European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 273-285
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 22

*Cybersecurity of Information Systems in the Public Healthcare Sector**

Carlos Galán Cordero
(Associate Professor of State Public Law and Administrative Law at Carlos III University of Madrid, Agencia de Tecnología Legal)

ABSTRACT In the digital era, where interconnection and immediacy in information management prevail, information systems have become essential assets for various institutions, and among them, the healthcare system stands out. In Spain, this system stores an enormous amount of sensitive data, ranging from clinical records to biomedical research, which are of interest not only to health professionals but also to malicious actors. Ensuring the cybersecurity of these systems is therefore not an option, but an absolute necessity. To face these challenges, the National Security Framework (ENS) in Spain establishes a series of measures, protocols and good practices aimed at protecting information and critical infrastructures, including healthcare infrastructures. This paper, although it also contemplates legislative actions emanating from the European Union, the United States and international initiatives, aims to analyse the importance of cybersecurity in the Spanish healthcare system, highlighting the relevance and applicability of the ENS in this context. We will address the main threats, current challenges and how the ENS guidelines provide a robust framework for effective defence.

1. *Introduction*

This paper, which is part of the research projects "Artificial intelligence in the national health system: solutions to specific legal problems" (PID2021-128621NB-I00) and "The impact of artificial intelligence on public services: A legal analysis of its scope and consequences in healthcare" (PGC2018-098243-B-I00) directed by Prof. Dr. José Vida Fernández and funded by the Spanish Ministry of Science and Innovation (MCIN/AEI/10. 13039/501100011033/) and by "FEDER: A way of doing Europe", aims to briefly present the regulatory framework for cybersecurity of public-information systems, especially when such systems are responsible for supporting public services in the field of healthcare.

2. *Information systems and cybersecurity*

2.1. *Information systems and cybersecurity concepts*

Before we dive into the subject and multifaceted content of cybersecurity, and in order to facilitate understanding, we should begin by recalling some essential concepts.

As with any scientific approach, the first thing to do is to define the field of our study: information systems and their cybersecurity.

Based on current regulations, we can define an information system as:[1]

Any of the following elements:

1. The electronic communications networks used by the entity within the scope of application of this royal decree over which it has management capacity.
2. Any device or group of interconnected or interrelated devices, in which one or more of them carry out, by means of a programme, the automatic processing of digital data.
3. Digital data stored, processed, retrieved or transmitted by means of the elements referred to in numbers 1 and 2 above, including those necessary for the operation, use, protection and maintenance of those elements.

In turn, we can define cybersecurity (or information systems security) as the ability of networks and information systems to withstand, at a given level of reliability, any action that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data, or the corresponding services offered by or accessible through such networks and information systems.[2]

It should be noted that, from these definitions, some conclusions can already be drawn:

* Article submitted to double-blind peer review.

[1] According to Annex IV-Glossary of Royal Decree 311/2022 of 3 May, regulating the National Security Framework (ENS)

[2] *Idem.* This definition also coincides with that contained in article 3 b) of Royal Decree-Law 12/2018, issued under the exclusive competences of the State in matters of telecommunications and general-communication regime (art. 149.1.21 CE) and public security (art. 149.1.29 CE), which defines the security of information networks and systems in the same way.

1. The concept of information system comprises any physical (*hardware*) or logical (*software*) element involved in the processing of data, whatever the data may be.
2. Cybersecurity does not seek to guarantee absolute immunity of the information systems concerned from threats at all times and in all situations - which is impossible to achieve - but rather to build a security model based on *resistance* measures - those that reasonably prevent the penetration of the attack and, in general, the progress of the cyber-incident - and on *resilience* measures - those aimed at recovering the full functionality of an information system once the cyber-incident is over.

2.2. *Cybersecurity as a manifestation of security*

Having defined the essential concepts of the work, we must go on to analyse to what extent *security* and *cybersecurity* are legally distinct concepts; an analysis that is not trivial, since, if they are located within a common protected legal asset, it could be deduced that the clarifications that could be made regarding either of them could be equally applicable.

First of all, we should mention the provisions of Law 36/2015, of 28 September, on National Security, which identifies cybersecurity in its article 10 as one of the "areas of special interest of national security... that require specific attention, as they are essential to preserve the rights and freedoms, as well as the well-being of citizens, and to guarantee the provision of essential services and resources".

Likewise, Law 8/2011, of 28 April, on measures for the Protection of Critical Infrastructures - defines them as strategic infrastructures "whose operation is essential and does not allow alternative solutions, so that their disruption or destruction would have a serious impact on essential services", issued under the competence attributed to the State by virtue of Article 149.1.29 of the Spanish Constitution (EC), it refers to cybersecurity. Article 2 of this Law defines strategic infrastructures as "the physical and information technology facilities, networks, systems and equipment on which the functioning of essential services is based", understanding that such services are those necessary for the maintenance of basic social functions, health, security, the social and economic well-being of citizens, or the efficient functioning of State institutions and public administrations.

Furthermore, the maintenance of cybersecurity is one of the functions of the National Intelligence Centre (CNI), as established in article 4 b) of Law 11/2002, of 6 May, regulating the National Intelligence Centre.

Finally, we should mention Royal Decree-Law 12/2018, of 7 September, on the security of networks and information systems, which transposes into Spanish law Directive (EU) 2016/1148 of the European Parliament and of the Council, of 6 July 2016, on measures to ensure a high common level of security of networks and information systems in the Union. The purpose of this regulation is to regulate the security of networks and information systems used for the provision of essential services and digital services and to establish an incident-notification system, as well as an institutional framework for its application and coordination between competent authorities and with the relevant cooperation bodies at EU level. As it is known, this Royal Decree-Law applies to essential services dependent on information networks and systems included in the strategic sectors defined in the annex to Law 8/2011, as well as to information-society services within the meaning of letter a) of the annex to Law 34/2002, of 11 July, on information-society services and electronic commerce.

The Constitutional Court has ruled on these issues in its judgment 142/2018 of 20 December 2018, in relation to the appeal of unconstitutionality 5284-2017 filed by the President of the Government regarding Law 15/2017, of 25 July, on the Cybersecurity Agency of Catalonia, on competences in the areas of telecommunications, defence and public security.[3]

By way of summary, the most significant consequences of the aforementioned judgement and the regulations it invokes are:

- Cybersecurity, as a synonym for network security, is an activity that is integrated into public security, as well as telecommunications. From its conceptualisation as a set of mechanisms aimed at protecting computer infrastructures and the digital information

[3] Boletín Oficial del Eestado, No. 22, Friday 25 January 2019.

they house, it is easy to infer that, as it is dedicated to the security of information technologies, it has a protective component that is specifically projected onto the specific area of the protection of networks and information systems used by citizens, companies and public administrations, (FJ 1).

- Cybersecurity is included in matters of state competence insofar as, by referring to the necessary actions of prevention, detection and response to cyberthreats, it affects issues related to public security and defence, infrastructures, networks and systems and the general telecommunications regime, (FJ 1).[4]

All these issues have been definitively consolidated in Royal Decree 1150/2021, of 28 December, approving the National Security Strategy 2021, in which public cybersecurity is configured as an integral part of National Security, cyberspace is included among the material objects of the security required of global common spaces, and the cybersecurity-governance model is integrated into the framework of the National Security System.

2.3. *The dimensions of cybersecurity*

As it has been pointed out,[5] cybersecurity is a multifaceted concept that can be studied from different points of view, taking into account precisely the guarantees required for the information processed or the services that must be preserved.

The National Security Framework (ENS), following the MAGERIT risk analysis and management methodology,[6] establishes five security dimensions: Confidentiality, Integrity, Authenticity, Traceability and Availability, to which we have added one more, of a generic nature: Legal Compliance.

The following table shows the definitions of these dimensions, as well as their applicability to the information processed or the services provided by the information systems concerned.

Cybersecurity dimension	Definition	Applicability
Confidentiality	The property or characteristic that information is neither made available nor disclosed to unauthorised individuals, entities or processes.	Information
Integrity	The property or characteristic that the information asset has not been altered in an unauthorised manner.	Information
Authenticity	The property or characteristic that an entity is who it claims to be or that it guarantees the source from which the data originates.	Information and Services
Traceability	The property or characteristic that the actions of an entity (person or process) can be indisputably traced back to that entity.	Information and Services
Availability	Property or characteristic of assets that authorised entities or processes have access to them when required.	Information and Services
Legal Compliance	Property or characteristic of the technologies, products, solutions or services that support operations, in order to remain permanently aligned with the provisions of applicable national, European or international legislation.	Information Systems, as a whole.

Of course, depending on the specific application or service in question, certain security dimensions will be more important

[4] Indeed, the aforementioned TC 142/2018 ruling states that "public security is, in principle, the exclusive competence of the State ex Article 149.1. 29 EC, a constitutional precept which shows that it already establishes exceptions ("without prejudice to") which, in a certain sense, come to modulate the exclusivity of State competence, proclaimed in the initial paragraph of Article 149 EC", adding that "*the exclusive competence of the State in matters of public security admits no exception other than that deriving from the creation of the autonomous police forces*" (STC 104/1989, of 8 June, FJ 3).

[5] Galán Pascual, Carlos Manuel. El Derecho a la Ciberseguridad, in Sociedad Digital y Derecho. Various authors. BOE, 2018.

[6] MAGERIT version 3: Information Systems Risk Analysis and Management Methodology. Available in: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

than others. In the case of telecommunications, all of them, to a greater or lesser extent, constitute the essential elements of cyber security, as will be seen throughout this chapter.

3. *The National Security Framework*

As we are dealing with information systems intended to provide public services, and therefore disregarding at this point the analysis of other regulations, we will focus on the assessment of the National Security Framework, implemented by Royal Decree 311/2022, of 3 May, which, among other areas of application that we will also comment on, regulates the (cyber)security of public-information systems.

Article 103.1 of the Spanish Constitution of 1978 proclaims: "The Public Administration serves the general interest objectively and acts in accordance with the principles of efficiency, hierarchy, decentralisation, deconcentration and coordination, with full submission to the Law".

Thus, generically protected by the inalienable principle of efficiency, the deployment of the services that the Public Sector (Public Administrations and the Institutional Public Sector) must provide to citizens, especially when using Information and Communication Technologies (ICT), requires - in order to comply with that constitutional requirement - the most appropriate administrative procedures, methods and tools to guarantee the security and reliability of their actions to all recipients: citizens and companies, but also the rest of the Public Sector.

Indeed, it would be of little use to have magnificent technologies that enable the processing and communication of millions of data if the actors involved in the life of administrative procedures did not perceive the information systems on which their relationship is based as secure infrastructures that are as reliable as the very essence that their activities require.

There is no doubt - as it has been stated - that better service to the citizen is the reason for the reforms that have been undertaken in Spain since the approval of the Constitution to configure a modern Administration that makes the principles of effectiveness and efficiency its ultimate reason, and always with an eye to the citizens and the general interest.

This interest was the main raison d'être of Law 11/2007, on Citizens' Electronic Access to Public Services (LAECSP, hereinafter), the original backbone of what has come to be known as e-Government, with the aim of keeping up with our times and the appropriate positioning of our Public Administrations in the European and international framework. The publication of Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations (LPACAP, hereinafter) and Law 40/2015, of 1 October, on the Legal Regime of the Public Sector (LRJSP, hereinafter), which repeal the previous one, consolidate the primacy of the use of electronic means in the development of public entities.

The general recognition of electronic relations in and with the public sector raises several questions that need to be considered:

- The increasing use of electronic means raises the question of the privacy of data provided electronically in connection with a file.
- Entitled parties have the right to access the status of the administrative procedure, as well as to examine the documents of which it is composed. This should at least be the case for a file initiated or processed electronically. Such a file should allow online access to parties interested in checking its status, without undermining privacy guarantees.
- In any case, the progressive use of electronic communications, derived from the recognition of the right to communicate electronically with the Administration, raises the question not only of how to adapt the Administration's human and material resources to a new way of relating with citizens, but also of how to adapt its actions and processing of files and, in general, rationalise, simplify and adapt procedures, taking advantage of the new reality imposed by ICTs.
- Recognising the right (obligation, in some cases) of citizens to communicate electronically with the Administration raises, firstly, the need to clearly define the electronic administrative headquarters with which relations are established, promoting a regime of identification, authentication, minimum content, legal protection, accessibility, availability and responsibility.

There are many precepts contained in our

administrative laws of reference (Law 39/2015 and Law 40/2015, both of 1 October) that insist on the need for the development of the Public-Sector entities.The development of procedures that respond to the general exercise of their competences must take place within the framework of an environment that contemplates all the security measures necessary to guarantee the integrity, confidentiality, authenticity and traceability of the information processed and the availability of the services provided, in compliance with the legislation in force.

Law 39/2015, of 1 October, includes, among the rights of individuals in their relations with Public Administrations, the one relating to "the protection of personal data, and in particular to the security and confidentiality of the data contained in the files, systems and applications of Public Administrations". It also makes various mentions of compliance with security guarantees and measures, when referring to registers, filing of documents and copies.

For its part, Law 40/2015, of 1 October, which includes the National Security Framework in Article 156, also mentions security when referring to administrations' electronic means of comunication and realtion, electronic headquarters, electronic filing of documents, electronic exchanges in closed-communication environments and data transmissions between Public Administrations.

The National Security Framework (ENS), currently operated by Royal Decree 311/2022 of 3 May, is one of the best European examples of cybersecurity treatment.

The current ENS, updated and heir to the one originally regulated in Royal Decree 3/2010 of 8 January, has the following objectives:

- To align the ENS to the existing regulatory framework and strategic context to ensure security in the digital administration, seeking to clearly reflect its scope of application for the benefit of cybersecurity and citizens' rights, as well as to update references to the current legal framework and review the formulation of certain issues in the light of this, in accordance with the National Cybersecurity Strategy 2019, so as to achieve simplification, precision or harmonisation of the mandates of the ENS, and to eliminate aspects that may have been considered excessive, or to add others identified as necessary.
- Introduce the ability to adjust the ENS requirements to ensure that they are adapted to the reality of certain groups or types of systems, taking into account the similarity of a multiplicity of entities or services in terms of the risks to which their information systems and services are exposed. This makes it advisable to include in the ENS the concept of a "Specific Compliance Profile" which, approved by the National Cryptologic Centre, allows for a more effective and efficient adaptation of the ENS, rationalising the resources required without undermining the pursued and enforceable protection.
- Facilitate a better response to cybersecurity trends, reduce vulnerabilities and promote continuous vigilance by revising basic principles, minimum requirements and security measures.

It should be remembered that the subjective scope of application of this regulation covers all entities included in the so-called Public Sector, in the terms defined in article 2 of Law 40/2015, of 1 October, and in accordance with the provisions of article 156. 2 of the same, being also applicable to the information systems of private-sector entities, when, in accordance with the applicable regulations and by virtue of a contractual relationship, they provide services or solutions to public-sector entities for the exercise of administrative powers and competences. This also applies, albeit in an instrumental manner, telecommunication operators and also extends to the supply chain of the aforementioned contractors or suppliers, to the extent necessary and in accordance with the results of the corresponding risk analysis.

In summary, the ENS consists of the basic principles and minimum requirements necessary for an adequate protection of the information processed and the services provided by the entities within its scope of application, in order to ensure access, confidentiality, integrity, traceability, authenticity, availability and preservation of the data, information and services used by electronic means that they manage in the exercise of their competences.

BASIC PRINCIPLES	MINIMUM REQUIREMENTS
- Security as an integral process. - Risk-based security	- Organisation and implementation of the security process.

management. - Prevention, detection, response and preservation. - Existence of lines of defence. - Continuous vigilance. - Periodic reassessment. - Differentiation of responsibilities.	- Risk analysis and management. - Personnel management. - Professionalism. - Authorisation and control of access. - Protection of installations. - Procurement of security products and contracting of security services. - Least privilege. - System integrity and updating. - Protection of information stored and in transit. - Prevention of other interconnected information systems. - Logging of activity and detection of malicious code. - Security incidents. - business continuity - Continuous improvement of the security process.

The ENS provides that entities within its scope of application adopt specific security measures, of organisational and technical nature, according to the following distribution:

Organizational framework	Security policy Security regulations Security procedures Authorization process
Operational framework	Planning (5 measures) Access control (6 measures) Operation (10 measures) External resources (4 measures) Cloud services Continuity of service (4 measures) System monitoring (3 measures)
Protective measures	Protection of facilities and infrastructure (7 measures) Staff management (4 measures) Protection of equipment (4 measures) Protection of communications (4 measures) Protection of information media (5 measures) Protection of IT applications (2 measures) Protection of information (6 measures) Protection of services (4 measures)

- Organisational framework: measures related to the overall security organisation.
- Operational framework: measures to protect the operation of the system as an integral set of components for a purpose.
- Protection measures: to protect specific assets, according to their nature, with the required level, in each security dimension.

As stated in the Royal Decree itself, the provisions of the ENS, insofar as they affect the information systems used for the provision of public services, must be considered to be included in the resources and procedures that the National Security System set out in Law 36/2015, of 28 September, on National Security.

The scope of application of the ENS is broad and logical, and extends to information systems:

- Of the entities of the entire public sector, as this term is defined in article 2 of Law 40/2015.
- That deal with classified information.
- Of private-sector entities when they provide services or solutions to the above, including the elements of the supply chain to the extent that a risk analysis so determines.

To ensure such compliance, the specifications for public tenders shall include the requirements in accordance with the ENS.

As telecommunications constitute an additional significant risk to ensure compliance with the aforementioned security dimensions, especially those of the latest generation, the reference to the installation, deployment and operation of 5G networks or the provision of 5G services by public-sector entities could not be left out of this new ENS.

Finally, the first additional provision of Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights, confers on the ENS the inclusion of the measures that must be implemented in the event of processing of personal data to prevent their loss, alteration or unauthorised access, adapting the criteria for determining the risk in the processing of data to those established in article 32 of Regulation (EU) 2016/679, obliging the data controllers listed in article 77. 1 of this organic law to apply to the processing of

personal data the security measures that correspond to those provided for in the National Security Framework, as well as to promote a degree of implementation of equivalent measures in the companies or foundations linked to them even if subject to private law. An obligation that extends to cases in which a third party provides a service under a concession, management assignment or contract. In these cases, the security measures will correspond to those of the originating public administration and will be comply with the National Security Framework.

An interesting aspect of this new ENS are the so-called Specific Compliance Profiles, which comprise the set of security measures that, as a result of the mandatory risk analysis, are suitable for a specific security category, making it possible to adjust the ENS requirements to the specific needs of certain groups such as Local Entities, Universities, Paying Bodies, etc., or specific technological areas, such as cloud services, for example.

There is nothing to prevent the development of a specific Compliance Profile for information systems that provide public healthcare services, should the need arise.

Regarding the response to cyber incidents, the ENS states that public entities are obliged to notify the CCN-CERT of the security incidents of which they are victims, while private-sector organisations that provide services to public entities will notify INCIBE-CERT, which will immediately inform the CCN-CERT.

The CCN-CERT will technically determine the risk of reconnection of affected systems, indicating procedures to follow and safeguards to implement, and the General Secretariat for Digital Administration, of the State Secretariat for Digitalisation and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation, will authorise the reconnection to common means and services in its area of responsibility, if a CCN-CERT exposure surface report determines that the risk is assumable.

It should be noted that compliance with the ENS (and its public display) is achieved through two paths: a Self-Assessment, only applicable to information systems in the Basic security category; or a Formal Audit, applicable to information systems of any category (Basic, Medium or High), carried out by an ENS Certification Body previously accredited by the National Accreditation Body (ENAC), as provided for in the Resolution of 27 March 2018, of the State Secretariat for Public Administration, which approves the Technical Security Instruction on Information Systems Security Auditing and the Resolution of 13 October 2016, of the State Secretariat for Public Administrations, which approves the Technical Security Instruction in accordance with the National Security Framework.

Finally, the ENS confers the General Secretariat for Digital Administration (of the Secretariat of State for Digitalisation and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation) and the National Cryptologic Centre (attached to the National Intelligence Centre of the Ministry of Defence), within their respective competences, the responsibility to ensure the proper implementation, development and monitoring of the ENS in the entities within its scope of application.

4. *The most significant European and international regulations on the matter*

In relation to the regulation of the cybersecurity of medical devices, the European Union has taken two particularly significant approaches:

- Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (hereinafter MDR Regulation).
- Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in-vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (hereinafter IVDR Regulation).

Both regulations focus on ensuring that devices placed on the EU market are prepared to deal adequately with cyber threats by establishing certain essential cybersecurity requirements, requiring manufacturers of such devices to take appropriate measures during their manufacture taking into account these risks, based on the security dimensions mentioned above, in particular the confidentiality and integrity of the information processed by such devices, ensuring their

availability and controlling access to them.

Cybersecurity is explicitly addressed in Annex I, sections 17.2, 17.3, 17.4 and 18.8 of the MDR, namely:

> 17.2. For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation.
> 17.3. Software referred to in this Section that is intended to be used in combination with mobile computing platforms shall be designed and manufactured taking into account the specific features of the mobile platform (e.g. size and contrast ratio of the screen) and the external factors related to their use (varying environment as regards level of light or noise).
> 17.4. Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.
> …
> 18.8. Devices shall be designed and manufactured in such a way as to protect, as far as possible, against unauthorised access that could hamper the device from functioning as intended.

Cybersecurity is similarly addressed in Annex I, sections 16.2, 16.3 and 16.4 of the IVDR Regulation, namely:

> 16.2. For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation.
> 16.3. Software referred to in this Section that is intended to be used in combination with mobile computing platforms shall be designed and manufactured taking into account the specific features of the mobile platform (e.g. size and contrast ratio of the screen) and the external factors related to their use (varying environment as regards level of light or noise).
> 16.4. Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.

On the other hand, and as the healthcare sector is one of the most important areas for guaranteeing the maintenance of the cybersecurity of the information systems used for healthcare, the Directives colloquially known as the NIS Directive and the NIS Directive2 should be added to the list of important regulations.

Indeed, what has come to be known as the NIS Directive (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of security of network and information systems in the Union), published in the OJEU on 19 July 2016, considered it essential for all EU Member States to have minimum capabilities and a strategy to ensure a high level of security of network and information systems on their territory, especially with regard to what the European standard defined as operators of essential services and digital-service providers, which should result in the adoption of a set of cybersecurity measures aimed at improving the functioning of the internal market.

The ultimate addressees of the regulation are shown in the table below:

Operators of essential services, in the sectors…[7]
Energy: electricity, oil and gas.
Transport: air, rail, maritime and inland waterway and road.
Banking.
Financial market infrastructures.
Health sector: health care environments (including hospitals and private clinics).
Drinking-water supply and distribution.
Digital infrastructure: IXP, DNS Service Providers and Top Level Domain Name Registries.
Digital service providers
Online marketplaces.
Online search engines.
Cloud computing services.

The criteria for the identification of essential operators were:

[7] Provided that they are: a) an entity providing a service essential to the maintenance of crucial social or economic activities; b) the provision of that service depends on networks and information systems; and c) an incident would have significant disruptive effects on the provision of that service.

a) It provides a service essential for the maintenance of crucial social or economic activities;
b) The provision of such a service is dependent on networks and information systems; and
c) An incident would have a significant disruptive effect on the provision of that service.

The NIS Directive, in summary

a) Established an obligation for all Member States to adopt a national strategy for the security of network and information systems;
b) Established a Cooperation Group to support and facilitate strategic cooperation and information exchange between Member States and to develop trust and confidence between them;
c) Established a network of Computer Security Incident Response Teams (CSIRT Network[8]), in order to contribute to the development of trust and security between Member States and to promote rapid and effective operational cooperation;
d) Established security and notification requirements for operators of essential services and for digital-service providers;
e) Established obligations for Member States to designate competent national authorities, single points of contact and CSIRTs with functions related to the security of network and information systems.

On 8 September 2018, the Official State Gazette published Royal Decree-Law 12/2018, of 7 September, on the security of networks and information systems, fulfilling the mandate to transpose the NIS Directive.

Although the Directive from which it stemmed limited its scope of application to the so-called "operators of essential services" and "digital-service providers", the Spanish law took advantage of the mandate to extend its scope to sectors not expressly included in the European Directive (without this entailing a covert repeal or regulatory displacement of the Spanish legislation in force). Significant examples of this extension are trust-service providers or operators of electronic-communication networks and services, which are included among those covered by the regulation, insofar as they may be designated as critical operators.

At this point, it is worth noting the effort made by the working group drafting the RD-Law to harmonise the three state regulations of special significance in the area of (cyber)security: Royal Decree 3/2010, of 8 January, which regulates the National Security Framework (ENS),[9] Law 8/2011, of 28 April, which establishes measures for the protection of Critical Infrastructures, and Law 36/2015, of 28 September, on National Security.[10]

The governance model set out in this RD-Law is based on the scheme of competences that the current National Security and Cybersecurity Strategies have drawn up: the National Security Council, the National Cybersecurity Council, the Competent Authorities and the reference CSIRTs, conferring on the so-called Competent Authorities the functions of supervision, surveillance and sanctioning, reserving for the reference CSIRTs the more operational functions, such as risk analysis and national-operational management of the response to incidents, a national action protected by the provisions of art. 1491.29 of our Constitution, which confers exclusive powers on the State in matters of national security, cybersecurity being one of its manifestations, as we have pointed out above.

These reference CSIRTs constitute, in our opinion, the cornerstone on which the treatment of cybersecurity rests, since, beyond the functions legally granted to the Competent Authorities, they materialise the mechanisms for prevention, detection and response to incidents. As of the entry into force of this new RD-Law, these functions require maximum coordination from all of them, as also provided for in the regulation, which confers on the CCN-CERT (of the National Cryptologic Centre, attached to the National Intelligence Centre) the function of national coordinator in cases of particular seriousness.

Despite being a regulation in force and therefore enforceable, the Royal Decree-Law postponed certain issues to its regulatory development, which we will see below.

At present, there are numerous regulations with a technological substratum that prescribe the notification of incidents to the competent

[8] *Computer Security Incident Response Team.*

[9] Recently repealed by Royal Decree 311/2022 of 3 May, which regulates the National Security Framework.

[10] We recall that the strategic sectors defined in Law 8/2011, of 28 April, are: Administration; Space; Nuclear Industry; Chemical Industry; Research Facilities; Water; Energy; Health; ICT; Transport; Food and the Financial and Tax System.

body. This diversity, which often applies to the same obliged subject, encourages and justifies the existence of a Common Platform for incident notification, capable of providing a response, through a single process (including initial, intermediate and final notification) automatically addressed to each competent authority by virtue of the legislation affected, which may constitute, in our opinion, one of the most innovative measures of this Royal Decree-Law in cybersecurity matters, in the image of what the CCN-CERT has been developing in the Public Sector with the LUCIA platform.

The RD-Law exhibits a particularly-rigorous infringement regime. Just one example: in certain circumstances, it classifies as very serious the failure to adopt measures to remedy the deficiencies detected or repeated failure to comply with the obligation to notify incidents.

The regulatory development referred-to above took place by Royal Decree 43/2021 of 26 January, which regulated the following aspects:

- The identification of specific factors in the sectors of essential service operators to determine whether an incident could have significant disruptive effects.
- In the determination of the Competent Authorities, the corresponding sectoral authority by reason of the subject matter, when critical operators are not involved.
- Within the functions of the Competent Authorities, the establishment of communication channels with the operators of essential services and digital-service providers, and the protocols for coordination with the reference CSIRTs.
- The identification of essential service operators with an impact on National Defence.
- The determination of particularly serious cases that require the national coordination of the CCN-CERT.
- Determination of the coordination mechanisms of the reference CSIRTs with the Cybernetic Coordination Office of the National Centre for Infrastructure Protection and Cybersecurity of the Ministry of the Interior, when the response activities may affect a critical operator.
- Determining the technical and organisational measures to be adopted by operators of essential-service and digital-service providers.
- The setting of deadlines for the designation and communication to the Competent Authority by the operators of essential services of the person, unit or collegiate body responsible for information security and the identification of their functions.
- Identification, for notification purposes, of events or incidents that could affect networks and information systems, even if they have not yet done so.
- The identification of the necessary measures concerning the notification of incidents by operators of essential services.
- The body of the authority competent to impose penalties in the case of serious or minor infringements.

A new Directive, colloquially referred to as NIS2, was published at the end of 2022, repealing the previous one, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure 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.

Indeed, during the second half of 2020, the European Commission carried out an evaluation of the results achieved with the NIS Directive, including a public consultation that concluded, from various perspectives, the need to improve the transposition of the standard, its scope and its definition.

As a result, the Commission presented a proposal for a revision[11] that sought to improve some of the problems that the first NIS Directive had not solved and which, as mentioned,[12] appeared in the above-mentioned evaluation, such as low business cyberresilience, different implementation from country to country, low situational awareness and lack of common responses.

In its Explanatory Memorandum, the Commission acknowledges that:

- 'The scope of the NIS Directive has become too small due to the advance of digitisation and connectivity in recent years and does not include relevant digital services.

[11] Commission Proposal for a Directive COM (2020) 823 (final) of 16 December on measures for a high common level of cybersecurity in the EU and Annexes on critical and important entities.

[12] F. Arteaga, *La evaluación y la revisión de la Directiva NIS: la directiva NIS2.0*, in *R.I. Elcano*, Feb. 2021

- It also does not include all relevant actors because the criteria in the Directive and in the national transpositions for identifying digital service providers have not been clear.
- For the same reasons, the procedure for incident reporting by providers of essential services is not the same and the sanctions and enforcement obligations vary in each Member State.
- The exchange of information between public and private actors remains very low and unsystematic.
- The disparity in the budgetary and human resources available to the Member States affects their level of maturity and their cyber-resilience capacity.

The new Directive thus reflects the Commission's desire to extend the scope of application of the European standard to other actors, such as providers of public communication services or networks, content or data providers, social-networking platforms and those dedicated to fostering trust in the above or to public administrations, postal services, water management, space, food, among others, eliminating the current classification of operators of essential services and digital-service providers, replacing them with essential entities and important entities.

The classification by sector of the entities covered by the new NIS2 Directive is as follows:

Essential Entities	Important Entities
- Energy (Electricity, District Heating and Cooling, Oil, Gas, Hydrogen) - Transport (Air, Rail, Water, Road). - Banking. - Financial market infrastructures. - Health. - Drinking water. - Wastewater. - Digital infrastructure.[13]	- Postal and courier services. - Waste management. - Chemical manufacturing, production and distribution. - Food production, processing and distribution. - Manufacturing.[14] - Digital providers (Online marketplaces, Online search engines, Social networking service platforms). - Research.
- Public administrations - Space.	

In both groups, the new text obliges states to supervise (by means of *ex ante* or *ex post* actions, depending on their affiliation) the security measures to be adopted by the entities affected, which, in the event of non-compliance, would entail significant sanctions.

Once again, prior risk analysis, as a method for determining the appropriate security measures, is also an essential element of this new regulation, as it has already been, for example, in the Spanish case with the National Security Framework analysed above.

Finally, in response to calls for action by the Council[15] and the Parliament[16] to review the current approach to the security of critical entities and ensure greater harmonisation with the NIS Directive, 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 aims to improve the provision in the internal market of services that are essential for the maintenance of vital societal functions or economic activities, by enhancing the resilience of critical entities providing such services, addressing the increased interconnection between the physical and digital world through a legislative framework with robust resilience measures for both cyber and physical aspects, as set out in the Strategy for a Security Union.[17]

As its introductory text points out, the

[13] These include: - Internet Exchange Point providers - DNS service providers, excluding root name server operators - TLD name registries - Cloud computing service providers - Data centre service providers - Content delivery network providers - Trusted service providers referred to in point (19) of Article 3 of Regulation (EU) no. No 910/2014(1) - Providers of public electronic communications networks as referred to in point (8) of Article 2 of Directive (EU) 2018/1972(2) or providers of electronic communications services as referred to in point (4) of Article 2 of Directive (EU) 2018/1972 where their services are publicly available. ICT Service Management (B2B); ICT Service Management (B2B); Managed Service Providers (MSP) - Managed Security Service Providers (MSSP).

[14] Manufacture of medical devices and in-vitro diagnostic medical devices; computer, electronic and optical products; machinery and equipment n.e.c.; motor vehicles, trailers and semi-trailers and other transport equipment.

[15] Council conclusions of 10 December 2019 on complementary actions to increase resilience and combat hybrid threats (doc. 14972/19).

[16] Report on the conclusions and recommendations of the European Parliament's Special Committee on Terrorism (2018/2044 (INI)).

[17] COM(2020) 605.

standard reflects national approaches that emphasise cross-sectoral and cross-border interdependencies, where protection is only one element alongside risk prevention and mitigation, business continuity and recovery (resilience).

This Directive therefore aims to:

- Establish obligations on Member States to take certain measures aimed at ensuring the provision in the internal market of services essential for the maintenance of vital societal functions or economic activities, in particular to identify entities and critical entities to be considered as equivalent in certain respects and to enable them to fulfil their obligations;
- Establish obligations on critical entities aimed at increasing their resilience and improving their ability to provide such services in the internal market;
- To lay down rules on the supervision and enforcement of critical institutions, and the specific supervision of critical institutions considered to be of particular European importance.

The scope of application covers (public or private) entities falling in the types mentioned in its Annex, and identified as "critical entities" by a Member State. In accordance with Article 5 of the Directive, the types of entities related to the Digital Infrastructure sector are the following:

- Internet Exchange Point Providers (from the NIS2 Directive).
- DNS service providers (from the NIS2 Directive).
- Top Level Domain Name Registries (from the NIS2 Directive).
- Cloud computing service providers (from the NIS2 Directive).
- Data centre service providers (from the NIS2 Directive).
- Content delivery network providers (from the NIS2 Directive).
- Providers of trust services referred to in Article 3(19) of Regulation (EU) No 910/2014 (eIDAS Regulation).
- Providers of public electronic communications networks as referred to in Article 2(8) of the already discussed Directive 2018/1972/EU (European Electronic Communications Code) or providers of electronic communications services within the meaning of Article 2(4) of Directive (EU) 2018/1972, to the extent that their services are available to the public.

This also includes providers of public electronic-communication networks.

We cannot conclude this review of European initiatives on the subject without mentioning the work being carried out by ENISA (European Union Agency for Cybersecurity), in particular its research and dissemination work.

In this regard, and in the aspects that interest us now, we should highlight the document *Cybersecurity and Privacy in AI - Medical Imaging Diagnosis* (June 2023), an in-depth study, that for the first time identifies the assets, the actors, their roles, the relevant processes, the AI algorithms used and the cybersecurity and privacy requirements.

Drawing on previous ENISA work, such as the *Securing Machine Learning Algorithms* report, as well as legislation such as the GDPR, the paper has identified the cybersecurity and privacy threats and vulnerabilities that can be exploited in the scenario under consideration. While the focus is on threats and vulnerabilities related to *Machine Learning* techniques, broader AI-related considerations have also been taken into account.

It is worthwhile to spend a few lines examining the state of play of this issue in the United States.

A number of authors[18] have been urging the U.S. Food and Drug Administration (FDA) to take action on this issue and develop a new regulatory framework to address the risks of cyber threats to medical devices, arguing that cyber-physical medical devices pose new challenges to the FDA's traditional approach to assessing their safety and effectiveness because, unlike other software, cyber-physical devices are embedded in an unpredictable and limitless environment and that, unlike traditional-hardware devices, risks to patients can arise not only from malfunction but also from malicious external agents.

Although there is no clear FDA guidance on this issue, the FDA has been issuing a series of guidance focused on cybersecurity, most recently in 2023.[19] These guidance

[18] Such as Christopher S. Yoo and Bethany Lee of the University of Pennsylvania Carey Law School in their paper *Optimising Cybersecurity Risk in Medical Cyber-Physical Devices*.

[19] Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions -

documents recognise that residual risks are unavoidable and that certain risk-acceptance criteria must be established for medical devices to be considered "trustworthy".

Finally, at the global level, it is important to mention the *Medical Device Cybersecurity Guide*[20] by the Medical Device Regulators Forum (IMDRF), which aims to promote a globally-harmonised approach to medical-device cybersecurity.

This Forum has published the following papers:

- Technical document (IMDRF/CYBER WG/N73) Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity (13 April 2023).[21]
- Technical document (IMDRF/CYBER WG/N70) Principles and Practices for the Cybersecurity of Legacy Medical Devices (11 April 2023).[22]
- Technical document (IMDRF/CYBER WG/N60) Principles and Practices for Medical Device Cybersecurity (20 April 2020).[23]

These IMDRF technical documents provide guidance including, among other issues, definitions of medical-device cybersecurity, shared responsibility of stakeholders and information sharing.

5. *Conclusions*

As we have been able to analyse in the preceding paragraphs, as far as Spain is concerned and in view of the risks derived from operating in cyberspace, cybersecurity is a *sine qua non* condition for the adequate provision of public services, without which the principles of public attention set out in our administrative laws, in the National Security Strategy and in the Constitution cannot be met.

Therefore, having discarded from its scope of application the current wording of the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 medical devices for human use (regulated in Regulation (EU) 2017/745), the cybersecurity model to be applied to information systems (and their individual constituent elements) aimed at providing healthcare services must comply with the provisions of the aforementioned Royal Decree 311/2022, of 3 May, regulating the National Security Framework, which we have reported on in these pages.

Now is the time, therefore, to generate confidence in the ultimate recipients of healthcare services, guaranteeing that the information systems used by public entities in their provision are secure and reliable.

Guidance for Industry and Food and Drug Administration Staff. (27 September 2023).

[20] Medical Device Cybersecurity Guide; see: http://www.imdrf.org/workitems/wi-mdc-guide.asp

[21] https://www.imdrf.org/documents/principles-and-practices-software-bill-materials-medical-device-cybersecurity

[22] https://www.imdrf.org/documents/principles-and-practices-cybersecurity-legacy-medical-devices

[23] https://www.imdrf.org/documents/principles-and-practices-medical-device-cybersecurity