MINISTRY
OF THE INTERIOR

PRELIMINARY DRAFT LAW ON CYBERSECURITY COORDINATION AND GOVERNANCE

Chapter I
General provisions

Chapter II
Strategic and institutional framework

Chapter III
Cybersecurity risk-management measures and reporting obligations

EXPLANATORY NOTE

I

The daily use of networks and information systems has become a crucial aspect of the development of social and economic activities thanks to the speed of digital transformation and the increasing interconnection of society. This positive progress has, however, led to an expansion of the range of cyber threats, with the consequent emergence of new challenges and risks that require appropriate, coordinated and innovative responses. The number, magnitude, sophistication, frequency and impacts of cyber incidents pose a serious threat to the functioning of networks and information systems, which can disrupt economic activities, undermine user confidence and cause major damage to the economy, society and national security, and require sustained effort to combat them. Proof of this is the fact that General Telecommunications Law 11/2022 of 28 June 2022 requires operators of public electronic communications networks and publicly available electronic communications services to adequately manage security risks potentially affecting their networks and services in order to ensure an adequate level of security and to avoid or minimise the impact of security incidents on users and on other networks and services. All of this makes improving cybersecurity preparedness more essential than ever.

Royal Decree-Law 12/2018 of 7 September 2018 on the security of information networks and systems transposed into Spanish law Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, the objective of which was to develop cybersecurity capabilities and reduce threats to network and information systems used to provide essential services in key sectors, ensuring the continuity of those services in the event of incidents, while also fostering cooperation on this matter at European Union level. Despite these achievements, the revision of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 revealed some inherent weaknesses that prevented it from effectively addressing current and emerging challenges in the field of cybersecurity, affecting in particular the cross-border provision of services and the level of cyber resilience between different Member States due to the implementation of disparate measures.

In order to overcome these difficulties, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, was approved. The objectives of this Directive, which is transposed by this regulation, are to regulate an institutional framework, improve coordination between competent authorities and relevant cooperation bodies at Community level, provide comprehensive coverage of sectors and services of vital importance to fundamental social and economic activities

within the internal market and ensure legal certainty regarding measures for managing cybersecurity risks and reporting obligations.

In particular, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 establishes a uniform criterion for determining which entities fall within its scope of application of the standard and should therefore comply with cybersecurity risk-management measures. To this end, entities are classified into two categories: essential entities and important entities, depending on the degree of criticality of their sectors or the type of service they provide, as well as their size. At the same time, given the intensification and sophistication of cyber threats in the modern world, it is ensured that the entities excluded from the scope of this standard achieve a high level of cybersecurity, supporting the implementation of equivalent cybersecurity risk-management measures that reflect the sensitive nature of these entities, maintaining an appropriate level of cooperation and communication between the respective competent authorities.

Furthermore, in view of the interlinkages that exist between cybersecurity and the physical security of entities, a consistent approach should be ensured between the provisions transposing Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 and Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. To this end, there is a need for the national cybersecurity strategy to establish a framework for action to improve coordination between competent authorities in the context of information-sharing on cybersecurity-related risks, cyber threats and incidents, as well as on non-cybersecurity-related risks, threats and incidents, and on the exercise of supervisory tasks. In this regard, on the one hand, entities that have been identified as critical in the context of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 should also be considered essential entities for the purposes of this Law; on the other hand, the obligations imposed on entities belonging to the digital infrastructure sector should comprehensively address the physical security of networks and information systems as part of their measures for the management of cybersecurity risks and reporting obligations. Since these matters fall within the scope of this Law, the obligations established in this regard in Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 do not apply to those entities.

On the other hand, the preamble to the Directive being transposed provides for the possibility of cybersecurity crises with a significant external or common security and defence policy dimension, although it does not address matters relating to national defence, which, being the exclusive competence of Member States, should be left to national regulation, without renouncing a common strategy. In this regard, it is important to note that the 2020 European Cybersecurity Strategy includes, among the measures of its second line of action, those aimed at boosting cyber defence capabilities, including the consolidation of cyberspace as the domain of military operations and the establishment

of the Military CERT Network, of which ESPDEF-CERT of the Joint Cyberspace Command is already part, to significantly contribute to cooperation between EU Member States. The need to foster this same line of collaboration is maintained in the 2022 European Union Cyber Defence Policy.

II

The International Telecommunication Union defines cybersecurity as 'the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets'. In turn, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 ('Cybersecurity Act'), includes within the concept of cybersecurity 'activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats'. Given the transversal and interconnected nature of information and communications technologies and the concept of cybersecurity as a set of mechanisms aimed at protecting the IT infrastructure and digital information accommodating these interconnected systems, it is not a concept or matter that can be managed under a single attribution of powers.

Cybersecurity thus remains inextricably linked to national security. In this regard, Law 36/2015 of 28 September 2015 on National Security expressly includes cybersecurity as an area of particular interest for national security, which requires specific attention, as does Order PRA/33/2018 of 22 January 2018 publishing the Agreement of the National Security Council regulating the National Cybersecurity Council; attention that is manifested through Order PCI/487/2019 of 26 April 2019 publishing the National Cybersecurity Strategy 2019, approved by the National Security Council, as a reference framework for an integrated model based on the involvement, coordination and harmonisation of all State actors and resources, public-private collaboration and the participation of citizens, which sets out the priorities, objectives and appropriate measures for achieving and maintaining a high level of network and information system security; and within the scope of which the current National Cybersecurity Plan was approved by Agreement of the Council of Ministers on 29 March 2022.
Likewise, in view of the nature of national defence as a fundamental component of national security and in compliance with the obligations that Law 36/2015 imposes on public administrations with competences in areas of special interest to national security, support mechanisms for operators with an impact on national defence must be connected with those for coordinating and sharing information, especially in relation to surveillance and alert systems for possible risks and threats that affect national defence and the armed forces.

Similarly, given its characterisation as a set of mechanisms aimed at protecting technological infrastructures and the digital information that they host, it can be inferred that, as a dedicated to the security of information technologies, cybersecurity has a protective component that is expressly projected into the specific field of protection of information networks and systems used by citizens, companies and public administrations. Therefore, as a synonym for network security, cybersecurity is an activity that is embedded into public security, as well as telecommunications. Public security is an exclusive competence of the State and it is established doctrine of the Constitutional Court that it is only limited by the attribution to the Autonomous Communities of powers relating to the creation of their own police, as a way for them to participate in the exercise of that competence. It must be borne in mind, however, that matters of public security extend beyond the functions proper to the security forces and bodies, such that the latter constitute only part of the broader matter of public security. In this sense, in addition to the police services that are in any case reserved for State security forces and bodies, the State has the remaining powers and administrative faculties, which, while being relevant to public security, such as those relating to the field of cybersecurity, are not particular or inherent to police functions or services.

This is also affected by the exclusive competence of the State in the field of telecommunications and the general communications regime, which, from a global perspective, integrates both the technical aspects and the regulatory powers relating to it, and also entails conferral of the supervisory and enforcement powers necessary to ensure continuity of services and set up a materially unitary and uniform system throughout national territory, which is necessary not only for the development of the sector but also for the security and guarantee of citizens' rights.

III

This Law consists of 50 articles, structured in 7 chapters, as well as 8 additional provisions, 3 transitional provisions, 1 repealing provision and 5 final provisions.

Chapter I regulates the objective and subjective purpose and scope of the law and defines the criteria for identifying essential and important entities. It includes the main definitions to be applied and known, so that all actors involved in interpreting it are aware of the basic elements for understanding the meaning and scope of each provision.

Chapter II establishes the national, strategic and institutional framework for network and information system security, with the aim of achieving and maintaining a high level of cybersecurity. To this end, it determines the minimum content to be addressed by the national cybersecurity strategy. The main innovation and most significant aspect of this chapter is its provision for the creation of a National Cybersecurity Centre is contemplated, which will overcome the current dispersion of competence in cybersecurity matters by becoming the sole competent national authority in the matter for the management, promotion and coordination of all of the activities provided for in

this Law, as a single point of contact to ensure cross-sectoral and cross-border cooperation with other competent authorities, as well as the national cybersecurity crisis management authority. Measures are also established to ensure effective, efficient and secure cooperation at European Union level.

Chapter III regulates cybersecurity risk-management measures and reporting obligations. This part provides for an individualised risk assessment by the different entities and details the actions that they should carry out to ensure and raise the security levels of their networks and information systems and prevent the risk of incidents, as well as for the obligation to report significant incidents that occur in their operation or in the provision of their services. In order to comply with the reporting obligations, the National cyber incident reporting and monitoring platform shall be made available to all actors involved, enabling technical information-sharing and incident monitoring. It also includes the figure of the information security officer: the person or body designated by the essential and important entities, responsible for the functions of contact person and technical coordinator for the matters covered by this Law.

For its part, the most prominent feature of Chapter IV is the imposition of the obligation to establish and regularly update cross-border registries, particularly of digital service providers and infrastructure, as well as entities providing domain name registration services, in order to ensure a clear overview of the entities falling within the scope of this legislation. At the same time, Chapter V is dedicated to the voluntary sharing of relevant information between entities with the aim of strengthening the level of cybersecurity and preventing, detecting, responding to, recovering from, or reducing the impact of incidents, as well as notifying the supervisory authority, through the reference national CSIRTs, of those incidents for which no reporting obligation is established.

Chapter VI is dedicated to the regulation of supervisory and enforcement functions in respect of essential and important entities, as well as cross-border cooperation; Chapter VII covers the development of disciplinary powers, in compliance with the provisions of Article 36 of the Directive, in order to ensure effective compliance with the obligations set out in this Law. To this end, this chapter incorporates the necessary provisions for compliance with the above, establishing a system that, in addition to complying with the provisions of European Union regulations, guarantees, in accordance with our legal system, all the rights of the persons concerned.

The Law also incorporates seven additional and three transitional provisions. The former include the creation of the National Cybersecurity Centre, with the status, character and administrative structure to be determined, in order to comply with the provisions of this Law to make it possible to achieve a high level of national cybersecurity in all its areas. Likewise, for the management, monitoring and resolution of cybersecurity incidents that may be presumed to be criminal , which affect essential and important entities, provision is made for processing known as the database of security incidents that are of a criminal nature.

The transitional provisions transpose into the legislation the obligations of communication and notification to the Commission of the different milestones and information relating to implementation of the provisions of the Directive and establish the current jurisdictional regime until the institutional development provided for in this Law has taken place, permitting compliance with the obligations that it contains.

Lastly, the final provisions amend Law 5/2014 of 4 April 2014 on Private Security to include staff performing cybersecurity tasks as accredited staff.

Likewise, it is stated that this legislation transposes into Spanish law Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive) and, in line with the provisions of the Directive being transposed, the repealing provision in turn repeals the national rules that previously transposed Directive (EU) 2016/1148.

IV

This regulation was drafted according to the principles of good regulation set out in Article 129 of Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations.

Firstly, it is necessary legislation, given that the transposition of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) requires the development of legislation with legal status. The principle of necessity is closely linked to that of legal certainty, as regards the subject matter of regulation, since the transposition of the aforementioned Directive is carried out by means of a law. Therefore, its processing and integration into the legal system enjoy the guarantees covered by legislation of this nature.

With regard to the principle of proportionality, this Law provides the necessary guarantees to ensure that any adverse effects on the rights that may be involved and the obligations addressed to the entities and persons concerned are proportionate, timely, minimum and sufficient, in order to meet the objectives pursued, namely to ensure the unobstructed provision in the internal market of services essential for the maintenance of vital societal functions and economic activities, to identify critical entities, to support them in complying with the obligations established, particularly those implemented in order to increase their resilience and ability to provide the services referred to and to ensure supervision of the legislation, including the development of a penalties regime.

It also complies with the principle of transparency, since this Law has been subject to the corresponding procedures of public participation, that is, prior consultation and public hearing and information.

In the process, in addition to the various Ministries concerned by the matter, the Spanish Data Protection Agency and the Public Prosecutor's Office have issued a report. It has also been the subject of an opinion of the Council of State.

Finally, this Law is issued in accordance with Article 149(1) points (4), (21) and (29) of the Spanish Constitution, which grant the State exclusive competence in matters of defence, the general telecommunications regime and public security respectively.

Chapter I
General provisions

Article 1. *Purpose.*

The purpose of this Law is to establish measures to achieve a high common level of cybersecurity in Spain and to contribute to the cybersecurity of the European Union.
To that end, it establishes:

a) obligations requiring the adoption of a national cybersecurity strategy and the designation or establishment of competent authorities, supervisory authorities, a cybersecurity crisis management authority, a single point of contact for cybersecurity (hereinafter 'single point of contact') and computer security incident response teams (CSIRTs);

b) cybersecurity risk-management measures and reporting obligations for entities regulated by this Law whose type is listed in Annexes I or II; as well as for entities identified as critical pursuant to Law XXX (Directive (EU) 2022/2557);

c) rules and obligations regarding information-sharing on cybersecurity;

d) monitoring and enforcement obligations.

Article 2. *Definitions.*

For the purposes of this Law, the following terms and definitions apply.

a) Information networks and systems.
   i. 'Electronic communications networks' means transmission systems, whether or not they are based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources. The term can cover network elements that are not active, and that permit the transmission of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile networks, electricity cable systems – to the extent that they are used to transmit signals, radio and television broadcasting networks, and cable television networks, irrespective of the type of information conveyed.
   ii. Any device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data.
   iii. The computer data stored, processed, retrieved or transmitted by the devices referred to in letters i. and ii. for the purposes of its or their operation, use, protection and maintenance.

b) ‘Network and information system security’ means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems.
c) ‘Cybersecurity’ means all activities necessary to protect network and information systems, the users of such systems and other persons affected by cyber threats.
d) ‘National cybersecurity strategy’ means a coherent framework of a Member State providing strategic objectives and priorities in the area of cybersecurity and the governance to achieve them in that Member State.
e) ‘Near miss’ or ‘incident without impact’ means an event that could have compromised the availability, authenticity, confidentiality integrity, or traceability of stored, transmitted or processed data, or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialise.
f) ‘Incident’ means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.
g) ‘Significant incident’ means one that
    i. has caused or is likely to cause serious operational disruption of services or economic loss to the entity concerned;
    ii. has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.
h) ‘Large-scale cybersecurity incident’ means an incident which causes a level of disruption that exceeds a Member State’s capacity to respond to it or which has a significant impact on at least two Member States;
i) ‘Incident handling’ means any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident.
j) ‘Cyber threat’ means a cyber threat as defined in point (8) of Article 2 of Regulation (EU) 2019/881;
k) ‘Significant cyber threat’ means a cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity’s services by causing considerable material or non-material damage.
l) ‘Risk’ means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident.
m) ‘Vulnerability’ means a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat.
n) ‘Domain Name System (DNS)’ means a hierarchical distributed naming system which enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those services and resources.

a) ‘DNS service provider’ means an entity that provides publicly available recursive domain name resolution services for internet end-users; or authoritative domain name resolution services for third-party use, with the exception of root servers.
o) ‘Top-level domain name registry’ or ‘TLD name registry’ means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers, irrespective of whether any of those operations are carried out by the entity itself or are outsourced, but excluding situations where TLD names are used by a registry only for its own use.
p) ‘Entity providing domain name registration services’ means a registrar or an agent acting on behalf of registrars, such as a privacy or proxy registration service provider or reseller.
q) ‘Online marketplace’ means a service using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders or consumers.
r) ‘Online search engine’ means a digital service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found.
s) ‘Cloud computing service’ means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations.
t) ‘Data centre service’ means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of IT and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control.
u) ‘Content delivery network’ means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers.
v) ‘Social networking services platform’ means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations.
w) ‘Managed service provider’ means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers’ premises or remotely.

x) ‘Managed security service provider’ means a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management.
y) ‘General cybersecurity risk-management measures’ means a set of technical, operational and organisational measures used by an entity in its operations or in the provision of its services, which aim to manage risks to the security of network and information systems and to prevent or minimise the impact of incidents on its users and other services.
z) ‘Entities or operators with an impact on national defence’ means those essential or important entities, in any sector, providing goods or services necessary for the operation of the Ministry of Defence and in particular for fulfilment of the missions of the armed forces, which are established in accordance with Articles 3 and 4 of this Law.
aa) ‘Specific Compliance Profile’ (SCP) means a set of security measures, whether or not included in Annex II to Royal Decree 311/2022 of 3 May 2022 regulating the National Security Scheme (ENS), which, as a result of the mandatory risk analysis, are applicable to a specific entity or sector of activity and for a specific security category, and which has been authorised by the National Cryptological Centre.
bb) ‘Security audit’ means a systematic, independent and documented process that seeks to obtain objective evidence and evaluate it to determine the extent to which the audit criteria are met in relation to the adequacy of the security controls adopted and compliance with the security policy, standards and operating procedures established, and to detect deviations from the aforementioned criteria.
cc) ‘European Network of Security Operation Centres (ENSOC)’ refers to European technological infrastructure made up of a set of national centres belonging to the Member States, organised around a European consortium, whose objective is to establish a cross-border Security Operations Centre (SOC) platform to improve the detection and prevention of cyber threats, provide timely warnings to authorities and stakeholders and, consequently, strengthen the European Cybersecurity Alert System.

Article 3. *Scope.*

1. This Law will apply to public or private entities that are resident in Spain for tax purposes and which fall within the sectors of high criticality and other critical sectors listed in Annexes I and II, where they are considered to be medium-sized or large undertakings because they have 50 or more employees and an annual turnover or annual balance sheet total exceeding EUR 10 million.

2. It will apply to entities included in Annex I or II, irrespective of their size, in the following cases:

a) the services are provided by:
   i. providers of public electronic communications networks or publicly available electronic communications services;
   ii. trust service providers;
   iii. top-level domain name registries and domain name system service providers;
b) the entity is the only provider in Spain of a service essential for the maintenance of critical social or economic activities;
c) disruption of the service provided by the entity could have a significant impact on national security, public security, public order, public health, economic activity or the provision of public services;
d) a disruption of the service provided by the entity could induce significant systemic risks, in particular for sectors where such a disruption could have repercussions of a cross-border nature;
e) the entity belongs to the public sector in accordance with Article 2 of Law 40/2015 of 1 October 2015 on the Legal Regime of the Public Sector;
f) critical entities, in accordance with the regulations applicable to measures for the protection of critical infrastructure;
g) universities and research centres involved in research issues or projects related to high criticality and other critical sectors;
h) companies in which 25% or more of their capital or voting rights are controlled, directly or indirectly, by one or more bodies or administrations belonging to the public sector and which are thus identified by the supervisory authority, unless it can be considered a related company;
i) any other entity that the supervisory authority identifies as an essential or important entity by applying the criteria of this Article, by reasoned resolution.

3. The provisions of this Law will also apply to entities that, having their residence or domicile in another Member State of the European Union, offer their services or develop their competences through a permanent establishment located in Spain, in accordance with the following criteria:

a) Providers of public electronic communications networks or publicly available electronic communications services, when they provide services in Spain.

b) The providers of services and technological infrastructure referred to in Article 26(1), when they have their main establishment in Spain.

   They shall be considered to have their main establishment in Spain when:

i) decisions on cybersecurity risk-management measures are taken predominantly on Spanish territory;

ii) in the event that it cannot be determined where such decisions are taken, or in the event that it is done outside the European Union, when the cybersecurity operations are carried out in Spain;

iii) in the event that it is not possible to determine in which Member State of the European Union the decisions are taken, when the entity's establishment in the European Union with the highest number of workers is in Spain.

4. The National Cybersecurity Centre will implement the necessary procedures to identify which entities are included in the previous sections, with the help of the supervisory authorities and sectoral points of contact.

5. The following are excluded from its scope:

a) public administration entities carrying out activities in the fields of national security, national defence or public security, including the prevention, investigation, detection and prosecution of criminal offences, except in those activities in which they act as providers of trust services available to third parties;

b) The Instituto de Crédito Oficial (Institute of official credit).

6. The provisions of this Law relating to cybersecurity risk-management and reporting obligations and to supervision and enforcement will not apply to the financial institutions included in Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) No 2016/1011. Nor will the provisions of Article 33, or the provisions contained in Chapter VII on the penalties regime, be applicable to this type of entity, without prejudice to the obligation of collaboration and information-sharing of the financial sector with the supervisory authorities and the complementary nature of this Law with respect to the provisions of the aforementioned Regulation.

Article 4. *Essential and important entities*.

1. The following are considered essential entities.

a) Entities belonging to the sectors listed in Annex I that are considered large companies because they employ 250 or more workers and have an annual turnover of more than EUR 50 million or an annual balance sheet total of more than EUR 43 million.

b) Qualified trust service providers and top-level domain name registries, as well as DNS service providers, regardless of their size.

c) Providers of public electronic communications networks or publicly available electronic communications services that are considered medium-sized enterprises because they employ 50 or more workers, but no more than 250, and have an annual turnover or annual balance sheet of more than EUR 10 million and not more than EUR 50 million.

d) Entities of the general State administration and the administrations of the Autonomous Communities, in accordance with Article 2 of Law 40/2015 of 1 October 2015, provincial councils, town halls and island councils and large-population municipalities, as defined in Title X of Law 7/1985 of 2 April 1985 Regulating the Bases of the Local Regime. The institutional public sector entities of all of the above shall be deemed essential, unless the supervisory authority issues a reasoned resolution to the contrary or regulations provide otherwise.

e) Any other entity in the sectors listed in Annex I or II to this Law, which the supervisory authorities identify as an essential entity under Article 3(2)(b) and (c).

f) Entities identified as critical entities under Law xxxx.

g) Entities identified as operators of essential services before 16 January 2023 pursuant to Royal Decree-Law 12/2018 of 7 September 2018 on the security of information networks and systems.

2. Important entities are all entities belonging to the sectors listed in the aforementioned Annexes I or II that cannot be considered essential entities pursuant to paragraph 1 of this Article. This includes entities identified by supervisory authorities as important entities pursuant to points (b), (c), (d), (e) and (f) of Article 3(2) and, in any case, municipalities that are not large-population municipalities and have a population of more than 20 000 inhabitants, and entities in their institutional public sector.

3. The National Cybersecurity Centre shall, on the basis of the information provided by the supervisory authorities, draw up a list of essential and important entities. This list shall be reviewed regularly, at least every two years, and updated where appropriate.

4. For the creation of the list, the entities referred to in the previous paragraph must assess their inclusion in the categories of essential and important entities and, where appropriate, submit at least the following information to the supervisory authorities within a maximum of three months of acquiring their status as such:

a) the name of the entity;

b) the up-to-date address and contact details, including email addresses, IP ranges and telephone numbers, including, where applicable, the contact details of the entity's information security officer;
c) where applicable, the sector and subsector to which they belong, in accordance with Annexes I and II;
d) where applicable, a list of the Member States of the European Union in which they provide services falling within the scope of the Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 ('NIS 2 Directive').

The entities referred to in paragraph 3 shall notify the supervisory authorities of any changes to the information they have submitted as soon as possible and in any event within two weeks of the date on which the change occurred.

Mechanisms may be established by regulation to enable entities to comply with the obligations of this section by registering themselves.

5. The supervisory authorities shall be responsible for identifying, at the proposal of the Chief of Defence, those entities deemed to be entities with an impact on national defence and communicating to them their registration or deregistration as such.

In the case of critical entities, in accordance with Law xxxx transposing Directive (EU) 2022/2557, this identification will require the prior report of the Cybersecurity Coordination Office.

Within the scope of this Law, the Chief of Defence, through the Joint Cyberspace Command (JCCC), shall be responsible, together with the National Cybersecurity Centre and the supervisory authorities or, in the case of critical entities, with the authorities designated pursuant to Law xxxx transposing Directive (EU) 2022/2557, for coordinating the support provided to entities with an impact on national defence.

6. ESPDEF-CERT of the Joint Cyber Command shall be responsible for registration of the designated entities with an impact on national defence and shall inform the reference national CSIRT, as well as the competent authorities designated pursuant to Law xxxx transposing Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, in the case of critical entities, of the identities thereof.

7. Where a piece of national or Community legislation lays down obligations for a particular sector in terms of the security of network and information systems or reporting of incidents that have effects at least equivalent to those of the obligations under this Law, the original requirements and corresponding supervisory mechanisms shall prevail.

Chapter II
Strategic and institutional framework

Article 5. *National cybersecurity strategy*.

1. The National cybersecurity strategy shall set out the strategic objectives, the necessary resources and the appropriate policy and regulatory measures to achieve and maintain a high level of cybersecurity. Its content shall be consistent with the National security strategy.

2. The National cybersecurity strategy shall set out, inter alia, the following issues.

a) Its objectives and priorities, in particular the sectors listed in Annexes I and II, and the list of the authorities and stakeholders involved in its implementation.

b) The governance framework for achieving the objectives and priorities referred to in point (a) of this paragraph, including the policies referred to in paragraph 3.

c) A governance framework clarifying the roles and responsibilities of the relevant stakeholders at national level, supporting cooperation and coordination at national level, led by the National Cybersecurity Centre, between the supervisory authorities, the reference national CSIRTs and the sectoral points of contact, as well as coordination and cooperation between those bodies and the competent authorities pursuant to sectoral legal acts of the Union.

d) A procedure enabling cybersecurity risks to be assessed.

e) The necessary strategic measures to ensure preparedness, response capacity and recovery from incidents. To this end, mechanisms should be established for cooperation between the public and private sectors.

f) The policy framework for coordination with the competent authorities designated pursuant to Law xxxx transposing Directive (EU) 2022/2557 for the purpose of information-sharing on risks, cyber threats and incidents, as well as on risks, threats and incidents not related to cybersecurity and the exercise of supervisory functions.

g) A plan of measures to improve citizens' cybersecurity awareness.

3. Similarly, within the framework of the National cybersecurity strategy, policies will be adopted concerning the following issues in particular:

a) cybersecurity in the supply chain of information and communication technology (ICT) products and services used by entities for the provision of their services;

b) the inclusion and specification of cybersecurity requirements to be applied to ICT products and services in public procurement, including those relating to cybersecurity certification, encryption and the use of open-source cybersecurity products, without prejudice to their additional incorporation into the regulations governing public procurement;

c) the management of vulnerabilities, including measures for coordinated promotion and disclosure, in accordance with the provisions of Article 11(1);

d) the general availability, integrity and confidentiality of the public core of the open Internet, as well as the cybersecurity, where applicable, of data centres and submarine communications cables;

e) the development and integration of advanced technologies aimed at implementing state-of-the-art cybersecurity risk-management measures;

f) the promotion and development of education and training in cybersecurity, cybersecurity skills, awareness-raising and research and development initiatives, as well as guidance on good practices and controls in cyber hygiene, intended for citizens, stakeholders and entities, as well as support for academic and research institutions for the development, improvement and implementation of cybersecurity tools and secure network infrastructure;

g) procedures and tools for sharing information to support voluntary information-sharing on cybersecurity between entities;

h) reinforcement of the cyber resilience and cyber hygiene baseline of small and medium-sized enterprises, especially those excluded from the scope of this Law, by providing easily accessible guidance and support for their specific needs;

i) promotion of active cyber protection as part of a comprehensive defence strategy, established by the authority at the highest level.

4. The National Cybersecurity Council shall check the degree of compliance with the National cybersecurity strategy, as well as with the development instruments adopted on the basis of the indicators it establishes. To this end, it shall submit an annual report to the National Security Council, which shall include proposals for improvement and address whether or not there is a need to approve a new strategy.

5. The National Cybersecurity Centre shall notify the National Cybersecurity Strategy to the Commission within three months of its adoption. Information with an impact on national security may be excluded from this notification.

Article 6. The National Cybersecurity Centre.

The National Cybersecurity Centre is the single national competent authority for cybersecurity governance, responsible for the direction, promotion and coordination, within the scope of this Law, of all activities necessary to ensure a high level of cybersecurity in Spain and contribute to the cybersecurity of the European Union.

It will act as the national crisis management authority and single point of contact and assume the role of senior management and coordination of the supervisory authorities and sectoral points of contact in the performance of their implementation and supervision functions, as well as the reference national CSIRTs.

In addition, within the framework of this Law, it will carry out the following tasks:

a) act as a superior body for the governance and coordination of cybersecurity activities provided for in this Law and in its implementing regulations, without prejudice to the powers that the different bodies and agencies have legally established;
b) act as national competent authority in the field of cybersecurity, without prejudice to the existence of supervisory authorities and sectoral points of contact under its coordination;
c) inform the public about incidents affecting more than one supervisory authority, where the dissemination of such information is necessary to prevent an incident or to manage an incident that has already occurred;
d) establish, in situations of justified need approved by reasoned resolution, with the advice of the supervisory authorities, the specific obligations necessary to ensure the security of networks and information systems;
e) promote and approve, where appropriate, the use of standards, guides, specifications, technical instructions and any other provisions on the security of networks and information systems.

It shall also assume any other functions entrusted to it in the field of national cybersecurity, without prejudice to the powers legally reserved to other bodies and institutions.

Article 7. Supervisory authorities, single point of contact and sectoral points of contact.

1. The supervisory authorities, responsible for the supervisory and enforcement functions referred to in Chapter VI of this Law, are as follows:

a) the Ministry of Defence, through the National Cryptologic Centre, for essential and important entities that, being non-critical entities, fall within the scope of Law 40/2015 of 1 October 2015 on the Public Sector Legal Framework;

b) the Ministry for the Digital Transformation and Civil Service, through the State Secretariat for Telecommunications and Digital Infrastructure and the State Secretariat for Digitalisation and Artificial Intelligence, for essential and important entities in the digital infrastructure and digital service providers sectors, as well as important entities in the other sectors, which have not been designated as critical entities;

c) the Ministry of the Interior, through the Cybersecurity Coordination Office of the Secretary of State for Security, for critical entities and essential entities of the sectors not included in points (a) or (b), as well as for all essential and important entities of the private security sector.

For the exercise of these supervisory and enforcement functions, they shall be entrusted with the following competences.

a) To establish communication channels with essential and important entities, including the National cyber incident reporting and monitoring platform provided for in Article 19.

b) To receive and follow up on incident notifications submitted under this Law through the reference national CSIRTs.

c) To inform the public about certain incidents, where the dissemination of such information is necessary to prevent an incident or to manage an incident that has already occurred.

d) To participate, on a voluntary basis, in peer reviews organised pursuant to Article 19 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022.

e) To propose mandatory cybersecurity risk-management measures for entities falling within the scope of this legislation.

f) Any other competence attributed in this Law or in its regulatory development.

2. The National Cybersecurity Centre is established as a single point of contact to exercise a liaison function that ensures cross-border cooperation with the relevant authorities in other Member States and, where appropriate, with the Commission and the European Union Agency for Cybersecurity (ENISA), as well as to ensure cross-sectoral cooperation with other competent national authorities.

To that end, it shall have the following competences.

a) To transmit information on cybersecurity incidents having a cross-border impact to the single points of contact of other affected Member States of the European Union.

b) To submit to ENISA the information in the registry of providers of digital services and infrastructure referred to in Article 26(1).

c) To submit to the Commission and the Cooperation Group the information on essential and important entities set out in Article 4(3).

d) Provide the reference national CSIRTs with relevant information on significant incidents that might have disruptive effects on essential and important services received from the supervisory authorities, CSIRTs or competent authorities of the relevant Member States, to take appropriate action in the performance of their tasks.

e) To prepare and submit a quarterly report to ENISA on the type and number of incidents reported in accordance with this Law, their effects on the services provided or on other services and their national or cross-border nature within the European Union, for which it may collect the necessary information from the supervisory authorities.

f) Any other competence attributed in this Law or in its regulatory development.

3. For each of the sectors listed in Annexes I and II, at least one ministerial body or body or entity governed by public law linked to or dependent on the general State administration shall be designated, which shall be, within the framework of its competences, the specialised point of contact with the National Cybersecurity Centre and the supervisory authorities. These sectoral points of contact shall have the following functions.

a) To promote cybersecurity policies and ensure the application of and compliance with the obligations derived from this Law.
b) To encourage the organisations constituting their community of competent entities and supervise their appropriate self-registration as an essential or important entity.
c) To collaborate with the National Cybersecurity Centre and the supervisory authorities in the development of the following activities:
    i. identification of essential and important entities in their community of reference;
    ii. elaboration of the specific profiles of compliance with the obligations of Article 15.3;

iii. supervision of compliance by essential and important entities with the obligations set forth in this Act;
iv. establishment of appropriate channels of communication with the essential and important entities that, where appropriate, will be developed by regulation.

d) Any other that is assigned to it by regulation.

4. The Autonomous Communities shall collaborate with the National Cybersecurity Centre or, where appropriate, with the supervisory authorities, to promote and ensure compliance with cybersecurity policies and the obligations arising from this Law; particularly in identifying and notifying the entities in Article 4 .

Article 8. *National cyber crisis management framework*.

1. The National Cybersecurity Centre, as the national cybersecurity crisis management authority, will be responsible for coordinating the management of large-scale cybersecurity incidents and crises.

2. The capabilities, assets and procedures to be deployed in the event of a cybersecurity crisis will be established by regulation.

3. Similarly, the National Cybersecurity Centre will adopt a large-scale cybersecurity incident and crisis response plan setting out the objectives and measures for managing large-scale cybersecurity incidents and crises. Said plan will in any case include:

a) the objectives of the readiness measures and activities;
b) the roles and responsibilities assigned to the authorities with competence in cybersecurity;
c) cybersecurity crisis management procedures, including their integration into the general crisis management framework, and channels for information-sharing;
d) readiness measures, which should include exercises and training activities;
e) the relevant public and private stakeholders and the infrastructure involved;
f) The procedures and mechanisms to ensure the participation and support of Spain in the coordinated management of large-scale cybersecurity incidents and crises at European Union level.

Article 9. *Reference national computer security incident response teams (CSIRT)*.

1. The following are reference national computer security incident response teams (CSIRT), as regards network and information system security:

1º CCN-CERT, of the National Cryptological Centre (CCN), which will be responsible for the reference community consisting of the entities considered essential or important in accordance with this Law that are included within the scope of Law 40/2015 of 1 October 2015.

In any case, CCN-CERT, following the instructions of the National Cybersecurity Centre, shall coordinate the technical response of CSIRTs nationally in significant incidents or particularly severe cases.

2º INCIBE-CERT, of the National Cybersecurity Institute of Spain, which will be responsible for the reference community consisting of the entities considered essential or important in accordance with this Law and which are not included within the scope of Law 40/2015 of 1 October 2015.

3º ESPDEF-CERT, of the Ministry of Defence Joint Cyberspace Command (*Mando Conjunto del Ciberespacio*), which will cooperate with CCN-CERT and INCIBE-CERT in situations where they need it to do so and, necessarily, in situations relating to incidents affecting the Ministry of Defence and entities with an impact on national defence, in which case they will coordinate with the Ministry any aspects liable to affect national defence, the Ministry of Defence or the operational readiness of the armed forces; without prejudice to the provisions of this article for incidents affecting critical entities.

2. In incidents involving entities classified as critical in accordance with Law xxxx, the CSIRT-MIR-PJ of the Cybersecurity Coordination Office (OCC) will operate jointly with the relevant reference CSIRT.

3. The National Cybersecurity Centre will assume the coordination functions of the reference national CSIRTs within the scope of this Law, specifically:

    a) It will ensure the coordination of national and international CSIRTs in incident response and security risk-management for which they are responsible.

    b) It will cooperate and share relevant information with sectoral or cross-sectoral communities of essential and important entities and, where appropriate, with their suppliers or service providers, as set out in Article 30.

    c) It will coordinate the effective, efficient and secure cooperation of its CSIRTs in the European Union CSIRTs network.

    d) It will exercise the highest coordination of any cooperation relationships that the reference national CSIRTs might establish with the national computer security incident response teams of third countries in accordance with paragraph 5 of this Article.

e) It will coordinate and channel the participation of the reference national CSIRTs in the peer reviews organised in accordance with Article 13 of this Law.

4. Without prejudice to the provisions for cyber incidents affecting critical entities, when the activities they carry out may affect an entity in the private security sector or in relation to the investigation of crimes or the discovery and securing of criminals by the security forces and bodies, the reference national CSIRTs will coordinate with the Ministry of the Interior through the Cybersecurity Coordination Office of the Secretariat of State for Security, ensuring their access to all of the information necessary for the performance of their functions.
   The National Cybersecurity Centre shall guarantee the coordination referred to in the previous paragraph.

5. If an entity with an impact on National Defence is affected by an incident, it shall analyse its scope to determine whether it could affect the functioning of the Ministry of Defence or the effectiveness of the Armed Forces. If so, it shall be immediately made known to the reference national CSIRT, who shall inform ESPDEF-CERT of the Joint Cyberspace Command through the established channels. Similarly, the reference national CSIRTs concerned shall inform ESPDEF-CERT of all incidents notified to them by operators with an impact on the national defence of their reference community, as well as of developments in the handling of the incident. In such cases, where the operation of the Armed Forces so requires, ESPDEF-CERT may provide direct support to the affected entity in coordination with the reference national CSIRT.

6. The reference national CSIRTs may establish cooperative relationships with national computer security incident response teams in third countries, enabling effective, efficient and secure information-sharing, using the relevant information-sharing protocols, including the Traffic Light Protocol (TLP) and personal data, in accordance with Union data protection legislation.

7. The reference national CSIRTs may cooperate with national computer security incident response teams of third countries or equivalent bodies of third countries, in particular with a view to providing them with cybersecurity assistance.

8. Each reference national CSIRT shall have adequate resources to carry out its tasks effectively.

9. The reference national CSIRTs shall have at their disposal appropriate, secure and resilient communication and information infrastructure for information-sharing with essential and important entities and other relevant stakeholders. To this end, each reference national CSIRT shall contribute to the deployment of secure tools for information-sharing.

Article 10. *Obligations, technical capabilities and competences of the reference national CSIRTs.*

1. The reference national CSIRTs shall comply with the following requirements.

a) Ensure that their communication channels are available, avoiding simple isolated failures, and must have, at all times, several means of communication enabling them to contact and be contacted by others. They should also specify what these communication channels are and communicate them to user groups and collaborating partners.

b) Ensure that their premises and those of the supporting information systems should be located in places that meet the necessary security conditions in accordance with the applicable legislation in each case.

c) Be equipped with an appropriate system for managing and channelling requests that facilitates, in particular, the effectiveness and efficiency of transfers.

d) Ensure the confidentiality and reliability of their operations.

e) Have sufficient staff to ensure the availability of their services at all times and to ensure appropriate training of their staff.

f) Be equipped with redundant systems and backup workspaces to ensure the continuity of their services.

2. The reference national CSIRTs will have the following duties within their respective spheres of activity.

a) Monitor and analyse cyber threats, vulnerabilities and incidents occurring at national level and, upon request, provide assistance to essential and important entities concerned in real-time or immediate monitoring of their network and information systems, in coordination with the supervisory authorities.

b) Disseminate early warnings, alerts, notices and information about cyber threats, vulnerabilities and incidents occurring among the affected essential and important entities, as well as between supervisory authorities and other stakeholders in real or immediate time

c) Respond to incidents and provide assistance to essential and important entities with regard to the degree of impact on services or data stored, transmitted or processed.

d) Collect and analyse forensic data and perform dynamic cybersecurity risk and incident and situational awareness analysis.

e) Provide, at the request of an affected critical or important entity, a proactive exploration of the affected entity's information networks and systems to detect vulnerabilities that might have significant consequences.

f) Participate in the European Union CSIRTs network provided for in Article 15 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 and in the European Network of Cybersecurity Operations Centres to enhance the automatic exchange of indicators of compromise to provide other members of the CSIRTs network with real-time information on ongoing cyberattacks and provide mutual assistance, in accordance with their capabilities and competences, upon request.

g) Contribute to the deployment of secure information-sharing tools.

h) Where appropriate, act as coordinator for the purposes of the coordinated vulnerability disclosure process.

In the implementation of these actions, priority may be given to tasks identified on the basis of a risk-based approach.

3. The reference national CSIRTs may carry out a non-intrusive proactive exploration of the publicly accessible information networks and systems of their respective reference communities. Said exploration will be carried out for the purpose of identifying vulnerabilities and unsafe configurations in network and information systems and informing affected entities. Said exploration must not have any negative impact on the operation of the entities' services, nor may it affect individuals' privacy.

4. The reference national CSIRTs, under the coordination of the National Cybersecurity Centre, shall cooperate with private sector stakeholders and promote the adoption and use of common or standardised practices, classification systems and taxonomies in relation to:

a) incident-handling procedures;
b) cybersecurity crisis management;
c) coordinated vulnerability disclosure.

Article 11. *Coordinated vulnerability disclosure.*

1. The National Cybersecurity Centre shall designate the reference national CSIRT to perform the functions of coordinating body for the purpose of coordinated vulnerability

disclosure, acting as trusted intermediary and facilitating, where necessary, the interaction between the natural or legal person notifying a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, at the request of either party. The tasks of the coordinating reference national CSIRT shall include:

a) identifing and contacting affected entities;
b) providing assistance to natural or legal persons reporting a vulnerability;
c) negotiating disclosure deadlines and managing vulnerabilities affecting multiple entities.

2. In carrying out its coordination function, the designated reference national CSIRT shall ensure that natural or legal persons who so request may report a detected vulnerability anonymously. In the same way, it will ensure that diligent monitoring of the reported vulnerability is carried out. Where the reported vulnerability is likely to have a significant impact on entities in more than one Member State, it shall cooperate, where appropriate, with the CSIRTs designated as coordinators within the framework of the European CSIRTs network.

Article 12. *Cooperation at national level*.

The National Cybersecurity Centre shall perform the following tasks in terms of cooperation at national level.

a) In order to ensure the effective performance of its tasks and obligations, the National Cybersecurity Centre shall cooperate and collaborate with public bodies and agencies with competence in matters of national security, national defence, public security, citizen security, digital administration and personal data protection, as well as any entity with competence within its scope, particularly with national authorities in the field of civil aviation and aviation security, supervisory bodies relating to electronic identification and trust services for electronic transactions in the internal market, competent authorities for digital operational resilience of the financial sector, national regulatory authorities within the framework of the European Electronic Communications Code, and competent authorities for the resilience of critical entities.

b) It shall cooperate and regularly exchange information with competent authorities designated pursuant to Law XXXXX on the identification of critical entities, risks, cyber threats and ICT-related incidents, as well as on risks, threats and non-cyber incidents affecting essential entities identified as critical entities, and on measures taken in response thereto. It shall also share information in relation to ICT-related incidents and cyber threats with competent authorities in the areas of electronic identification and trust services for electronic transactions in the internal market,

digital operational resilience of the financial sector, and electronic communications.

c) It shall cooperate with the competent authorities in the sectors subject to the specific cybersecurity regulations in order to harmonise the regulations.

d) It shall cooperate with the competent authorities of other Member States of the European Union to identify essential and important entities that offer their services in several Member States, as well as to identify and resolve any incidents that occur within the framework of this Law and which affect multiple Member States.

Article 13. *Cooperation at European Union level*.

The National Cybersecurity Centre shall perform the following tasks in terms of cooperation at European Union level:

a) Assume national representation in the Cooperation Group provided for in Article 14 of Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022, established in order to support and facilitate strategic cooperation and the information-sharing between Member States and to strengthen trust and collaboration, as well as to coordinate the participation of the reference national supervisory authorities and CSIRTs in their working groups.

b) Assume national representation in the European cyber crisis liaison organisation network (EU-CyCLONe). (EU-CyCLONe), provided for in Article 16 of Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022, established to support the coordinated management of large-scale cybersecurity incidents and crises in the operational field and to ensure the regular exchange of relevant information between Member States and the European Union.

c) Ensure the effective cooperation of national CSIRTs in the European Union CSIRTs Network, as provided for in Article 15 of Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022, as well as with the European Network of Cybersecurity Operations Centres, with a view to contributing to the strengthening of trust, security and the promotion of swift and effective operational cooperation between Member States.

d) Coordinate participation in peer reviews in accordance with Article 19 of Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022.

e) Assume national representation in the ENISA Administrative Board and in the network of national liaison officers.

Chapter III
Cybersecurity risk-management measures and reporting obligations

Article 14. *Governance.*

1. The management bodies of essential and important entities shall be responsible for implementing the cybersecurity risk-management measures included in this Law, for supervising their effective implementation and, where appropriate, shall assume responsibility for non-compliance.

This is without prejudice to the applicable rules on the liability of public administration, public employees and elected or appointed officials.

2. Members of the management bodies of essential and important entities shall also receive appropriate training on a regular basis in order to acquire sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity. Likewise, the management bodies must periodically organise similar training for their employees.

Article 15. *General cybersecurity risk-management measures.*

1. The National Cybersecurity Centre shall identify appropriate and proportionate technical, operational and organisational measures to be put in place by essential and important entities to manage the risks evidenced by the ex ante analysis of the security of the network and information systems they use in their operations or in the provision of their services and to prevent or minimise the impact of incidents on recipients of their services and on other services, and shall ensure that supervisory authorities urge essential and important entities to take such measures.

2. The security measures referred to in the preceding paragraph shall be based on those provided for in both the National Security Scheme and equivalent European and international technical standards; they shall ensure an adequate level of security of network and information systems, as well as of their physical environment, that is appropriate to the risks posed; and they shall include at least the following elements:

a) network and information system security policies and risk analysis;
b) incident handling;
c) business continuity, such as backup management and disaster recovery, and crisis management;
d) supply chain security, which shall include security aspects relating to the relationships between each entity and its direct suppliers or service providers, as well as the main security point of contact for each of the suppliers;

e) security in the acquisition, development and maintenance of networks and information systems, including the management and disclosure of vulnerabilities;
f) policies and procedures for assessing the effectiveness of cybersecurity risk-management measures;
g) basic cyber hygiene and cybersecurity training practices;
h) policies and procedures relating to the use of cryptography and, where applicable, encryption;
i) human resource security, access control policies and asset management;
j) the use of multi-factor authentication or continuous authentication solutions, voice, video and text communications and secure emergency communications systems in the entity, where applicable.

In the case of entities subject to Royal Decree 311/2022 of 3 May 2022, the corresponding National Security Scheme Specific Compliance Profile for essential and important entities will certify compliance with the cybersecurity risk-management measures of this regulation. The same shall apply to those essential or important entities that are not subject to Royal Decree 311/2022 and which voluntarily obtain a satisfactory assessment vis-à-vis the National Security Scheme Specific Compliance Profile.

The supervisory authorities shall provide the National Cybersecurity Centre with all information necessary for determination of these measures.

3. In order to take due account of the different degrees of exposure of institutions to risks, the size of the institution and the likelihood and severity of incidents, including their social and economic impacts, as well as the specificity of certain sectors and operators, the National Cybersecurity Centre may approve specific compliance profiles.

These compliance profiles shall take into account the specific vulnerabilities of each direct supplier, as well as the overall quality of the products and cybersecurity practices of their suppliers and service providers, including their secure development procedures, taking into account the results of coordinated security risk assessments of critical supply chains performed in accordance with Article 22(1) of Directive (EU) 2022/2555.

In addition, the specific compliance profiles shall be designed incrementally on the general cybersecurity risk-management measures referred to in paragraphs 1. and 2.

The sectoral points of contact shall collaborate with the supervisory authorities in the creation of these specific compliance profiles for approval by the National Cybersecurity Centre, which will ensure their harmonisation and consistency.

4. Essential and important entities must demonstrate compliance with the obligations referred to in this Article. In the case of essential entities, compliance will be evidenced by obtaining and maintaining a conformity accreditation certificate. Important entities will

be able to choose between the above certification and carrying out a self-assessment of their security position.

Essential or important entities that are expressly included in the scope of Royal Decree 311/2022 of 3 May 2022 shall comply with its provisions regarding certification of Conformity with the National Security Scheme.

The certification procedures shall be established by the National Cybersecurity Centre in accordance with the principles of necessity, proportionality and efficiency. In addition, it shall ensure that the procedure and requirements for the acquisition of this certification are designed in such a way that it attests at the same time to compliance with the national safety scheme and international technical standards at their concordant levels.

5. These measures will apply to assets or systems used for the provision of their services or operations and must be included in a document signed by the information security officer called the system applicability declaration. This document must be submitted to the relevant supervisory authority within six months of the acquisition of essential or important entity status.

6. Essential and important entities shall properly implement the implementing acts adopted by the European Commission laying down the technical and methodological requirements for the measures set out in paragraph 2 with respect to the entities referred to in Article 26(1).

In addition, the National Cybersecurity Centre or, where appropriate, the supervisory authorities shall urge essential and important entities other than those indicated in the previous paragraph to apply the implementing acts adopted by the European Commission.

Article 16. *Information security officer*.

1. Essential and important entities shall designate a person, unit or collegiate body as information security officer, to exercise the functions of point of contact and technical coordination with the supervisory authorities and reference national CSIRTs. In the event that the information security officer is a collegiate unit or body, a representative natural person shall be appointed, as well as a replacement for them who will assume their duties in the event of absence, vacancy or illness.

2. Essential or important entities shall notify the supervisory authorities of the designation of the information security officer within three months of their designation. They shall also communicate successive appointments and dismissals within one month of their occurrence.

3. In essential entities, the information security officer, or their representative natural person and the latter's replacement in the case of a collegiate body, regardless of the technical capacity and training requirements, must be staff accredited by the Ministry of the Interior. In the case of essential entities that are also considered critical under Law XXXXXXX, this obligation will be similarly extended to the rest of the staff responsible for carrying out the cybersecurity tasks provided for in this Law.

The manner of obtaining, maintaining and losing the status of accredited staff referred to in the previous paragraph shall be regulated by regulation in accordance with the provisions of Law 5/2014 of 4 April 2014 on Private Security and within the framework of competence established in Organic Law 2/1986 of 13 March 1986 on Security Forces and Bodies. The National Cybersecurity Centre shall be responsible for determining the functions of the information security officer, as well as, where appropriate, the specific training required.

The information security officer shall have the following functions:

a) developing and submitting the security strategy and policies to the organisation for approval; these must include the technical, organisational and proportionate cybersecurity risk-management measures set out in this standard;

b) supervising and developing the implementation of security policies, standards and procedures derived from the organisation, supervising their effectiveness and conducting periodic security audits;

c) monitoring compliance with the applicable regulations on the security of network and information systems;

d) serving as a trainer for good practices in information network and system security, for both hardware and software aspects;

e) managing the cybersecurity incidents referred to in Article 17;

f) forwarding to the supervisory authorities, through the reference national CSIRTs, without undue delay, notifications of incidents that have had disruptive effects on service provision, as well as any vulnerabilities detected;

g) receiving, interpreting and supervising the implementation of instructions and guidelines issued by the supervisory authority, both for normal operation and for the correction of identified shortcomings;

h) collecting, preparing and providing information or documentation to the supervisory authority and reference national CSIRTs, upon request or on its own initiative;

i) preparing and signing the system or asset applicability document;

j) ensuring that external companies and suppliers comply with the information security criteria established by the entity.

To perform these functions, they may rely on the collaboration of services provided by third parties.

4. Essential entities shall ensure that their information security officer meets the following requirements:

a) has the support of staff with suitable expertise and experience in cybersecurity, from a legal, organisational and technical perspective, to perform the relevant functions;

b) has access to the resources needed to perform their functions;

c) holds a position in the organisation that facilitates the development of their functions, participating in an appropriate manner and in all matters relating to safety and maintaining real and effective communication with the Administrative Board;

d) maintains due independence from information network and system managers.

Article 17. *Security incident handling*.

1. Essential and important entities shall manage and resolve security incidents affecting their own network and information systems. In the event that these incidents affect external networks and systems, they must take the measures necessary to guarantee that said actions are undertaken by the third-party providers.

This obligation applies both to incidents detected by the entity or provider itself and to those reported by the supervisory authority, through the reference national CSIRTs, when it becomes aware of any circumstances that raise suspicions of the existence of an incident.

2. Without prejudice to the provisions of the first paragraph, essential and important entities may voluntarily request the specialised assistance of their reference national CSIRT for incident handling, and in such cases must take into account the indications they

receive from the latter to resolve the incident, mitigate its effects and restore the affected systems.

3. In order to resolve incidents, essential and important entities shall apply the relevant aspects of the security management policy for information networks and systems, as well as the specific obligations established by the supervisory authorities where appropriate.

Article 18. *Reporting obligations.*

1. Essential and important entities shall report any significant incident that has occurred in their operation or in the provision of their services, as determined by regulation, based on its danger level and impact, to the supervisory authority without undue delay, through their reference national CSIRT. Where appropriate, they shall also notify recipients of their services who are likely to be affected, within the shortest possible time, any significant incidents likely to cause them substantial harm. These reports shall be sent via the information security officer.

The supervisory authorities shall ensure that the obliged entities report, among other details, any information enabling the cross-border impact of the incident to be determined.

2. Reports issued by essential or important entities shall refer to incidents affecting the information networks and systems used in their operation or in the provision of their services, whether they are their own networks and services or they belong to external providers.

3. The national reference CSIRTs shall use the National cyber incident reporting and monitoring platform to facilitate and automate reporting processes, communications and incident information and shall have access, confidential and complete, to full information, provided that it relates to their respective responsibilities and competences.

4. The obligation to report incidents does not detract from compliance with the legal duty to report facts that have the character of an offence to the competent authorities, in accordance with the provisions of Article 259 et seq. of the Code of Criminal Procedure, or to the competence to investigate them. Regardless of the obligations laid down in this Article, in the event of incidents with criminal characteristics, the provisions of Article 21 shall be followed.

5. The essential and important entities shall inform natural and legal persons receiving their services, as soon as possible, of any significant cyber threat that might affect them, as well as any measures or solutions that they might apply in response. They shall also act in the same manner with regard to cyber threats and cyber incidents reported to them by the supervisory authority or its reference national CSIRT.

6. The entities concerned shall submit the following to the supervisory authority, as soon as possible, through their reference national CSIRT.

a) Without undue delay and in any event within 24 hours of becoming aware of a significant incident, an early warning indicating, where appropriate, whether the significant incident is suspected of being caused by unlawful or malicious action or is likely to have cross-border implications.

b) No later than 72 hours after becoming aware of the significant incident, an incident report, updating the information referred to in point (a), where appropriate, and setting out an initial assessment of the significant incident, including its danger level and impact, as well as the indicators of compromise (IOCs), if available.

For trust service providers, where the incident affects the provision of their services, the time limit in the previous subparagraph shall be reduced to a maximum of 24 hours.

The reports referred to in this Article shall be forwarded to the supervisory authority immediately.

c) At the request of its reference national CSIRT or, where applicable, the supervisory authority, an interim report containing any updates on the situation.

d) A final report, not later than one month after submission of the incident report provided for in point (b), including the following:

i. a detailed description of the incident, including its danger level and impact;
ii. the type of main threat or cause likely to have triggered the incident;
iii. the mitigating measures that have been or are being applied;
iv. where applicable, the cross-border impact of the incident;
v. indicators of compromise (IoCs), as well as tactics, techniques and procedures (TTPs) detected in the incident;

e) if the incident is still ongoing at the time of submission of the final report provided for, the entities concerned shall submit a progress report at that time and a final report within one month of having managed the incident.

8. The supervisory authority or the reference national CSIRT in each case shall, without undue delay and where possible within 24 hours of receipt of the early warning referred to in paragraph 6(a), provide a response to the reporting entity, including its initial comments on the significant incident and, at the request of the entity, operational guidance or advice on the implementation of possible mitigation measures.

Where the reference national CSIRT is not the initial recipient of the report referred to in paragraph 1, the guidance shall be provided by the supervisory authority in collaboration with the reference national CSIRT. The reference national CSIRT shall provide additional technical support if so requested by the entity concerned. Where the incident is suspected to be of a criminal nature, the reference national CSIRT or supervisory authority shall also provide guidance for the purpose of reporting the significant incident to law enforcement authorities.

9. Where appropriate and particularly if the significant incident affects two or more Member States, the National Cybersecurity Centre shall inform the other Member States concerned and ENISA, without undue delay. This information shall include the type of information received in accordance with paragraph 6. In doing so, it shall, in accordance with the Union or national legal system, preserve the security and commercial interests of the entity, as well as the confidentiality of the information provided.

10. Where general knowledge of the significant incident is necessary in order to prevent other significant incidents or deal with another ongoing significant incident, or where disclosure is in the public interest, the National Cybersecurity Centre, the supervisory authorities and the CSIRTs or the competent authorities of other affected Member States may, after consulting the affected entity, publicly report the significant incident or require the entity to do so.

11. The National Cybersecurity Centre shall forward the reports received from the supervisory authorities pursuant to the provisions of paragraph 1 to the single points of contact of the Member States concerned without delay.

12. The National Cybersecurity Centre shall submit a summary report to ENISA every three months, including anonymised and aggregated data on significant incidents and incidents, cyber threats and near misses reported in accordance with paragraph 1 and Article 29.

13. The reference national CSIRTs, through the Cybersecurity Coordination Office under the Secretary of State for Security, shall provide the competent resilience authorities of critical entities, designated in accordance with the provisions of Law XXXX, with information on significant incidents, incidents, cyber threats and near misses reported in accordance with paragraph 1 and voluntary reports made in accordance with Article 29 by entities equivalent to critical entities.

14. The reports referred to in this Article shall be subject to the provisions of the National Cyber-incident Reporting and Management Instruction.

Article 19. *National cyber incident reporting and monitoring platform.*

1. Reporting obligations should preferably be met via the National cyber incident reporting and monitoring platform. This platform will be adapted, maintained and managed by CCN-CERT under the direction of the National Cybersecurity Centre without prejudice to the necessary collaboration mechanisms with INCIBE-CERT and ESPDEF-CERT. The requirements, procedures, mechanisms and responsibilities for operation of the platform by users shall be developed by regulation. The platform may be used for the notifications required by sectoral regulations.

2. Similarly, this platform will enable essential and important entities, the National Cybersecurity Centre, the supervisory authorities and the reference national CSIRTs to share technical information and monitor incidents in a secure and reliable manner, without prejudice to the specific requirements applicable to personal data protection.

3. The design and management of the platform will ensure the availability, authenticity, integrity, traceability and confidentiality of information, as well as the transparency of data processing before the National Cybersecurity Centre, the supervisory authorities and the reference national CSIRTs.

4. The platform will also provide various communication channels between the National Cybersecurity Centre, the supervisory authorities, sectoral points of contact and reference national CSIRTs, and will ensure that they have access to all information relating to incidents, within the scope of its competence. Specifically, they will be able to access all information enabling them to monitor and control their situation status and technical management at all times. Likewise, they will have access to all of the statistical data hosted on the platform in order to know the situation status within the scope of national cybersecurity.

5. The incident reporting and management procedure must also be carried out through the platform. It shall be available 24 hours a day, every day of the year, and shall have at least the following capabilities:
a) cyber-incident handling, incorporating taxonomy, criticality and third-party notifications;
b) information-sharing on cyber threats;
c) sample analysis;
d) vulnerability logging and reporting;
e) secure communication between parties involved in different forms and on different platforms;
f) bulk data exchange;
g) generation of aggregate reports and statistics.

6. Managers and users of the platform, in accordance with their respective competences, shall develop the corresponding personal data protection processes.

Article 20. *Incident information.*

1. The reference national CSIRTs shall provide reporting essential and important entities with information on the follow-up to the notification of an incident and particularly such information as may facilitate effective management of the incident.

In addition, the supervisory authorities and the reference national CSIRTs shall provide essential and important entities that may be affected by such incidents with any information that may be relevant to them, to prevent and, where appropriate, resolve the incident.

2. In providing the information referred to in the previous paragraph, the commercial interests of essential and important entities shall be safeguarded, taking into account the confidentiality of the information.

Article 21. *Action in response to incidents presumed to be criminal.*

1. All incidents that are considered significant and which may involve intentionality rather than accidental or fortuitous events will be considered cyber incidents presumed to be criminal.

2. To determine the possible criminal nature of incidents reported to the supervisory authorities via the reference national CSIRTs, the latter shall transfer the information they hold on these incidents to the Cybersecurity Coordination Office. The Cybersecurity Coordination Office may require the affected entities, supervisory authorities and reference national CSIRTs to provide any additional information relating to the incident that may be deemed necessary for this purpose.

3. In compliance with the provisions of Article 262 of the Code of Criminal Procedure, the Cybersecurity Coordination Office shall report any security incidents presumed to be criminal in nature that are reported to the supervisory authorities via the reference national CSIRTs, to the Public Prosecutor's Office. Where appropriate, the Cybersecurity Coordination Office, in the exercise of its functions, shall forward the information to the corresponding Organic Judicial Police Units, in accordance with their respective competences.

4. The Cybersecurity Coordination Office, in the exercise of its functions, may request that service and Internet service providers (ISPs) provide identification of the beneficial ownership of a technological asset involved, as well as associated information in the registries of country code top-level domain names (ccTLDs) '.es'.

Article 22. *Protection for the reporting party.*

1. Reporting does not involve any greater responsibility on the part of the entity.

2. Staff who are in a service relationship with the essential or important entity, who participate in the provision of its services and who report incidents, may not be sanctioned or suffer adverse consequences in their job or in the entity, except in cases where it can be proven that they have acted in bad faith and the corresponding workplace disciplinary file has been processed.

3. Any decisions taken by employers contrary to or to the detriment of the rights of workers who acted in accordance with the Article shall be deemed null and void.

Article 23. *Information and collaboration obligations.*

Essential and important entities shall provide the reference national CSIRTs or supervisory authorities with all information required for the performance of their tasks. In particular, they may be required to provide any additional information necessary to analyse the nature, causes and effects of the incidents reported and to complete the tasks assigned to them under this Law.

Article 24. *Cooperation in terms of the incidents that affect personal data*.

The supervisory authorities shall cooperate closely with the Spanish Data Protection Agency and, where appropriate, with the independent supervisory authorities of the Autonomous Communities, to deal with incidents that give rise to personal data breaches, informing them of any incidents that might compromise the security of personal data and should be reported, as well as their development. This is without prejudice to the tasks assigned to data controllers in relation to reports of possible breaches in the protection of personal data in accordance with the provisions of Organic Law 3/2018 of 5 December 2018 on the protection of personal data and the guarantee of digital rights and, where applicable, Organic Law 7/2021 of 26 May 2021 on the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties.

Article 25. *Authorisation for releasing personal data*.

If the reporting of incidents or their management, analysis or resolution requires the communication of personal data, the processing thereof shall be restricted to what is strictly appropriate and relevant and limited to what is necessary in relation to the purpose, of the actions indicated, pursued in each case.

The release of said data for such purposes shall only be deemed authorised in the following cases:

a) from essential and important entities to reference national CSIRTs or supervisory authorities;
b) between the reference national CSIRTs and the supervisory authorities;
c) between the reference national CSIRTs and the designated CSIRTs in other EU Member States;
d) between the reference national CSIRTs and other national or international CSIRTs;
e) between the single point of contact and the single points of contact of other Member States of the European Union.

Chapter IV
Registries of entities of a cross-border nature

Article 26. *Registry of providers of digital services and infrastructure.*

1. The National Cybersecurity Centre shall establish and maintain a registry with the list of providers of services and digital infrastructure. To this end, the supervisory authorities shall require DNS service providers, top-level domain name registries, entities providing domain name registry services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers and managed security service providers, providers of online marketplaces, online search engines and social networking services platforms, to submit the following information:

h) the name of the public entity;
i) the sector, subsector and type of entity referred to in Annexes I or II, where applicable;
j) the address of the main establishment of the entity and of its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 4(4);
k) the updated contact details, in particular the email addresses and telephone numbers of the institution and, where applicable, of its representative designated pursuant to Article 4(4);
l) the Member States in which the entity provides services;
m) the entity's IP ranges.

2. They shall also notify any changes to the information submitted without delay and in any event within three months of the date of the change.

3. Upon receipt of the information referred to in paragraphs 1 and 2, with the exception of the information referred to in paragraph 1(f), the National Cybersecurity Centre shall, without undue delay, transmit the information gathered to ENISA for inclusion in its registry of entities. The National Cybersecurity Centre may access the register upon

request to ENISA, without prejudice to the adoption by ENISA, where appropriate, of measures to ensure the confidentiality of the information.

4. Where appropriate, the information referred to in paragraphs 1. and 2. shall be transmitted in a secure manner through the national mechanisms put in place for that purpose.

Article 27. *Database of domain name registration data*.

1. For the purpose of contributing to the security, stability and resilience of the DNS, top-level domain name registries and entities providing domain name registration services shall collect and maintain accurate and complete data on the registration of domain names in a database in accordance with the provisions of the personal data protection regulation.

2. To this end, the database of domain name registration data shall contain the information necessary to identify and contact the domain name holders and the entities administering the domain names in the top-level domains. This information shall include the following elements:

a) the name of the domain
b) the registry date
c) the applicant's name, contact email address and telephone number
d) The contact email address and telephone number of the contact point administering the domain name if they are not those of the applicant.

3. Top-level domain name registries and entities providing domain name registration services shall develop policies and procedures, including checking procedures, to ensure that the databases referred to in paragraph 1 include accurate and complete information. These policies and procedures shall be public.

4. The registries of first-level domain names and entities providing domain name registration services shall make public, without undue delay after the registration of a domain name, that registry data that is not of a personal nature. They shall also grant legitimate requesters access to specific data on the domain name register, in accordance with the regulations on the protection of personal data, upon lawful and duly justified request. The request for access shall be decided upon without undue delay and in any event within 72 hours of receipt. The policies and procedures for the disclosure of such data shall be public.

5. Compliance with these obligations may not involve the collection of domain name registration data in duplicate. To this end, top-level domain name registries and entities providing domain name registration services shall cooperate with each other.

Chapter V
Information-sharing

Article 28. *Cybersecurity information-sharing arrangements*.

1. Entities falling within the scope of this Law and, where appropriate, other entities may voluntarily exchange relevant cybersecurity information with each other, in particular that relating to cyber threats, near misses, vulnerabilities, tactics, techniques and procedures, indicators of compromise, threat-actor-specific information, cybersecurity alerts and recommendations on configurations of security tools to detect cyber-attacks, provided that such information-sharing:

a) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;

b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or preventing their spread, or supporting a set of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyber threat research between public and private entities.

2. Information-sharing may take place between sectoral or cross-sectoral communities of essential and important entities and, where appropriate, between their providers or service providers, through cybersecurity information-sharing mechanisms that shall respect the potentially sensitive nature of the information shared and the fundamental rights of individuals.

3. These reporting mechanisms may specify operational elements, including the use of specific ICT platforms such as the National Network of Security Operations Centres, and automation tools, including the content and conditions of information-sharing mechanisms. Conditions may be imposed on the information that the supervisory authorities or the reference national CSIRTs must provide in these mechanisms.

4. The essential and important entities shall notify the supervisory authorities of their participation in the cybersecurity information-sharing mechanisms at the time of their incorporation or, where appropriate, their withdrawal.

Article 29. *Voluntary notification of relevant information*.

1. Without prejudice to the reporting obligations set out in Article 18, essential and important entities may report to the supervisory authorities, via the reference national CSIRTs, any incidents, cyber threats and near misses that they address.

Similarly, entities that provide vital or necessary services to the community and do not meet the requirements of Article 4 to be considered essential or important may report significant incidents, cyber threats or near misses.

Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon the notifying entity to which it would not have been subject had it not submitted the notification.

2. The notifications referred to in the previous paragraph shall be governed by the provisions of this Title and shall be reported to the National Cybersecurity Centre.

3. Mandatory notifications shall take precedence over voluntary notifications for the purposes of their management by the competent bodies.

Chapter VI
Supervision and enforcement

Article 30. *General aspects concerning the supervision of essential and important entities.*

1. Under the superior direction of the National Cybersecurity Centre, as the competent national authority, the supervisory authorities shall supervise and take the necessary measures to ensure compliance with this Law. Supervisory methodologies may be established to allow prioritisation of such tasks using a risk-based approach.

2. In the exercise of supervisory functions, essential and important entities may be required to provide all information necessary to assess the security of network and information systems, including documentation on security policies. In addition, they may request information from the operators regarding the effective application of their security policy, as well as audit or require the entity to submit the security of its networks and information systems to an audit by a security compliance framework certification entity.

In particular, the actions of the supervisory authorities shall aim to:

a) monitor compliance with the standards, guidelines, specifications and technical instructions, as well as any other provisions that may be applicable to the entities subject to their supervision;

b) check that the functions of the information security officer designated by the essential and important entities are being carried out.

c) Carry out the controls, inspections, tests and reviews necessary to check compliance with the security measures.

3. Essential and important entities shall collaborate in this supervision by facilitating inspection actions, providing all information required to that effect, and implementing orders or instructions issued, where appropriate, to remedy the deficiencies identified. These measures may also apply to third-party ICT service providers providing services in favour of supervised entities.

Article 31. *Supervisory and enforcement measures in relation to essential entities*.

1. The supervisory or enforcement measures imposed by the supervisory authorities on essential entities in relation to their obligations shall be effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. The supervisory authorities, in the exercise of their supervisory functions, may take at least the following measures in relation to essential entities.

a) On-site inspections and off-site supervision, which may include random checks conducted out by qualified professionals.
b) Regular and targeted security audits carried out, when applicable, by an accredited Certification Body of the National Security Scheme. In any other case, the assessment may be carried out by an accredited cybersecurity conformity assessment body, in accordance with the procedures and at the intervals determined by the regulations of the National Cybersecurity Centre. Such security audits shall be based on risk assessments, their results shall be communicated to the supervisory authority and to the National Cybersecurity Centre and their costs shall be borne by the audited entity, except in duly substantiated cases where the National Cybersecurity Centre adopts another resolution.
c) Extraordinary audits, including where justified on the ground of a significant incident or an infringement by the essential entity.
d) Security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned.
e) Requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the supervisory authority.
f) Requests to access data, documents and information necessary to carry out their supervisory tasks.
g) Requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

3. When exercising its powers under points (e), (f) or (g) of paragraph 2, the supervisory authority shall indicate the purpose of the request and specify the information required. In the exercise of its supervisory functions, the supervisory authority may collect and analyse the Audit and Certification Reports to which the entity has been subject.

4. When exercising its enforcement powers, the supervisory authority may at least:

a) warn the entities concerned about infringements;
b) adopt binding instructions, which shall set out the measures necessary to prevent or remedy an incident, the deadlines for implementing those measures and notifying their implementation, or an order requiring the entities concerned to remedy the deficiencies or infringements identified;
c) where appropriate, order the entities concerned to cease conduct that infringes this legislation and desist from repeating that conduct;
d) order the entities concerned to ensure the compliance of their cybersecurity risk-management measures or to comply with the reporting obligations in a specified manner and within a specified period;
e) order the entities concerned to inform the natural or legal persons for whom they provide services or carry out activities which may be affected by a significant cyber threat of the nature of the threat, as well as of any possible corrective or remedial measures that may be taken by those persons in response to that threat;
f) order the entities concerned to implement the recommendations provided following a security audit, within the deadline set by the supervisory authority;
g) designate a monitoring officer to oversee, for the period to be determined, the compliance of the institutions concerned with their obligations;
h) order the entities concerned to make public certain aspects of infringements in a specified manner;
i) exercise the legal authority to impose penalties in the cases and terms provided for, as well as process the administrative procedures derived from this Law in all cases.

5. Where the enforcement measures adopted pursuant to points (a), (b), (c), (d) and (f) of paragraph 4 are ineffective in achieving the purposes for which they are intended, the supervisory authority shall set a deadline for the essential entity to take the necessary measures to remedy the deficiencies or comply with the requirements, without prejudice to any responsibilities that may be required. If these measures are not taken within the established time limit, the supervisory authority, after coordination of the National Cybersecurity Centre, shall have the power to:

a) temporarily suspend, or request a certification or authorisation body, or a court or tribunal, in accordance with the legal system, to suspend temporarily a certification or authorisation relating to some or all of the services or activities concerned provided by the essential entity;

b) request that the relevant bodies, courts or tribunals, in accordance with the legal system, prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level in the essential entity from exercising managerial functions.

Temporary suspensions or prohibitions that are imposed shall be applied only until the affected entity takes the necessary measures to remedy the deficiencies or comply with the requirements of the supervisory authority. The imposition of such temporary suspensions or prohibitions shall be subject to appropriate safeguards in accordance with the general principles of the legal system.

The enforcement measures provided for shall not be applicable to public sector entities within the scope of this Law.

6. Natural persons representing essential entities, as well as the authority competent to take decisions on their behalf or to exercise their control, shall supervise compliance with the provisions of this regulation, assuming, where appropriate, responsibility for the breach of this duty.

7. Where one of the enforcement measures referred to in paragraphs 4 or 5 is adopted, the same circumstances provided for in Article 38 must be considered.

8. The supervisory authority shall duly justify the enforcement measures it adopts and shall, prior to their adoption, notify its preliminary findings to the entities concerned. They shall also be given a period of 15 days to make representations, except in duly substantiated cases where immediate action to prevent or respond to incidents would otherwise be impeded.

9. The supervisory authority shall inform the competent authorities for the protection of critical entities when exercising its supervisory and enforcement powers in order to ensure compliance with this Law by an entity identified as critical. Where appropriate, the competent authorities for critical entities may request the supervisory authority to exercise their supervisory and enforcement powers in respect of an entity that is identified as a critical entity.

10. The supervisory authority shall also cooperate with the authorities designated pursuant to Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022. In particular, it shall ensure compliance with the reporting obligations vis-à-vis the Supervisory Forum.

11. The National Cybersecurity Centre may urge the supervisory authorities to exercise supervisory and enforcement powers in respect of any essential entity.

12. Where necessary, the supervisory authorities may request the support of CCN-CERT, as the reference national CSIRT for essential entities, for the performance of their monitoring and enforcement tasks.

Article 32. *Supervisory and enforcement measures in relation to important entities*.

1. When provided with evidence, indication or information that an important entity allegedly does not comply with the provisions of this Law, the supervisory authority shall, where appropriate, apply ex post supervision measures. These measures must be effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. For the exercise of its supervisory functions over important entities, the supervisory authority shall have the powers to grant at least:

a) On-site inspections and ex-post off-site supervisions conducted by trained professionals.
b) Regular and targeted security audits carried out, when applicable, by an accredited Certification Body of the National Security Scheme. In any other case, the assessment may be carried out by an accredited cybersecurity conformity assessment body, in accordance with the procedures and at the intervals determined by the regulations of the National Cybersecurity Centre. Such security audits shall be based on risk assessments, their results shall be communicated to the supervisory authority and to the National Cybersecurity Centre and their costs shall be borne by the audited entity, except in duly substantiated cases where the National Cybersecurity Centre adopts another resolution.
c) Security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned.
d) Requests for information necessary to assess ex post the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the supervisory authority.
e) Requests to access data, documents and information necessary to complete their supervisory tasks.
f) Requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

The targeted security audits referred to in point (b) shall be carried out in accordance with the risk assessments carried out by the supervisory authority or the audited entity.

The results of the targeted security audits carried out shall be submitted to the supervisory authority. The costs of said targeted security audit carried out by an

independent body shall be borne by the audited entity, except in duly substantiated cases where the supervisory authority decides otherwise.

When exercising its powers under points (d), (e) or (f), the supervisory authority shall indicate the purpose of the request and specify the information required.

3. For the exercise of its enforcement functions in relation to important entities, the supervisory authority shall have powers to at least:

a) warn the entities concerned about infringement of this Law;
b) adopt binding instructions or an order requiring the entities concerned to remedy the deficiencies or infringements identified;
c) order the entities concerned to cease conduct that infringes this Law and desist from repeating that conduct;
d) order the entities concerned to ensure that their cybersecurity risk-management measures comply with the provisions of Article 15 or to comply with the reporting obligations laid down in Article 18, in a specified manner and within a specified period;
e) order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which may be affected by a significant cyber threat of the nature of the threat as well as of any possible corrective or remedial measures that may be taken by those persons in response to that threat;
f) order the entities concerned to implement the recommendations provided following a security audit within the legally authorised deadline or, failing that, within a reasonable deadline;
g) order the entities concerned to make public certain aspects of infringements of this Law;
h) exercise the legal authority to impose penalties in the cases and terms provided for, as well as process the administrative procedures derived from this Law in all cases.

4. The provisions of paragraphs 6, 7 and 8 of the previous Article shall also apply to the supervisory and enforcement measures provided for in this Article in the case of important entities.

5. The supervisory authority shall cooperate with the competent authorities designated for digital operational resilience in the financial sector pursuant to Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022. In particular, when exercising its supervisory and enforcement powers to ensure compliance by an important entity that is designated as an essential ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554, it shall report to the Supervisory Forum.

6. Where necessary, the supervisory authorities may request the support of the reference national CSIRT for the performance of their monitoring and enforcement tasks.

Article 33. *Use of European cybersecurity certification schemes.*

The National Cybersecurity Centre, through the supervisory authorities, shall encourage essential and important entities to comply, where appropriate, with the requirements expressed by the implementing acts of the European Commission regarding the mandatory use of certain certified ICT products, ICT services, ICT processes or managed security services or certification under a European cybersecurity certification scheme pursuant to Article 49 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Regulation).

Article 34. *Mutual assistance.*

1. The monitoring and enforcement functions shall be carried out in cooperation with the competent national authorities of other Member States of the European Union when they concern entities providing services in more than one Member State, or providing services in one or more Member States and their network and information systems are located in one or more other Member States. Such cooperation shall involve at least:

a) informing and consulting the respective national competent authorities, via the single points of contact; concerning the supervisory and enforcement measures taken;
b) requesting the adoption of supervisory or enforcement measures between national competent authorities;
c) providing assistance proportionate to the resources at their disposal, at the reasoned request of the competent national authorities of another Member State, so that supervisory or enforcement measures can be applied in an effective, efficient and consistent manner.

This mutual assistance may cover requests for information and supervisory measures, including requests for on-site inspections, off-site supervision or targeted security audits.

2. Requests for assistance shall be binding on the supervisory authorities, unless they are not competent to provide the assistance required or such assistance is not in accordance with their supervisory tasks, or the request concerns information or involves activities which, if disclosed or carried out, would be contrary to essential interests of national security, public security or defence. Before denying such a request, at the petition of one of the Member States concerned, the National Cybersecurity Centre shall consult the European Commission and ENISA.

3. By mutual agreement, the supervisory authorities may undertake joint supervisory measures with the competent national authorities of other Member States.

Chapter VII
Penalties regime

Section 1. General rules

Article 35. *Responsible parties*.

1. Responsibility for the envisaged offences shall reside with the essential and important entities responsible for the action constituting the offence.

2. The members of the management bodies of the entities shall be jointly and severally liable for offences committed by the latter.

Article 36. *Powers to impose penalties*.

The following parties shall have powers to impose penalties:

in the case of very serious offences, the person in charge of the Ministry of Defence, the Ministry for the Digital Transformation and Civil Service or the Ministry of the Interior with respect to the entities respectively included within the scope of competence of the supervisory authorities under them, following a mandatory report from the National Cybersecurity Centre;

in the case of serious and minor offences, the supervisory authorities designated in accordance with Article 7(1) in respect of the entities included within the scope of their respective competence.

Article 37. *Criteria for progressive penalties*.

In order to determine the penalty applicable in each case, in addition to those set out in Article 29 of Law 40/2015 of 1 October 2015 on the Legal Regime of the Public Sector, the following circumstances will be taken into account:

a) the nature, gravity and duration of the offence or non-compliance,
b) the intentional or culpable nature of the offence,
c) the repetition of more than one offence of a similar nature within 2 years, where a final administrative decision to this effect has been issued,
d) the degree of cooperation with the supervisory authorities of the essential or important entity,
e) failure to report or remedy significant incidents, as well as failure to remedy deficiencies after receiving binding instructions from the supervisory authorities,

f) the degree of obstruction of the audits or supervisory activities ordered by the supervisory authority following the finding of non-compliance,
g) the provision of false or manifestly inaccurate information in relation to established cybersecurity risk-management measures or reporting obligations,
h) material or non-material damage caused, including financial or economic losses, effects on other services and the number of users affected,
i) measures taken by the entity to prevent or reduce material or non-material damage or damage,
j) any adherence to approved codes of conduct or certification mechanisms,
k) the nature and size of the essential or important entity, as provided for in Article 4,
l) the degree of responsibility of the essential and important entity, taking into account the technical and organisational measures adopted to comply with this Law,
m) the degree of impact on provision of the essential service.

Section 2. Offences and penalties

Article 38. *Classification of offences.*

The administrative offences described in this Law are classified as very serious, serious and minor.

Article 39. *Very serious offences.*

The following constitute very serious offences.

a) Failure to implement, without undue delay, the technical, operational and organisational measures identified by the National Cybersecurity Centre vis-à-vis the management of security risks in network and information systems, as referred to in Article 15, where that omission has caused a significant incident.
b) Repeated non-compliance with the obligation to report significant incidents as provided for in Article 18. The non-compliance shall be deemed repeated after the second instance.
c) Failure to take the technical, operational and organisational measures necessary to resolve a significant incident in accordance with the provisions of Article 17(1).
d) Failure to provide the information required by the Cybersecurity Coordination Office to determine the possible criminal nature of incidents in the terms required by Article 21, where the conduct of an investigation has been seriously impaired or where repeated non-compliance is involved. The non-compliance shall be deemed repeated after the second instance.
e) Failure to comply with the specific obligations to ensure the security of network and information systems established by the National Cybersecurity Centre in situations of justified need.

f) Repeated failure to provide the information requested by the supervisory authority pursuant to Article 23. The non-compliance shall be deemed repeated after the second instance.

Article 40. *Serious offences*.

The following constitute serious offences:

a) failure or unjustified delay in the implementation of the technical, operational and organisational measures determined by the National Cybersecurity Centre vis-à-vis the management of security risks in network and information systems, as referred to in Article 15;
b) Impediment, hindrance or failure to carry out the actions agreed by the supervisory authority in the exercise of its supervisory functions, in accordance with the provisions of Articles 31(2) and 32(2);
c) serious failure to comply with binding orders or instructions issued by the supervisory authority in the exercise of enforcement functions, as well as the implementation deadlines, provided for in Articles 31(4) and 32(3);
d) non-compliance, within the time allowed for that purpose, or poor compliance with the remedial measures or requirements imposed upon the essential entities by the supervisory authority as referred to in Article 30(3), where the enforcement measures adopted pursuant to points (a) to (d) and (f) of Article 31(4) are ineffective;
e) dissemination of false or misleading information to the public regarding standards met or valid security certification held;
f) failure to comply with the obligation to report significant incidents as referred to in Article 18;
g) failure to provide the information required by the supervisory authority or the reference national CSRIT in accordance with Article 23;
h) failure to provide the information required by the Cybersecurity Coordination Office to determine the possible criminal nature of incidents in the terms required by Article 21;
i) failure to designate a person, unit or collegiate body as information security officer in accordance with Article 16, or the latter lacks the required accreditation or does not comply with the provisions included in this legislation concerning their capabilities or functions within the entity;
j) failure to comply with the obligation laid down in Article 31(6) that natural persons with powers of representation or decision, or exercising control in this regard have competence to ensure compliance with this rule and, where appropriate, may be held liable for the breach of their duties within the framework of this Law;
k) failure to comply with the obligations laid down in Article 4(4) to communicate their inclusion in the list of essential and important entities or their self-

registration, where appropriate, or to submit the information provided for therein;

l) failure to comply with the obligations to submit information required in accordance with Article 26(1), as well as the late submission referred to in Article 26(2);
m) failure to collect and maintain accurate and complete data on the registration of domain names as reflected in Article 27;
n) failure to request specialist assistance from the reference national CSIRT if the essential and important entities cannot resolve incidents themselves.

Article 41. *Minor offences*

The following constitute minor offences:

a) serious failure to comply with binding orders or instructions issued by the supervisory authority in the exercise of enforcement functions, as well as the implementation deadlines, provided for in Articles 31(4) and 32(3);
b) compliance with the obligation to report significant incidents without collecting the information to be gathered by the different incident notification reports taking into account the provisions of Article 18;
c) submission of incomplete, inaccurate or unduly delayed information to the supervisory authority or to the reference national CSIRT in accordance with Article 23;
d) failure to inform the natural or legal persons for whom they provide services or with regard to which they carry out activities which may be affected by a significant cyber threat, about the nature of the threat, as well as about any possible corrective or protective measures that those persons may take in response to it;
e) non-compliance with the obligation to inform the respective supervisory authority in good time of the designation of the information security officer, as well as subsequent appointments and dismissals;
f) failure to comply with the training obligations for employees and management bodies included in this Law;
g) incomplete or inaccurate communication of the information referred to in Article 4(4) or failure to comply with the duty to communicate any changes to the information submitted, in the form and within the time limits laid down in that Article.

Article 42. *Penalties.*

1. Very serious offences shall be punishable by a fine of EUR 500 001 to EUR 2 000 000.

However, very serious offences referred to in Article 39(a) and (b) committed by an essential entity may be punishable by a fine of up to EUR 10 000 000 or an amount

equivalent to 2% of the total worldwide annual turnover achieved by the undertaking to which the essential entity belongs during the preceding financial year, whichever is higher.

Very serious offences referred to in Article 39(a) and (b) committed by an important entity may be punishable by a fine of up to EUR 7 000 000 or an amount equivalent to 1.4% of the total annual worldwide turnover achieved by the company to which the important entity belongs during the previous financial year, whichever is higher.

2. Serious offences shall be punishable by a fine of EUR 100 001 to EUR 500 000.

3. Minor offences shall be punishable by a fine of EUR 10 000 to EUR 100 000.

4. The fine imposed for very serious and serious offences may be accompanied by the ancillary penalty of public reprimand in the Official State Gazette, which shall indicate the person responsible and the nature of the offence.

Article 43. *Public sector offences.*

1. Offences committed by public sector bodies, agencies or entities shall not be subject to penalties. However, the body competent to impose penalties shall, by means of a resolution, take such measures as it deems appropriate to end and remedy the effects of the offence. This resolution shall be notified to the offending body or entity and to those affected, if any.

In addition, the body imposing the penalty may also propose launching disciplinary action as it deems necessary.

2. The resolutions adopted to implement the measures referred to in the previous paragraph shall be communicated to the body imposing the penalty.

Section 3. Penalties procedure

Article 44. *Legal regime.*

The exercise of legal authority to impose penalties shall be governed by the provisions of Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations and Law 40/2015 of 1 October 2015 on the Legal Regime of the Public Sector, without prejudice to the specialties regulated in this chapter.

Article 45. *Concurrence of offences.*

1. Actions that have already been subject to criminal or administrative penalties may not be punished when the identity of the subject is established in legal fact and basis.

2. If, as a result of action to impose penalties, deeds come to light that could constitute offences under other laws, they will be reported to the competent bodies or agencies for the purposes of initiating the appropriate penalties procedure, where appropriate.

Article 46. Subordination of the administrative penalties procedure to the criminal procedure.
1. Facts established by final criminal court decisions shall be binding on the administrative body in respect of penalty proceedings based on the same facts.

2. If the existence of a criminal offence has not been established, or if any other decision has been issued to terminate the criminal proceedings, the penalty proceedings may be initiated or continued.

3. In any of the above cases, the judicial authority or the Public Prosecutor's Office shall notify the administrative body of the resolution or agreement that they have adopted, in order that it may decide whether or not to pursue the corresponding penalties procedure.

Article 47. *Provisional measures.*

Provisional measures may be adopted in accordance with Article 56 of Law 39/2015 of 1 October 2015, which must be ratified, amended or revoked in the agreement to initiate the procedure, within a maximum period of 15 days from their adoption.

The supervisory authorities are empowered to set a time limit within which the essential entity must take the necessary measures to remedy the deficiencies or comply with the requirements of those authorities. If the required measures are not taken within the set time limit, the supervisory authorities shall be empowered to:

a) temporarily suspend or request a certification body, in accordance with the legal system, to temporarily suspend a certification or authorisation relating to some or all of the services or activities concerned provided by the essential entity;

b) request that the competent bodies or courts in accordance with the legal system temporarily prohibit the exercise of their functions by any person exercising managerial responsibilities at the level of director-general or legal representative in that essential entity.

3. The provisional measures provided for shall not apply to public sector entities subject to this Law.

Article 48. *Expiry of the proceedings.*

1. The proceedings shall expire six months after their initiation without notification of their resolution, although calculation of this period must take into account any stoppages for reasons attributable to the interested party, or any suspension agreed due to the existence of criminal judicial proceedings in which the subject is identified and there are facts and grounds, until the end of these proceedings.

2. The resolution declaring expiry shall be notified to the party concerned and shall terminate the proceedings, without prejudice to the fact that the administration may decide to initiate new proceedings until such time as the offence is time-limited.

3. Expired proceedings shall not interrupt the limitation period.

Article 49. *Limitation of offences.*

1. The administrative offences referred to in this Law shall be time-limited to six months, one year or two years from the date on which they were committed, depending on whether they are minor, serious or very serious, respectively.

2. The time limits laid down in this Law shall be calculated from the day on which the offence was committed. However, in the case of continuous offences and offences with permanent effects, the time limits shall be calculated from the end of the offending behaviour or from the last action constituting the offence, respectively.

3. The limitation period shall be interrupted by initiation of the penalties procedure, with the knowledge of the interested party, and the limitation period shall be restarted if the disciplinary proceedings are suspended for more than one month for a reason that cannot be attributed to the party presumed to be responsible.

4. Similarly, the limitation period shall be suspended as a result of the opening of criminal judicial proceedings for the same facts, until the judicial authority informs the administrative body of their termination, in which case the administrative body shall refrain from continuing with the penalty procedure until the judicial authority issues a final judgment or decision that ends the criminal proceedings, or the Public Prosecutor’s Office agrees that it is inappropriate to initiate or continue with criminal proceedings; until such time, the limitation period remains suspended .

Article 50. *Limitation of penalties.*

1. Penalties for very serious offences shall expire after three years, those imposed for serious offences after two years, and those imposed for minor offences after one year from the day following that on which the resolution imposing the penalty became final.

2. The limitation period shall be interrupted by initiation of the enforcement procedure, with the knowledge of the person concerned, and the time limit shall be resumed if it is suspended for more than one month for reasons not attributable to the offender.

First additional provision. *National Cyber Security Centre*

The Government shall, no later than 12 months after the entry into force of this Law, approve the Royal Decree determining the status, nature and administrative structure of the National Cybersecurity Centre, attached to the Cabinet of the Presidency of the Government, directing and coordinating, under a single authority, the exercise of the State powers provided for in this Law.

It shall also assume any other functions entrusted to it in the field of national cybersecurity, without prejudice to the powers legally reserved to other bodies and institutions.

Second additional provision. *Special regime for the Bank of Spain.*

The provisions of this Law shall apply without prejudice to the powers and duties conferred upon the Bank of Spain, the European Central Bank and the European System of Central Banks, in accordance with the Treaty on the Functioning of the European Union, the Statute of the European System of Central Banks and of the European Central Bank, Council Regulation (EU) No 1024/2013 of 15 October 2013, conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions, and Law 13/1994 of 1 June 1994 on the Autonomy of the Bank of Spain.

Third additional provision. *Incident information in the financial system.*

The supervisory authorities and reference national CSIRTs shall inform the head of the Secretariat of State for Economic Affairs and Business Support, through the General Secretariat of the Treasury and International Finance, of any incidents that might have significant impacts on the essential services of the financial system.
For these purposes, it will be understood that they have significant effects when their threshold or level of impact is critical, very high or high, as indicated in the instructions and incident communication guides, including the Spanish National Guidelines for Reporting and Managing Cyber Incidents included as an Annex to Royal Decree 43/2021 of 26 January 2021 on the security of networks and information systems.

Fourth additional provision. National cyber incident reporting and monitoring platform.

The National cyber incident reporting and monitoring platform included in Article 19 of this Law, will be the common platform provided for in Article 19(4) of Royal Decree-Law 12/2018 and developed by Article 11 of Royal Decree 43/2021.

Fifth additional provision. *Database of security incidents that are of a criminal nature.*

1. The Directorate-General for Coordination and Studies, of the State Secretariat for Security, will be the body responsible for processing the database of security incidents that are of a criminal nature.

2. The purpose of this processing is to use the data obtained in the management, monitoring and resolution of cybersecurity incidents affecting essential or important entities, when they can be presumed to be criminal.

3. At least the data relating to the identity of persons, data identifying terminals and connectivity devices and the personal identity and contact data of the controllers, managers and users of the processing file may be processed.

4. The recipients of the data will be the criminal courts, the Public Prosecutor's office and security forces and bodies, as well as other entities legally provided for.

These recipients shall also be responsible for the processing of the data communicated to them in accordance with the provisions of this Law.

5. The main legal basis of the processing in accordance with the objective and purpose of this Law is compliance in accordance with the provisions of Articles 11 and 13 of Organic Law 7/2021 of 26 May 2021 on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties, without prejudice to the application to this processing of the legislation governing the exercise of judicial power or any other that may apply.

The legal basis applicable to transfers of personal data to third countries or international organisations shall comply with the provisions of Articles 43 to 47 of Organic Law 7/2021 of 26 May 2021.

6. Only such data as is necessary for fulfilment of the established purposes shall be collected, in accordance with the principle of data minimisation.

7. Data collection will be carried out in accordance with the legislation in force, with particular attention to compliance with the duty to inform the data subjects, as well as possible recipients, of the conditions, rights and obligations associated with the processing, under the terms provided for in law.

8. According to the purpose of the processing, the data collected will be retained for such time as is necessary to fulfil the purpose for which it was collected, under Article 8 of Organic Law 7/2021 of 26 May 2021 and, where appropriate, for the time necessary to address any responsibilities deriving from its processing before the competent administrative or judicial bodies. Once that retention period has elapsed, the data shall be deleted or redacted in such a way that it cannot be correlated with or used to identify the data subjects.

9. Data controllers must ensure the application of the mandatory security measures resulting from the corresponding risk analysis, taking into account, in any case, the provisions of Royal Decree 311/2022 of 3 May 2022 regulating the National Security Scheme.

10. The exercise of rights for natural persons subject to data protection legislation shall be guaranteed in accordance with that legislation. Requests for such rights will be met by the data controller in the terms established in the legislation in force in accordance with each of the specific cases and the corresponding point in the procedure.

Depending on the possible procedural stage or situation of the processing in which the data is found, in order that investigations are not hindered and to avoid compromising the detection, investigation and prosecution of offences, the data controller will act in accordance with Article 26 of Organic Law 7/2021, of 26 May 2021, or restrict the rights of access, rectification, limitation and deletion with respect to the processing of data in the file.

This restriction will affect the content of the information to be provided in the event that exercise of any of these rights is requested, being replaced depending on the case, by a neutral wording or one that informs about the existence of the restriction, its reasons and the possibility of filing a complaint with the data protection authority. The information shall be provided in accordance with the provisions of Article 24 of Organic Law 7/2021 of 26 May 2021, within a period of one month, extendable by another two months from receipt of the request and via the means that the interested party has used to make it. The data controller shall document the factual and legal grounds on the basis of which the decision to refuse exercise of the right has been taken. That information shall be made available to the data protection authorities.

Should criminal proceedings be initiated as a result of the processing of personal data, the duty to provide information under the terms provided for in the Code of Criminal Procedure must be complied with.

Sixth additional provision. Safeguarding of essential State interests and functions.

1. The obligations established shall not involve the provision of any information whose disclosure would be contrary to the essential interests of Spain in terms of national security, public security or national defence. Information that is considered confidential in accordance with the legal system of the European Union or national law shall be exchanged with the Commission and other competent authorities only where necessary for the purposes of application of this Law, and shall be limited to information that is relevant and proportionate to the purpose of that exchange. In any case, the confidentiality, security and commercial interests of the entities concerned shall be preserved.

2. The provisions of this Law are without prejudice to the regulations concerning the exercise of powers for the safeguarding of national security and defence, as well as other essential functions of the State including the management of electoral processes and direct consultations with the electorate, maintenance of public security and classified information, and the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties.

Seventh additional provision. *Representation at the European Industrial Competence Centre*.

Under the supervision and direction of the National Cybersecurity Centre, the State Secretariat for Telecommunications and Digital Infrastructure of the Ministry for the Digital Transformation and Civil Service will represent Spain on the Administrative Board of the European Cybersecurity Industrial, Technology and Research Competence Centre, established by Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021. Similarly, the National Cybersecurity Institute shall also act as the National Coordination Centre for the purposes of that regulation, under the supervision and direction of the National Cybersecurity Centre.

Eighth additional provision. *National Cybersecurity Certification Authority*.

1. In accordance with Article 58(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) and with Articles 1 and 2(2)(c) of Royal Decree 421/2004 of 12 March 2004 regulating the National Cryptological Centre, the director of that body will be the national cybersecurity certification authority.

2. The National Cybersecurity Certification Authority shall have the functions and powers set out in Article 58(7) and (8) of the aforementioned European Regulation.

3. The National Cybersecurity Certification Authority is empowered to issue the necessary provisions to ensure that the European certification schemes to be established function correctly at national level.

4. In all matters relating to the application of this Law, the National Cybersecurity Certification Authority shall exercise its functions, powers and faculties under the supervision and direction of the National Cybersecurity Centre.

First transitional provision. *Communication obligations.*

1. The National Cybersecurity Council, through the Permanent Cybersecurity Commission as a working group supporting the Council, chaired by the Department of National Security, shall, by 17 April 2025:

a) notify the Commission and the European Union Cooperation Group of the number of essential and important entities in each sector and subsector referred to in Annex I or II;

b) notify the Commission of relevant information on the number of essential and important entities identified, the sector and sub-sector identified in Annex I or II to which they belong, the type of service they provide and the provision under which they were identified.

These notifications will then subsequently be updated every two years through the National Cybersecurity Centre.

The names of the essential and important entities referred to in point (b) may be notified to the Commission at its request and before 17 April 2025.

2. The National Cybersecurity Council, through the Department of National Security, after approval by the Standing Committee on Cybersecurity, shall notify the European Commission of the identity of its cybersecurity crisis management authority and any subsequent amendments thereto within three months of the entry into force of this Law.

3. The National Cybersecurity Council, through the Department of National Security, after approval by the Standing Committee on Cybersecurity, shall, within three months of its adoption, submit to the European Commission and the European cyber crisis liaison organisation network (EU-CyCLONe) the relevant information concerning to the requirements of the Large-scale Cybersecurity Incident and Crisis Response Plan, being able to exclude information where and to the extent necessary for national security.

4. The National Cybersecurity Council, through the Department of National Security, after approval by the Standing Committee on Cybersecurity, shall notify the European

Commission without undue delay of the identity of the reference national CSIRTs designated pursuant to Article 10 and any subsequent changes to the notification.

Second transitional provision. *Registry of entities*.

1. The National Cybersecurity Council, through the Permanent Commission on Cybersecurity as a working group in support of the Council, chaired by the Department of National Security, shall draft the list of essential and important entities referred to in Article 4(3) by 17 April 2025, using the National cyber incident reporting and monitoring platform.

2. In addition, providers of digital services and infrastructure referred to in Article 26(1) must submit the data referred to in Article 28 to the supervisory authority by 17 January 2025.

Third transitional provision. *Transitional regime*.

1. Until the National Cybersecurity Centre starts its activities, the provisions of Royal Decree-Law 12/2018 of 7 September 2018 and Royal Decree 43/2021 of 26 January 2021 relating to the competent authorities, reference national CSIRTs and single point of contact shall remain in force on a temporary basis.

2. Until such time as the National Instruction on Notification and Management of Cyber Incidents is amended, replaced or repealed, significant incidents will be considered those that can be categorised with a high, very high or critical level of danger or impact, in accordance with the provisions of said Instruction.

3. Until the establishment of the National Cybersecurity Centre, issuance of the report required under Article 36 shall not be mandatory in penalty proceedings for very serious offences.

Sole repealing provision. *Repeal of regulations*.

1. The following instruments are now repealed:

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

b) Royal Decree 43/2021 of 26 January 2021 implementing Royal Decree-Law 12/2018 of 7 September 2018 on the security of information networks and systems, are repealed, with the exception of the National Cyber-incident Reporting and Management Instruction contained in its annex, which shall remain in force until expressly amended, replaced or repealed.

2. Similarly, any provisions of equal or lower rank that are contrary to the provisions of this Law shall be repealed.

First final provision. *Attribution of powers*.

This Law is issued in accordance with Article 149(1) points (21) and (29) of the Spanish Constitution, which respectively grant the State exclusive competence in matters relating to the general telecommunications regime and public security.

Second final provision. *Amendment of Law 5/2014 of 4 April 2014 on Private Security*.

Article 3(2) of Law 5/2014 of 4 April 2014 on Private Security is amended to read as follows:
'2. Similarly, to the extent relevant in each case, they shall apply to establishments required to have security measures, to users of private security services, to engineers and technicians carrying out the tasks assigned to them by this Law, to security operators, to staff performing cybersecurity tasks in cases determined by law or regulation, to teachers at training centres, to companies providing IT security services, to reception stations for private alarms and to training centres for private security staff.'

Article 2(9) of Law 5/2014 of 4 April 2014 on Private Security is amended to read as follows:
'9. Accredited staff: teachers at training centres, engineers and technicians carrying out the tasks assigned to them by this Law; security operators; and staff performing cybersecurity tasks in cases determined by law or regulation.'

Third final provision. *Regulatory development*.

The heads of the Ministries of Defence, the Interior and for the Digital Transformation and Civil Service, as well as the heads of the Ministries and bodies listed in Article 7, are empowered, within the scope of their respective competences, to issue the necessary provisions for the development and application of the provisions of this Law.

Fourth final provision. *Incorporation into European Union law*.

This Law incorporates into Spanish law Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 ('NIS 2 Directive').

Fifth final provision. *Entry into force*.

This Law will enter into force on the day after its publication in the Official State Gazette (*Boletín Oficial del Estado*).

ANNEX I

HIGHLY CRITICAL SECTORS

Sector		Subsector		Type of entity	Sectoral point of contact
1.	Energy	a)	Electricity	Electricity undertakings as defined in Article 2(57) of Directive (EU) 2019/944 of the European Parliament and of the Council (1) performing the function of 'supply' as defined in Article 2(12), of that Directive	Ministry for the Ecological Transition and the Demographic Challenge, through the Secretariat of State for Energy.
				Distribution system operators, as defined in Article 2, point (29) of Directive (EU) 2019/944	
				Transmission system operators, as defined in Article 2(35) of Directive (EU) 2019/944	
				Producers, as defined in Article 2(38) of Directive (EU) 2019/944	
				Nominated electricity market operators, as defined in Article 2(8) of Regulation (EU) 2019/943 of the European Parliament and of the Council (2)	
				Market participants, as defined in Article 2(25), of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services, as defined in Article 2(18), (20) and (59) of Directive (EU) 2019/944	
				Charging point operators who may be responsible for	

				the management and operation of a charging point that provides a charging service to users, including in the name and on behalf of a mobility service provider.	
		b)	District heating and cooling systems	Operators of district heating or cooling systems, as defined in Article 2(19) of Directive (EU) 2018/2001 of the European Parliament and of the Council (3)	
		c)	Crude	Operators of crude oil transport pipelines	
				Operators of crude oil production, refining and processing facilities, storage and transport	
				Central stockholding entities, as defined in Article 2(f) of Council Directive 2009/119/EC (4)	
		d)	Gas	Gas supply undertakings, as defined in Article 2(8) of Directive 2009/73/EC of the European Parliament and of the Council (5)	
				Distribution system operators, as defined in Article 2(6) of Directive 2009/73/EC	
				Transmission system operators, as defined in Article 2(4) of Directive (EU) 2009/73/EC	
				Storage system operators, as defined in Article 2(10) of Directive 2009/73/EC	
				LNG system operators, as defined in Article 2(12) of Directive 2009/73/EC	
				Natural gas undertakings, as defined in Article 2(1) of Directive 2009/73/EC	
				Operators of natural gas refinery and processing facilities	

		e)	Hydrogen	Hydrogen production, storage and transport operators	
2.	Transport	a)	Air transport	Air carriers, as defined in Article 3(4) of Regulation (EC) No 300/2008, used for commercial purposes	Ministry of Transport, Mobility and Urban Agenda through the Secretariat of State for Transport, Mobility and Urban Agenda.
				Airport managing bodies, as defined in Article 2(2) of Directive 2009/12/EC of the European Parliament and of the Council (6); airports as defined in Article 2(1) of said Directive, in particular the airports of the core and comprehensive network listed in Annex II(2) to Regulation (EU) No 1315/2013 of the European Parliament and of the Council (7); and entities operating annexed facilities within the enclosures of airports	
				Traffic management control operators providing air traffic control services, as defined in Article 2(1) of Regulation (EC) No 549/2004 of the European Parliament and of the Council (8)	
		b)	Rail transport	Infrastructure managers, as defined in Article 3(2) of Directive 2012/34/EU of the European Parliament and of the Council (9)	
				Railway undertakings, as defined in Article 3(1) of Directive 2012/34/EU, including operators of service facilities, as defined in Article 3(12) of that Directive	
		c)	Maritime and inland waterway transport	Maritime, inland waterway and cabotage transport undertakings, both passenger and goods, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council (10), not including private vessels operated by such undertakings	

				Managing bodies of ports, as defined in Article 3(1) of Directive 2005/65/EC of the European Parliament and of the Council (11), including their port facilities, as defined in Article 2(11) of Regulation (EC) No 725/2004, and entities operating works and equipment located in ports	
				Operators of vessel traffic services (VTS), as defined in Article 3(o) of Directive 2002/59/EC of the European Parliament and of the Council (12)	
		d)	Road transport	Road authorities, as defined in Article 2(12), of Commission Delegated Regulation (EU) 2015/962 (13), responsible for traffic management control, excluding public entities for which traffic management or operation of Intelligent Transport Systems is a non-essential part of their general activity	
				Operators of Intelligent Transport Systems, as defined in Article 4(1) of Directive 2010/40/EU of the European Parliament and of the Council (14)	
3.	Banking			Credit institutions, as defined in Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council (15)	The Bank of Spain
4.	Financial market infrastructure			Operators of trading venues, as defined in point of Article 4(24) of Directive 2014/65/EU of the European Parliament and of the Council (16)	The National Securities Market Commission.

			Central Counterparties (CCPs), as defined in Article 2(1) of Regulation (EU) No 648/2012 of the European Parliament and of the Council (17)	The National Securities Market Commission.
5.	Health sector		Healthcare providers, as defined in Article 3(g) of Directive 2011/24/EU of the European Parliament and of the Council (18)	The Ministry of Health, through the Secretariat of State for Health.
			EU reference laboratories, as defined in Article 15 of Regulation (EU) .../... of the European Parliament and of the Council (19)	
			Entities carrying out research and development activities on medicinal products as defined in Article 1(2) of Directive 2001/83/EC of the European Parliament and of the Council (20)	
			Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2	
			Entities manufacturing medical devices that are considered essential in public health emergency situations ('public health emergency critical devices list') within the meaning of Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council (21)	
6.	Drinking water		Suppliers and distributors of water intended for human consumption as defined in Article 2(1)(a) of Directive (EU) 2020/2184 of the European Parliament and of the Council (22), excluding distributors for which the distribution of water intended for human consumption	The Ministry for the Ecological Transition and the Demographic Challenge, through the Secretariat of State for Environment.

			is a non-essential part of their general activity of distribution of other goods and commodities	
7.	Waste water		Undertakings engaged in the collection, disposal or treatment of urban, domestic or industrial waste water as defined in Article 2(1) to (3) of Council Directive 91/271/EEC (23), excluding undertakings for which the collection, disposal or treatment of urban, domestic or industrial waste water is a non-essential part of their general activity	The Ministry for the Ecological Transition and the Demographic Challenge, through the Secretariat of State for Environment.
8.	Digital infrastructure		Internet Exchange Point providers	Ministry for the Digital Transformation and Civil Service, through the Secretariat of State for Digitalisation and Artificial Intelligence and the Secretariat of State for Telecommunications and Digital Infrastructures.
			DNS service providers, excluding root server operators	
			Top-level domain name registries	
			Cloud computing service providers	
			Data Centre Service Providers	
			Content delivery network providers	
			Trust service providers	
			Providers of public electronic communications networks	
			Providers of publicly available electronic communications services,	
9.	ICT Service Management (business to business)		Managed service providers	Ministry for the Digital Transformation and Civil Service, through the Secretary of State for Digitalisation and Artificial Intelligence and the Secretary of State for Telecommunications and Digital Infrastructures.
			Managed security service providers	

10.	Public administration entities, excluding the judiciary, parliaments and central banks		Central public administration entities, as defined in the Member State in accordance with the provisions of national law	Ministry of Defence, through the National Cryptological Centre
			Public administration entities at regional level, as defined in the Member State in accordance with the provisions of national law	
11.	Space		Operators of terrestrial infrastructure owned, managed and operated by Member States or private entities, that supports the provision of space services, except providers of public electronic communications networks	Ministry of Defence and Ministry of Science, Innovation and Universities, through the Spanish Space Agency
12.	Nuclear industry		Nuclear plants and entities associated with the use, production, storage and transport of nuclear or radiological goods and materials	1.º The Ministry for the Ecological Transition and the Demographic Challenge, through the Secretariat of State for Energy.
				2.º The Nuclear Security Council.

ANNEX II

OTHER SECTORS

Sector		Subsector	Type of entity	Sectoral point of contact
1.	Postal and courier services		Postal service providers as defined in Article 2(1) (a) of Directive 97/67/EC, including courier service providers	Ministry of Transport, Mobility and Urban Agenda, through the Permanent Secretariat for Transport and Sustainable Mobility
2.	Waste management		Undertakings carrying out waste management, as defined in Article 3(9) of Directive 2008/98/EC of the European Parliament and of the Council (1), except those for which waste management is not their main economic activity	The Ministry for the Ecological Transition and the Demographic Challenge, through the Secretariat of State for Environment.
3.	Manufacture, production and distribution of chemical substances and mixtures		Undertakings manufacturing substances and distributing substances or mixtures, as defined in Article 3(9) and (14) of Regulation (EC) No 1907/2006 of the European Parliament and of the Council (2) and undertakings producing articles, as defined in Article 3(3) of that Regulation, from substances and mixtures	The Ministry of the Interior, through the Secretariat of State for Security.

4.	Production, processing and distribution of food		Food businesses as defined in Article 3(2) of Regulation (EC) No 178/2002 of the European Parliament and of the Council (3) engaged in wholesale distribution and industrial production and processing	1º The Ministry of Agriculture, Fisheries and Food, through the General Secretariat for Agriculture and Food.
				2.º The Ministry of Health, through the Secretariat of State for Health.
				3.º The Ministry of Industry, Trade and Tourism, through the Secretariat of State for Trade.
				4.º The Ministry of Social Rights, Consumer Affairs and Agenda 2030, through the National Centre for Food Safety and Nutrition (AESAN).

5.	Manufacturing	a)	Manufacture of medical devices and in vitro diagnostic medical devices	Entities manufacturing medical devices, as defined in Article 2(1) of Regulation (EU) 2017/745 of the European Parliament and of the Council (4), and entities manufacturing in vitro diagnostic medical devices, as defined in Article 2(2) of Regulation (EU) 2017/746 of the European Parliament and of the Council (5), with the exception of the entities manufacturing medical devices referred to in the 5th indent of point (5) of Annex I to this Directive	Ministry of Industry, Trade and Tourism, through _____
		b)	Production of computer, electronic and optical products	Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2	
		c)	Manufacture of electrical equipment	Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2	
		d)	Manufacture of machinery and equipment n.e.c.	Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2	
		e)	Manufacture of motor vehicles, trailers and semi-trailers	Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2	

		f)	Manufacture of other transport equipment	Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2	
6.	Digital service providers.			Providers of online marketplaces	Ministry for the Digital Transformation and Civil Service, through the Secretariat of State for Digitalisation and Artificial Intelligence and the Secretariat of State for Telecommunications and Digital Infrastructures.
				Providers of online search engines	
				Providers of social networking services platforms	
7.	Research			Research bodies	Ministry of Science and Innovation, through the Secretariat-General for Research
8.	Private security			Private security companies and detective offices in accordance with Law 5/2014 of 4 April 2014 on Private Security.	The Ministry of the Interior, through the Secretariat of State for Security.