EnCaViBS

WP 2: The NIS Directive and its transposition into national law.

Member State:

Spain

Royal Decree-Law 12/2018 of 7 September on security of networks and information systems

Important notice:

This text is an unofficial translation conducted at the SnT/ University of Luxembourg in the framework of the research project EnCaViBS.

The original legal acts which Member States notified to the European Commission as national execution measures were retrieved from official national databases. In order to focus on the core of the research project, only selected transpositions have been translated.

The translations only serve the purpose of being an information resource; there is no guarantee whatsoever that the translations correctly correspond to the original versions of the laws. Therefore, evidently, the texts have no legal value. The original, as well as the translated version of the legal acts, are available at www.encavibs.uni.lu, where additional information on the research project may be found.

This research project is funded by the Luxembourg National Research Fund (FNR), C18/IS/12639666/EnCaViBS/Cole,

https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurity-across-vital-business-sectors-encavibs/.

Fonds National de la Recherche Luxembourg

Member State: Spain

Royal Decree-Law 12/2018 of 7 September on security of networks and information systems

Official State Gazette No. 218, 8 September 2018, pages 87675 - 87696

I

The evolution of information and communication technologies, especially along with the internet development, has made information networks and systems to currently play a crucial role in our society, their reliability and security being essential aspects for the normal development of economic and social activities.

For this reason, the incidents that, by affecting networks and information systems, alter said activities, represent a serious threat, even more if they are fortuitous or if they come from deliberate actions, they can generate financial losses, undermine the confidence of the population and, in short, can cause serious damage to the economy and society, with the possibility, in the worst case scenario, of affecting one's own national security.

The transversal and interconnected character of information and communication technologies, which also characterises their threats and risks, limits the effectiveness of the measures used to counteract them when they are taken in isolation. This transversal character also runs the risk of losing effectiveness if the information security requirements are defined independently for each of the sectorial areas affected.

Therefore, it is appropriate to establish mechanisms that, with a comprehensive perspective, allow to improve protection against threats that affect information networks and systems, facilitating the coordination of actions carried out in this matter both at a national level and with neighbouring countries, in particular, within the European Union.

II

For this purpose, this royal decree-law is issued, which transposes into the Spanish legal system the (EU) Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 regarding the measures destined 1227 Royal Decree-Law 12/2018 of 7 September on the security of networks and information systems to ensure a high common level of security for networks and information systems in the Union. The Royal Decree-Law is also supported by the regulations, the incident response instruments and the existing state coordination bodies in this matter, which, together with the reasons indicated in section I, justifies that its content transcends the one of the Directive itself.

The Royal Decree-Law will apply to the entities that provide essential services for the community and depend on the networks and information systems for the development of their activity. Its area of application extends to sectors that are not expressly included in the Directive, to give this Royal Decree-Law a global approach, although its specific legislation is preserved. Additionally, in the case of network exploitation activities and the provision of electronic communications services and associated resources, as well as electronic trust services, expressly excluded from said Directive, the Royal Decree-Law will apply only in as far as critical operators are concerned.

The Royal Decree-Law will also apply to the providers of certain digital services. The (EU) Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 subjects them to a maximum harmonisation regime, equivalent to a regulation, since it is considered that its regulation at the national level would not be effective as it is intrinsically transnational in nature. The role of national authorities is therefore limited to supervising its application by providers established in their country and coordinating with the corresponding authorities in other countries of the European Union.

Following the aforementioned Directive, the Royal Decree-Law identifies the sectors in which it is necessary to guarantee the protection of networks and information systems, and establishes procedures to identify the essential services offered in said sectors, as well as the main operators that provide said services, which are, ultimately, the recipients of this Royal Decree-Law.

Operators of essential services and providers of digital services must adopt adequate measures to manage the risks that arise for the security of the networks and information systems they use, even if their management is externalised. The security obligations they assume must be proportionate to the level of risk they face and be based on a prior assessment of the same. The implementing regulations for this Royal Decree-Law may specify the security obligations required of essential service operators, including, where appropriate, the inspections to be carried out or the participation in crisis management activities and exercises.

The Royal Decree-Law also requires that operators of essential services and digital service providers notify incidents that they suffer in the networks and information services they use to provide essential and digital services, and have significant disruptive effects on the same, while providing for the notification of events or incidents that may affect essential services, but have not yet had a real adverse effect on them, and outlines the notification procedures.

The notification of incidents is part of the risk management culture that the Directive and the Royal Decree-Law promote. For this reason, the Royal Decree-Law protects the notifying entity and the personnel who report incidents that have occurred; confidential information is reserved from its disclosure to the public or to other authorities other than the one notified and the notification of incidents is allowed when its communication is not required.

The Royal Decree-Law emphasises the need to take into account European and international standards, as well as the recommendations emanating from the cooperation group and the CSIRT network (Computer Security Incident Response Team) established at a community level by the Directive, with a view on applying the best practices learned in these forums and contributing to the promotion of the internal market and the participation of our companies in it.

In order to increase its effectiveness and, at the same time, reduce the administrative and economic burdens that these obligations imply for the affected entities, this Royal Decree-Law tries to guarantee its coherence with those derived from the application of other regulations regarding information security, both of horizontal and sectoral character, and the coordination in its application with the responsible authorities in each case.

Regarding horizontal regulations, the links established with Laws 8/2011 of 28 April, which establish measures for the protection of critical infrastructures, and 36/2015 of 28 September of National Security stand out, and with Royal Decree 3/2010 of 8 January, which regulates the National Security Scheme in the area of Electronic Administration, as special regulations regarding the security of the public sector information systems.

Thus, the scope of this Royal Decree-Law approaches that of Law 8/2011 of 28 April, adding to the sectors provided by the (EU) Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 the additional strategic sectors contemplated in that Law; it is based on it in order to define the concept of «essential service», and its collegiate bodies are assigned the determination of essential services and of operators of essential services subject to this present Royal Decree-Law. Taking into account Law 36/2015 of 28 September, the National Security Council is assigned the function of acting as a point of contact with other countries of the European Union and a coordinating role of cybersecurity policy through the Strategy of National Cybersecurity.

III

The National Cybersecurity Strategy that Spain has had since 2013 sets out the priorities, objectives and appropriate measures to achieve and maintain a high level of security for networks and information systems. Said Strategy will continue to develop the institutional framework for cybersecurity that this

Royal Decree-Law outlines, made up of the competent public authorities and the reference CSIRTs, on the one hand, and public-private cooperation, on the other.

The competent authorities will exercise the surveillance functions derived from this Royal Decree-Law and will apply the sanctioning regime when appropriate. Likewise, they will promote the development of the obligations that the Royal Decree-Law imposes, in consultation with the sector and with the authorities that exercise competences by reason of the matter when they refer to specific sectors, to avoid the existence of duplicate, unnecessary or excessively expensive obligations.

CSIRTs are incident response teams that analyse risks and supervise incidents at a national scale, disseminate alerts about them, and provide solutions to mitigate their effects. The term CSIRT is the one commonly used in Europe instead of the protected term CERT (Computer Emergency Response Team), registered in the USA.

The Royal Decree-Law defines the functional scope of action of the reference CSIRTs provided in it. Said CSIRTs are the gateway for incident notifications, which will allow to quickly organise the response towards them, but the recipient of the notifications is the respective competent authority, which will take this information into account for the supervision of the operators. In any case, the operator is responsible for resolving incidents and restoring the affected information systems and networks to their ordinary functioning.

The use of a common platform for the notification of incidents is foreseen, in such a way that the operators do not have to make several notifications depending on the authority to which they should address. This platform may also be used to notify personal data security breaches according to the (EU) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 regarding the protection of natural persons regarding the processing of personal data and the free circulation of these data and by which Directive 95/46/EC is abolished.

IV

This Royal Decree-Law consists of seven titles that contain, first, the definitions of the terms that are used throughout the text, the safeguarding of essential state functions, such as national security and other general provisions. Next, in title II the form and criteria for identifying the essential services and the operators that provide them to which the Royal Decree-Law will apply are determined. The order in which they will be identified for the first time is established in the first additional provision of the Royal Decree-Law. Title III includes the strategic and institutional framework for the security of networks and information systems that has been described above. A specific precept is dedicated to cooperation between public authorities, as a pillar of an adequate exercise of the different competing competences regarding the matter.

Title IV deals with the security obligations of the operators, and it provides the preferential application of sectoral regulations that impose obligations equivalent to those provided in this Royal Decree-Law, without prejudice to the coordination exercised by the National Security Council and the duty of cooperation with the competent authorities by virtue of this Royal Decree-Law.

In title V, the most extensive, the notification of incidents is regulated and attention is paid to incidents with cross-border impact and also to the information and coordination with other States of the European Union for their management. Title VI provides the authorities of inspection and control of the competent authorities and cooperation with the national authorities of other Member States, and in title VII the infractions and sanctions of this Royal Decree-Law are classified. In this regard, the Royal Decree-Law opts for promoting the correction of the offense before its punishment, which, if it is necessary to dispense it, will be effective, proportionate, and dissuasive, according to what is ordered by the (EU) Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016.

The Royal Decree-Law closes with a final part that includes the additional and final provisions necessary to complete the regulation.

This provision has been submitted to the information procedure of technical regulations and regulations related to information society services, provided in the (EU) Directive 2015/1535 of the European Parliament and of the Council of 9 September 2015 , through which an information procedure is established, regarding technical regulations and rules related to information society services, as well as the Royal Decree 1337/1999 of 31 July, which regulates the referral of information regarding the norms and technical regulations and regulations related to the information society services. Likewise, it complies with the principles of good regulation established in article 129 of Law 39/2015 of October 1 of the Common Administrative Procedure of Public Administrations, in accordance with which Public Administrations must act in the exercise of the legislative initiative, such as the principles of necessity, effectiveness, proportionality, legal certainty, transparency and efficiency.

This Royal Decree-Law is issued by virtue of the exclusive powers attributed to the State in matters of the general telecommunications and public security regime by article 149.1.21.ª and 29.ª of the Constitution.

The Royal Decree-Law constitutes a constitutionally lawful instrument, provided that the purpose that justifies the emergency legislation, is, as our Constitutional Court has repeatedly demanded (Statements 6/1983 of 4 February, F. 5; 11/2002 of 17 January, F. 4, 137/2003 of 3 July, F. 3 and 189/2005 of 7 July, F.3), to cope with a specific situation, within the governmental objectives, which for reasons that are difficult to foresee requires immediate normative action in a shorter period of time than that required by a normal method or by the emergency procedure for the parliamentary processing of the Laws.

On the other hand, the use of the legal instrument of the Royal Decree-Law, in the present case, is also justified by the doctrine of the Constitutional Court, which, in its Sentence 1/2012 of 13 January has endorsed the concurrence of the budget authorising the extraordinary and urgent need of Article 86.1 of the Constitution, when there is a delay in the transposition of directives.

In effect, the deadline for transposition of the aforementioned (EU) Directive 2016/1148, of the European Parliament and of the Council of 6 July 2016 has already expired on 9 May 2018. The end of the transposition period of this Directive has motivated the initiation by the European Commission of a formal infringement procedure No. 2018/168.

Consequently, it is understood that in the ensemble and in each of the measures adopted by means of the projected Royal Decree-Law, the circumstances of extraordinary and urgent necessity that are required by Article 86 of the Constitution concur, due to their nature and purpose, as enabling budgets for the approval of a Royal Decree-Law.

By virtue, making use of the authorisation contained in Article 86 of the Spanish Constitution, at the proposal of the Vice President of the Government and Minister of the Presidency, Relations with the Courts and Equality, the Ministry of Internal Affairs and the Minister of Economy and Business and after deliberation by the Council of Ministers, at its meeting on 7 September 2018,

IT IS ORDERED:

TITLE I

General provisions

Section 1. Subject Matter.

1. The purpose of this Royal Decree-Law is to regulate the security of the networks and information systems used for the provision of essential services and digital services, and to establish an incident notification system.

2. Likewise, it establishes an institutional framework for the application of this Royal Decree-Law and the coordination between competent authorities and with the relevant cooperation bodies at the community level.

Section 2. Scope of application.

1. This Royal Decree-Law shall apply to the provision of:

a) The essential services dependent on the networks and information systems included in the strategic sectors defined in the annex to Law 8/2011, of 28 April, through which measures are established for the protection of critical infrastructures.

b) Digital services, considered compliant as determined in section 3 e), which are online markets, online search engines and cloud computing services.

2. The following will be subject to this Royal Decree-Law:

a) Operators of essential services established in Spain. It will be understood that an essential services operator is established in Spain when its residence or registered office is within Spanish territory, provided that these coincide with the place where the administrative management and the management of its businesses or activities are effectively centralised.

   Likewise, this Royal Decree-Law will apply to essential services that resident or domiciled operators in another State offer through a permanent establishment located in Spain.

b) Digital service providers that have their registered office in Spain and that constitute their main establishment in the European Union, as well as those that, not being established in the European Union, designate in Spain their representative in the Union for the compliance of the (EU) Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to guarantee a high common level of security for networks and information systems within the Union.

3. This Royal Decree-Law will not apply to:

a) Operators of electronic communications networks and services and trusted electronic service providers that are not designated as critical operators by virtue of Law 8/2011 of 28 April.

b) Digital service providers in the case of micro or small companies, in accordance with the definitions contained in Commission Recommendation 2003/361/EC of 6 May 2003 regarding the definition of micro, small and medium enterprises.

Section 3. Definitions.

For the purposes of this Royal Decree-Law, the following will be understood:

a) Networks and information systems, any of the following elements:

   1st. Electronic communications networks, exactly as defined in number 31 of annex II of Law 9/2014 of 9 May on General Telecommunications;

   2nd. Any device or group of devices interconnected or related to each other, in which one or more of them perform, through a program, the automatic processing of digital data;

   3rd. The digital data stored, processed, recovered or transmitted through the elements described in numbers 1 and 2 above, including those necessary for the functioning, usage, protection and maintenance of said elements.

b) Security of networks and information systems: the capacity of networks and information systems to withstand, with a certain level of reliability, any action that compromises the availability, authenticity, integrity or confidentiality of the data stored, transmitted or processed, or the corresponding services offered by such networks and information systems or accessible through them.

c) Essential service: service necessary for the maintenance of basic social functions, health, security, social and economic well-being of the citizens, or the effective functioning of State Institutions and Public Administrations, which depends for their provision of networks and information systems.

d) Essential services operator: public or private entity that is identified considering the factors established in section 6 of this Royal Decree-Law, that provides said services in any of the strategic sectors defined in the annex to Law 8/2011of 28 April.

e) Digital service: information society service understood in the sense set forth in letter a) of the annex to Law 34/2002 of 11 July, regarding information society services and electronic commerce.

f) Digital service provider: legal entity that provides a digital service.

g) Risk: any reasonably identifiable circumstance or fact that has a possible adverse effect on the security of networks and information systems. It can be quantified as the probability of materialisation of a threat that produces an impact in terms of operability, physical integrity of people or material or image.

h) Incident: unexpected or unwanted event with consequences to the detriment of the security of networks and information systems.

i) Incident management: procedures followed to detect, analyse and limit an incident and respond to it.

j) Representative: natural or legal person established in the European Union who has been expressly designated to act on behalf of a digital service provider not established in the European Union, to whom, in substitution of the digital service provider, a national competent authority or a CSIRT, in relation to the obligations that, by virtue of this Royal Decree-Law, the digital service provider has.

k) Technical standard: a standard within the meaning of Article 2.1 of the (EU) Regulation No. 1025/2012 of the European Parliament and of the Council of 25 October 2012 regarding European standardisation.

l) Specification: a technical specification within the meaning of Article 2.4 of the (EU) Regulation No. 1025/2012 of the European Parliament and of the Council of 25 October 2012.

m) Internet Exchange Point («IXP»): a network installation that allows more than two independent autonomous systems to be interconnected, mainly to facilitate the exchange of Internet traffic. An IXP allows autonomous systems to be interconnected without requiring Internet traffic passing between any pair of participating autonomous systems to pass through a third autonomous system, and without modifying or otherwise interfering with such traffic.

n) Domain Name System («DNS»): a hierarchically distributed system that responds to queries by providing information associated with domain names, in particular, related to the identifiers used to locate and address computers on the Internet.

o) DNS service provider: entity that provides DNS services on the Internet.

p) First-level domain name register: entity that manages and directs the register of Internet domain names in a specific first-level domain.

q) Online market: digital service that allows consumers and entrepreneurs, as defined respectively in sections 3 and 4 of the consolidated text of the General Law for the Defense of Consumers and Users and other complementary Laws, approved through the Royal Legislative Decree 1/2007 of 16 November, enter into contracts for the sale or provision of online services with entrepreneurs, either on a specific website of the online market service, or on a website of an entrepreneur who uses computer services provided for this purpose by the provider of the online market service.

r) Online search engine: digital service that allows users to search, in principle, all websites or of websites in a specific language, by means of a query on a topic in the form of a keyword, phrase

or another type of entry, and that, in response, shows links in which information related to the requested content can be found.

s) Cloud computing service: digital service that enables access to a modular and elastic set of computing resources that can be shared.

Section 4. Community guidelines and orientations.

In the application of this Royal Decree-Law and in the preparation of the regulations and guides provided in it, the acts of implementation of the (EU) Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016, as well as all the recommendations and guidelines emanating from the cooperation group established by Article 11 of the aforementioned Directive, and the information regarding good practices compiled by said group and the CSIRT network, regulated in Article 12 thereof.

Section 5. Safeguarding essential state functions.

The provisions of this Royal Decree-Law shall be understood without prejudice to the actions taken to safeguard national security and essential state functions, including those aimed at protecting classified information or whose disclosure is contrary to the essential interests of the State, or those that have as purpose the maintenance of public order, the detection, investigation and prosecution of crimes, and the prosecution of their perpetrators.

TITLE II

Essential services and digital services

Section 6. Identification of essential services and operators of essential services.

1. The identification of essential services and operators that provide them will be carried out by the bodies and procedures provided for by Law 8/2011 of 28 April and its implementing regulations. The relation between essential services and the operators of said services will be updated, for each sector, on a biennial basis, in conjunction with the review of the sectoral strategic plans provided in Law 8/2011 of 28 April.

An operator will be identified as an essential service operator if an incident suffered by the operator may have significant disruptive effects on the provision of the service, for which at least the following factors will be taken into account:

a) In relation to the importance of the service provided:

   1st.The availability of alternatives to maintain a sufficient level of essential service provision;

   2nd.The assessment of the impact of an incident on the provision of the service, evaluating the extension or geographical areas that could be affected by the incident; the dependence of other strategic sectors regarding the essential service offered by the entity and the impact, in terms of degree and duration, of the incident in economic and social activities or public safety.

b) In relation to the clients of the evaluated entity:

   1st. The number of users who trust the services provided by it;

   2nd. Its market share.

By regulation, sector-specific factors may be added to determine whether an incident could have significant disruptive effects.

2. In the case of a critical operator designated in compliance with Law 8/2011 of 28 April, it will be enough to verify its dependence on the networks and information systems for the provision of the essential service in question.

3. In identifying the essential services and operators of essential services, the pertinent recommendations adopted by the cooperation group will be taken into consideration to the greatest extent possible.

4. When an operator of essential services offers services in other Member States of the European Union, the single contact points of said states will be informed of the intention to identify it as an operator of essential services.

Section 7. Communication of activity by the digital service providers.

The digital service providers indicated in section 2 must communicate their activity to the competent authority within a period of three months from when they start it, for the sole purpose of their knowledge.

TITLE III

Strategic and institutional framework

Section 8. Strategic framework for the security of networks and information systems.

The National Cybersecurity Strategy, under and aligned with the National Security Strategy, frames the objectives and measures to achieve and maintain a high level of security for networks and information systems.

The National Cybersecurity Strategy will address, among other issues, those established in Article 7 of the (EU) Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016.

Thus, the National Security Council will promote the review of the National Cybersecurity Strategy, in accordance with the provisions of Article 21.1 e) of Law 36/2015 of 28 September on National Security.

Section 9. Competent authorities.

1. The following are competent authorities for the security of networks and information systems:

a) For the operators of essential services:

   1st. In the event that these are also designated as critical operators in accordance with Law 8/2011 of 28 April, and its implementing regulations, regardless of the strategic sector in which such designation is made: the Secretary of State for Security, from the Ministry of Internal Affairs, through the National Centre for the Protection of Infrastructures and Cybersecurity (NCPIC).

   2nd. In the event that they are not critical operators: the corresponding sectoral authority by reason of the matter, as determined by regulation.

b) For digital service providers: the Secretary of State for Digital Advancement, of the Ministry of Economy and Business.

c) For the operators of essential services and digital service providers that are not critical operators and fall within the scope of Law 40/2015 of 1st October, on the Legal Regime of the Public Sector: the Ministry of Defense, through the National Cryptological Centre.

2. The National Security Council, through its specialised committee on cybersecurity, will establish the necessary mechanisms for the coordination of the actions of the competent authorities.

Section 10. Functions of the competent authorities.

The competent authorities shall exercise the following functions:

a) Supervising the compliance of essential service operators and digital service providers to the obligations that are determined, in accordance with those established in title VI.

b) Establishing timely communication channels with essential service operators and with digital service providers that, where appropriate, will be developed in a regulated manner.

c) Coordinating with the reference CSIRTs through the action protocols that, depending on the case, will be developed in a regulated manner.

d) Receiving notifications about incidents that are presented within the framework of this Royal Decree-Law, through the reference CSIRTs, in accordance with the provisions of title V.

e) To inform the unique point of contact about the notifications of incidents presented within the framework of this Royal Decree-Law, in accordance with the provisions of section 27.

f) To inform, where appropriate, the public about certain incidents, when the dissemination of said information is necessary to avoid an incident or manage one that has already occurred, in accordance with the provisions of section 26.

g) Cooperating, within the scope of this Royal Decree-Law, with the competent authorities in matters of personal data protection, public security, citizen security and national security, as well as with the corresponding sector authorities, in accordance with the established in sections 14 and 29.

h) To establish specific obligations in order to guarantee the security of networks and information systems and on incident notification, and issue technical instructions and guides to detail the content of said obligations, in accordance with the provisions of sections 16 and 19.

i) Exercising the sanctioning power in the cases provided for in this Royal Decree-Law, in accordance with the provisions of title VII.

j) Promoting the use of standards and technical specifications, in accordance with the provisions of section 17.

k) Cooperating with the competent authorities of other Member States of the European Union in the identification of operators of essential services between entities that offer such services in several Member States.

l) To inform the unique point of contact about incidents that may affect other Member States, in the terms provided in section 25.

Section 11. Reference computer security incident response teams.

1. The following are computer security incident response teams (CSIRT) of reference in matters of network and information systems security:

a) Regarding the relations with the essential service operators:

1st. The CCN-CERT, of the National Cryptological Centre, which corresponds to the reference community constituted by the entities of the subjective scope of application of Law 40/2015 of 1 October.

2nd. The INCIBE-CERT, of the National Institute of Cybersecurity of Spain, to which corresponds the reference community constituted by those entities not included in the subjective scope of application of Law 40/2015 of 1 October. The INCIBE-CERT will be operated jointly by the INCIBE and the CNPIC in everything that refers to the management of incidents that affect critical operators.

3rd. The ESPDEF-CERT, of the Ministry of Defense, which will cooperate with the CCN-CERT and the INCIBE-CERT in those situations that they require in support of the operators of essential services and, necessarily, in those operators that have an impact on National Defense and that are determined in a regulated manner.

b) Regarding the relationships with digital service providers that are not included in the CCN-CERT reference community: the INCIBE-CERT.

The INCIBE-CERT will also be itself a reference incident response team for citizens, private legal entities and other entities not previously included in this section 1.

1. The reference CSIRTs will coordinate with each other and with the rest of the national and international CSIRTs in responding to incidents and managing security risks that correspond to them. In the cases of special gravity that are determined by regulation and that require a level of coordination higher than what is necessary in ordinary situations, the CCN-CERT will exercise the national coordination of the technical response of the CSIRTs.

When the activities they carry out may affect a critical operator in any way, the reference CSIRTs will coordinate with the Ministry of the Interior, through the Cybernetic Coordination Office of the National Centre for the Protection of Infrastructures and Cybersecurity (CNPIC), of the form that is determined in a regulated manner.

Section 12. Requirements and functions of the reference CSIRTs.

1. CSIRTs must meet the following requirements:

a) They will guarantee a high level of availability of their communications services avoiding occasional failures and will have various means by which they can be contacted and can contact others at all times. Furthermore, the communication channels will be clearly specified and will be well known to user groups and collaborating partners.

b) Its facilities and those of the support information systems will be located in safe places.

c) They guarantee the continuity of activities. For that:

1st. They will be equipped with an adequate system to manage and channel requests in order to facilitate transfers.

2nd. They will have enough staff to guarantee their availability at all times.

3rd. They will have access to communication infrastructures whose continuity is assured.

For this purpose, they will have redundant systems and reserve workspaces.

d) They must have the ability to participate, when they wish, in international cooperation networks.

2. CSIRTs will perform, as a minimum, the following functions:

a) Monitor incidents at a national scale.

b) Disseminate early warnings, alerts, notices and information on risks and incidents among the interested parties.

c) Respond to incidents.

d) Carry out a dynamic analysis of risks and incidents and knowledge of the situation.

e) Participate in the CSIRT network.

2. CSIRTs will establish cooperative relationships with the private sector. In order to facilitate cooperation, CSIRTs will encourage the adoption and use of common or standard practices of:

a) Incident and risk management procedures.

b) Incident, risk and information classification systems.

Section 13. Unique point of contact.

The National Security Council will exercise, through the Department of National Security, a linking function to ensure cross-border cooperation of the competent authorities designated in accordance with section 9, with the competent authorities of other Member States of the European Union, as well as with the cooperation group and the CSIRT network.

Section 14. Cooperation with other authorities with competences in information security and with sectoral authorities.

1. The competent authorities, the reference CSIRTs and the single point of contact will consult, where appropriate, with the bodies with powers in matters of national security, public security, citizen security and protection of personal data and will collaborate with them in the exercise of their respective functions.

2. They will also consult, when appropriate, with the bodies with competences by reason of the matter in each of the sectors included in the scope of application of this Royal Decree-Law, and will collaborate with them in the exercise of their functions.

3. When the reported incidents present criminal characters, the competent authorities and the reference CSIRTs will report it, through the Office of Cybernetic Coordination of the Ministry of Internal Affairs, to the Public Prosecutor for the appropriate purposes, transferring at the time how much information they have in relation to it.

Section 15. Confidentiality of sensitive information.

Without prejudice to the provisions of section 5, the competent authorities, the reference CSIRTs and the single point of contact shall preserve, as appropriate in law, the security and commercial interests of essential service operators and digital service providers, as well as the confidentiality of the information they collect from them in the exercise of the functions entrusted to them by this current Royal Decree-Law.

When it is necessary, the exchange of sensitive information will be limited to that which is relevant and proportionate for the purpose of said exchange.

TITLE IV

Safety obligations

Section 16. Safety obligations of the essential service operators and digital service providers.

1. Operators of essential services and providers of digital services must adopt technical and organisational measures, adequate and proportionate, in order to manage the risks that arise for the security of the networks and information systems used in the provision of the services subject to this Royal Decree-Law.

Without prejudice to their duty to report incidents under title V, they must take adequate measures to prevent and minimise the impact of incidents that affect them.

2. The regulatory development of this Royal Decree-Law will provide the necessary measures for compliance with the provisions of the previous section by the operators of essential services.

3. Operators of essential services will designate and communicate to the competent authority, within the period established by regulation, the person, unit or collegiate body responsible for the security of the information, as a point of contact and technical coordination with it. Its specific functions will be those provided in a regulated manner.

4. The competent authorities may establish by ministerial order specific obligations to guarantee the security of the networks and information systems used by the operators of essential services. Likewise, they may issue technical instructions and guidance guides to detail the content of said orders.

When elaborating the regulatory provisions, instructions and guides, they will take into account the sectorial obligations, the relevant guidelines that are adopted in the cooperation group and the information security requirements, to which the operator is subject by virtue of other regulations, such as Law 8/2011of 28 April, and the National Security Scheme, approved by Royal Decree 3/2010 of 8 January.

5. The competent authorities must coordinate with each other and with the different sectoral bodies with competences by reason of the matter, with regard to the content and application of the orders, technical instructions and guides that they issue in their respective fields of competence, in order to avoid duplications of the required obligations and facilitate their fulfilment by the operators of essential services.

6. Digital service providers will determine the security measures they will apply, taking into account, as a minimum, technical advances and the following aspects:

a) The security of the systems and facilities;

b) Incident management;

c) The management of the continuity of the activities;

d) Supervision, audits and tests;

e) Compliance with international standards. Digital service providers will also attend to the implementing acts by which the European Commission details the aforementioned aspects.

Section 17. Technical standards.

The competent authorities will promote the use of regulations, standards or technical specifications regarding the security of networks and information systems drawn up within the framework of the (EU) Regulation 1025/2012 of the European Parliament and of the Council of 25 October 2012 on the European standardisation.

In the absence of said standards or specifications, they will promote the application of the international standards or recommendations approved by international standardisation bodies, and, where appropriate, of the standards and technical specifications accepted at the European or international level that are relevant in this matter.

Section 18. Sectors with equivalent specific regulations.

When a national or community regulation establishes for a sector security obligations for networks and information systems or for the notification of incidents that have effects, at least equivalent to those of the obligations provided in this Royal Decree-Law, those requirements and the corresponding supervision mechanisms will prevail.

This will not affect the duty of cooperation between the competent authorities, the coordination exercised by the National Security Council or, insofar as it is not incompatible with sector legislation, the application of title V on incident notification.

TITLE V

Incident notification

Section 19. Obligation to notify.

1. Operators of essential services shall notify the competent authority, through the reference CSIRT, of incidents that may have significant disruptive effects on said services.

Notifications may also refer, as determined by regulation, to events or incidents that may affect the networks and information systems used for the provision of essential services, but that have not yet had a real adverse effect on them.

2. Likewise, digital service providers will notify the competent authority, through the reference CSIRT, of incidents that have significant disruptive effects on said services.

The obligation to notify the incident will only apply when the digital service provider has access to the information necessary to assess the impact of an incident.

3. The notifications from both essential service operators and digital service providers will refer to incidents that affect the networks and information systems used in the provision of the indicated services, whether it is their own networks and services or if they are coming from external providers, even if they are digital service providers subject to this Royal Decree-Law.

4. The competent authorities and the reference CSIRTs will use a common platform to facilitate and automate the processes of notification, communication and information regarding incidents.

5. The regulatory development of this Royal Decree-Law will provide the necessary measures for compliance with the provisions of this section by the operators of essential services. The competent authorities may establish, by ministerial order, specific notification obligations from the operators of essential services. Likewise, they may issue technical instructions and guidance guides to detail the content of said orders.

When elaborating the regulatory provisions, instructions and guides, the sectoral obligations, the relevant guidelines adopted in the cooperation group and the requirements regarding the notification of incidents to which the operator is subject by virtue of other regulations will be taken into account, such as Law 8/2011 of 28 April and the National Security Scheme, approved by Royal Decree 3/2010 of 8 January.

6. The obligation to notify incidents set forth in the preceding paragraphs does not prevent the fulfilment of the legal duties of reporting those events that have the character of a crime before the competent authorities, in accordance with the provisions of Articles 259 and the following ones from the Criminal Procedure Law and taking into account the provisions of section 14.3 of this Royal Decree-Law.

Section 20. Notifier protection.

1. The notifications considered in this title will not subject the entity that makes them to a greater responsibility.

2. Employees and personnel who, due to any type of labour or commercial relationship, participate in the provision of essential or digital services, who report incidents may not suffer adverse consequences at their job or with the company, except in the cases in which their actions are considered being done in bad faith.

Employer decisions taken to the damage or detriment of the labour rights of the workers who have acted in accordance with this section shall be deemed null and void and without legal effect.

Section 21. Factors to determine the importance of the effects of an incident.

1. For the purposes of the notifications referred to in section 19.1, first paragraph, the importance of an incident will be determined taking into account, at least, the following factors:

a) The number of users affected by the disruption of the essential service.

b) The duration of the incident.

c) The extension or geographic areas affected by the incident.

d) The degree of disturbance in the operation of the service.

e) The extent of the impact on crucial economic and social activities.

f) The importance of the systems affected or of the information affected by the incident for providing the essential service.

g) Damage to reputation.

2. In the notifications referred to in section 19.2, the importance of an incident will be determined in accordance with the provisions of the implementing acts provided for in paragraphs 8 and 9 of Article 16 of the (EU) Directive 2016/1148 of the European Parliament and of the Council, of 6 July 2016.

Section 22. Initial notification, intermediate notifications and final notification.

1. The operators of essential services must make a first notification of the incidents referred to in section 19.1 without undue delay.

The notification will include, among other data, information that makes it possible to determine any cross-border effects of the incident.

2. The operators of essential services will carry out the intermediate notifications that are necessary to update the information included in the initial notification and report on the evolution of the incident, while it is not resolved.

3. The essential service operators will send a final notification of the incident after its resolution. An incident will be considered resolved when the affected networks and information systems have been restored and the service is operating normally.

Section 23. Flexibility in observing deadlines for the notification.

Operators of essential services and digital service providers may omit, in the communications they make about incidents that affect them, the information that they do not yet have regarding their impact on essential services or other services that depend on them for their provision, or other information that they do not have. As soon as they know this information, they must send it to the competent authority.

If, after a reasonable period of time from the initial notification of the incident, the operator of essential services or the provider of digital services has not been able to gather the relevant information, he will send to the competent authority, without delay, a report justifying the actions taken to collect the information and the reasons why it has not been possible to obtain it.

Section 24. Incidents that affect digital services.

Operators of essential services and digital service providers subject to this Royal Decree-Law, as well as any other interested party, who have knowledge regarding incidents that significantly affect digital services offered in Spain by providers established in other Member States of the European Union, may

notify the competent authority by providing the relevant information, in order to facilitate cooperation with the Member State in which the aforementioned provider is established.

Similarly, if they have news that said providers have failed to comply with the applicable security or incident notification requirements in Spain, they may notify the competent authority by providing the relevant information.

Section 25. Processing of incidents with a cross-border impact.

1. When the competent authorities or the reference CSIRTs have news of incidents that may affect other Member States of the European Union, they will inform the affected Member States through the single point of contact, specifying whether the incident may have significant disturbing effects on the essential services provided in those States.

2. When information is received through said contact point about incidents reported in other countries of the European Union that may have significant disruptive effects for the essential services provided in Spain, the relevant information will be sent to the competent authority and the reference CSIRT, so that they adopt the pertinent measures in the exercise of their respective functions.

3. The actions considered in the previous sections are understood without prejudice to the exchanges of information that the competent authorities or the reference CSIRTs may carry out directly with their counterparts from other Member States of the European Union in relation to incidents that may result from mutual interest.

Section 26. Information to the public.

1. The competent authority may require essential service operators or digital service providers to inform the public or potentially interested third parties about the incidents when their knowledge is necessary in order to avoid new incidents or manage one that has already occurred, or when the disclosure of an incident is in the public interest.

2. The competent authority may also decide to directly inform the public or third parties about the incident.

In these cases, the competent authority will consult and coordinate with the essential services operator or digital service provider before informing the public.

Section 27. Annual information to the single point of contact and the cooperation group.

1. The competent authorities shall transmit to the unique point of contact an annual report on the number and type of reported incidents, their effects on the services provided or on other services and their national or cross-border nature within the European Union.

The competent authorities will prepare the report following the instructions issued by the unique point of contact, taking into account the indications of the cooperation group regarding the format and content of the information to be transmitted.

2. The unique point of contact will send the cooperation group before 9 August of each year a summary annual report on the notifications received and will subsequently send it to the competent authorities and the reference CSIRTs, for their information.

Section 28. Obligation to resolve incidents, information and mutual collaboration.

1. The operators of essential services and digital service providers have the obligation to resolve security incidents that affect them, and to request specialised help, including that of the reference CSIRT, when they cannot resolve the incidents themselves.

In such cases, they must attend to the instructions they receive from the reference CSIRT to resolve the incident, mitigate its effects, and replace the affected systems.

2. The operators of essential services and providers of digital services must provide the reference CSIRT and to the competent authority with all the information required for the performance of the functions entrusted to them through this present Royal Decree-Law.

In particular, additional information may be required from essential service operators and digital service providers to analyse the nature, causes and effects of the reported incidents, and to compile statistics and gather the necessary data to prepare the annual reports considered in section 27.

When circumstances allow it, the competent authority or the reference CSIRT will provide essential service operators or digital service providers affected by incidents with the information derived from their follow-up that may be relevant to them, in particular, to resolve the incident.

Section 29. Cooperation regarding incidents that affect personal data.

The competent authorities and the reference CSIRTs will cooperate closely with the Spanish Data Protection Agency to deal with incidents that give rise to breaches of personal data.

The competent authorities and the reference CSIRTs will notify without delay the Spanish Agency for Data Protection regarding incidents that may involve a violation of personal data and will keep it informed about the evolution of such incidents.

Section 30. Authorisation for the transfer of personal data.

If the notification of incidents or their management, analysis or resolution requires the communication of personal data, its treatment will be restricted to those that are strictly adequate, pertinent and limited to what is necessary in relation to the purpose, of those indicated, that is pursued in each case.

Its assignment for these purposes will be understood as authorised in the following cases:

a) From essential service operators and digital service providers to the competent authorities, through the reference CSIRTs.

b) Between the reference CSIRTs and the competent authorities, and vice versa.

c) Between the reference CSIRTs, and between these and the designated CSIRTs in other Member States of the European Union.

d) Between the reference CSIRTs and other national or international CSIRTs.

e) Between the unique contact point and the unique contact points of other Member States of the European Union.

Section 31. Voluntary notifications.

1. The operators of essential services and the providers of digital services may report incidents for which no notification obligation will be established.

Likewise, entities that provide essential services and have not been identified as essential service operators and that are not digital service providers may report the incidents that affect said services.

These notifications oblige the entity that makes them to resolve the incident in accordance with the provisions of section 28.

2. The notifications referred to in the preceding section shall be governed by the provisions of this title, and the sole contact point shall be informed about them in the annual report provided for in section 27.1.

3. Mandatory notifications will have priority over voluntary notifications for the purposes of their management by the CSIRTs and by the competent authorities.

TITLE VI

Supervision

Section 32. The supervision of operators of essential services.

1. The competent authorities may require operators of essential services to provide them with all the information necessary to assess the security of networks and information systems, including documentation regarding security policies.

They may request information about the effective application of their security policy, as well as audit or require the operator to submit the security of their networks and information systems to an audit by an external, solvent and independent entity.

2. In view of the information collected, the competent authority may require the operator to correct the deficiencies detected and indicate how it should be done.

Section 33. The supervision of digital service providers.

1. The competent authority for the supervision of digital services will only inspect compliance with the obligations derived from this Royal Decree-Law when it becomes aware of any breach, including by reasoned request from other bodies or by a complaint.

In this case, the competent authority may require the digital service provider to provide it with all the information necessary to assess the security of its networks and information systems, including documentation on security policies, and to correct the deficiencies detected.

2. When the competent authority has news of incidents that significantly disturb digital services offered in other Member States by providers established in Spain, it will adopt the pertinent supervisory measures. For these purposes, it shall take particular account of the information provided by the competent authorities of other Member States.

Section 34. Cross-border cooperation.

1. The supervision will be carried out, where the case may be, in cooperation with the competent authorities of the Member States in which the networks and information systems used for the provision of the service are located, or in which the operator of essential services is based, the digital service provider or its representative.

2. The competent authorities will collaborate with the competent authorities of other Member States when they require their cooperation in the supervision and adoption of measures by operators of essential services and providers of digital services in relation to networks and information systems located in Spain, as well as regarding digital service providers established in Spain or whose representative in the European Union has their residence or registered office in Spain.

TITLE VII

Sanctions regime

Section 35. Responsibles.

Operators of essential services and providers of digital services included in the scope of this Royal Decree-Law will be considered responsible.

Section 36. Infringements.

1. Violations of the precepts of this Royal Decree-Law are classified as very serious, serious and minor.

2. Very serious infringements are:

a) Failure to adopt measures to correct the deficiencies detected, in accordance with the provisions of sections 32.2 or 33.1, when these have made it vulnerable to an incident with significant disruptive effects on the service and the operator of essential services or the digital service provider would not have met the requirements dictated by the competent authority prior to when the incident occurred.

b) Repeated failure to comply with the obligation to report incidents with significant disruptive effects on the service. It will be considered repeated starting from the second breach.

c) Failure to take the necessary measures to resolve incidents in accordance with the provisions of section 28.1 when they have a significant disruptive effect on the provision of essential services or digital services in Spain or in other Member States.

3. Serious infringements are:

a) Failure to comply with the regulatory provisions or the technical security instructions issued by the competent authority regarding the minimum precautions that the essential service operators must adopt in order to guarantee the security of networks and information systems.

b) Failure to adopt measures to correct deficiencies detected in response to a requirement issued in accordance with sections 32.2 or 33.1, when that is the third neglected requirement issued in the last five years.

c) Failure to comply with the obligation to report incidents with significant disruptive effects on the service.

d) The demonstration of a notorious lack of interest in solving incidents with significant disruptive effects reported when they lead to further degradation of the service.

e) Provide false or misleading information to the public about the standards that it meets or the security certifications that it maintains in force.

f) Adding obstacles to the performance of audits by the competent authority.

4. Minor infringements are:

a) Failure to comply with the regulatory provisions or technical safety instructions issued by the competent authority under this Royal Decree-Law, when it does not involve a serious offense.

b) Failure to adopt measures to correct deficiencies detected in response to a request for correction issued in accordance with sections 32.2 or 33.1.

c) Failure to provide the information required by the competent authorities regarding their security policies, or provide incomplete or late information without justification.

d) Failure to submit to a security audit as ordered by the competent authority.

e) Failure to provide the reference CSIRT or the competent authority with the information requested by virtue of section 28.2.

f) Lack of notification of events or incidents for which, although they have not had a real adverse effect on the services, there is an obligation to notify by virtue of the second paragraph of section 19.2.

g) Failure to complete the information that must be gathered in the notification of incidents, taking into account the provisions of section 23, or failure to send the supporting report on the impossibility of gathering the information provided for in said section.

h) Failure to follow the instructions received from the reference CSIRT to resolve an incident, in accordance with section 28.

Section 37. Sanctions.

1. For the commission of the infractions included in the previous section, the following sanctions will be imposed:

a) For committing very serious offenses, a fine of 500,001 up to 1,000,000 euros.

b) For committing serious offenses, a fine of 100,001 up to 500,000 euros.

c) For committing minor offenses, a warning or a fine up to 100,000 euros.

2. The final administrative sanctions for very serious and serious infractions may be published, at the expense of the sanctioned, in the "Official State Gazette" and on the website of the competent authority, in attention to the concurrent facts and in accordance with the next section.

Section 38. Grading of the amount of penalties.

The sanctioning body will establish the sanction taking into account the following criteria:

a) The degree of guilt or the existence of intent.

b) The continuity or persistence in the offending conduct.

c) The nature and amount of the damages caused.

d) The recidivism, by committing in the last year of more than one offense of the same nature, when this has been declared by a firm resolution in administrative proceedings.

e) The number of affected users.

f) The volume of billing of the person in charge.

g) The use by the person in charge of reward programs for the discovery of vulnerabilities in their networks and information systems.

h) The actions taken by the person in charge to alleviate the effects or consequences of the infringement.

Section 39. Proportionality of sanctions.

1. The sanctioning body may establish the amount of the sanction by applying the scale relative to the class of offenses that immediately precedes the one in which the one considered in the case in question is integrated, in the following cases:

a) When there is a qualified decrease in the guilt of the accused as a consequence of the significant concurrence of several of the criteria set forth in section 38.

b) When the offending entity has diligently regularised the irregular situation.

c) When the offender has spontaneously acknowledged his guilt.

2. The bodies with sanctioning competence, taking into account the nature of the facts and the significant concurrence of the criteria established in the previous section, may not agree on the initiation of the sanctioning procedure and, instead, warn the responsible subject so that, in the term that the sanctioning body determines, certifies the adoption of the corrective measures that, in each case, are pertinent, provided that the following assumptions concur:

a) That the facts constitute a minor or serious infringement in accordance with the provisions of this Royal Decree-Law.

b) That the competent body had not sanctioned or warned the offender in the previous two years as a result of the commission of infractions provided for in this Royal Decree-Law.

If the warning is not attended within the period that the sanctioning body has determined, the corresponding sanctioning procedure for said non-compliance will proceed.

3. The minor offenses described in section 36.4 c), d) and e) and the serious offense provided for in section 36.3 e) may not be subject to warning.

Section 40. Infringements of public administrations.

1. When the offenses referred to in section 36 were committed by bodies or entities of the Public Administrations, the sanctioning body shall issue a resolution establishing the measures to be adopted to cease or correct the effects of the offense. This resolution will be notified to the offending body or entity and to those affected, if any.

In addition to the above, the sanctioning body may also propose the initiation of disciplinary actions, if applicable.

2. The resolutions that fall in relation to the measures and actions referred to in the previous section must be communicated to the sanctioning body.

Section 41. Sanctioning capacity.

1. The imposition of sanctions will correspond, in the case of very serious infractions, to the competent Minister by virtue of the provisions of section 9, and in the case of serious and minor infractions to the body of the competent authority that is determined by the regulations for the development of this Royal Decree-Law.

2. The sanctioning power will be exercised in accordance with the principles and procedure set forth in Laws 39/2015 of 1st October of the Common Administrative Procedure of Public Administrations, and 40/2015 of 1st October of the Legal Regime of the Public Sector.

3. The exercise of the sanctioning power will be subject to the applicable procedure, in general, to the actions of public administrations. However, the maximum duration of the procedure will be one year and the period for allegations will not last less than one month.

Section 42. Concurrence of offenses.

1. The imposition of sanctions as provided in this Royal Decree-Law will not proceed when the acts constituting the infringement are also included in another typified in the sectoral regulations to which the service provider is subject and there is an identity of the protected legal asset.

2. When, as a consequence of a sanctioning action, there is knowledge of facts that could constitute infractions typified in other laws, they will be reported to the competent bodies or agencies for their supervision and sanction.

First additional provision. Initial relationship of essential services and essential service operators.

The National Commission for the Protection of Critical Infrastructures will approve a first list of essential services within the sectors included in the area of application of this Royal Decree-Law and will identify the operators that provide them that must be subject to this Royal Decree-Law in the following order:

a) Before 9 November 2018: essential services and operators corresponding to the strategic sectors of energy, transport, health, financial system, water, and digital infrastructures.

b) Before 9 November 2019: essential services and operators corresponding to the rest of the strategic sectors included in the annex to Law 8/2011 of 28 April.

Second additional provision. Electronic communications and trusted services.

The application of this Royal Decree-Law to the operators of networks and electronic communication services and electronic trusted services that are designated as critical operators by virtue of Law 8/2011 of 28 April will not prevent the application of its specific safety regulations.

The Ministry of Economy and Business, as the competent body for the application of said regulations, and the Ministry of Internal Affairs will act in a coordinated manner in the establishment of obligations that fall on critical operators. Thus, they will maintain a fluid exchange of information regarding incidents that affect them.

Third additional provision. Notification of personal data security violations through the common platform provided for in this Royal Decree-Law.

The common platform for the notification of incidents provided for in this Royal Decree-Law may be used for the notification of breaches of the security of personal data according to the (EU) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 regarding the protection of natural persons with regard to the processing of personal data and the free circulation of these data and by which Directive 95/46/EC is repealed, in the terms agreed by the Spanish Agency of Data Protection and the bodies that manage said platform.

Fourth additional provision. Existing digital service providers.

Digital service providers that have already been providing services must communicate their activity to the Secretary of State for Digital Advancement of the Ministry of Economy and Business, within three months from the entry into force of this Royal Decree-Law.

First final provision. Jurisdictional authority.

This Royal Decree-Law is issued by virtue of the exclusive powers attributed to the State in matters of the general telecommunications and public security regime by Article 149.1.21.ª and 29.ª of the Constitution.

Second final provision. Incorporation of European Union Law.

This Royal Decree-Law incorporates into the internal legal system the (EU) Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to guarantee a high common level of security for networks and systems information in the Union.

Third final provision. Authorisation for regulatory development.

The Government is empowered to develop the regulations provided for in this Royal Decree-Law without prejudice to the competence of the Ministers to set the specific obligations by means of a Ministerial Order in the cases provided for in the Articles of this norm.

Fourth final provision. Entry into force.

The present Royal Decree shall enter into force on the day following its publication in the «Official State Gazette».

Ordered in Madrid, 7 February 2018.

FELIPE R.

The President of the Government, PEDRO SÁNCHEZ PÉREZ-CASTEJÓN