure a high, common level of cybersecurity across the European Union. Consequently, in line with and in coordination with the forthcoming legislation on cybersecurity and critical infrastructures transposing the NIS2 and CER Directives, it is considered necessary to adopt a Royal Decree establishing specific security and resilience obligations for the electronic communications networks and services sector and certain digital infrastructures. These obligations are to be consistent with the legislation on cybersecurity and critical infrastructures, in accordance with Article 63 of Law 11/2022 of 28 June, the General Telecommunications Act, and Royal Decree 12/2018 of 7 September on the security of networks and information systems.

B) Establishing non-binding technical recommendations ("guidelines")

The possibility of issuing technical recommendations containing the necessary provisions, without imposing legally binding obligations, was also considered. This option was rejected due to its limited enforceability and supervisory value, especially in emergency or crisis situations, where a coordinated, rapid and legally supported response is required.

C) Developing a specific regulatory framework by means of a Royal Decree.

In light of the issues described above, it has been decided to draw up a Royal Decree to regulate, in a proportionate and balanced manner, the security of networks, electronic communications services, their associated resources and certain digital infrastructures, whilst ensuring consistency and coordination with national and European cybersecurity regulations.



I.5.- INCLUSION IN THE ANNUAL REGULATORY PLAN AND EX-POST EVALUATION.

This Royal Decree has not been included in the 2025 Annual Regulatory Plan, as the drafting of this regulatory text is based on the consequences of recent incidents which have highlighted the urgent need to strengthen regulations on the security of digital networks and infrastructures. In particular, the effects of the DANA (Isolated High-Level Low-Pressure System) in September 2025, which caused serious interruptions to telecommunications services in various parts of the country, as well as the widespread power cut in October of the same year, which affected critical infrastructure and highlighted systemic vulnerabilities, have created a new risk scenario that had not been anticipated when the Regulatory Plan was drawn up. The consequences of these incidents justify the adoption of specific regulatory measures, by Royal Decree, to strengthen the resilience of the sector and its capacity to respond to complex and multifaceted threats.

No ex post evaluation will be carried out.

II.- CONTENT AND LEGAL ANALYSIS

II.1.- CONTENT

The draft Royal Decree comprises an explanatory section and a substantive section, divided into seven chapters, containing 37 articles, five additional provisions, a single repealing provision and three final provisions.

Chapter I under the heading “General provisions”

Chapter I comprises the first two articles:

Article 1 sets out the purpose of the Royal Decree, which is to establish the conditions and actions aimed at ensuring the security and resilience of networks, electronic communications services, their associated facilities and certain digital infrastructures, particularly in the event of situations and events affecting network security, causing service interruptions or resulting in a significant degradation in service provision. The purpose of this Royal Decree is also to regulate the circumstances and requirements under which obliged entities are required to notify the Ministry for Digital Transformation and the Civil Service when a security incident occurs that has a significant impact on the provision of networks or services.

Section 4 describes what is meant by network or service resilience for the purposes of this Royal Decree.

Article 2 determines the scope of application of this Royal Decree. In this sense, it is established that it shall apply to the owners and operators of publicly available



electronic communications services located in Spain, and to the providers of publicly available electronic communications services provided in Spain; to the owners or operators of any associated resource that serves as support for the deployment of public networks or the provision of any publicly available electronic communications service located in Spain, including passive infrastructures that serve to host mobile communications access networks.

This Royal Decree also applies to the owners or operators of digital infrastructures located in Spain, including, among others, submarine cables, satellite systems, content distribution networks (CDN), data processing centres (DPC) or internet exchange points (IXP), and any associated resources of these infrastructures when they contribute to the deployment of publicly available electronic communications networks.

For these purposes, owners and operators of public electronic communications networks and providers of publicly available electronic communications services shall identify the digital infrastructures that contribute to the deployment of their own networks or the provision of their electronic communications services and shall communicate that information to the Secretary of State for Telecommunications and Digital Infrastructure by 31 January of each calendar year.

Once owners and operators of public electronic communications networks and providers of publicly available electronic communications services have identified and notified the Secretary of State for Telecommunications and Digital Infrastructure of the digital infrastructures that contributes to the operation of their own networks or the provision of their electronic communications services, they must also notify the owners and operators of those digital infrastructures of this fact and, consequently, of the applicability of this Royal Decree.

All obliged persons identified in the previous point must comply with a number of parameters set out in Article 2(3). The Royal Decree provides that these parameters may be amended by ministerial order.

This Royal Decree also applies to centres receiving emergency calls via the 112 emergency number and public warnings, in accordance with the provisions of Chapter IV.

This Royal Decree does not apply to the owners and operators of electronic communications networks, electronic communications services and digital infrastructures linked to National Security and Defence.

In all matters not covered by this Royal Decree, as well as in relation to cybersecurity incidents, the national and European regulations concerning the coordination and governance of cybersecurity and the protection and resilience of critical entities shall apply.

Article 3 provides that, in emergency situations involving security incidents affecting network security, service continuity or the conditions under which services are provided, electronic communications networks and services, their



associated facilities and certain digital infrastructures are to be regarded as essential installations or services.

In such emergency situations, all authorities, administrative bodies and the State's security forces shall cooperate and contribute to facilitating the swiftest and most comprehensive possible restoration of the network's integrity and security, the resumption of service and the operational capability of the infrastructure, or to facilitating its maintenance, in coordination with civil emergency planning and critical infrastructure protection planning, within the scope of their respective competences, through the adoption of any administrative, technical or operational measures that may be necessary. These measures include the issuance of safe-conduct passes and access permits to enable staff of operators and owners or managers of associated resources and digital infrastructure, as well as staff of companies contracted by them, to access the facilities and infrastructure for the purposes of repair, reconstruction or maintenance. Priority shall be given to, and urgency declared in, the processing of any procedure whose ultimate aim is to restore the integrity and security of the network, re-establish the service or operational capability of the infrastructure, or facilitate its maintenance. This may include the granting of provisional and temporary licences and permits—whether relating to town planning, land-use planning, the environment or any other area—or, where appropriate, substituting these with responsible declarations, so as to enable operators and owners or managers of associated resources and digital infrastructure to restore the safety and operational capability of the facilities and infrastructures.

It is also envisaged that the State Security Forces and Corps will provide the necessary assistance and support to enable staff to carry out their activities and operations aimed at restoring the security and operational capability of the installations and infrastructure, or facilitating their maintenance.

In the specific case of interruption to the electricity supply, those facilities or infrastructures deemed by the operator to be essential at the first and intermediate levels, in accordance with Article 7(4), shall be given priority in the restoration of the electricity supply. Equally, in cases where the repair, reconstruction or maintenance of facilities and infrastructures of electronic communications networks and services, their associated resources and digital infrastructures require the supply of fuel, such supply shall be a priority for those facilities and infrastructures.

Chapter II, entitled 'Planning to ensure the security and resilience of electronic communications networks and services, their associated resources and certain digital infrastructures'.

Contains articles 4 to 9:

Article 4 defines the 'National Security and Resilience Plan for networks, certain digital infrastructures, electronic communications services and associated resources'. This Plan shall be approved, by means of Ministerial Order, by the Ministry for Digital Transformation and the Civil Service. Its aim is to develop and coordinate a response and recovery plan for security incidents, setting out the



objectives, functions and responsibilities assigned to the various authorities, crisis management procedures, coordination mechanisms for the Autonomous Communities in the monitoring and updating of the Plan, and possible proactive measures such as training activities. Finally, the territorial distinctiveness of the Autonomous Communities of the Balearic Islands and the Canary Islands, and the Autonomous Cities of Ceuta and Melilla is recognised with regard to matters relating to the submarine cables and satellite systems connecting their territories.

It is expected that this National Plan should be drawn up within one year of the entry into force of this Royal Decree and updated every two years.

Article 5 lays down the obligation to manage security risks appropriately. To this end, obliged entities are required to manage security risks appropriately, with a view to preventing or minimising the impact of security incidents on both users and networks. In this sense, this also includes the obligation on operators to ensure the greatest possible availability of publicly available electronic communications services and, in particular, of voice communications and internet access services provided over telecommunications networks in the event of a catastrophic network failure or in cases of force majeure, and shall take all necessary measures to ensure uninterrupted access to emergency communications services and the uninterrupted transmission of public warnings.

Article 6 lays down the obligation to have a 'General Action Plan of each obliged entity to ensure the security and resilience of electronic communications networks and service'. In addition to a risk analysis of the security of its network, this Plan must determine whether the network or infrastructure is essential, and must also set out the prevention and detection measures, as well as the mechanisms and priorities for the measures to be adopted to manage and restore services in the event of an interruption or significant degradation in service provision.

In this General Plan, operators shall identify the buildings and facilities deemed essential and in respect of which specific and priority measures will be taken to ensure the security of the networks and the continuity of services. It will also detail the criteria taken into account to identify buildings as essential, as well as the specific and priority measures that have been taken in each building or facility to ensure the security of networks and the continuity of services.

The General Plan must be submitted by each operator of public electronic communications networks and provider of publicly available electronic communications services that is classified as an obliged entity pursuant to the provisions of this Royal Decree to the Secretary of State for Telecommunications and Digital Infrastructure within six months of the Royal Decree coming into force, and must be updated every two years.

Any owner or manager of an associated resource or digital infrastructure who is classified as an obliged entity pursuant to the provisions of this Royal Decree must submit the General Action Plan when required to do so by the Secretary of State for Telecommunications and Digital Infrastructures, within the time limit specified in the request itself.



Article 7 sets out the obligation for each obliged entity to have a “Specific Plan for each network, service, associated resource or digital infrastructure used to ensure its security”.

This specific plan must be submitted as a comprehensive whole for each of the following categories of networks, services, associated resources and digital infrastructures:

- a) Fixed communications networks and services.
- b) Mobile communications networks and services, including passive infrastructures used to host mobile communications access networks.
- c) Instant messaging services.
- d) Networks supporting nationwide terrestrial broadcasting audiovisual communication services that are subject to coverage obligations.
- e) Submarine cables.
- f) Satellite systems.
- g) Certain digital infrastructures that contribute to the deployment of public electronic communications networks and the provision of the electronic communications service, as previously identified by electronic communications operators, in accordance with Article 2(2) of this Royal Decree, such as Content Delivery Networks (CDN), Data Processing Centres (DPCs) and Internet Exchange Points (IXPs).

It is anticipated that, as a result of the dynamic nature of the electronic communications and digital infrastructure sectors, the constant process of technological innovation characteristic of these fields, and the continuous and successive regulatory, economic, commercial and competitive changes faced by market participants, the above provisions and classifications may be amended by an Order approved by the Minister for Digital Transformation and the Civil Service.

In addition, obliged entities are required to submit a Specific Plan for each type of incident as determined by Order. The following types of incidents are initially identified: serious interruption to the external network infrastructure; interruption of the electricity supply, a meteorological event causing serious impact on the network, service or infrastructure, volcanic eruption, earthquake, flooding, fire, serious IT failure and major cyberattack.

In both specific plans, the obliged parties shall describe the priorities and measures for prevention and detection, as well as the measures to be adopted for the recovery of services in the event of interruption or significant degradation of the conditions for the provision of these services.

Specific plans may provide that, as measures aimed at properly managing the incident, the obliged party may take decisions to ensure the maintenance of the most basic and essential electronic communications services, enable communication to be maintained as widely as possible for different citizens and territories, and avoid traffic congestion. To this end, the plan may provide for, and the obliged party may, if necessary, implement measures such as prioritising certain types of traffic—such as that linked to emergency services, official communications or communications to official accounts—prioritising traffic



consisting of voice calls and SMS messages over data transmission traffic, or temporarily suspending the use or operation of certain technologies or services that demand higher energy consumption or greater data transmission capacity. Under no circumstances may the obliged party discriminate against or disadvantage the traffic of any operator or agent within the same service or technology.

Furthermore, these specific plans will include estimates of the percentage of traffic and service availability for which, in the event of natural disasters or potential energy emergencies, the network infrastructure is capable of ensuring the continuity, operability and functioning of the service. In particular, in the event of a power cut, the obliged party, under these specific plans, must identify, within the network, service, associated resource or digital infrastructure, those facilities or infrastructure elements that are considered essential due to their importance and impact on maintaining the service's operability and functioning. These essential first-level installations or infrastructures must guarantee their operability an interruption of the electricity supply for at least 24 hours; essential intermediate-level installations or infrastructures for at least 12 hours; and all other installations and infrastructures must guarantee their operability for at least 4 hours.

In the specific case of the access network of a mobile communications network through which publicly available electronic communications services are provided in harmonised European bands, this access network must be designed and equipped with its own generating equipment and electrical supply elements to ensure its operability and continuity of service as the ultimate objective for at least 4 hours for at least 75% of the population in Spain.

This ultimate objective must be achieved within three years of the entry into force of this Royal Decree and maintained thereafter. In order to achieve this ultimate objective, the access network must be designed and equipped with the appropriate power supply equipment to ensure operability and continuity of service for at least 4 hours for a minimum of 50% of the population in Spain before the end of the first year of this Royal Decree's entry into force, and for at least 4 hours for a minimum of 65% of the population in Spain before the end of the second year of this Royal Decree's entry into force.

In the design, planning and implementation of this strategy to maintain the operational readiness of infrastructures and facilities and to ensure the continuity of service provision, the operator may use all base stations, whether fixed or portable, frequency bands and technologies it deems appropriate, and may prioritise all locations, centres and facilities it considers appropriate based on their connection to the provision of public services and services of economic and social importance.

In implementing this strategy to maintain the operational readiness of infrastructure and facilities and to ensure the continuity of service provision, the various authorities and bodies, within the scope of their respective powers, may adopt the administrative, technical and operational measures necessary to facilitate the implementation of this strategy, such as prioritising and declaring the urgent need for the granting of licences and permits—whether relating to town planning, land-



use planning, the environment or any other area—or allowing these to be replaced by responsible declarations.

Installations or infrastructures that are considered by the operator to be essential—at both the primary and intermediate levels—in the event of interruption to the electricity supply must be communicated to the transmission company and the electricity distribution companies so that they can be included in their electrical contingency plans.

Furthermore, the installations or infrastructures necessary to maintain the operability and functioning of submarine cables and satellite systems connecting any island of the Autonomous Communities of the Balearic Islands and the Canary Islands, or the Autonomous Cities of Ceuta and Melilla must also be communicated to the transmission company and the electricity distribution companies so that they can be included in their electricity contingency plans..

In the specific plans and in the design of mitigation and incident management measures for the possible consequences and damage that may be caused, the obliged party must incorporate the most advanced and innovative mechanisms and techniques in the detection and prevention of risks and in the management of incidents that occur, in particular, those techniques linked to the use of artificial intelligence services that contribute to the planning, design and management of risks that make it possible to have and provide electronic communications networks and services, their associated resources and safer and more resilient digital infrastructures.

Every operator of public electronic communications networks and of publicly available electronic communications services that is classified as an obliged entity pursuant to the provisions of this Royal Decree must submit these specific plans to the Secretary of State for Telecommunications and Digital Infrastructure within a maximum period of six months from the entry into force of this Royal Decree, and must update them every two years.

Any owner or manager of an associated resource or digital infrastructure who is classified as an obliged entity pursuant to the provisions of this Royal Decree must submit these specific plans when required to do so by the Secretary of State for Telecommunications and Digital Infrastructures, within the time limit specified in the request itself.

Article 8 establishes that the Secretary of State for Telecommunications and Digital Infrastructures shall analyse the different plans submitted by the obliged parties and, in the light of the analysis, may issue instructions and guidelines to modify them with the aim of ensuring the security of electronic communications networks and services, their associated resources and digital infrastructures.

When adopting these instructions and guidelines, the Secretary of State for Telecommunications and Digital Infrastructure must provide adequate grounds, justifying them on the basis of the need to ensure the security and resilience of electronic communications networks and services, their associated resources and the digital infrastructure that contributes to their operation, to complement the risk



analysis or the application of mitigation techniques that are generally accepted by the electronic communications and digital infrastructure sector and other obliged entities, and to implement those measures that have been specified in the routine and ad hoc audits which obliged entities are required to submit to under this Royal Decree.

Likewise, in approving these instructions and guidelines, the Secretary of State for Telecommunications and Digital Infrastructure must take into account the costs associated with the different measures and solutions that may be imposed, taking into account the economic situation of the obliged party and the configuration of the network, service or infrastructure.

The instructions and guidelines shall be approved by the Secretary of State for Telecommunications and Digital Infrastructure following a hearing with the obliged entity. They shall constitute the final administrative decision and may be challenged directly before the administrative courts.

The Secretary of State for Telecommunications and Digital Infrastructure may draw up templates for a General Action Plan and Specific Plans so that they can be followed and implemented by the obliged parties.

Article 9 establishes the “National Civil Emergency Plan for Electronic Communications Networks and Services”, under which a strategy will be drawn up to mobilise resources and assets relating to electronic communications networks and services and certain digital infrastructures, with a view to restoring normal conditions as soon as possible.

The preparation of the Plan shall take into account the territorial uniqueness of the Autonomous Communities of the Balearic Islands and the Canary Islands, and the Autonomous Cities of Ceuta and Melilla, as regards the issues related to submarine cables and satellite systems connecting their territories.

This Plan must be updated every two years.

Chapter III entitled ‘Notifications of security incidents affecting electronic communications networks and services, their associated resources and certain digital infrastructures’

It contains Articles 10 to 18.

Article 10 sets out the obligation on obliged entities to report security incidents that have had a significant impact on networks, electronic communications services, their associated resources and certain digital infrastructures, as well as the criteria used to determine the significance of the impact of a security incident. Furthermore, it stipulates that the parties subject to this obligation must have the necessary material and human resources to comply with the notification requirement, irrespective of the resources available to restore the situation to normal.



Article 11 defines the concept of security incidents affecting electronic communications networks and services, their associated facilities, and certain digital infrastructures. It also establishes the parameters for considering whether an incident should be regarded as minor or significant, as well as the point in time at which a security incident is deemed to commence and to end. Similarly, it is envisaged that the Head of the Secretary of State for Telecommunications and Digital Infrastructure will, by means of a resolution, determine the procedure for calculating the number of lines or services affected, the definition of the threshold for service quality impairment, and the conditions under which the interruption or degradation of services must be notified where there is no direct impact on electronic communications service lines or users, or where it is not possible to determine such an impact.

Article 12 sets out the types, procedures and content of the initial, intermediate and final notifications that the obliged entity must submit to the Secretary of State for Telecommunications and Digital Infrastructure.

As regards initial notifications, these are to be made in all cases where the operator experiences a significant security incident as defined in Article 11(3). This notification must be sent by email to the Secretary of State for Telecommunications and Digital Infrastructure within a maximum of 1 hour of the data controller becoming aware of the incident. Should it not be possible to send the notification by email, the obliged entity must contact the Secretary of State for Telecommunications and Digital Infrastructure by whatever means are available, and the method for transmitting the notification and the information will be agreed upon.

As regards the content, it shall include at least the following information: information on the exact time the incident began, a brief description of its cause and, in particular, whether it is currently considered at that time to be a cybersecurity incident, an incident of another nature, or a hybrid incident; the services affected and, in particular, whether the incident affects the emergency communications service or the public warning service; a contact person and their contact details; and any other information that the obliged party considers relevant.

For intermediate notifications, if more than 2 hours have elapsed since the initial notification and the incident has not yet been fully resolved, the obliged party must send, by email, at the 2-hour mark, and subsequently, during the first 24 hours from the start of the incident, every 3 hours, to the Secretary of State for Telecommunications and Digital Infrastructure all necessary interim notifications to update the information contained in the initial notification and to provide any additional information requested by the Secretary of State for Telecommunications and Digital Infrastructure. In terms of content, the information reported in the initial notification shall be provided in more detail. A detailed description of the incident and the digital infrastructure affected shall be provided, along with the impact of the fault; whether the emergency communications service or public warning service has been restored; whether other operators are affected; an update on the number of lines or users affected by service; a preliminary analysis of the cause of the fault; whether the cause is internal or external and details of the cause thereof, whether it is due to system failure, network congestion, human error, malicious



acts, natural phenomena, or failure on the part of third parties such as the electricity supply, cable theft or breakage, earthquakes or floods, as well as any additional information that the operator may be able to report.

Equally, it is stipulated that if the incident affects more than one obliged entity, the Secretary of State for Telecommunications and Digital Infrastructure shall specify, within the first 24 hours, the exact times for the submission of intermediate notifications. In the first 24 hours of the start of the incident, intermediate notifications shall be sent at 9: 00, at 16:00 and at 21:00, by e-mail, until the final notification is made. However, the Secretary of State for Telecommunications and Digital Infrastructure may amend the periods of time and the times identified above depending on the impact and severity of the incident.

Finally, it is provided that once the incident has been resolved, the obliged party will send a final notification by email as soon as it becomes aware that the affected service has been restored. However, without prejudice to the foregoing, within a maximum of 24 hours of the operator notifying the resolution of the incident, the obliged party shall send a final notification stating, in addition to the exact time of the incident's resolution, an update that is as detailed as possible on the latest information reported.

Finally, 10 days after the final notification, the obliged party must submit, by email, a detailed report containing the information specified in Article 11.

Without prejudice to the information requested in each notification, the Secretary of State for Telecommunications and Digital Infrastructure may draw up and send to the obliged parties a specific notification form during the initial, intermediate and final notification processes, requesting specific and additional information tailored to the particular security incident and in accordance with the needs and severity of the impact on the service.

It is also envisaged that the obliged entities will provide the Secretary of State for Telecommunications and Digital Infrastructure, within three months of the entry into force, with the contact details of the persons responsible for these notifications. These details will be updated at least once a year.

Finally, it is envisaged that obliged entities that suffer a significant security incident requiring work or actions to be carried out on public roads must notify the owner or operator of the road, without undue delay, the need for action on that public road, so that such work can be co-ordinated safely and carried out as soon as possible, in accordance with the provisions of Article 123 of Royal Decree 899/2025 of 9 October, approving the General Road Regulations.

Article 13 sets out the mitigating measures that the Secretary of State for Telecommunications and Digital Infrastructure may adopt in relation to the contingency measures taken by obliged entities during notified incidents or to reduce the risk of such incidents recurring. Specifically, it is stipulated that recommendations, guidance or advice may be provided to obliged entities regarding the implementation of possible corrective measures.



Article 14 sets out the procedure for collaboration with other Member States concerned. To this end, the Secretary of State for Telecommunications and Digital Infrastructure shall inform the other Member State.

Article 15 sets out the measures for informing natural and legal persons receiving services affected by a security incident involving the electronic communications network or services. In order to do so, the obliged persons must ensure that natural and legal persons who are recipients of electronic communications services are adequately informed, through public communications—such as publication on their websites—or through customer service channels and services, about the impact on their services, as soon as such communication or information can be provided following an incident affecting the provision of electronic communications services, as well as about the measures or solutions adopted to resolve the incident promptly.

Article 16 sets out the requirements for notifying other competent authorities in the event of significant security incidents affecting critical infrastructures and in relation to cybersecurity.

Article 17 provides for the possibility of reporting, on a voluntary basis, other types of incidents or relevant information.

Article 18 sets out the information that the Secretary of State for Telecommunications and Digital Infrastructure may provide to obliged entities and to centres receiving emergency calls and public warnings. Specifically, it is envisaged that, where it deems it appropriate in view of the number of obliged entities affected, the type of incident and its repercussions, etc., and in order to facilitate the flow of information to be provided by the obliged entities and access by those entities to the information most relevant to them, or to achieve better coordination in the resolution of the incident and the more rapid and effective restoration of service and infrastructure operability, shall provide information on the incident, its extent of impact, and the mitigating and resilience measures that may be adopted or are being adopted by other parties or obliged entities, whilst safeguarding the confidentiality of information and trade secrets pertaining to each obliged entity.

It is also envisaged that the Secretary of State for Telecommunications and Digital Infrastructure shall provide information to centres receiving emergency calls via the 112 emergency number and public warnings when the incident affects the origination, routing or reception of this type of communication or warnings.

Chapter IV contains under the heading ‘Emergency communications via the 112 emergency number and public warnings’.

It contains Articles 19 to 21:

Article 19 establishes the obligation of centres receiving emergency calls via the 112 emergency number and public warnings to ensure security and adopt measures to enable the routing of emergency calls and public warnings. To this



end, they shall adopt such technical measures as they deem appropriate, including specific plans, strategies, redundancies and service alternatives, either through the operator providing the emergency communications routing service or through one or more other service providers.

These measures must be presented to the Secretary of State for Telecommunications and Digital Infrastructure within a maximum period of 6 months from the entry into force of this Royal Decree. The measures adopted by centres receiving emergency calls via the 112 emergency number and public warnings, as well as any specific plans or contingency and alternative arrangements, shall be updated and submitted to the Secretary of State for Telecommunications and Digital Infrastructure every two years.

In cases where the provision of emergency call-handling services via the 112 emergency number and public warnings is carried out through contracts with third parties, the centres receiving the calls must review and, where necessary, update the measures adopted whenever there are changes to the service providers as a result of public procurement procedures. Once updated, these measures must be submitted to the Secretary of State for Telecommunications and Digital Infrastructure.

Article 20 describes the obligation of obliged entities to ensure the continuity of service to centres receiving emergency calls via the 112 emergency number and public warnings. Obligated entities are required to submit to the Secretary of State for Telecommunications and Digital Infrastructure, within 6 months of the entry into force of this Royal Decree—and updated and submitted to the Secretary of State for Telecommunications and Digital Infrastructures every two years—a specific plan, prepared in coordination with the reception centres, which includes the measures to ensure the continuity of service and the transmission of emergency communications to centres receiving emergency calls via the 112 emergency number and public warnings, including, where appropriate, various redundancy mechanisms or other alternative arrangements to guarantee the continuity of the service. In the light of the alternatives, the Secretary of State may amend that Plan.

When adopting these instructions and guidelines, the Secretary of State for Telecommunications and Digital Infrastructure must provide adequate grounds, justifying them on the basis of the need to ensure the security and resilience of electronic communications networks and services, in order to ensure continuity of service to centres receiving emergency calls via the 112 emergency number and public warnings, to complement the risk analysis or the application of mitigation techniques that are generally accepted by the electronic communications and digital infrastructure sector and other obliged entities, and to implement those measures that have been specified in the ordinary and extraordinary audits which obliged entities are required to submit in accordance with the provisions of this Royal Decree.

Likewise, in approving these instructions and guidelines, the Secretary of State for Telecommunications and Digital Infrastructure must take into account the costs associated with the different measures and solutions that may be imposed, taking



into account the economic situation of the obliged party and the configuration of the network, service or infrastructure.

The instructions and guidelines shall be approved by the Secretary of State for Telecommunications and Digital Infrastructure, following a report from the receiving centre and after the obliged entity has been given the opportunity to be heard. They shall constitute the final administrative decision and may be challenged directly before the administrative courts.

Article 21 sets out the obligation on the part of centres receiving emergency calls via the 112 emergency number or the public warning service.

In the event of an interruption to the service routing emergency calls to the 112 emergency number or to the public warning service, both the centres receiving emergency calls and the obliged parties, are required to notify the Secretary of State for Telecommunications and Digital Infrastructure of such an incident without delay, within a maximum of one hour of becoming aware of it.

In order to determine the impact of the interruption of the emergency communication service or public warnings, certain parameters identified in paragraph 2 shall be taken into account.

It is envisaged that, in order to comply with the obligation to notify any interruption to the emergency communications service or the public warning service, both the centres receiving emergency calls via the 112 emergency number and public warnings, and the entities subject to this obligation, must have the necessary material and human resources to fulfil the notification obligation, irrespective of the means and resources allocated to resolving the security incident and restoring normal service.

Similarly, it is stipulated that the interruption of this type of service constitutes a significant incident and that the following notifications must be made to the Secretary of State:

An initial notification, which will be sent by email to the Secretary of State for Telecommunications and Digital Infrastructures, by both the reception centres for emergency communications and public warnings and by the obliged parties, within a maximum period of 1 hour from when the reception centre or the obliged party became aware of the incident. In terms of content, the initial notification shall include at least information on the exact time of the start of the incident, a brief description of the cause that gave rise to the incident, the geographical area affected, the number of estimated lines affected, contingency measures taken during the first hour that the emergency communications service or public warning service has been interrupted, plans envisaged for the recovery of the affected service, estimated duration of the incident and contact person and communications channels used to inform both users and the administration and any other relevant information.

If, one hour after the initial notification, the emergency communications service or the public warning service has not been restored, both the reception centres and



the obliged parties must submit, one hour after becoming aware of the incident and subsequently every two hours thereafter, by email to the Secretary of State for Telecommunications and Digital Infrastructure, as many intermediate notifications as necessary to update the information contained in the initial notification and to provide any additional information requested by the Secretary of State for Telecommunications and Digital Infrastructure within the specified time and in the specified manner.

Intermediate notifications shall be submitted until the final notification is made, without prejudice to the Secretary of State for Telecommunications and Digital Infrastructure's option to modify this period of time depending on the impact and severity of the security incident that has occurred.

In the intermediate notifications to be made to the Secretary of State for Telecommunications and Digital Infrastructure, the information reported in the initial notification shall be provided in more detail. A detailed description shall be provided of the incident and the networks, services, associated resources and digital infrastructure affected, the impact of the fault, whether other operators are affected, an update on the number of lines affected, a preliminary analysis of the cause of the fault, whether the cause is internal or external and details of the cause, whether it is due to system failure, network congestion, human error, malicious acts, natural phenomena, or failure by third parties such as power supply issues, cable theft or breakage, earthquakes or floods, as well as any additional information that the operator may report.

Finally, as soon as they are aware that the service has been restored, the reception centres and the designated entities shall notify the Secretary of State by email. Furthermore, within a maximum of 24 hours of being notified that the incident has been resolved, the reception centres and the obliged parties shall send a final notification stating, in addition to the exact time at which the emergency communications service or the public warning service was restored, an update that is as detailed as possible regarding the latest information reported in the initial notification or in the intermediate notifications, if such notifications were issued.

A detailed report on the incident shall be sent to the Secretary of State for Telecommunications and Digital Infrastructure within 5 working days of notification of the restoration of the communications service to the emergency number or the public warning service.

Paragraph 5 provides that the Secretary of State may prepare and issue a specific notification form for initial, intermediate and final notifications. Paragraph 6 also stipulates that both reception centres and obliged parties must notify the Secretary of State for Telecommunications and Digital Infrastructure, within three months of the approval of this Royal Decree, of the persons responsible for submitting notifications. This information must be updated annually.

Chapter V under the heading 'Assumption by the General State Administration of the direct management of certain publicly available



electronic communications services in order to ensure public security and national security or the fulfilment of public service obligations'

Article 22 provides for the assumption by the General State Administration of the direct management of certain electronic communications services in order to ensure public security and national security. These decisions shall be adopted by the Government, on an exceptional basis, following a report from the National Commission on Markets and Competition, either on its own initiative or at the request of a competent public administration.

Prior to assuming the direct management or intervening in electronic communications services that may affect access to or operation of emergency communications via the 112 emergency number or public warning systems, the Government shall cooperate with the competent Autonomous Communities in the management of those emergency communications and public warning services, in order to assess the impact of the measure on their operations and ensure appropriate institutional coordination.

Furthermore, paragraph 6 stipulates that agreements to assume the direct management of the service must be notified by the Government within 24 hours to the competent judicial authority so that, within 48 hours, the court may determine whether they are consistent with fundamental rights and public freedoms, and annul them if they are not.

Chapter VI under the heading 'Supervision and Cooperation'

Contains articles 23 to 28.

Article 23 refers to the supervision and enforcement of security and resilience obligations relating to the network, electronic communications services, their associated resources and certain digital infrastructures.

The competent authority in Spain for receiving the notifications referred to in Chapter III of this Royal Decree, for supervising the regulated security and resilience obligations, and for adopting measures to ensure compliance with the obligations set out in this Royal Decree is the Secretary of State for Telecommunications and Digital Infrastructure. It is envisaged that, in adopting these measures, the Secretary of State will be able to establish supervisory methodologies that allow for prioritisation using a risk-based approach.

Furthermore, it is envisaged that, in order to monitor compliance, the Secretary of State may require the obliged entities to provide all relevant information. It may also require the entity to carry out, at their own expense, an external audit to verify compliance with the information requirements. In all cases, the obligations shall be effective, proportionate and dissuasive.

In the event that the enforcement measures taken by the Secretary of State prove ineffective, the Secretary shall set a time limit for remedying the identified deficiencies.



Paragraph 10 of this article provides that, in matters not expressly regulated in this article, the enforcement and supervisory measures set out in national and European legislation on cybersecurity and the resilience of critical infrastructure shall apply.

Article 24 sets out the national cooperation procedure involving the competent cybersecurity bodies and the National Commission on Markets and Competition.

Article 25 establishes the cooperation mechanism with the Autonomous Communities. Specifically, it is envisaged that mechanisms for mutual cooperation will be developed to enable both the Secretary of State for Telecommunications and Digital Infrastructure and the Autonomous Communities to exercise the functions and powers assigned to them by law, and coordinate as effectively as possible in the exercise of these powers, thereby contributing to the common objective of ensuring the swiftest and most effective resolution of incidents and the fastest and fullest restoration of the security of the networks, the continuity of the services and the operability of the infrastructures referred to in this Royal Decree.

In particular, it is envisaged that the Secretary of State for Telecommunications and Digital Infrastructure shall establish the appropriate channels for the transmission of information so that the Autonomous Communities may receive information as quickly as possible regarding significant incidents affecting electronic communications networks and services and certain digital infrastructures, in particular those networks, services and infrastructures located within their territories. It is also envisaged that it will develop the appropriate cooperation mechanisms to enable the Autonomous Communities to contribute to setting the objectives, practices and instruments designed to strengthen the security and resilience of public electronic communications networks, publicly available electronic communications services and their associated resources, and the digital infrastructures that contribute to their deployment and the provision of those services.

Article 26, in turn, sets out the cooperation procedure at the European Union level.

Article 27 sets out the cooperation procedure for incidents involving personal data and Article 28 establishes the authorisation procedure for the disclosure of personal data.

Chapter VII under the heading ‘Inspection and sanctioning regime in the field of security and continuity of electronic communications networks and services, their associated resources and digital infrastructures’

Contains articles 29 to 37.

Article 29, concerning inspection powers, provides that responsibility for carrying out inspections lies with the Secretariat of State for Telecommunications and Digital Infrastructure.

Article 30, in turn, sets out the inspection powers. Specifically, it establishes that the inspection services of the Secretary of State for Telecommunications may



carry out the inspections they deem necessary in order to verify compliance with the obligations established in this Royal Decree. To this end, they may collect any additional data they deem necessary, as well as carry out their own measurements and checks of the operators' networks and information systems.

It is envisaged that obliged entities will be required to submit to inspections carried out by inspection staff, and that any refusal or obstruction in relation to attending inspections, carrying out technical tests, or providing the required information or documentation will be penalised as obstruction of the inspection process.

Article 31 concerns administrative liability for infringements of the provisions contained in this Royal Decree. Such liability shall be incurred by the natural or legal person that materially carries out or engages in the activity alleged to constitute the infringement.

Article 32 provides that any breach by the obliged entities of any of the obligations set out in this Royal Decree that is directly related to the integrity and security of the provision of electronic communications services or the supply of electronic communications networks, and, in particular, the obligations to draw up and submit the general and specific plans established in this Royal Decree, and the obligations relating to the notification of incidents provided for therein, shall be regarded as a serious infringement pursuant to Article 107(22) of Law 11/2022 of 28 June, without prejudice to the commission of any other possible infringements that may be committed and which are defined in Articles 106, 107 and 108 of Law 11/2022 of 28 June, which shall be penalised in accordance with the provisions of Title VIII of the aforementioned Law.

Article 33 also provides that the commission of serious infringements as defined in Article 107(22) of Law 11/2022 of 28 June shall be punishable with a fine of up to EUR 2 million, in accordance with Article 109 of Law 11/2022 of 28 June.

For the commission of other offences set out in Articles 106, 107 and 108 of Law 11/2022 of 28 June, the offender shall be subject to the penalties laid down in Article 109 of Law 11/2022 of 28 June.

Article 34 sets out the criteria for determining the amount of the penalty. In addition to defining these criteria, it stipulates that, in the case of an infringement consisting of providing misleading, incorrect or incomplete information, either knowingly or through gross negligence, for the purposes of drawing up the reports provided for in the Royal Decree, the amount of the sanction shall be determined taking into account, amongst other criteria, the harm caused to competition, to users or to the public administration.

Article 35 provides for the possibility for the Secretary of State for Telecommunications and Digital Infrastructure to adopt intermediate measures, pursuant to Articles 111 and 112 of Law 11/2022 of 28 June, with a view to bringing about the cessation of the alleged infringements and ensuring compliance with the provisions of this Royal Decree.



With regard to the limitation period, Article 36 states that serious infringements shall be time-barred after two years, in accordance with Article 113 of Law 11/2022 of 28 June. The limitation period shall begin to run from the date on which the offences were committed and shall be suspended by the initiation of sanctioning proceedings, provided that the person concerned has been notified thereof. It is also stated that the limitation period shall start to run again if the disciplinary proceedings are halted for more than 1 month for reasons not attributable to the alleged offender.

In the case of a continuing infringement, the limitation period shall begin to run from the date on which the infringing activity ceases or from the date of the last act by which the infringement was completed. However, the infringement shall be deemed to continue for as long as the telecommunications equipment or installations that are the subject of the proceedings have not been made available to the Administration or until there is conclusive evidence that they cannot be used.

Similarly, it is stated that sanctions imposed for serious offences shall be subject to a limitation period of two years. The limitation period for sanctions shall be counted from the day after the final ruling imposing the sanction becomes enforceable or the period for appealing it has expired. The limitation period shall be interrupted by the commencement of the enforcement procedure, with notification sent to the interested party, and shall restart if the latter is halted for more than 1 month for reasons not attributable to the accused.

In accordance with Article 37, the power to impose sanctions lies with the Secretary of State for Telecommunications and Digital Infrastructure, pursuant to Article 114 of Law 11/2022 of 28 June.

Additional Provisions

Contains five Additional Provisions:

First Additional Provision: It sets out how this Royal Decree is to be coordinated with the regulations on cybersecurity coordination and governance and on the resilience of critical entities.

Specifically, it is stipulated that this Royal Decree shall apply to security incidents as described in Article 11 of this Royal Decree. All other security incidents shall be governed by the relevant national or European regulations on the coordination and governance of cybersecurity and on the resilience of critical infrastructure.

Without prejudice to the foregoing, it is envisaged that the parties subject to this Royal Decree shall also be subject to national or European legislation relating to the coordination and governance of cybersecurity and the resilience of critical entities in respect of matters not provided for or regulated in this Royal Decree.

Second Additional Provision. Coordination Committee for the Security and Resilience of Electronic Communications Networks and Services.



This Second Additional Provision governs the Coordination Committee for the Security and Resilience with the aim of facilitating collaboration, coordination, cooperation, the exchange of information and the participation of all stakeholders involved in the security and resilience of electronic communications networks and services, as well as contributing to the continuous improvement of the capacity to respond to significant incidents. The Coordination Committee for the Security and Resilience of Electronic Communications Networks and Services is hereby established.

The Committee will act as a body for strategic and technical cooperation, a forum for dialogue and consultation, and a platform for drawing up proposals, recommendations and best practices in the field of security and resilience, without assuming any direct operational coordination functions in incident management.

This Committee is composed of representatives from the Ministry for Digital Transformation and the Civil Service, the Ministry of the Interior, the Ministry of Defence, the Department of National Security, the Autonomous Communities, the Spanish Federation of Municipalities and Provinces, the National Commission on Markets and Competition, and the most representative associations of electronic communications operators, digital infrastructure providers, telecommunications equipment manufacturers, and consumers and users. The specific composition of the committee shall be determined by order of the Minister for Digital Transformation and the Civil Service.

It is anticipated that the Coordination Committee for the Security and Resilience of Electronic Communications Networks and Services will adopt its rules of organisation and operation and may propose the carrying out of tests, drills and practical exercises with the aim of verifying the effectiveness of the measures and obligations established regarding the security and resilience of electronic communications networks and services, drawing conclusions on the implementation of these measures, and proposing ways to improve the security and resilience of these networks and services.

Third Additional Provision. Amendment of contracts entered into between operators providing public electronic communications networks or publicly available electronic communications services and the owners or operators of their associated resources, electronic communications networks providing wholesale services, and certain digital infrastructures.

It is anticipated that compliance with the obligations set out in this Royal Decree may give rise to the amendment of contracts entered into between, on the one hand, operators providing public electronic communications networks or publicly available electronic communications services and, on the other hand, the owners or operators of their associated resources, electronic communications networks providing wholesale services, and certain digital infrastructures.

In the event that no agreement is reached on the need for, or the technical, financial or operational terms of, the amendment to the relevant contract between electronic communications operators, or between electronic communications operators and the owners or operators of associated resources, any of the parties



may refer the matter to the National Commission on Markets and Competition, in accordance with the provisions of Article 28 of Law 11/2022 of 28 June. In the decision resolving the dispute, the National Commission for Markets and Competition shall seek to achieve the objectives set out in Article 3 of the aforementioned Law. In particular, with regard to the allocation of costs that may arise from compliance with the obligations set out in Article 7(4) relating to electricity supply infrastructures intended to ensure the operational continuity and uninterrupted provision of electronic communications services, it shall establish the appropriate measures to ensure that such cost allocation is fair, reasonable and proportionate.

Fourth Additional Provision. Adaptation of ex ante regulation.

It is anticipated that compliance with the provisions of this Royal Decree will necessitate amendments to the ex ante obligations approved pursuant to the provisions of Chapter IV of Title II of Law 11/2022 of 28 June. The National Commission for Markets and Competition shall have a period of one year from the moment the regulated operator informs the said Commission of the need to amend and adapt the aforementioned ex ante regulation to the provisions of this Royal Decree.

Fifth Additional Provision. Technological adaptation of the transmission of security incident notifications.

It is envisaged that the Minister for Digital Transformation and the Civil Service may, by order, decide that the transmission by email of notifications of significant security incidents pursuant to Articles 12 and 21 may be replaced or supplemented by other means or channels of transmission or communication, including transmission via a telematic platform or service that may be established for this purpose by the Ministry for Digital Transformation and the Civil Service or in accordance with the provisions of national or European legislation.

Equally, by order, it may be stipulated that security incidents of minor significance must be reported through an online platform or service, to which the various public administrations within whose territory the affected networks are located shall have access. This order will specify the online platform or service to be used, its terms of use and the date on which it will come into effect.

Repealing Provision

It contains a repealing provision which repeals Chapter IV of Order IET/1990/2014 of 16 June, which regulates the conditions relating to service quality in the provision of telecommunications services, specifically concerning incidents leading to a significant degradation in service quality, as well as any provisions of equal or lower rank to this Royal Decree that conflict with its provisions.

Final Provisions



Contains three final provisions setting out the title of competence, the regulatory development and application, as well as the entry into force, which, as set out in the third final provision, will be the day after its publication in the 'Official State Gazette'.

II.2.- LEGAL ANALYSIS

Consistency with the national legal order

This Royal Decree complies with the national legal order by developing the content of Article 63 of Law 11/2022 of 28 June and Royal Decree-Law 12/2018 of 7 September. Part of this content, in particular the procedure for reporting security incidents, has hitherto been governed by the so-called Quality Order, the provisions of which are incorporated and updated in this Royal Decree, in order to provide a more coherent, systematic and effective regulatory framework.

In addition, the Royal Decree is fully consistent with Royal Decree-Law 7/2022 of 29 March laying down the requirements for ensuring the security of fifth-generation electronic communications networks and services, as well as with Royal Decree 443/2024 of 30 April approving the National Security Scheme for 5G networks and services.

In line with and in coordination with the NIS2 and CER Directives, the adoption of this Royal Decree is currently considered to be consistent with national legislation. It establishes specific obligations for a particular sector such as the one in question, in order to ensure the security and resilience of networks, electronic communications services and certain digital infrastructures.

Consistency with European Union law.

This Royal Decree is consistent with the NIS2 Directive and the CER Directive, which establish a general and cross-cutting regulatory framework applicable to all sectors, aimed at strengthening resilience and the response to security incidents. These Directives regulate in a complementary manner the management of security incidents affecting essential sectors and critical services, laying down specific obligations to strengthen operational resilience and cybersecurity in the European Union.

From a legal perspective, the NIS2 Directive establishes a common regulatory framework for achieving a high level of cybersecurity in the European Union, imposing an obligation on Member States and public and private entities in essential and critical sectors to take technical, operational and organisational measures to manage cybersecurity risks. In particular, it regulates the mandatory reporting of significant incidents, risk management, supervision by competent authorities and the exchange of information on threats.

For its part, the CER Directive focuses on the resilience of critical entities to a wide range of risks, including those of natural, human or technological origin, and lays



down requirements for the identification of critical entities, risk assessment, business continuity planning and reporting of incidents that seriously affect the provision of essential services.

It is also consistent with Articles 40 and 41 of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code. These articles regulate the security of networks and services, as well as the management of risks related to cybersecurity and operational resilience. They have, however, been amended by the NIS2 Directive which strengthens cybersecurity and coordination obligations between Member States.

With regard to the security of networks and services, it is stipulated that Member States must ensure that providers of public electronic communications networks and services take appropriate technical and organisational measures to manage risks affecting the security of networks and services. These measures must ensure a level of security commensurate with the existing risk, particularly in relation to:

- ✓ Prevention of unauthorised access.
- ✓ Protection of the integrity and availability of networks.
- ✓ Reporting of significant security incidents to the competent national authorities.

In addition, it provides for the possibility for national regulatory authorities to impose additional requirements depending on technological developments and the nature of the risks.

With regard to risk management and incident reporting, Article 41 supplements Article 40 by setting out specific obligations regarding the reporting of security incidents. In particular:

- ✓ Providers should inform the competent authority, without undue delay, of any incident that has a significant impact on the provision of their services.
- ✓ The authorities may inform the public where they consider it necessary to prevent or mitigate the effects of the incident.
- ✓ Cooperation between national and European authorities is envisaged to share information on threats and vulnerabilities.

However, this Royal Decree goes further by focusing specifically on the field of electronic communications networks and services, as well as certain digital infrastructures, adopting concrete and operational measures that allow a direct and specialised application of the general principles established by the aforementioned European directives, taking into account the technical and functional particularities of the telecommunications and digital services sector.



Validity of the regulation and entry into force

This Royal Decree shall enter into force on the day after its publication in the Official State Gazette.

In accordance with Article 2(1) of the Civil Code, the regulations enter into force on the twentieth day following their full publication in the Official State Gazette, unless otherwise provided for therein. In this sense, the Royal Decree can validly establish in its final provision that its entry into force occurs the day after its publication, making use of the legal authorisation to set a different deadline.

In the case in question, it is necessary to bring the date of entry into force forward in order to apply urgent measures immediately in the face of an imminent contingency requiring rapid implementation, particularly as the Royal Decree sets out security measures to deal with potential significant security incidents that could lead to service interruption or a significant degradation in service quality, such as those we have experienced in recent years. Consequently, the entry into force on the day following its publication is fully in line with the Spanish legal framework and ensures that the effectiveness of the regulations in the event of an immediate security incident requiring the obligations to come into force as soon as possible.

III.- DESCRIPTION OF THE PROCEDURE FOLLOWED

III.1.- PRELIMINARY PUBLIC CONSULTATION WITH STAKEHOLDERS

Commencement of the procedure

On 11 September 2025, the Secretary of State for Telecommunications and Digital Infrastructure published the prior public consultation on the future Royal Decree on the security and resilience of digital infrastructure, with the aim of gathering input from operators, citizens and other stakeholders. The closing date for the submission of observations was 26 September 2025. This initiative was undertaken in accordance with Article 133(1) of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations.

Submissions made by the stakeholders.

- **On the necessity and appropriateness of the regulation:**

Divergent positions have been expressed regarding the necessity and timeliness of the regulation. One view is that networks have demonstrated a high level of responsiveness to recent crises, and therefore any new obligation must be duly justified, technically feasible and in line with the principle of proportionality, whilst another view welcomes the proposal, highlighting the need to strengthen resilience



in critical situations and recognising the complementary role of different technologies.

- **Regulatory coordination and legal certainty:**

There is broad consensus on the need to ensure regulatory coherence. Stakeholders called for the legislation be brought into line with the European NIS2 and CER Directives, so as to avoid regulatory duplication, overlaps and contradictions with the legislation to be adopted pursuant to Article 63 of Law 11/2022 of 28 June. Some propose that any implementing measure should take the form of “*guidelines*” or recommendations, rather than being introduced as directly binding regulatory requirements.

- **Energy autonomy and operational continuity**

Most operators agree to reject generalised obligations on electricity autonomy by pointing out technical, economic and logistical constraints, especially in rural or external locations. However, another group of respondents supports strengthening energy self-sufficiency in critical facilities, provided that public funding mechanisms are put in place and priority access to essential supplies is guaranteed in emergencies.

- **Financial resilience and sustainability plans**

Some operators argue that the plans already in place are effective and sustainable, and are calling for the legislation to recognise those existing arrangements and avoid administrative duplication. Stakeholders called for any regulatory changes be framed as technical recommendations and for public funding be made available, particularly in areas of low profitability.

- **Incident reporting:**

There is a widely held view that the current framework should be maintained, whilst retaining the deadlines and thresholds set out in the Quality Order. It is proposed to incorporate a new category of “other relevant incidents” and to move towards a controlled digital environment (online) that allows automatic analysis by the administration.

- **Inclusion and accessibility**

One stakeholder requested that the regulation adopt an inclusive approach, recognising the varying levels of critical importance of services for people with disabilities. It is proposed that information during crises be universally accessible and that vital connections be given priority in restoration plans.

- **Institutional collaboration and shared governance:**

A part of the claimants support the creation of an ‘emergency committee’ coordinated by the administration, with the participation of operators, suppliers, law



enforcement and local authorities. It calls for multilevel coordination (regional, national, European) and the creation of a shared repository of information.

▪ **Obligated parties and the digital value chain**

It is requested to extend the scope of the standard to other relevant actors in the digital ecosystem, such as OTT providers, social networks, cloud platforms and artificial intelligence. It is proposed that specific obligations be defined for these agents, such as protocols for recovery and notification in the event of outages affecting critical Service Level Agreements (SLAs).

▪ **Technological diversity and hybrid solutions**

Some companies defend the strategic role of satellite and broadcasting as complementary technologies, particularly in emergency situations. Stakeholders also called for the regulatory recognition of hybrid solutions (terrestrial + satellite) and for emergency connectivity points to be set up in public institutions.

▪ **Physical safety and protection against vandalism**

Stakeholders also called for tougher criminal legislation to tackle copper theft and acts of vandalism affecting critical infrastructure. They also proposed ensuring safe-conduct passes, access to fuel, police support and the swift processing of licences during emergency situations.

III. 2. PUBLIC HEARING AND INFORMATION PROCESS

In order to give the affected members of the public a chance to be heard and to gather any comments that individuals and organisations might wish to make regarding the Draft Royal Decree on the security and resilience of electronic communications networks and services, the draft was submitted for public consultation in accordance with the provisions of Article 133(2) of Law 39/2015 of 1 October on Common Administrative Procedures in Public Administration and Article 26(6) of Law 50/1997 of 27 November on the Government. The deadline for stakeholders to submit comments was 26 January 2026.

During the course of the proceedings in question, numerous submissions were received from both the autonomous communities and obliged entities and sectoral associations. These have been taken into account and incorporated into the draft text of the Royal Decree, which is now being put forward for a second round of public consultation.

In summary, **operators and other obliged entities** state that this Royal Decree pre-empted the transposition of the NIS2 and CER Directives, which could give rise to potential overlaps, contradictions and duplication.

With regard to the energy autonomy obligations, they consider that the measures introduced are disproportionate from both a technical and economic point of view.



In particular, they consider that the requirement to ensure four hours of autonomy for 85% of the population is excessive, costly and inefficient.

As regards the subjective scope—that is, who should be subject to the obligation—some operators consider that owners of passive infrastructure and associated resources should be expressly included, whilst others categorically state the opposite.

With regard to the incident reporting procedure, the thresholds are considered to be excessively low, leading to over-reporting and administrative overload. There is considered to be a risk of duplication with the NIS2 Directive and the CER Directive, as well as with the Royal Decree on the National Security Framework, the reporting deadlines (1 hour) are considered unworkable and the obligation to notify users of incidents within 72 hours is rejected.

As regards action plans, the main operators consider that the submission of such plans places an excessive burden on them and that the deadlines for submission are too short. They are therefore calling for the plans to be reviewed at longer intervals.

Finally, operators have highlighted the need to impose obligations on electricity suppliers and to strengthen coordination.

As for the **sectoral associations**, they generally agree that the draft Royal Decree, as currently drafted, contains measures that are disproportionate from both an economic and an administrative point of view. They consider that the obligations set out in the Royal Decree are not aligned with the NIS2 and CER Directives and therefore result in duplication. They also consider that the scope of this draft Royal Decree is too broad and that it imposes impracticable obligations regarding electricity supply continuity and notification.

Finally, the **Autonomous Communities** generally called for their role in planning, supervision and incident management to be strengthened; for their powers in relation to the 112 emergency service and civil protection to be fully respected; for obligations to be adapted to local circumstances (insularity, rural areas); and for effective operational coordination with 112 centres to be ensured.

III.3. REQUESTED REPORTS

The following reports must be obtained during the processing procedure:

- Report of the National Commission on Markets and Competition, in accordance with Article 5(2)(a) of Law 3/2013 of 4 June establishing the National Commission on Markets and Competition.
- Report of the Technical General Secretariat of the Ministry of Digital Transformation and the Civil Service, in accordance with the provisions of Article 26(5), fourth paragraph, of Law 50/1997 of 27 November on the Government.



- Reports from the Ministry of the Interior, Ministry of Defence, Ministry of Finance, Ministry of Territorial Policy and Democratic Memory, and the National Security Department of the Presidency of the Government, in accordance with the first paragraph of Article 26(5) of Law 50/1997 of 27 November on the Government.
- Report of the Ministry of Territorial Policy and Democratic Memory in accordance with Article 26(5), sixth subparagraph, of Law 50/1997 of 27 November on the Government.
- Report of the Office of Coordination and Regulatory Quality of the Ministry of the Presidency, Justice and Relations with the Courts in accordance with the provisions of Article 26(9) of Law 50/1997 of 27 November on the Government.
- Opinion of the Council of State, in accordance with the provisions of Articles 19(1) and 22(3) of Organic Law 3/1980 of 22 April on the Council of State.

IV.- ADAPTATION OF THE REGULATION TO THE ORDER OF DISTRIBUTION OF POWERS

This Royal Decree is issued under the provisions of Article 149(1)(21) of the Spanish Constitution, which confers on the State exclusive competence in the field of telecommunications.

This constitutional provision enables the State to establish the basic framework and ensure the general coordination of economic activity in this area, thereby guaranteeing market unity and regulatory consistency throughout the country.

Consequently, the provisions contained in this regulation fall within the scope of the legitimate exercise of that exclusive competence and are necessary to ensure the effective, secure and harmonised operation of electronic communications networks and services, as well as strategic digital infrastructures.

V.- IMPACT ANALYSIS

1. Economic and budgetary impact
2. Impact on market unity and competition
3. Analysis of administrative burdens
4. Gender impact
5. Impact on childhood and adolescence
6. Impact on family
7. Impact on the environment and climate change
8. Impact on equal opportunities, non-discrimination and universal accessibility for persons with disabilities



9. Impact on health
10. Impact on data protection

V.1. Economic and budgetary impact

This Royal Decree entails an additional economic and budgetary impact on the obliged parties, given the costs they may incur in drawing up plans – both general and specific – and, in particular, the obligation introduced in Article 7(4) of this Royal Decree, which stipulates that in the event of a power cut, the obliged party must maintain the electricity supply to infrastructure it has designated as ‘first-level’ for at least 24 hours, to ‘intermediate-level’ infrastructures for at least 12 hours, and to all other facilities for at least 4 hours.

In the specific case of the access network forming part of a mobile communications network through which publicly available electronic communications services are provided using harmonised European frequency bands, the access network must be designed and equipped with its own generating equipment and electrical supply elements that guarantee, as the ultimate objective, its operability and continuity of service for at least 4 hours for at least 75% of the population in Spain. To that end, operators may use any base stations, whether fixed or portable, together with any frequency bands and technologies they consider appropriate. They may also prioritise all those locations, centres and facilities that they deem appropriate, based on their relevance to the provision of public services and services of economic and social importance.

This ultimate objective must be achieved within three years of the entry into force of this Royal Decree and maintained thereafter. In order to achieve this ultimate objective, the access network must be designed and equipped with the appropriate power supply equipment to ensure operability and continuity of service for at least 4 hours for a minimum of 50% of the population in Spain before the end of the first year of this Royal Decree’s entry into force, and for at least 4 hours for a minimum of 65% of the population in Spain before the end of the second year of this Royal Decree’s entry into force.

An analysis has been carried out of the economic impact that this obligation could have on telecommunications operators based on information and data provided by operators and by analysing national and international references (BEREC, GSMA, Ofcom, FCC).

According to the analysis carried out by the Secretary of State for Telecommunications and Digital Infrastructure, the cost associated with the additional deployment of batteries or generating equipment for all mobile communications networks through which publicly available electronic communications services are provided using harmonised European frequency bands in Spain is between EUR 45 million and EUR 90 million, taking into account the following:



- the total number of sites to be covered (75% population coverage) is 9,200,
- The gross unit cost per site, gross (before volume discounts), is estimated to be in the range of €7,500 to €15,000. After applying volume discounts of around 33%, the cost per site falls within the range of €5,000 to €10,000, as will be explained in more detail below.

The following is an analysis of the indicated cost:

Mobile sites and population coverage

In its “Economic and Sectoral Report 2024”, published on 18 June 2025, the CNMC mentions that: *“A total of 41,867 sites have been declared in 2024 at which telecommunications operators had installed 194,443 base stations, averaging between 4 and 5 base stations per site.”*

In other words, there are at least 42,000 sites (each with at least one mobile base station) that are potential candidates for upgrading with batteries or generators to ensure an uninterrupted power supply for at least 4 hours.

On the other hand, the population of Spain (Oct 2025) was 49 million inhabitants (INE). The aim is to cover a minimum of 75% of the population. This corresponds to approximately 36.75 million people.

- On a nationwide basis, the average population served per site is: 49 million / 42,000 $\approx$ 1,167 people per site (including rural and small cells). However, this ‘average density’ across the country reflects areas with widely differing population densities.
- In densely populated areas, a coverage layer site (700/800 MHz) typically serves a significantly larger proportion of the population than the national average (due to overlapping layers and higher user density). Consequently, to reach 75% of the population with an ‘optimal’ selection of sites in densely populated areas requires a substantially smaller number of sites than $0.75 \times 41,867$.

In this respect,

- a. In Spain, approximately 82% of the population lives in urban areas (2024) ¹.
 - b. Large urban areas (>50,000 inhabitants) account for approximately 69% of the population and more than 77% of employment. Furthermore, 40.2% live in municipalities with more than 100,000 inhabitants. This makes it possible to cover a large proportion of the population with relatively few, well-chosen sites.
- To estimate the minimum number of sites required to ensure coverage for 75% of the population, a parameter of **4,000 people per site** is adopted. This hypothesis is based on

¹ <https://data.worldbank.org/indicator/SP.URB.TOTL.IN.ZS?end=2024&locations=ES&start=1960>



- (i) the strong **urban concentration** in Spain ($\approx 82\%$ in urban areas; 69% in large urban areas),
- (ii) **municipal population densities** that comfortably exceed 4–5 thousand inhabitants per square kilometre in town centres and peri-urban areas, and
- (iii) **inter-site distances** (average distance between sites) of **0.6–1.0 km** for coverage layers **<1 GHz**, documented in 3GPP/ETSI/Ofcom references². Under these conditions, the effective coverage area per *site* ($0.866 \times \text{ISD}^2$) multiplied by the typical population densities yields **PSS $\geq 4,000$** . Therefore, the value **is considered prudent and proportionate** for a scenario involving the prioritised selection of *sites*

In short, the minimum number of sites required to provide coverage for at least 4 hours to at least 75% of the population would be $36.75 \text{ M} / 4,000 \approx 9,188$ sites.

Volume discounts

Furthermore, the sector reports that the price range for batteries varies depending on the required power output – between 4.8 kW and 9.6 kW – or whether the installation is indoor or outdoor, with prices ranging from €7,500 to €15,000 per site. Considering the economies of scale that would be involved in an additional deployment: in national operations with 70–90% coverage, it is standard to negotiate multi-annual framework contracts with volume-based tiered pricing ($\geq 1,000/\geq 5,000/\geq 10,000$ units), standardise engineering and installation and optimise logistics and joint purchases (in this case, batteries and rectifiers), which structurally reduces the unit cost.

For estimation purposes, the following assumption is adopted: **an average discount of 33% on the reference unit cost (€7,500–€15,000/site)** when the procurement of energy backup solutions is organised as a joint purchase through framework agreements and phased lots between operators.

This assumption is based on:

- empirical evidence of joint procurement in the European/UK public sector, with savings of up to 3% and above in standardised categories,³
- a battery market environment characterised by price falls of around 20% year-on-year, driven by economies of scale and competition amongst suppliers, and
- the generalisation of tiered/volume pricing schemes of 25-35 % in high-volume B2B contracts. Although 'engineering' economies of scale may be conditioned by site restrictions, this does not prevent operators from capturing relevant commercial discounts on supply under a well-designed framework agreement.⁴

² https://www.etsi.org/deliver/etsi_tr/138900_138999/138901/18.00.00_60/tr_138901v180000p.pdf

³ <https://wires.onlinelibrary.wiley.com/doi/full/10.1002/wene.463>

⁴ <https://hbr.org/2020/10/what-b2b-companies-get-wrong-about-volume-discounts>



Existing infrastructure

The estimated cost of between €45 million and €90 million to be jointly incurred by mobile communications operators in ensuring service continuity for 75% of the population, including access to emergency communications services through the 112 emergency number, for at least four hours, is proportionate and balanced in relation to the intended objective of preventing the interruption of electronic communications services in emergency situations.

It should also be noted that the cost calculation is based on the number of **physical sites** and not on the number of operators present at each site or the number of base stations installed. This approximation is consistent with the reality of the Spanish market, where a very significant part of the mobile sites are shared by several operators or managed by neutral infrastructure operators (*TowerCos*), as indicated in the CNMC's Economic and Sectoral Report 2024: *'In recent years, mobile operators have signed infrastructure sharing agreements in order to reduce their deployment costs. In this regard, operators stated that they had installed base stations at 34,660 physical sites owned by another mobile operator.'*

In such cases, the backup power solution may be organised through shared power supply systems or through technical and contractual coordination arrangements between the operators present on site, so that the cost of providing an independent power supply to the *site* is not automatically multiplied by the number of operators hosting equipment there.

The obligation to ensure energy self-sufficiency for at least four hours may be met through shared solutions, managed by the site owner, by the relevant *TowerCo*, or through agreements between operators, without prejudice to each operator's responsibility to ensure the continuity of its own services.

For the Administration, there is no direct budgetary impact: supervisory, coordination and response functions can be carried out using existing structures, although marginal costs should be taken into account for incident management tools, the drafting of technical guidelines and verification/audit campaigns. No public expenditure commitments are envisaged unless a co-financing or grant scheme is set up; in that event, the budgetary impact would be as determined by the relevant regulations in the corresponding call for applications.

V.2 Impact on market unity and competition.

This Royal Decree is compatible with the principles of market unity. It does not introduce any unjustified or discriminatory barriers and, furthermore, applies objective and proportionate criteria, without distorting competition. Firstly, the obligations imposed by this Royal Decree apply to all the obliged persons listed in Article 2. Only electronic communications operators with an annual turnover of less than EUR 50 million within the same business group would be excluded.



Consequently, the exclusion of these operators does not, under any circumstances, affect competition.

As regards the obligation laid down in Article 7(4) of the Royal Decree, whereby, in the event of an interruption to the electricity supply, the access network forming part of a mobile communications network through which publicly available electronic communications services is provided using harmonised European frequency bands, must be designed and equipped with dedicated generating equipment and power supply systems capable of ensuring, as their ultimate objective, its operational capability and continuity of service for at least four hours for no less than 75% of the population in Spain, that obligation principally affects the main mobile communications operators, particularly those operating their own networks under authorisations to use radio spectrum. However, the obligations apply equally to those operators without in any case affecting competition. Moreover, those operators are the principal participants in the telecommunications sector, while smaller operators and those with lower annual turnover are not subject to these obligations.

V.3. Analysis of administrative burdens.

With regard to administrative burdens, this Royal Decree includes certain amendments to the incident reports that obliged entities are required to submit to the Secretary of State for Telecommunications and Digital Infrastructure.

Whilst, as described above, the current regulations based on the General Telecommunications Act and its implementing regulations in this area already set out the main obligations regarding the reporting of incidents to the authorities, the new obligation to report—not only at the start and end of an incident, but also at regular intervals whilst it is ongoing—represents an increase in reporting obligations. This has been calculated on the basis of statistical data on reports of service interruption incidents from previous years (based on complaints lodged in the year 2024).

Estimated burden in accordance with the Instructions for the quantification of Administrative Burdens:

(6) Submission of an electronic communication (€2) x 9,638 complaints (Estimated number of annual procedures): **EUR 19,276**

V.4 Gender impact

In accordance with the provisions of Article 26(3)(f) of Law 50/1997 of 27 November and Article 19 of Organic Law 3/2007 of 22 March on the effective equality of women and men, this Royal Decree does not give rise to any differentiated impacts on the basis of gender in the application of this regulation.



V.5 Impact on childhood and adolescence

In accordance with the provisions of Article 22 quinquies of Organic Law 1/1996 of 15 January on the Legal Protection of Minors, partially amending the Civil Code and the Civil Procedure Act, a particular piece of legislation is considered to have a positive impact on children and young people where appropriate. According to the description above, this Royal Decree has no impact on children and adolescents.

V.6 Impact on family.

This Royal Decree has no impact on family.

V.7 Impact on the environment and climate change.

The non-significant environmental impact caused by the installation of batteries is justified by the objective of ensuring the security and resilience of electronic communications networks and services.

V.8 Impact in relation to equal opportunities, non-discrimination and universal accessibility for persons with disabilities.

This Royal Decree has no direct impact on equal opportunities, non-discrimination and universal accessibility for persons with disabilities.

However, as stated in a written submission, this Royal Decree may create a resilience gap for vulnerable groups. In this regard, it is argued that the assessment of the impact of incidents should not be based solely on quantitative criteria (such as the number of users affected) but also on the criticality of the service for people with disabilities (telecare, geolocation, alarm services).

They also consider that the information provided during significant incidents should be accessible. In this regard, communications issued by operators and authorities must be compatible with screen readers, include subtitles and sign language interpretation, and be written in plain language.

V.9 Impact on health

This Royal Decree has no direct impact on health, although failure to comply with the obligations established in this Royal Decree for the routing and receipt of emergency communications via the 112 emergency number and public warnings may put people's health and lives at risk.

V.10 Impact on data protection.

This Royal Decree has no direct impact on data protection, although Articles 27 and 28 provide for cooperation in relation to incidents affecting personal data and authorisation for the transfer of personal data where this is deemed necessary.