# ROYAL DECREE 311/2022, OF 3 MAY, REGULATING THE NATIONAL SECURITY FRAMEWORK

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DIGITALIZACION E INTELIGENCIA ARTIFICIAL
SECRETARÍA GENERAL DE ADMINISTRACIÓN DIGITAL

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

# Royal Decree 311/2022, of 3 May, regulating the National Security Framework

**Translated into English by:** ISDEFE
**Translation coordinated by**:
Secretariat-General for Digital Administration (SGAD)

**Edited by**:
© Ministry of Economic Affairs and Digital Transformation
Office of the General Technical Secretary
Publishing Centre

July 2022

Series: *Administración electrónica*

**NIPO: 094-22-074-8**

Publication available at the eGovernment Web Portal, Portal de Administración Electrónica (PAe): http://administracionelectronica.gob.es

# Royal Decree 311/2022, of 3 May, regulating the National Security Framework


| | |
|---|---|
| **Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad** | Published in the «BOE» no. 106, 4 May 2022 |
| Reference: | BOE-A-2022-7191 |
| Link to the official version | https://www.boe.es/eli/es/rd/ |
| Permalink ELI: | 2022/05/03/311 |


## I. GENERAL PROVISIONS

## MINISTRY OF ECONOMIC AFFAIRS AND DIGITAL TRANSFORMATION

**7191** *Royal Decree 311/2022 of 3 May regulating the National Security Framework.*

INDEX

I

Royal Decree 3/2010 of 8 January 2010 regulating the National Security Framework in the field of electronic administration (*Esquema Nacional de Seguridad* hereinafter ENS) was intended to determine the security policy in the use of electronic means of the entities within its scope, being constituted by the basic principles and minimum requirements that have been adequately guaranteeing the security of the information processed and the services provided by those entities.

The ENS, whose scope of application included all public administrations entities, sought to build confidence that the information systems provide their services properly and safeguard the information without interruptions or out of control modifications and that the information cannot reach unauthorized persons, establishing measures to guarantee the security of systems, data, communications and electronic services, so as to make it easier for citizens and public administrations to exercise their rights and fulfil their obligations by electronic means.

Since 2010, there have been significant changes in Spain and the European Union, including the progressive digital transformation of our society, the new cybersecurity scenario and the advance of application technologies. It has also become evident that information systems are increasingly exposed to the materialization of cyberspace threats, with a notable increase in cyber-attacks, both in volume and frequency and in sophistication, with agents and actors with greater technical and operational capabilities; threats that occur in a context of high dependence on information and communication technologies in our society and of great interconnection of information systems. All of this significantly affects an increasing number of public and private entities, their supply chains, citizens and, therefore, national cybersecurity, which compromises the country's normal social and economic development and the exercise of citizens' rights and freedoms, as recognized by both the Spanish 2013 National Cybersecurity Strategy and, in particular, the Spanish 2019 National Cybersecurity Strategy.

Royal Decree 3/2010 of 8 January 2010 established that the ENS should be developed and be permanent updated in accordance with the progress of e-government services, the evolution of technology, the new international standards on security and auditing, and the consolidation of the infrastructures that support it.

At the regulatory level, accompanied by these changes and sometimes as a source of them, both the European framework (with four regulations and one Directive) and the Spanish framework have been modified, referring to national security, regulation of the administrative procedure and the legal regime of the public sector, protection of personal data and security of network and information systems, and the strategic framework for cybersecurity has evolved.

Thus, Law 36/2015 of 28 September 2015 on National Security considers cybersecurity as an area of special interest to National Security, as stated in Article 10, and which therefore, requires specific attention as it is essential to preserve the rights and freedoms and well-being of citizens and to guarantee the provision of essential services and resources. In accordance with the provisions of Article 4.3 was approved the Royal Decree 1008/2017 of 1 December 2017 approving the National Security Strategy 2017, and subsequently Royal Decree 1150/2021 of 28 December 2017 approving the National Security Strategy 2021, both of them identifying cyberspace as a common global space, which the 2021 Strategy describes as a connecting area characterized by its functional openness, lack of physical borders and easy accessibility, adding that in global common spaces it is difficult to attribute any irregular or criminal action, given its extension, weak regulation and lack of sovereignty.

Furthermore, Article 3 of Law 40/2015 of 1 October 2015 on the Legal Regime of the Public Sector extended the scope of the ENS to the entire public sector, which regulates the general principles, the need for public administrations to relate with each other and with their bodies, public bodies and related or dependent entities by electronic means, ensuring the interoperability and security of the systems and solutions adopted by each of them , guaranteeing the protection of personal data, and preferably facilitating the joint provision of services to data subjects, identifying the ENS as an essential instrument for achieving these objectives in its Article 156.

Likewise, Law 39/2015 of 1 October 2015 on Common Administrative Procedure of Public Administrations, among the rights of individuals in their relations with public administrations provided for in Article 13 includes the right to the protection of personal data and, in particular, the right to security of data contained in the files, systems and applications of public

administrations.

In implementation of the two previous laws, Royal Decree 203/2021 of 30 March approving the Regulation on the performance and operation of the public sector by electronic means, lays down in various provisions the obligation to comply with the security measures provided for in the ENS, such as those relating to the electronic exchange of data in closed communication environments, concerted key systems and other identification systems for interested persons, the single electronic archive or internet portals, among others.

Coinciding in time with the adoption of the three aforementioned laws, Royal Decree 951/2015 of 23 October 2015 amending Royal Decree 3/2010 of 8 January 2010 regulating the National Security Framework in the field of eGovernment updated the ENS in the light of the experience and knowledge of its application, the current cybersecurity situation, and the evolution of the legal framework, to comply with Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (known as "eIDAS Regulation").

Regarding ENS the security measures in the processing of personal data, Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights, ordered in its first additional provision that such security measures shall be implemented in case of processing of personal data in order to prevent their loss, alteration or unauthorized access, adapting the criteria for determining the risk in the processing of the data to the provisions of Article 32 of Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). On the other hand, the first additional provision also prescribes the implementation of the ENS security measures to public sector entities and private sector entities collaborating with them in the provision of public services that involve the processing of personal data. Finally, and in the same vein, Article 37 of Organic Law 7/2021 of 26 May on the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences and enforcement of criminal penalties has established the obligation to apply the ENS measures to the processing of personal data by the competent public authorities.

On the other hand, with regard to the security of network and information systems, since the entry into force of Royal Decree 3/2010 of 8 January 2010, two regulations and a directive have been adopted in the European Union setting the framework for action in national legal systems.

Thus, firstly, Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 on the European Union Agency for Network Security (ENISA) and repealing Regulation (EC) No 460/2004. Secondly, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and on the certification of cybersecurity of information and communication technologies and repealing Regulation (EU) No 526/2013 ('the Cybersecurity Regulation').

Thirdly, the 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, known as the 'NIS (*Security of Network and Information Systems)* Directive', which has been transposed in Spain by Royal Decree-Law 12/2018 of 7 September 2018 on network and information systems security, noting the need to take the ENS into account when drafting regulatory provisions, instructions and guides, and adopting the measures applicable to entities within the scope of that directive. This Royal Decree-Law 12/2018 of 7 September 2018 has been implemented by Royal Decree 43/2021 of 26 January with regard to the strategic and institutional framework for the security of network and information systems, the monitoring of compliance with the security obligations of operators of essential services and digital service providers, and the management of security incidents. Thus, Royal Decree 43/2021, of 26 January, provides that the measures to comply with the security obligations of operators of essential services and digital service providers shall take as reference those set out in Annex II to Royal Decree 3/2010 of 8 January 2010.

As set out in the 2017 National Security Strategy, Spain needs to ensure the safe and responsible use of information and communications networks and systems by strengthening capacities to prevent, detect and respond to cyber-attacks by enhancing and adopting specific measures to contribute to the promotion of a secure and reliable cyberspace. In this regard, the

National Security Council approved on 12 April 2019 the National Cybersecurity Strategy 2019, published by Order PCI/487/2019 of 26 April 2019, with the aim of establishing the general guidelines in the field of cybersecurity in order to achieve the objectives set out in the 2017 National Security Strategy.

The 2019 National Cybersecurity Strategy contains an overall objective and five specific objectives, and seven lines of action with a total of 65 measures are proposed to achieve them. The first of these objectives is the security and resilience of public sector information systems and communications networks and essential services and is developed through two lines of action and 24 specific measures, including ensuring the full implementation of the National Security Framework. To develop this strategy, the Council of Ministers approved on 29 March 2022 the National Cybersecurity Plan, which provides for nearly 150 initiatives, between actions and projects, for the next three years.

In addition, the 2019 National Cybersecurity Strategy sets out among its objectives the consolidation of a coherent and integrated national framework that ensures the protection of information and personal data processed by the systems and network of the public sector, whether essential or not, noting that their compliance requires the implementation of security measures aimed at improving the capacities for prevention, detection and response to incidents, through the development of new solutions, and the strengthening of coordination and adaptation of the legal system.

**II**

The evolution of threats, new attack vectors, the development of modern response mechanisms and the need to maintain compliance and alignment with European and national implementing regulations require adapting security measures to this new reality. Strengthening cybersecurity demands economic, human and technological resources that must be sized according to the principle of proportionality and the level of security required, in accordance with adequate planning and with the participation of the actors involved, according to a dynamic of continuous adaptive improvement.

Therefore, in a hyperconnected world like the current one, implementing security in cyberspace has become a strategic priority. However, the risk in cyberspace is too great for the public sector or companies to address on their own, as both share the interest and responsibility to face that challenge together. As the role of technology in society grows, cybersecurity becomes a growing challenge.

In fact, on 9 March, the European Parliament adopted by a very large majority a resolution on foreign interference in all democratic processes in the European Union, in particular disinformation. As that resolution states in its recitals, foreign interference constitutes a pattern of conduct that threatens or adversely affects values, democratic procedures, political processes, the security of States and citizens and the ability to deal with exceptional situations. Foreign interference tactics, often combined to have a greater effect, take, inter alia, cyber-attacks, assumption of critical infrastructure control, disinformation, suppression of information, manipulation of social media platforms and their algorithms, hacking and leak operations, threats and harassment to access voter information and interfere with the legitimacy of the electoral process, false personalities and identities, exerting pressure on foreign citizens living in the EU, instrumentalizing migrants and spying.

At the same time as the scenario described has been consolidated, the implementation of the ENS has been extended, resulting in a greater experience of its application, and a better understanding of the situation thanks to the successive editions of the National Security State Report (INES), the CCN-STIC security guides and the services and tools provided by the capacity to respond to information security incidents, the CCN-CERT, of the National Cryptological Centre (CCN).

In short, for all the reasons set out above, it is necessary to update the ENS to meet three major objectives.

First, align the ENS with the existing regulatory framework and strategic context to ensure security in digital administration. The aim is to clearly reflect the scope of the ENS for the benefit of cybersecurity and citizens' rights, to update the references to the existing legal framework and to review the formulation of certain issues in the light of it, in line with the 2019 National Cybersecurity Strategy and the National Cybersecurity Plan, so as to simplify, clarify or

harmonize the mandates of the ENS, remove aspects that may be considered excessive, or add those identified as necessary.

Secondly, to introduce the ability to adjust the requirements of the ENS, in order to ensure that they are adapted to the reality of certain groups or types of systems, taking into account the similarity of entities or services in terms of the risks to which their information systems and services are exposed. This advises the inclusion in the ENS of the concept of "specific compliance profile" which, approved by the National Cryptological Center, makes it possible to achieve a more effective and efficient adaptation of the ENS, rationalizing the resources required without undermining the protection sought and required.

Thirdly, to facilitate a better response to cybersecurity trends, reduce vulnerabilities and promote continuous monitoring by reviewing the basic principles, minimum requirements and security measures.

Finally, the adoption of this Royal Decree is also part of the implementation of the Digitalization Plan for Public Administrations 2021-2025, one of the main instruments for the implementation of the Recovery, Transformation and Resilience Plan and its Component 11 entitled "Modernization of Public Administrations", as well as for the development of investments and reforms foreseen in the Digital Spain 2025 agenda. This Digitalization Plan expressly envisages, among its reforms, the updating of the ENS in order to evolve the security policy of all Spanish public sector entities, taking into account European Union regulations aimed at increasing the level of cybersecurity of information systems. This reform is complemented by the establishment of the Cybersecurity Operations Centre of the General State Administration and its Public Agencies, which will serve as a reference for the other public administrations and will contribute to improving compliance with the ENS of the entities in their scope of application. This forecast has been supported by the Agreement of the Council of Ministers of 25 May 2021 on urgent actions in the field of cybersecurity, which mandates the processing and approval of a Royal Decree replacing Royal Decree 3/2010 of 8 January 2010 as a measure to strengthen the regulatory framework.

**III**

The Royal Decree is structured into 41 articles divided into seven chapters, three additional provisions, a transitional provision, a derogatory provision, three final provisions and four annexes

Chapter I covers the general provisions governing the subject matter and objectives of the Royal Decree, its scope of application, the reference to information systems processing personal data and the applicable definitions. The scope of application is that provided for in Article 2 of Law 40/2015 of 1 October 2015, to which the systems dealing with classified information are added, without prejudice to the applicable regulations, and it may be necessary to supplement the security measures of this Royal Decree with others specific to such systems, arising from the international commitments entered into by Spain or its membership in international bodies or fora in this field. The requirements of the ENS shall also apply to the information systems of private sector entities, where, in accordance with the applicable regulations and by virtue of a contractual relationship, they provide services to public sector entities for the exercise of their administrative powers and competencies. As noted above, considering that the digital transformation has increased the risks associated with the information systems that underpin public services and that the private sector is also immersed in the digital transformation of its business processes, both types of information systems are exposed to the same type of threats and risks. Therefore, the private sector operators who provide services to public sector entities, due to the high overlap between them, must guarantee the same level of security that applies to systems and information in the public sector, all in accordance with the special requirements laid down both in Organic Law 3/2018 of 5 December 2018 and in Organic Law 7/2021 of 26 May. Furthermore, where public sector entities carry out the installation, deployment and operation of 5G networks or the provision of 5G services, in addition to the provisions of this Royal Decree, the provisions of Royal Decree-Law No 7/2022 of 29 March on requirements to ensure the security of fifth generation electronic communications networks and services, in particular Article 17 thereof on security management by public administrations, as well as its implementing legislation, shall apply.

Chapter II, comprising Articles 5 to 11, regulates the basic principles to be governed by the ENS and which it lists in Article 5: integral security; risk-based security management; prevention, detection, response and conservation; existence of lines of defense; continuous monitoring and periodic re-evaluation; and differentiation of responsibilities.

Chapter III deals with the Security Policy and minimum requirements to allow for adequate protection of information and services. Articles 12 to 27 define those requirements: organization and implementation of the security process; risk management, consisting of a process of identification, analysis, evaluation and treatment of risks; personnel management; professionalism; authorization and control of access; protection of facilities; procurement of security products and procurement of security services; minimum privilege; system integrity and updating; protection of stored and transit information; prevention against other interconnected information systems; recording of activity and detection of harmful code; security incidents; business continuity; and continuous improvement of the security process. Next, Article 28 states that, in order to comply with those minimum requirements, the measures set out in Annex II must be adopted, in accordance with f considerations to that effect. However, such security measures may be replaced by other compensatory measures, provided that it is documented that the protection they provide is at least equivalent and fullfil the basic principles and minimum requirements set out above. Article 29 calls for the use of common infrastructure and services of public administrations in order to achieve greater efficiency and feedback from the synergies of each group. Finally, Article 30 establishes the possibility of implementing specific compliance profiles, as well as accreditation schemes for entities implementing secure configurations.

Chapter IV deals with security audit, security status report and response to security incidents. The security audit is carried out in full in Article 31, detailing the characteristics of the audit procedure and the related reports. For its part, Article 32, on the report on the state of security, highlights the role of the Sectoral eGovernment Commission in this area, as well as the CCN and the competent collegiate bodies in the field of digital administration in the General State Administration.

The prevention, detection and response to security incidents is regulated by articles 33 and 34, separating, on the one hand, the aspects of response capacity and, on the other hand, those relating to the provision of security incident response services, both to public sector entities and to private sector organizations providing services to them.

Chapter V, Articles 35 to 38, defines the standards of conformity, which are specified in four: Digital eAdministration, service and system lifecycle, control mechanisms and ENS compliance determination procedures.

For its part, Chapter VI, composed of its sole article, 39, establishes the obligation to update permanently, in accordance with the legal framework in force at all times, the evolution of technology and security and systems standards, as well as the aforementioned new threats and vectors of attack.

The operative part concludes with Chapter VII, which develops the procedure for categorizing information systems, defining in Article 40 the security categories and in Article 41 the powers in this regard.

With regard to the three additional provisions, the first regulates, sensitization, awareness-raising and training programs for the staff of public sector entities to be developed by the CCN and the National Institute of Public Administration.

The second additional provision regulates mandatory technical security instructions and information and communication technology security guides (CCN-STIC guides).

Finally, the third additional provision provides for compliance with the so-called “do no significant harm principle” to the environment and the conditions of climate and digital labelling.

The single transitional provision provides for a period of 24 months for the information systems falling within the scope of this Royal Decree, which existed prior to its entry into force, to be fully adapted to the ENS.

The derogating provision repeals Royal Decree 3/2010 of 8 January 2010 and any provisions of equal or lower rank which are contrary to the provisions of this Royal Decree.

Finally, the Royal Decree has three final provisions. The first of these lists the jurisdictional titles; the second final provision empowers the head of the Ministry of Economic Affairs and Digital Transformation to make the necessary provisions for its implementation and development, without prejudice to the powers of the Autonomous Communities for the development and implementation of the basic legislation of the State, and the third final

provision orders the entry into force on the day following that of its publication in the Official Gazette of the State.

The Royal Decree is supplemented by four annexes: Annex I sets out the systems security categories, detailing the sequence of actions to determine the security category of a system; Annex II details the security measures; Annex III deals with the subject matter, levels and interpretation of the Security Audit and, finally, Annex IV contains the glossary of terms and definitions.

With regard, in particular, to Annex II, this details the security measures structured in three groups: the organizational framework, consisting of the set of measures related to the overall security organization; the operational framework, consisting of the measures to be taken to protect the operation of the system as a comprehensive set of components for one purpose; and protective measures, which focus on protecting specific assets, according to their nature and the quality required by the level of security of the dimensions concerned. As mentioned above, the modification of the tactical and operational framework in which cyber threats and their related safeguards unfolded has made it necessary to update the list of security measures in Annex II, with a view to adding, removing or modifying controls and sub-checks, while including a new, more modern and appropriate reference system, based on the existence of a general requirement and possible reinforcements, aligned with the level of security pursued. All this is done with the aim of ensuring proportionate security of the information systems concerned and facilitating their implementation and auditing.

**IV**

The Royal Decree, whose approval is included in the Annual Regulatory Plan of the General State Administration for the year 2022, complies with the principles of good regulation contained in Article 129 of Law 39/2015 of 1 October 2015 (principles of necessity, effectiveness, proportionality, legal certainty, transparency and efficiency).

Thus, the Royal Decree is in line with the principles of necessity and effectiveness, as it pursues a general interest in specifying the ENS regulation by developing in this respect Law 40/2015 of 1 October 2015 and other specific aspects of national and European Union legislation mentioned in this preamble. The Royal Decree is also in line with the principle of proportionality, as it contains the regulation necessary for the achievement of the above-mentioned objectives. It also complies with the principle of legal certainty, being consistent with the rest of the legal system, establishing a stable, integrated and clear regulatory framework. During the procedure for drawing up the regulation and even in the context of the application of the provisions of Article 27 of Law 50/1997 of 27 November 1997 on the Government, since it is an urgent procedure agreed by the Council of Ministers, the procedures for hearing and public information have been formalized, in accordance with the provisions of Article 133 of Law 39/2015 of 1 October 2015 and Article 26 of Law 50/1997 of 27 November 1997, in compliance with the principle of transparency, and the objectives pursued by this Royal Decree are also justified in the preamble. The project has been submitted for consultation with the Autonomous Communities and the Spanish Federation of Municipalities and Provinces through the Sectoral Commission for e-Government and has been informed by the National Commission for Markets and Competition A.A.I. and the Spanish Agency for Data Protection A.A.I.

Finally, by virtue of the principle of efficiency, the Royal Decree does not introduce any variation in the administrative burden as compared to the legislation it implements.

The Royal Decree is adopted in exercise of the powers provided for in Articles 149.1.18, 149.1.21 and 149.1.29 of the Constitution, which confer exclusive competence on the State on the basis of the legal regime of public administrations, on telecommunications and on public security, respectively.

By virtue of this, on a proposal from the Minister for Economic Affairs and Digital Transformation, with the prior approval of the Minister for Finance and the Civil Service, in agreement with the Council of State, and after deliberation of the Council of Ministers at its meeting on 3 May 2022,

I PROVIDE:

CHAPTER I

## General provisions

Article 1. *Subject matter and objectives.*

1. The purpose of this Royal Decree is to regulate the National Security Framework (hereinafter referred to as ENS), established in Article 156.2 of Law 40/2015 of 1 October 2015 on the Legal Regime of the Public Sector.

2. The ENS consists of the basic principles and minimum requirements necessary for the adequate protection of the information processed and the services provided by the entities within its scope, in order to ensure access, confidentiality, integrity, accountability, authenticity, availability and retention of the data, information and services used by electronic means that they manage in the exercise of their powers.

3. The provisions of this Royal Decree, insofar as it concerns the information systems used for the provision of public services, must be considered to be covered by the resources and procedures of the National Security System set out in Law 36/2015 of 28 September 2015 on National Security.

Article 2. *Scope of application.*

1. This Royal Decree applies to the entire public sector, as defined in Article 2 of Law 40/2015 of 1 October 2015 and in accordance with the provisions of Article 156.2 thereof.

2. Furthermore, without prejudice to the application of Law 9/1968 of 5 April 1968 on Official Secrets and other special regulations, this Royal Decree applies to systems handling classified information, and it may be necessary to adopt additional security measures, specific to these systems, arising from the international commitments entered into by Spain or its membership in international bodies or forums.

3. This Royal Decree also applies to the information systems of private sector entities, including the obligation to have the security policy referred to in Article 12, when, in accordance with the applicable regulations and by virtue of a contractual relationship, they provide services or provide solutions to public sector entities for the exercise by them of their administrative powers and competencies.

The security policy referred to in Article 12 shall be approved in the case of such entities by the body with the highest executive powers.

The specifications of administrative or technical requirements for contracts concluded by public sector entities included in the scope of this Royal Decree shall include all the requirements necessary to ensure compliance with the ENS of the information systems in which the services provided by the contractors are supported, such as the presentation of the corresponding Declarations or Certifications of conformity with the ENS.

This caution shall also extend to the supply chain of these contractors, to the extent necessary and in accordance with the results of the relevant risk analysis.

4. Where public sector entities carry out the installation, deployment and operation of 5G networks or the provision of 5G services, in addition to the provisions of this Royal Decree, the provisions of Royal Decree-Law 7/2022 of 29 March on requirements to ensure the security of fifth generation electronic communications networks and services shall apply, in particular the provisions of Article 17 thereof on security management by public administrations, as well as its implementing regulations.

Article 3. *Information systems that process personal data.*

1. Where an information system processes personal data, shall apply the provisions of Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and Organic Law 3/2018 of 5 December 2018protection of Personal Data and guarantee of digital rights, or, where applicable, Organic Law 7/2021, of 26 May, 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, the other applicable regulations, as well as the criteria to be established by the Spanish Data Protection Agency or in its area of competence, by the autonomous data protection authorities, without prejudice to the requirements established in this Royal Decree.

2. In such cases, the controller or processor, advised by the Data Protection Officer, shall carry out a risk analysis in accordance with Article 24 of the General Data Protection Regulation and, in the cases of Article 35 thereof, an impact assessment on data protection.

3. In any event, the measures to be implemented as a result of the risk analysis and, where appropriate, the impact assessment referred to in the previous paragraph shall prevail if they are aggravated by those provided for in this Royal Decree.

Article 4. *Definitions.*

For the purposes provided in this Royal Decree, definitions, words, expressions and terms must be understood in the sense indicated in the Glossary of Terms included in Annex IV.

## CHAPTER II

## **Basic principles**

Article 5. *Basic principles of the National Security Framework.*

The ultimate purpose of information security is to ensure that an organization can fulfil its objectives, carry out its functions and exercise its competences using information systems. The following basic principles should therefore be taken into account in the area of information security:

a) Security as an integral process.
b) Risk-based security management.
c) Prevention, detection, response and conservation.
d) Existence of lines of defense.
e) Continuous monitoring.
f) Periodic re-evaluation.
g) Differentiation of responsibilities.

Article 6. *Security as an integral process.*

1. Security is understood as an integral process consisting of all the human, material, technical, legal and organizational elements related to the information system. The implementation of the ENS will be presided over by this principle, which excludes any specific action or conjunctural treatment.

2. Maximum attention shall be paid to raising awareness among those involved in the process and that of the hierarchical managers, so that neither ignorance nor a lack of organization and coordination or inappropriate instructions are a source of risk for security.

Article 7. *Risk-based security management.*

1. Risk analysis and management is an essential part of the security process and must be an ongoing and permanently updated activity.

2. Risk management will allow the maintenance of a controlled environment, minimizing risks to acceptable levels. The reduction to these levels shall be achieved through an appropriate implementation of security measures, in a balanced and proportionate manner to the nature of the information processed, the services to be provided and the risks to which they are exposed.

Article 8. *Prevention, detection, response and conservation.*

1. The security of the system shall include actions relating to the prevention, detection and response aspects, in order to minimize its vulnerabilities and to ensure that threats do not materialize or, if so, do not seriously affect the information it handles or the services it provides.

2. Prevention measures, which may incorporate components geared towards deterrence or reduction of the exposure surface, should eliminate or reduce the likelihood of threats

materializing.

3. Detection measures will be aimed at discovering the presence of a cyber incident.

4. The response measures, which will be managed in a timely manner, will be aimed at the restoration of information and services that may have been affected by a security incident.

5. Without detriment to the other basic principles and minimum requirements laid down, the information system shall ensure the retention of data and information in electronic form.

Likewise, the system shall keep services available throughout the whole life cycle of digital information, through a design and procedures that are the basis for the preservation of digital heritage.

Article 9. *Existence of lines of defense.*

1. The information system shall have a protection strategy consisting of multiple layers of security, arranged in such a way that, when one layer is compromised, it allows:

a) Develop an appropriate response to incidents that have not been avoided, reducing the likelihood that the system will be compromised as a whole.

b) Minimize the final impact on it.

2. The lines of defense must consist of measures of an organizational, physical and logical nature.

Article 10. *Continuous monitoring and periodic re-evaluation.*

1. Continuous monitoring will allow the detection of anomalous activities or behaviors and their timely response.

2. Ongoing assessment of the security status of assets will make it possible to measure their evolution, detecting vulnerabilities and identifying configuration deficiencies.

3. Security measures shall be regularly reassessed and updated, adjusting their effectiveness to the evolution of risks and protection systems, and may lead to a rethinking of security, if necessary.

Article 11. *Differentiation of responsibilities.*

1. In the information systems, the person responsible for the information, the person responsible for the service, the person responsible for security and the person responsible for the system shall be distinguished.

2. Responsibility for the security of information systems shall be differentiated from the responsibility for the operation of the information systems concerned.

3. The security policy of the organization shall detail the responsibilities of each official and the mechanisms for coordination and resolution of conflicts.

## CHAPTER III

## **Security policy and minimum security requirements**

Article 12. *Security policy and minimum security requirements.*

1. Information security policy is the set of guidelines governing how an organization manages and protects the information it handles and the services it provides. To this end, the instrument approving such a security policy shall include at least the following points:

a) The objectives or mission of the organization.

b) The regulatory framework within which the activities will take place.

c) The security roles or functions, defining for each one their duties and responsibilities, as well as the procedure for their appointment and renewal.

d) The structure and composition of the security management and coordination committee(s), detailing its scope of responsibility and the relationship with other elements of the organization.

e) Guidelines for the structuring of the system's security documentation, its management and access.

f) The risks arising from the processing of personal data.

2. Each public administration shall have a security policy formally approved by the competent body. In addition, each body or entity with its own legal personality falling within the subjective scope of Article 2 shall have a security policy formally approved by the competent body.

However, all or part of the subjects of an institutional public sector may be included in the subjective scope of the security policy approved by the administration with which they are linked, dependent or seconded, when determined by the competent bodies in the exercise of organizational powers.

3. In the General State Administration, each ministry shall have its security policy, which shall be approved by the head of the Department. Public bodies and entities belonging to the State institutional public sector may have their own security policy, approved by the competent body, which shall be consistent with that of the Department with which it maintains the relationship of liaison, dependence or secondment, or fall within the subjective scope of its security policy. They may also have their own security policy, approved by the competent body, consistent with that of the Department to which they belong or to which they are attached, the management centers of the General State Administration itself which manage services under the declaration of shared services.

4. The Secretariat General for Digital Administration of the Ministry of Economic Affairs and Digital Transformation shall have its own security policy, which will be approved by the head of The Secretariat General.

5. Municipalities may have a common security policy drawn up by the regional or local entity that assumes responsibility for the information security of municipal systems.

6. The security policy shall be established in accordance with the basic principles set out in Chapter II and shall be developed by applying the following minimum requirements:

a) Organization and implementation of the security process.
b) Risk analysis and management.
c) Personnel management.
d) Professionalism.
e) Authorization and control of accesses.
f) Protection of the facilities.
g) Security products procurement and contracting of security services.
h) Minimum privilege.
i) System integrity and updating.
j) Protection of stored and transit information.
k) Prevention against other interconnected information systems.
l) Recording of activity and detection of harmful code.
m) Security incidents.
n) Continuity of activity.
ñ) Continuous improvement of the security process.

7. Minimum requirements shall be demanded in proportion to the risks identified in each system in accordance with Article 28, some of which may be omitted in systems without significant risks.

Article 13. *Organization and implementation of the security process.*

1. The security of the information systems must involve all members of the organization.

2. The security policy, in application of the principle of differentiation of responsibilities referred to in Article 11 and as detailed in Section 3.1 of Annex II, shall be known to all persons forming part of the organization and shall unequivocally identify those responsible for ensuring its performance, who shall have the following functions:

a) The information officer shall determine the requirements for the information processed.
b) The service manager shall determine the requirements for the services provided.
c) The security officer shall determine the decisions to meet the security requirements of information and services, supervise the implementation of the measures necessary to ensure that the requirements are met and report on these issues.

d) The system manager, by himself or through own or contracted resources, shall be responsible for developing the concrete way of implementing security in the system and for supervising the day-to-day operation of the system, and may delegate to administrators or operators under their responsibility.

3. The security officer will be different from the system manager, and there should not be hierarchical dependence between the two. In exceptional situations where the justified absence of resources makes it necessary for both functions to fall on the same person or on different persons among whom there is a hierarchical relationship, compensatory measures shall be applied to ensure the purpose of the principle of differentiation of responsibilities laid down in Article 11.

4. A Technical Security Instruction will regulate the Certification Scheme of Security Officers, which will include the conditions and requirements required of this figure.

5. In the case of outsourced services, except for justified and documented reasons, the organization providing such services shall designate a POC (Point or Contact Person) for the security of the information processed and the service provided, supported by the management bodies, and to channel and supervise both compliance with the security requirements of the service it provides or the solution it provides, as well as communications related to information security and incident management for the scope of this service.

This security POC will be the security officer of the contracted organization and will be part of its area or will have direct communication with it. This is without prejudice to the fact that the ultimate responsibility rests with the public sector entity receiving those services.

Article 14. *Risk analysis and management.*

1. Each organization that develops and implements systems for the processing of information or the provision of services shall carry out its own risk management.

2. This will be done through the analysis and treatment of the risks to which the system is exposed. Without prejudice to Annex II, an internationally recognized methodology shall be used.

3. The measures taken to mitigate or eliminate the risks must be justified and in any case, there shall be a proportionality between them and the risks.

Article 15. *Personnel management.*

1. Personnel, whether their own or external, related to the information systems subject to the provisions of this Royal Decree, shall be trained and informed of their duties, obligations and responsibilities in security matters . Its action, which shall be monitored to verify that established procedures are followed, shall apply the security operational rules and procedures adopted in the performance of its tasks.

2. The meaning and scope of the safe use of the system shall be specified and reflected in security standards to be approved by the relevant management or higher body.

Article 16. *Professionalism.*

1. The security of information systems shall be addressed and reviewed and audited by qualified, dedicated and trained personnel at all stages of their life cycle: planning, design, acquisition, construction, deployment, operation, maintenance, incident management and dismantling.

2. The entities within the scope of this Royal Decree shall require, in an objective and non-discriminatory manner, that organizations providing them with security services have qualified professionals and appropriate levels of management and maturity in the services provided.

3. The organizations shall determine the training requirements and the necessary experience of staff for the development of their job.

Article 17. *Authorization and control of accesses.*

Controlled access to the information systems falling within the scope of this Royal Decree must be limited to duly authorized users, processes, devices or other information systems and exclusively to the permitted functions.

Article 18. *Protection of the facilities.*

The information systems and their associated communications infrastructure must remain in controlled areas and have adequate and proportional access mechanisms based on risk analysis, without prejudice to the provisions of Law 8/2011 of 28 April 2011 establishing measures for the protection of critical infrastructures and Royal Decree 704/2011 of 20 May 2011 approving the Regulation on the protection of critical infrastructures.

Article 19. *Security products procurement and contracting of security services.*

1. In the purchase security products or contracting of information and communication technology security services to be used in the information systems within the scope of this Royal Decree shall be used, in a manner proportionate to the category of the system and determined security level, those which have certified security functionality related to the purpose of their acquisition.

2. The Certification Body for the National Information Technology Security Assessment and Certification Scheme of the National Cryptological Centre (CCN), established pursuant to Article 2.2.c of Royal Decree 421/2004 of 12 March 2004 regulating the National Cryptological Centre, taking into account the national and international criteria and evaluation methodologies recognized by this body and depending on the intended use of the specific product or service within its competence, shall determine the following:

a) The functional security and certification assurance requirements.
b) Other additional security certifications that are required by regulation.
c) Exceptionally, the criterion to be followed in cases where there are no certified products or services.

3. For the contracting of security services, the provisions of the preceding paragraphs and the provisions of Article 16 shall apply.

Article 20. *Minimum privilege.*

Information systems must be designed and configured granting the minimum privileges necessary for their proper performance, which implies incorporating the following aspects:

a) The system shall provide the necessary functionality for the organization to achieve its statutory or contractual objectives.
b) The functions of operation, administration and recording of activity shall be the minimum necessary and shall ensure that they are carried out only by authorized persons, from sites or equipment also authorized; time restrictions and authorized access points may be required, where appropriate.
c) Functions that are unnecessary or inappropriate to the intended purpose shall be removed or disabled by means of configuration control. The ordinary use of the system must be simple and safe, so that an unsafe use requires a conscious act on the part of the user.
d) Security configuration guides shall be applied for the different technologies, adapted to the categorization of the system, in order to eliminate or disable functions that are unnecessary or inappropriate.

Article 21. *System integrity and updating.*

1. The inclusion of any physical or logical element in the up-to-date catalogue of assets of the system, or its modification, shall require prior formal authorization.
2. The ongoing assessment and monitoring will allow the adaptation of the security status of the systems according to the configuration deficiencies, the vulnerabilities identified and the updates affecting them, as well as the early detection of any incidents that occur on them.

Article 22. *Protection of stored and in transit information.*

1. In the organization and implementation of security, particular attention shall be paid to information stored or in transit through portable or mobile equipment or devices, peripheral devices, information media and open network communications, which shall be analyzed in particular for adequate protection.

2. Procedures shall be implemented to ensure the retrieval and long-term preservation of electronic documents produced by the information systems falling within the scope of this Royal Decree, where this is required.

3. Any information in non-electronic media that has been the cause or direct consequence of the electronic information referred to in this Royal Decree, shall be protected with the same degree of security as the latter. For this purpose, measures corresponding to the nature of the medium shall be applied in accordance with the applicable rules.

Article 23. *Prevention against other interconnected information systems.*

The perimeter of the information system shall be protected, especially if it is connected to public networks, as defined in General Telecommunications Law 9/2014 of 9 May 2014, strengthening the tasks of prevention, detection and response to security incidents.

In any case, the risks arising from the interconnection of the system with other systems shall be analyzed and their point of connection monitored. The appropriate interconnection between systems shall be subject to the provisions of the relevant Technical Security Instruction.

Article 24. *Recording of activity and detection of harmful code.*

1. In order to satisfy the object of this Royal Decree, with full guarantees of the right to honor, personal and family privacy and the image of those affected, and in accordance with the regulations on the protection of personal data, public or employment data, and other applicable provisions, the activities of users will be recorded, retaining the information strictly necessary to monitor, analyses, investigate and document improper or unauthorized activities, allowing the identification at all times of the person who acts.

2. In order to preserve the security of information systems, ensuring strict compliance with the principles of action of public administrations, and in accordance with the provisions of the General Data Protection Regulation and compliance with the principles of limitation of purpose, minimization of data and limitation of the retention period set out therein, the subjects covered by Article 2 may, to the extent strictly necessary and proportionate, analyses incoming or outgoing communications, and only for information security purposes, so that it is possible to prevent unauthorized access to networks and information systems, stop denial of service attacks, prevent malicious distribution of harmful code as well as other damage to the aforementioned networks and information systems.

3. In order to correct or, where appropriate, hold accountable, each user accessing the information system must be uniquely identified, so that it is known at all times who is granted access rights, what type of access rights they are granted, and who has carried out a particular activity.

Article 25. *Security incidents.*

1. The entity owing the information systems within the scope of this Royal Decree shall have security incident management procedures in accordance with the provisions of Article 33, the corresponding Technical Security Instruction and, in the case of an operator of essential services or a digital service provider, in accordance with the provisions of the Annex to Royal Decree 43/2021 of 26 January, implementing Royal Decree-Law 12/2018 of 7 September 2018 on the security of network and information systems.

2. In addition, detection mechanisms, classification criteria, analysis and resolution procedures, as well as channels of communication to interested parties and the recording of actions will be available. This record shalll be used for continuous improvement of system security.

Article 26. *Continuity of activity.*

The systems shall have backups copies and the necessary mechanisms shall be put in place to ensure continuity of operations in the event of losing the usual operating methods.

Article 27. *Continuous improvement of the security process.*

The integral security process implemented shall be continuously updated and improved. To

this end, the criteria and methods recognized in national and international practice relating to information technology security management shall be applied.

Article 28. *Compliance with minimum requirements.*

1. To ensure compliance with the minimum requirements laid down in this Royal Decree, the entities falling within its scope shall adopt the corresponding security measures and reinforcements set out in Annex II, taking into account:

a) The assets constituting the information systems concerned.
b) The category of the system, as provided for in Article 40 and Annex I.
c) The decisions taken to manage identified risks.

2. The measures referred to in paragraph 1 shall have the status of minimum requirements and may be extended at the discretion of the security officer, who may include additional measures, taking into account the state of the technology, the nature of the information processed or services provided and the risks to which the information systems concerned are exposed. The list of selected security measures will be formalized in a document called the Statement of Applicability, signed by the security officer.

3. The security measures referred to in Annex II may be replaced by other compensatory measures, provided that they are documented to protect, equal or better, the risk to assets (Annex I) and the basic principles and minimum requirements set out in Chapters II and III are met. As an integral part of the Statement of Applicability, the correspondence between the compensatory measures put in place and the offsetting measures in Annex II shall be indicated in detail. The whole shall be formally approved by the security officer. A CCN-STIC Guide to those provided for in the second additional provision will guide the selection of such measures, as well as their registration and inclusion in the Statement of Applicability.

Article 29. *Common infrastructure and services.*

The use of common infrastructure and services of public administrations, including shared or cross-cutting services, will facilitate compliance with the provisions of this Royal Decree. The specific assumptions of the use of these infrastructures and services will be determined by each public administration.

Article 30. *Specific compliance profiles and accreditation of secure configuration implementation entities.*

1. In accordance with the principle of proportionality and seeking an effective and efficient application of the ENS to specific entities or sectors of activity, specific compliance profiles may be implemented, covering those security measures which, resulting from the mandatory risk analysis, are suitable for a specific category of security.

2. Similarly to the provisions of the previous section, in order to enable the proper implementation and configuration of solutions or platforms provided by third parties, to be used by the entities falling within the scope of this Royal Decree, schemes for accreditation of entities and validation of persons may be implemented, ensuring the security of such solutions or platforms and compliance with the provisions of this Royal Decree.

3. The CCN shall, in the exercise of its powers, validate and publish the relevant specific compliance profiles to be defined and the above accreditation and validation schemes, in accordance with the technical security instructions and security guides approved in accordance with the second additional provision.

4. The corresponding technical security instructions or, where applicable, the CCN-STIC Security Guides shall specify the conditions to which local-mode implementations of products, systems or services originally provided in the cloud or remotely, as well as the specific conditions for their evaluation and audit, shall be subject.

## CHAPTER IV

## **System security: audit, report and security incidents**

Article 31. *Security audit.*

1. The information systems falling within the scope of this Royal Decree shall be subject to a regular audit, at least every two years, to verify compliance with the requirements of the ENS.

Such an audit shall be carried out on an exceptional basis whenever there are substantial changes to the information systems, which may have an impact on the required security measures. The performance of the extraordinary audit shall determine the date of calculation of the two years established for the next regular audit, as indicated in the previous paragraph.

The two-year period referred to in the preceding subparagraphs may be extended for three months where there are force majeure impediments not attributable to the entity that owns the information system or systems concerned.

2. The audit shall be carried out on the basis of the category of the system and, where applicable, the relevant specific compliance profile, as set out in Annexes I and III and in accordance with the provisions of the Technical Security Instruction on Auditing the Security of Information Systems.

3. Generally recognized criteria, working methods and conduct, as well as national and international standardization applicable to such activities, shall be used in the conduct of security audits.

4. The audit report shall give an opinion on the degree of compliance with this Royal Decree, identifying the findings of compliance and non-compliance detected. It shall also include the methodological audit criteria used, the scope and purpose of the audit, and the data, facts and observations on which the conclusions drawn are based, all in accordance with the aforementioned Technical Security Instruction on Auditing the Security of Information Systems.

5. The audit reports shall be submitted to the system manager and the security officer. These reports will be analysed by the security officer who will present its findings to the system manager for appropriate corrective action.

6. In the case of HIGH-category systems, having regard to the audit opinion and taking into account the possible seriousness of the deficiencies found, the system manager may temporarily suspend the processing of information, the provision of services or the total operation of the system, until they are properly rectified or mitigated.

7. Audit reports may be requested by the heads of each organization, with competences on IT security, and by the CCN.

Article 32. *Security status report.*

1. The Sectoral Commission for e-Government shall collect the information related to the status of the main security variables in the information systems covered by this Royal Decree, so as to enable it to draw up a general profile of the state of security in the entities owning the information systems included in the scope of Article 2, which shall be reflected in the corresponding report.

2. The CCN shall articulate the procedures necessary for the collection and consolidation of the information, as well as the methodological aspects for its processing and exploitation, through the relevant working groups set up for that purpose within the Sectoral Commission of Electronic Administration and the competent collegiate bodies within the General State Administration.

3. The results of the report shall be used by the competent authorities which shall promote appropriate measures to facilitate the continuous improvement of the state of security using, where appropriate, scoreboards and indicators that contribute to decision-making through the use of the tools that the CCN provides for that purpose.

Article 33. *Information security incidents response capability.*

1. The CCN shall articulate the response to security incidents around the CCN-CERT structure, which will act without prejudice to the security incident response capabilities of each public administration and the CCN's national and international coordination function.

2. Without prejudice to Article 19.4 of Royal Decree-Law 12/2018 of 7 September 2018, public sector entities shall notify the CCN of incidents that have a significant impact on the security of the information systems concerned, in accordance with the relevant Technical Security Instruction.

3. Where an essential operator who has been designated as a critical operator suffers from an incident, the reference CSIRTs shall coordinate with the Ministry of Interior, through its

Cybersecurity Coordination Office, as provided for in Article 11.2 of Royal Decree-Law 12/2018 of 7 September 2018.

4. When an operator with an incident in the National Defense suffers an incident, it shall analyses whether, by its scope, it could have an impact on the functioning of the Ministry of Defense or on the operation of the Armed Forces, it shall immediately inform its CSIRT of reference, which will inform the response capacity and security incidents of reference for the national defense field, called ESPDEF-CERT, of the Joint Cyberspace Command (MCCE) through the established channels. In such cases, ESPDEF-CERT of the Joint Cyberspace Command shall be informed in due course of developments in the management of the incident and may cooperate in the supervision with the competent authority.

5. In accordance with the provisions of Royal Decree-Law 12/2018 of 7 September 2018, the CCN shall exercise the national coordination of the technical response of computer security incident response teams (hereinafter referred to as *Computer Security Incident Response Team,* hereafter CSIRT) on the security of public sector networks and information systems.

6. Following a security incident, the CCN-CERT shall technically determine the risk of reconnecting the affected system(s), indicating the procedures to be followed and the safeguards to be implemented in order to reduce the impact, so as to avoid the recurrence of the circumstances leading to it.

Following a security incident, the Secretariat General for Digital Administration, without prejudice to the rules governing the continuity of the information systems involved in public security or the regulations governing the continuity of military information systems involved in the National Defense that require the participation of ESPDEF-CERT of the Joint Cyberspace Command, shall authorize the reconnection to the common means and services falling within its scope of responsibility, including those shared or cross-cutting, if a CCN-CERT exposure surface report has determined that the risk is assumed.

In the case of a security incident involving a common medium or service under the responsibility of the General Controller of the State Administration, the latter shall participate in the process of authorizing the reconnection referred to in the preceding paragraph.

7. Private sector organizations providing services to public entities shall notify INCIBE-CERT, a referral security incident response center for citizens and private law entities in Spain operated by the Spanish National Cybersecurity Institute M.P., S.A. (INCIBE) under the Ministry of Economic Affairs and Digital Transformation, of incidents affecting them through their computer security incident response team, who, without prejudice to his powers and to the provisions of Articles 9, 10 and 11 of Royal Decree 43/2021 of 26 January, in relation to the Platform for the Notification and Monitoring of Cyberincidents, shall immediately inform the CCN-CERT.

Article 34. *Provision of security incident response services to public sector entities.*

1. In accordance with Article 33, the CCN-CERT shall provide the following services:

a) Support and coordination for the treatment of vulnerabilities and the resolution of security incidents that the entities within the scope of this Royal Decree have.

The CCN-CERT, through its technical support and coordination service, shall act as quickly as possible in the event of any aggression received in the information systems concerned.

In order to fulfil the purposes set out in the preceding paragraphs, reports, audit records and configurations of the systems concerned and any other information deemed relevant may be collected, as well as any computer media deemed necessary for the investigation of the incident of the systems concerned, without prejudice to the provisions of the applicable data protection regulations, as well as to the possible confidentiality of institutional or organizational data.

b) Research and dissemination of best practices on information security among all members of public sector entities. To this end, the series of documents CCN-STIC (CCN-Security of Information and Communication Technologies), prepared by the CCN, will provide standards, instructions, guides, recommendations and best practices to implement the ENS and to ensure the security of the information systems within the scope of this Royal Decree.

c) Training for public sector staff specializing in information technology security to facilitate the updating of knowledge and to raise awareness and improve their capacities for the prevention, detection and management of incidents.

d) Information on vulnerabilities, alerts and warnings of new threats to information systems, collected from a variety of well-known sources, including their own.

2. The CCN will develop a program that provides the information, training, recommendations and tools necessary to enable public sector entities to develop their own security incident response capabilities, and in which the CCN will be the coordinator at the state public level.

## CHAPTER V

## Conformity standards

Article 35. *Digital administration.*

1. The security of the information systems that underpin the digital administration shall be governed by the provisions of this Royal Decree.

2. The CCN is the competent body to ensure proper interoperability in cybersecurity and cryptography, in relation to the implementation of Royal Decree 4/2010 of 8 January 2010 regulating the National Interoperability Framework in the field of eGovernment.

Article 36. *Lifecycle of services and systems.*

Security specifications shall be included in the life cycle of the services and systems, accompanied by the relevant control procedures.

Article 37. *Control mechanisms.*

Each entity owing the information systems falling within the scope of this Royal Decree and, where appropriate, its bodies, public bodies, departments or units, shall establish its control mechanisms to ensure genuine and effective compliance with the ENS.

Article 38. *National Security Framework compliance determination procedures.*

1. Information systems falling within the scope of Article 2 shall be subject to a process to determine their compliance with the ENS. To this end, the MEDIUM or HIGH category systems shall require an audit to certify their conformity, without prejudice to the security audit provided for in Article 31 which may also be used for the purposes of certification, whereas BASIC category systems shall only require a self-assessment for their declaration of conformity, without prejudice to the possibility that they may also be subject to a certification audit.

Both the self-assessment procedure and the certification audit shall be carried out in accordance with Article 31, Annex III and with the terms determined in the relevant Technical Security Instruction, which shall also specify the requirements for certification entities.

2. The persons responsible for the information systems referred to in the previous paragraph shall publish the declarations and certifications of conformity in accordance with the ENS on the relevant internet portals or electronic site and with the provisions of the aforementioned Technical Security Instruction.

## CHAPTER VI

## National Security Framework updating

Article 39. *Permanent update.*

The ENS shall be kept update on a permanent basis, developed and refined over time, in parallel with the progress of services provided by public sector entities, technological developments, the emergence or consolidation of new international standards on security and auditing and the risks to which the information systems concerned are exposed.

## CHAPTER VII

## Categorization of information systems

Article 40. *Security categories.*

1. The security category of an information system shall modulate the balance between the importance of the information it handles and the services it provides and the security effort required, depending on the risks to which it is exposed, under the principle of proportionality.

2. The determination of the security category shall be based on the assessment of the impact of an incident affecting the security of information or services to the detriment of availability, authenticity, integrity, confidentiality or accountability, following the procedure described in Annex I.

Article 41. *Faculties.*

1. The power to carry out the assessments referred to in Article 40 and, where appropriate, their subsequent amendment shall be vested in the responsible or responsible for the information or services concerned.

2. On the basis of the assessments referred to in the previous paragraph, the security category of the system shall be determined by the security officer(s).

First additional provision. *Training.*

The CCN and the National Institute of Public Administration will develop sensitization, awareness-raising and training programs for the staff of public sector entities to ensure an adequate deployment of information and legal, organizational and technical capacities related to cybersecurity in public information systems, and to ensure permanent knowledge of the ENS among those entities.

Second additional provision. *Development of the National Security Framework.*

In accordance with the provisions of this Royal Decree, the Secretariat of State for Digitalization and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation, on the proposal of the Sectoral Commission for e-Government and at the initiative of the National Cryptological Center, shall approve the mandatory technical security instructions, which will be published by a Resolution of the Secretary of State.

The technical security instructions shall take into account the applicable European Union harmonized standards. For their drafting and maintenance, the relevant working groups shall be set up in the collegiate bodies with competence in the field of digital administration.

In order to better comply with the provisions of this Royal Decree, the CCN, in the exercise of its powers, will draw up and disseminate the corresponding information and communication technology security guides (CCN-STIC guides), particularly the 800 series, which will be incorporated into the set of documents used to carry out security audits.

Third additional provision. *Respect for the principle of 'do no significant harm' to the environment.*

In compliance with the provisions of the Recovery, Transformation and Resilience Plan (PRTR) and Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility, all actions under the PRTR pursuant to this Royal Decree must respect the principle of "do no significant harm" to the environment (*Do No Significant Harm)* and the climate and digital labelling conditions.

Single transitional provision. *Systems adequacy.*

1. The information systems within the scope of this Royal Decree, which are pre-existing at the time of its entry into force, including those owned by private sector contractors in the terms referred to in Article 2, shall have 24 months to achieve full compliance with the ENS, which shall be demonstrated by the display of the corresponding conformity stamp, in accordance with the provisions of Article 38.

2. During the above 24 months, the information systems pre-existing at the time of the entry into force of this Royal Decree which have the corresponding Conformity Stamps, derived from Declarations or Certifications in accordance with the ENS, may maintain their validity by renewing their conformity and in accordance with the terms indicated by Royal Decree 3/2010

of 8 January 2010 from which they brought the case.

3. The new information systems shall apply the provisions of this Royal Decree from its conception.

Single derogatory provision. *Repeal of legislation.*

Royal Decree 3/2010 of 8 January 2010 regulating the National Security Framework in the field of electronic administration, as well as any provisions of equal or lower rank contrary to the provisions of this Royal Decree, are hereby repealed.

Final provision first. *Jurisdictional titles*

This Royal Decree is issued pursuant to Articles 149.1.18, 149.1.21 and 149.1.29 of the Constitution, which confer exclusive competence on the State on the basis of the legal regime of public administrations, telecommunications and public security, respectively.

Second final provision. *Regulatory development.*

The head of the Ministry of Economic Affairs and Digital Transformation is empowered to issue the necessary provisions for the implementation and development of the provisions of this Royal Decree, without prejudice to the powers of the Autonomous Communities for the development and implementation of the basic legislation of the State.

Third final provision. *Entry into force.*

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

Given in Madrid, 3 May 2022.

FELIPE R.

The First Vice-President of the Government
and Minister for Economic Affairs and Digital Transformation,
NADIA CALVIÑO SANTAMARÍA

## ANNEX I

### Information systems security categories

*1. Bases for determining the security category of an information system*

The determination of the security category of an information system shall be based on an assessment of the impact that an incident affecting the security of the information processed or service provided would have on the organization in order to:

a) Achieve its objectives.
b) Protect the assets in charge.
c) Ensure compliance with the legal system.

The security category of the information systems concerned shall be re-assessed annually, or whenever significant changes occur to the above criteria.

*2. Security dimensions*

In order to determine the impact on the organization of an incident affecting the security of the information processed or services provided and consequently, to establish the security category of the information system in question, the following security dimensions shall be taken into account, which shall be identified by their initials in capital letters:

a) Confidentiality [C].
b) Integrity [I].
c) Accountability [Acc].
d) Authenticity [Auth].
e) Availability [A].

*3. Determination of the level of security required in a security dimension*

Information or service may be affected in one or more of its security dimensions. Each security dimension concerned shall be assigned to one of the following levels of security: LOW, MEDIUM or HIGH. If a security dimension is not affected, it will not be attached to any level.

1. LOW level. It shall apply where the consequences of a security incident affecting one of the security dimensions entail limited damage to the functions of the organization, its assets or the individuals concerned.

Limited damage shall be understood as:

1 A significant reduction in the capacity of the organization to carry out its functions and competences effectively, even if they continue to be performed.
2 Cause minor damage to the assets of the organization.
3 Formal breach of a law or regulation, that can be remedied.
4 Cause minor harm to any individual, who, despite being annoying, can easily be repaired.
5 Others of a similar nature.

2. MEDIUM level. It shall apply where the consequences of a security incident affecting one of the security dimensions cause serious damage about the functions of the organization, its assets or the individuals concerned.

Serious damage shall be understood as:

1 A significant reduction in the capacity of the organization to effectively carry out its functions and competences, even if they continue to be performed.
2 Cause significant damage to the assets of the organization.
3 Material breach of any law or regulation, or formal non-compliance that is not remediable.
4 Cause significant harm to an individual, difficult to repair.
5 Others of a similar nature.

3. HIGH level. It shall apply where the consequences of a security incident affecting one of the security dimensions cause very serious damage to the functions of the organization, its assets or the individuals concerned.

'Very serious damage' means:

1 The effective cancellation of the organization's ability to effectively carry out its functions and competences.
2 Cause very serious and even irreparable damage to the assets of the organization.
3 Serious breach of a law or regulation.
4 Cause serious harm to any individual, difficult or impossible to repair.
5 Others of a similar nature.

Where an information system treats different information and provides different services, the level of security of the system in each dimension shall be the highest level established for each information and service.

*4. Identification of the security category of an information system*

1. Three security categories are defined: BASIC, MEDIUM and HIGH.

a) An information system shall be of HIGH category if any of its security dimensions reaches the level of HIGH security.
b) An information system shall be MEDIUM category if one of its security dimensions reaches the MEDIUM security level and none reaches a higher level of security.
c) An information system shall be BASIC if one of its security dimensions reaches the LOW level, and none reaches a higher level.

2. The determination of the security category of an information system on the basis of what is stated in the previous paragraph shall not lead to a change in the level of security of the security dimensions which have not affected the determination of the security category of the information system.

*5. Sequence of actions to determine the security category of a system*

1. Identification of the level of security for each information and service, depending on the security dimensions, taking into account the provisions of paragraph 3 above.

2. Determination of the security category of the system, as set out in paragraph 4 above.

The CCN-STIC guides of the CCN will specify the criteria necessary for an appropriate categorization of information systems security.

## ANNEX II

## Security measures

### *1. General provisions*

1. In order to achieve compliance with the basic principles and minimum requirements established, the security measures set out in this Annex shall be applied, which shall be proportionate to:

a) The relevant security dimensions in the system to be protected.
b) The security category of the information system to be protected.

2. Security measures are divided into three groups:

a) Organizational framework [org]. It consists of the set of measures related to the global organization of security.
b) Operational framework [op]. Formed by the measures to be taken to protect the operation of the system as an integral set of components for an end.
c) Protective measures [mp]. These are focus on protecting specific assets, depending on their nature and the quality required by the level of security of the dimensions concerned.

### *2. Selection of security measures*

1. The following steps shall be taken for the selection of security measures:

a) Identification of the types of assets present.
b) Determination of the relevant security dimensions, taking into account the requirements set out in Annex I.
c) Determination of the level of security for each security dimension, taking into account the requirements set out in Annex I.
d) Determination of the security category of the system, as set out in Annex I.
e) Selection of security measures, together with appropriate reinforcements, from those contained in this Annex, in accordance with the dimensions and their security levels and for certain security measures, in accordance with the security category of the system.

2. For the purpose of facilitating compliance with the provisions of this Annex, when there are subsystems in an information system which require the application of a level of security measures different from that of the main system, they may be segregated from the main system, with the level of security measures with the corresponding reinforcement being applied in each case, and provided that the information and services concerned can be delimited.

3. The CCN-STIC guides of the CCN may establish specific compliance profiles, in accordance with Article 30 of this Royal Decree, for specific entities or sectors, which shall include the list of measures and reinforcements applicable in each case or the criteria for their determination.

4. The correlation between the security levels required in each dimension and the security measures with their reinforcements is as shown in the table below:

| Security Measures | | By category or dimension(s)[1] | Level of security dimensions | | |
|---|---|---|---|---|---|
| | | | LOW | MEDIUM | HIGH |
| | | | System Security Category | | |
| | | | BASIC | MEDIUM | HIGH |
| **org** | **Organizational framework** | | | | |
| org.1 | Security policy | Category | applies | applies | applies |
| org.2 | Security regulations | Category | applies | applies | applies |
| org.3 | Security procedures | Category | applies | applies | applies |
| org.4 | Authorization process | Category | applies | applies | applies |
| **PO** | **Operational framework** | | | | |
| op.pl | Planning | | | | |
| op.pl.1 | Risk analysis | Category | applies | + R1 | + R2 |
| op.pl.2 | Security Architecture | Category | applies | + R1 | + R1 + R2 + R3 |
| op.pl.3 | Acquisition of new components | Category | applies | applies | applies |
| op.pl.4 | Sizing/capacity management | A | applies | + R1 | + R1 |
| op.pl.5 | Certified components | Category | N.A. | applies | applies |
| op.acc | Access control | | | | |
| op.acc.1 | Identification | Acc Auth | applies | + R1 | + R1 |
| op.acc.2 | Access requirements | C I Acc Auth | applies | applies | + R1 |
| op.acc.3 | Segregation of functions and tasks | C I Acc Auth | N.A. | applies | + R1 |
| op.acc.4 | Access rights management process | C I Acc Auth | applies | applies | applies |
| op.acc.5 | Authentication mechanism (external users) | C I Acc Auth | + [R1 or R2 or R3 or R4] | + [R2 or R3 or R4] + R5 | + [R2 or R3 or R4] + R5 |
| op.acc.6 | Authentication mechanism (organization users) | C I Acc Auth | + [R1 or R2 or R3 or R4] + R8 + R9 | + [R1 or R2 or R3 or R4] + R5 + R8 + R9 | + [R1 or R2 or R3 or R4] + R5 + R6 + R7 + R8 + R9 |
| op.exp | Operation | | | | |
| op.exp.1 | Asset inventory | Category | applies | applies | applies |
| op.exp.2 | Security Configuration | Category | applies | applies | applies |
| op.exp.3 | Security Configuration Management | Category | applies | + R1 | + R1 + R2 + R3 |
| op.exp.4 | Security maintenance and updates | Category | applies | + R1 | + R1 + R2 |
| op.exp.5 | Change Management | Category | N.A. | applies | + R1 |
| op.exp.6 | Protection against harmful code | Category | applies | + R1 + R2 | + R1 + R2 + R3 + R4 |
| op.exp.7 | Incident management | Category | applies | + R1 + R2 | + R1 + R2 + R3 |
| op.exp.8 | Recording of the activity | Acc | applies | + R1 + R2 + R3 + R4 | + R1 + R2 + R3 + R4 +R5 |
| op.exp.9 | Incident management record | Category | applies | applies | applies |

[1] Confidentiality [C] / Integrity [I] / Accountability [Acc] / Authenticity [Auth] / Availability [A]

| Security measures | | By category or dimension(s)[2] | Level of security dimensions | | |
|---|---|---|---|---|---|
| | | | LOW | MEDIUM | HIGH |
| | | | System Security Category | | |
| | | | BASIC | MEDIUM | HIGH |
| op.exp.10 | Cryptographic Key Protection | Category | applies | + R1 | + R1 |
| op.ext | External resources | | | | |
| op.ext.1 | Contracting and service level agreements | Category | N.A. | applies | applies |
| op.ext.2 | Daily management | Category | N.A. | applies | applies |
| op.ext.3 | Protection of the supply chain | Category | N.A. | N.A. | applies |
| op.ext.4 | Interconnection of systems | Category | N.A. | applies | + R1 |
| op.nub | Cloud Services | | | | |
| op.nub.1 | Cloud Service Protection | Category | applies | + R1 | + R1 + R2 |
| op.cont | Continuity of service | | | | |
| op.cont.1 | Impact analysis | A | N.A. | applies | applies |
| op.cont.2 | Continuity plan | A | N.A. | N.A. | applies |
| op.cont.3 | Periodic tests | A | N.A. | N.A. | applies |
| op.cont.4 | Alternative means | A | N.A. | N.A. | applies |
| op.mon | System monitoring | | | | |
| op.mon.1 | Intrusion detection | Category | applies | + R1 | + R1 + R2 |
| op.mon.2 | Metrics system | Category | applies | + R1 + R2 | + R1 + R2 |
| op.mon.3 | Monitoring | Category | applies | + R1 + R2 | + R1 + R2 + R3 + R4 + R5 + R6 |
| MP | Protective measures | | | | |
| mp.if | Protection of facilities and infrastructure | | | | |
| mp.if.1 | Separate areas with access control | Category | applies | applies | applies |
| mp.if.2 | Identification of persons | Category | applies | applies | applies |
| mp.if.3 | Fitting-out of premises | Category | applies | applies | applies |
| mp.if.4 | Electrical energy | A | applies | + R1 | + R1 |
| mp.if.5 | Fire protection | A | applies | applies | applies |
| mp.if.6 | Flood protection | A | N.A. | applies | applies |
| mp.if.7 | Recording of entries and exits of equipment | Category | applies | applies | applies |
| mp.per | Staff management | | | | |
| mp.per.1 | Job characterization | Category | N.A. | applies | applies |
| mp.per.2 | Duties and obligations | Category | applies | + R1 | + R1 |
| mp.per.3 | Awareness | Category | applies | applies | applies |
| mp.per.4 | Training | Category | applies | applies | applies |
| mp.eq | Protection of equipment | | | | |
| mp.eq.1 | Clear desk | Category | applies | + R1 | + R1 |

[2] Confidentiality [C] / Integrity [I] / Accountability [Acc] / Authenticity [Auth] / Availability [A]

| Security measures | | By category or dimension(s)[3] | Level of security dimensions | | |
|---|---|---|---|---|---|
| | | | LOW | MEDIUM | HIGH |
| | | | System Security Category | | |
| | | | BASIC | MEDIUM | HIGH |
| mp.eq.2 | User session lockout | Auth | N.A. | applies | + R1 |
| mp.eq.3 | Protection of portable devices | Category | applies | applies | + R1 +R2 |
| mp.eq.4 | Other devices connected to the network | C | applies | + R1 | + R1 |
| mp.com | Protection of communications | | | | |
| mp.com.1 | Secure perimeter | Category | applies | applies | applies |
| mp.com.2 | Protection of confidentiality | C | applies | + R1 | + R1 + R2 + R3 |
| mp.com.3 | Protection of integrity and authenticity | I Auth | applies | + R1 + R2 | + R1 + R2 + R3 + R4 |
| mp.com.4 | Separation of information flows on the network | Category | N.A. | + [R1 or R2 or R3] | + [R2 or R3] + R4 |
| mp.si | Protection of information media | | | | |
| mp.si.1 | Marking | C | N.A. | applies | applies |
| mp.si.2 | Cryptography | C I | N.A. | applies | + R1 + R2 |
| mp.si.3 | Custody | Category | applies | applies | applies |
| mp.si.4 | Transport | Category | applies | applies | applies |
| mp.si.5 | Erasure and Destruction | C | applies | + R1 | + R1 |
| mp.sw | Protection of IT applications | | | | |
| mp.sw.1 | IT Applications development | Category | N.A. | + R1 + R2 + R3 + R4 | + R1 + R2 + R3 + R4 |
| mp.sw.2 | Acceptance and commissioning | Category | applies | + R1 | + R1 |
| mp.info | Protection of information | | | | |
| mp.info.1 | Personal data | Category | applies | applies | applies |
| mp.info.2 | Rating of information | C | N.A. | applies | applies |
| mp.info.3 | Electronic signature | I Auth | applies | + R1 + R2 + R3 | + R1 + R2 + R3 + R4 |
| mp.info.4 | Time stamps | Acc | N.A. | N.A. | applies |
| mp.info.5 | Clean-up of documents | C | applies | applies | applies |
| mp.info.6 | Backups | A | applies | + R1 | + R1 + R2 |
| mp.s | Protection of services | | | | |
| mp.s.1 | E-mail protection | Category | applies | applies | applies |
| mp.s.2 | Protection of web services and applications | Category | + [R1 or R2] | + [R1 or R2] | + R2 + R3 |
| mp.s.3 | Protection of web browsing | Category | applies | applies | + R1 |
| mp.s.4 | Protection against denial of service | A | N.A. | applies | + R1 |

[3] Confidentiality [C] / Integrity [I] / Accountability [Acc] / Authenticity [Auth] / Availability [A]

5. The following conventions have been used in the tables in this annex:

a) The third column indicates whether the measure is required based on the security level of one or more security dimensions, or according to the security category of the system. When required by dimensional security level, it is indicated which affect using their initials.

b) To indicate that a certain security measure shall be applied to one or more security dimensions, at a given level of security, the “applies” voice is used.

c) “N.A.” means “does not apply” for compliance purposes and is therefore not required, without prejudice to the fact that its implementation in the system could be technically beneficial.

d) To indicate a higher requirement, security reinforcements (R) that add (+) to the basic requirements of the measure are used but are not always incremental to each other.

e) To point out that one can choose to apply one reinforcement or another, it shall be indicated in square brackets and separated by “or” [Rn or Rn+ 1].

f) The colors green, yellow and red have been used with the following code: green to indicate that a measure is applied in BASIC or higher category systems; the yellow to indicate which measures and reinforcements begin to apply in the MEDIUM category or above; and red to indicate which measures or reinforcements are only applicable in the HIGH category or require a higher security effort than MEDIUM.

6. Below, each of the measures is described individually and organized as follows:

a) First, a table summarizes the security requirements of the measure according to the security category of the system and the security dimensions concerned.

b) Then a description of the basic requirements of the security measures.

c) Subsequently, a number of additional reinforcements may appear to complement the basic requirements, not in all cases required or demanded, and which could be applied in certain specific compliance profiles.

d) In addition, the set of requirements and reinforcements required according to the security levels or the security category of the system, as appropriate, is indicated. Where it is possible to choose between a reinforcement or another, in addition to bracketing [Rm or Rn], an explanatory flowchart shall be included.

e) Finally, some reinforcements are optional, not being required in all information systems. They will be applied as additional measures when the risk analysis recommends it.

## *3.* ***Organizational framework [ORG]***

The organizational framework consists of a set of measures related to the global organization of security.

### 3.1 Security policy [org.1].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

The security policy, which shall be approved in accordance with Article 12 of this Royal Decree, shall be reflected in a document clearly specifying at least the following:

– [org.1.1] The objectives or mission of the organization.
– [org.1.2] The legal and regulatory framework within which the activities will take place.
– [org.1.3] Security roles or functions, defining for each the duties and responsibilities of the post, as well as the procedure for their appointment and renewal.
– [org.1.4] The structure of the security management and coordination committee(s), detailing its area of responsibility, its members and the relationship with other elements of the organization.
– [org.1.5] Guidelines for the structuring of system security documentation, its management and access.

**Implementation of the measure.**

– BASIC Category: org.1.
– MEDIUM Category: org.1.
– HIGH Category: org.1.

**3.2 Security regulations [org.2].**

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

A number of documents shall be available describing:

– [org.2.1] The correct use of equipment, services and facilities, as well as what will be considered misuse.
– [org.2.2] Staff responsibility with respect to compliance or violation of regulations: rights, duties and disciplinary measures in accordance with the legislation in force.

**Reinforcement R1-Specific documents.**

[org.2.r1.1] Security documentation, developed as reflected in the CCN-STIC guides that are applicable, shall be available.

**Implementation of the measure.**

– BASIC Category: org.2.
– MEDIUM Category: org.2.
– HIGH Category: org.2.

**3.3 Security procedures [org.3].**

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

A number of documents shall be available detailing clearly and precisely how to operate the elements of the information system:

– [org.3.1] How to carry out the usual tasks.
– [org.3.2] Who should do what.
– [org.3.3] How to identify and report abnormal behaviors.
– [org.3.4.] The manner in which information is to be treated in consideration of the level of security required, specifying how to perform:

a) Your access control.
b) Your storage.
c) Making copies.
d) The labeling of supports.
e) Telematic transmission.
f) Any other activity related to such information.

**Reinforcement R1-Validation of procedures.**

[org.3.r1.1] Validation of security procedures by the relevant authority shall be required.

**Implementation of the measure.**

– BASIC Category: org.3.
– MEDIUM Category: org.3.
– HIGH Category: org.3.

**3.4 Authorization process [org.4].**

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

A formal authorization process covering all elements of the information system concerned shall be established:

– [org.4.1] Using of regular and alternative facilities.
– [org.4.2] Incorporation of equipment in production, in particular equipment involving cryptography.
– [org.4.3] Incorporation of application in production.
– [org.4.4] Establishment of communications links with other systems.
– [org.4.5] Using regular and alternative communication media.
– [org.4.6] Using information media.
– [org.4.7] Use of mobile equipment. Mobile equipment means laptops, tablets, mobile phones or other similar equipment.
– [org.4.8] Use of third party services, under contract or agreement, concession, commission, etc.

**Implementation of the measure.**

– BASIC Category: org.4.
– MEDIUM Category: org.4.
– HIGH Category: org.4.

## *4. Operational framework [op]*

The operational framework consists of the measures to be taken to protect the operation of the system as a comprehensive set of components for one purpose.

### 4.1 Planning [op.pl].

#### 4.1.1 Risk analysis [op.pl.1].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | + R1 | + R2 |

**Requirements.**

An informal risk analysis shall be carried out in natural language. That is, a textual exposition that:

– [op.pl.1.1] Identify the most valuable assets in the system. (See op.exp.1).
– [op.pl.1.2] Identify the most likely threats.
– [op.pl.1.3] Identify the safeguards that protect against such threats.
– [op.pl.1.4] Identify the main residual risks.

**Reinforcement R1- Semiformal risk analysis.**

A semiformal risk analysis shall be performed, using a specific language, with a basic threat catalog and defined semantics. That is, a presentation with tables that:

– [op.pl.1.r1.1] Value qualitatively the most valuable assets of the system.
– [op.pl.1.r1.2] Quantify the most likely threats.
– [op.pl.1.r1.3] Evaluate the safeguards that protect against such threats.
– [op.pl.1.r1.4] Evaluate residual risk.

**Reinforcement R2- Formal risk analysis.**

A formal risk analysis, using a specific language, with an internationally recognized mathematical basis, should be performed that:

– [op.pl.1.r2.1] Value qualitatively the most valuable assets of the system.
– [op.pl.1.r2.2] Quantify possible threats.
– [op.pl.1.r2.3] Evaluate and prioritize appropriate safeguards.
– [op.pl.1.r2.4] Evaluate and formally assume the residual risk.

**Implementation of the measure.**

– BASIC Category: op.pl.1.
– MEDIUM Category: op.pl.1 + R1.
– HIGH Category: op.pl.1 + R2.

#### 4.1.2 Security architecture [op.pl.2].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | + R1 | +R1+R2+R3 |

**Requirements.**

The security of the system will be the subject of a comprehensive approach detailing at least the following aspects:

– [op.pl.2.1] Documentation of facilities, including areas and access points.
– [op.pl.2.2] System documentation, including equipment, internal networks and external connections, and access points to the system (workstations and management consoles).
– [op.pl.2.3] Scheme of lines of defense, including interconnection points to other systems or other networks (especially if it involves the internet or public networks in general); firewall, DMZ, etc.; and the use of different technologies to prevent vulnerabilities that could simultaneously drill several lines of defense.
– [op.pl.2.4] User identification and authentication system, including the use of concerted keys, passwords, identification cards, biometrics, or others of a similar nature, and the use of files or directories to authenticate the user and determine their access rights.

**Reinforcement R1-Management System.**

[op.pl.2.r1.1] Management system, relating to planning, organization and control of information security resources.

**Reinforcement R2-Security Management System with Continuous Improvement.**

[op.pl.2.r2.1] Information Security Management System, regularly update and approved.

**Reinforcement R3-Validation of data.**

[op.pl.2.r3.1] Internal technical controls, including validation of input, output and intermediate data.

**Implementation of the measure.**

– BASIC Category: op.pl.2.
– MEDIUM Category: op.pl.2 + R1.
– HIGH Category: op.pl.2 + R1 + R2 + R3.

### 4.1.3 Acquisition of new components [op.pl.3].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

A formal process shall be established to plan for the acquisition of new components of the system, a process that:

– [op.pl.3.1] It shall be based on the conclusions of the risk analysis ([op.pl.1]).
– [op.pl.3.2] It shall be in accordance with the chosen security architecture ([op.pl.2]).
– [op.pl.3.3] It shall consider technical, training and financing needs together.

**Implementation of the measure.**

– BASIC category: op.pl.3.
– MEDIUM category: op.pl.3.
– HIGH category: op.pl.3.

### 4.1.4 Sizing/ capacity management [op.pl.4].

| dimensions | A | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | applies | + R1 | + R1 |

**Requirements.**

Prior to placing in operation, a study shall be carried out covering the following aspects:

– [op.pl.4.1] Processing needs.
– [op.pl.4.2] Information storage needs: during processing and during the period to be retained.
– [op.pl.4.3] Communication needs.
– [op.pl.4.4] Staffing requirements: quantity and professional qualification.
– [op.pl.4.5] Needs for facilities and auxiliary means.

**Reinforcement R1 — Continuous improvement of capacity management.**

– [op.pl.4.r1.1] A capacity forecast shall be made and kept up-to-date throughout the system life cycle.
– [op.pl.4.r1.2] Tools and resources shall be used for capacity monitoring.

**Implementation of the measure (by availability):**

– LOW level: op.pl.4.
– MEDIUM level: op.pl.4 + R1.
– HIGH level: op.pl.4 + R1.

### 4.1.5 Certified components [op.pl.5].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | N.A. | applies | applies |

**Requirements.**

– [op.pl.5.1]. The Catalogue of Information and Communication Technology Security Products and Services (CPSTIC) of the CCN shall be used to select the products or services provided by a third party that are part of the security architecture of the system and those expressly referred to in the measures of this Royal Decree.

If there are no products or services in CPSTIC implementing the required functionalities, certified products as described in Article 19 shall be used.

A Technical Security Instruction shall detail the criteria relating to the purchase of security products.

— [op.pl.5.2] If the system provides a security service to a third party within the scope of the ENS, the product(s) on which that service is supported must pass a qualification process and be included in the CPSTIC or provide a certification that complies with the functional security and assurance requirements in accordance with Article 19.

**Reinforcement R1-Protection of electromagnetic emissions.**

[op.pl.5.r1.1] Information shall be protected against TEMPEST threats in accordance with the regulations in force.

**Reinforcement R2 — List of software components.**

[op.pl.5.r2.1] Each product and service shall include in its description a list of software components, as specified in [mp.sw.1.r5].

**Implementation of the measure.**

– BASIC category: N.A.
– MEDIUM Category: op.pl.5.
– HIGH Category: op.pl.5.

### 4.2 Access control [op.acc].

Access control includes all preparatory and executive activities aimed at allowing or denying an entity, user or process access to a system resource for the implementation of a particular action.

Access control mechanisms shall balance the user-friendliness and protection of information and services, with priority given to the security category of the system.

When interconnecting systems in which identification, authentication and authorization take place in different security domains, under different responsibilities, where necessary, local security measures shall be accompanied by the corresponding collaboration agreements delimiting mechanisms and procedures for the effective attribution and exercise of the responsibilities of each system ([op.ext]).

#### 4.2.1 Identification [op.acc.1].

| dimensions | Acc Auth | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | applies | + R1 | + R1 |

**Requirements.**

The identification of the users of the system shall be carried out in accordance with the following:

– [op.acc.1.1] Identification systems provided for in the applicable regulation may be used as a unique identifier, including concerted key systems and any other system that the public administrations consider valid under the terms and conditions laid down in Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations.

– [op.acc.1.2] When the user has different roles in relation to the system (as a citizen or end user, as a staff of the entity or as a system administrator, for example) will receive unique identifiers for each profile, so that the corresponding activity records are always collected, delimiting the privileges corresponding to each profile.

– [op.acc.1.3] Each entity (entity, user or process) that accesses the system shall have a unique identifier that allows to know the recipient of them and the access rights it receives, as well as the actions taken by each entity.

– [op.acc.1.4] User accounts shall be managed as follows:

a) Each account (of entity, user or process) shall be associated with a unique identifier.

b) Accounts should be disabled in the following cases: when the user leaves the organization; when the user ceases to have the function for which the user account was required; or, when the person who authorized it gives an order to the contrary.

c) Accounts shall be retained for the period necessary to meet the accountability needs of the activity records associated with them. This period shall be referred to as the 'retention period'.

– [op.acc.1.5] In cases of electronic communications, the parties involved shall be identified on the basis of the mechanisms provided for in relevant European and national legislation, with the following correspondence between the levels of the authenticity dimension of the information systems to which access is available and the levels of security (low, substantial, high) of the electronic identification systems provided for in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and its implementing or implementing rules:

a) If a LOW level in the authenticity dimension is required (Annex I): Low, substantial or high security level (Article 8 of Regulation (EU) No 910/2014).
b) If a MEDIUM level is required in the authenticity dimension (Annex I): Substantial or high level of security (Article 8 of Regulation (EU) No 910/2014).
c) If a HIGH level is required in the authenticity dimension (Annex I): High security level (Article 8 of Regulation (EU) No 910/2014).

**Reinforcement R1-Advanced Identification.**

d) [op.acc.1.r1.1] The identification of the user shall allow the system manager, the security officer or their respective delegated administrators to single out the person associated with it, as well as their responsibilities in the system.
e) [op.acc.1.r1.2] Identification data shall be used by the system to determine user privileges in accordance with the access control requirements set out in the security documentation.
[op.acc.1.r1.3] An updated list of authorized users shall be ensured and maintained by the system administrator/system security administrator.

**Application of the measure (by accountability and authenticity).**

LOW level: op.acc.1.
MEDIUM level: op.acc.1 +R1.
HIGH level: op.acc.1+ R1.

**4.2.2 Access requirements [op.acc.2].**

| dimensions | C I Acc Auth | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | applies | applies | + R1 |

**Requirements.**

– [op.acc.2.1] The resources of the system shall be protected by any mechanism that prevents their use, except for entities with sufficient access rights.
– [op.acc.2.2] The access rights of each resource shall be established according to the decisions of the person responsible for the resource, in accordance with the system's security policy and regulations.
– [op.acc.2.3] In particular, access to operating system components and their configuration files or records shall be controlled.

**Reinforcement R1-Access privileges.**

– [op.acc.2.r1.1] All authorized users must have a set of security attributes (privileges) that can be maintained individually.
– [op.acc.2.r1.2] Access privileges shall be implemented to restrict the type of access a user may have (read, write, modify, delete, etc.).

**Reinforcement R2- Control Device Access.**

– [op.acc.2.r2.1] Solutions shall be available to establish access controls to devices according to the security policy of the organization.

**Application of the measure (by confidentiality, integrity, accountability and authenticity).**

– LOW level: op.acc.2.
– MEDIUM level: op.acc.2.
– HIGH level: op.acc.2+ R1.

**4.2.3 Segregation of functions and tasks [op.acc.3].**

| dimensions | C I Acc Auth | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | N.A. | applies | + R1 |

**Requirements.**

The access control system shall be organized in such a way as to require the participation of two or more persons to perform critical tasks, nullifying the possibility that a single authorized individual may abuse his rights to commit any unlawful or unauthorized action.

– [op.acc.3.1] Where possible, development and operational capabilities shall not lie with the same person.
– [op.acc.3.2] Where possible, the persons who authorize and control the use shall be different.

**Reinforcement R1-Strict Segregation.**

– [op.acc.3.r1.1] Where possible, the same person shall not combine system configuration and maintenance functions.
– [op.acc.3.r1.2] The same person may not combine audit or oversight functions with any other function.

**Reinforcement R2-Audit privileges.**

– [op.acc.3.r2.1] Accounts with strictly controlled and personalized audit privileges shall exist.

**Reinforcement R3-Access to security information.**

– [op.acc.3.r3.1] Access to system security information shall be allowed only to authorized security/system administrators, using the necessary access mechanisms (console, web interface, remote access, etc.).

**Application of the measure (by confidentiality, integrity, accountability and authenticity).**

– LOW level: N.A.
– MEDIUM level: op.acc.3.
– HIGH level: op.acc.3 + R1.

**4.2.4 Access rights management process [op.acc.4].**

| dimensions | C I Acc Auth | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |

| | | | |
|---|---|---|---|
| | applies | applies | applies |

**Requirements.**

The access rights of each entity, user or process shall be limited in accordance with the following principles:

– [op.acc.4.1] All access shall be prohibited, unless expressly authorized.
– [op.acc.4.2] Minimum privilege: the privileges of each entity, user or process shall be reduced to the minimum necessary to fulfil its duties or functions.
– [op.acc.4.3] Need to know and responsibility to share: privileges shall be assigned in such a way that entities, users or processes shall only have access to knowledge of the information required to fulfil their duties or functions. The information is the property of the organization and all that is necessary for the user will be at its.
– [op.acc.4.4] Capability to authorize: Access authorization to the resources may be granted, altered or cancelled only by the personnel with the authority to do so, in accordance with the criteria established by the person responsible. Access permits shall be reviewed on a regular basis.
– [op.acc.4.5] A specific remote access policy shall be established, requiring express authorization.

**Application of the measure (by confidentiality, integrity, accountability and authenticity).**

LOW level: op.acc.4.
MEDIUM level: op.acc.4.
HIGH level: op.acc.4.

### 4.2.5 Authentication mechanism (external users) [op.acc.5].

Referring to users who are not users of the organization.
The CCN-STIC guides will develop the mechanisms and qualities required for each type of authentication factor depending on the security levels required by the information system that is accessed, and the privileges granted to the user.

| dimensions | C I Acc Auth | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | + [R1 or R2 or R3 or R4] | + [R2 or R3 or R4] + R5 | + [R2 or R3 or R4] + R5 |

**Requirements.**

– [op.acc.5.1] Before providing authentication credentials to entities, users or processes, they must have been identified and registered in a reliable manner with the system or with a Qualified Trusted Service Provider or an electronic identity provider recognized by public administrations, in accordance with the provisions of Law 39/2015 of 1 October 2015.
– [op.acc.5.2] Before activating the authentication mechanism, the user shall recognize that has received them and that is aware of and accepts the obligations of its possession, in particular the duty of diligent custody, the protection of its confidentiality and the duty of immediate notification in the event of loss.
– [op.acc.5.3] Credentials shall be under the sole control of the user and shall be activated once they are under their effective control.
– [op.acc.5.4] Credentials shall be changed at intervals marked by the organization's security policy.
– [op.acc.5.5] Credentials shall be disabled, and may be regenerated if necessary,

when there is evidence or suspicion of loss, commitment or disclosure to unauthorized entities (persons, equipment or processes).

– [op.acc.5.6] Credentials shall be disabled when the entity (person, equipment, or process) that authenticates ends its relationship with the system.

– [op.acc.5.7] Before authorizing access, the information submitted by the system shall be the minimum necessary for the user to authenticate, avoiding anything that may, directly or indirectly, disclose information about the system or account, its characteristics, its operation or its status. Credentials will only be validated when all the necessary data is available and, if rejected, the reason for rejection will not be informed.

– [op.acc.5.8] The number of attempts allowed shall be limited, blocking the access opportunity once that number is exceeded, and requiring a specific intervention to reactivate the account, which will be described in the documentation.

– [op.acc.5.9] The system shall inform the user of its rights or obligations immediately after obtaining access.

**Reinforcement R1-Passwords.**

– [op.acc.5.r1.1] A password shall be used as an authentication mechanism.

– [op.acc.5.r1.2] Standards of minimal complexity and robustness against divination attacks shall be imposed (see CCN-STIC guides).

**Reinforcement R2-Password + OTP.**

— [op.acc.5.r2.1] A one- time password (OTP) shall be required to complement the user password.

**Reinforcement R3-Certified.**

— [op.acc.5.r3.1] Qualified certificates shall be used as an authentication mechanism.

— [op.acc.5.r3.2] The use of the certificate shall be protected by a second factor, of the PIN type or biometric type.

— [op.acc.5.r3.3] The credentials used must have been obtained after prior in-person registration, or telematic, using a qualified electronic certificate.

**Reinforcement R4-Certified in physical device.**

— [op.acc.5.r4.1] Qualified certificates shall be used as an authentication mechanism, in physical support (card or similar) using algorithms, parameters and devices authorized by the CCN.

— [op.acc.5.r4.2] The use of the certificate shall be protected by a second factor of the PIN type or biometric type.

— [op.acc.5.r4.3] The credentials used must have been obtained after prior in-person registration, or telematic, using qualified electronic certificate.

**Reinforcement R5-Registration.**

— [op.acc.5.r5.1] Successful and failed accesses shall be recorded.

— [op.acc.5.r5.2] The user shall be informed of the last access made with its identity.

**Reinforcement R6-Limitation of the access window.**

— [op.acc.5.r6.1] Points where the system will require a renewal of user authentication by unique identification shall be defined, not enough with the established session.

**Reinforcement R7-Suspension for non-use.**

— [op.acc.5.r7.1] Credentials shall be suspended after a defined period of non-use.

**Application of the measure (by confidentiality, integrity, accountability and authenticity).**

— LOW level: op.acc.5 + [R1 or R2 or R3 or R4].
— MEDIUM level: op.acc.5 + [R2 or R3 or R4] + R5.
— HIGH level: op.acc.5 + [R2 or R3 or R4] + R5.

#### 4.2.6 Authentication mechanism (organization users) [op.acc.6].

This measure concerns staff of the body, own or contracted, stable or circumstantial, who may have access to information contained in the system.

The CCN-STIC guides will develop the mechanisms and qualities required for each type of authentication factor, depending on the levels of security required by the information system that is accessed, and the privileges granted to the user.

| dimensions | C I Acc Auth | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | + [R1 or R2 or R3 or R4] + R8 + R9 | + [R1 or R2 or R3 or R4] + R5 + R8 + R9 | + [R1 or R2 or R3 or R4] + R5 + R6 + R7 + R8 + R9 |

**Requirements.**

– [op.acc.6.1] Before providing credentials to users, users must know and accept the organization's security policy in respect of matters affecting them.

– [op.acc.6.2] Before activating the authentication mechanism, the user shall acknowledge that has received the access credentials and that knows and accepts the obligations involved in their possession, in particular the duty of diligent custody, the protection of its confidentiality and the duty of immediate notification in the event of loss.

– [op.acc.6.3] Credentials shall be under the sole control of the user and shall be activated once they are under their effective control.

– [op.acc.6.4] Credentials shall be changed at intervals marked by the organization's security policy.

– [op.acc.6.5] Credentials shall be disabled, and may be regenerated if necessary, when there is evidence or suspicion of loss, commitment or disclosure to unauthorized entities (persons, equipment or processes).

— [op.acc.6.6] Credentials shall be disabled when the authenticating user ends their relationship with the system.

— [op.acc.6.7] Before authorizing access, the information submitted by the system shall be the minimum necessary for the user to authenticate, avoiding anything that may, directly or indirectly, disclose information about the system or account, its characteristics, its operation or its status. Credentials will only be validated when all the necessary data is available and, if rejected, the reason for rejection will not be informed.

— [op.acc.6.8] The number of attempts allowed shall be limited, blocking the access opportunity once this number is exceeded, and requiring a specific intervention to reactivate the account, which will be described in the documentation.

— [op.acc.6.9] The system shall inform the user of its rights or obligations immediately after obtaining access.

**Reinforcement R1-Passwords.**

— [op.acc.6.r1.1] A password shall be used as an authentication mechanism when access is made from controlled areas without crossing uncontrolled areas (see reinforcement R8).

— [op.acc.6.r1.2] Standards of minimal complexity and robustness against divination attacks will be imposed (see CCN-STIC guides).

**Reinforcement R2-Password + another authentication factor.**

— [op.acc.6.r2.1] A second factor such as "something you have" is required, i.e. a device, a one-time password (OTP) as a complement to the user password, or "something

that is".

**Reinforcement R3-Certified.**

— [op.acc.6.r3.1] Qualified certificates shall be used as an authentication mechanism.
— [op.acc.6.r3.2] The use of the certificate shall be protected by a second factor, of the PIN type or biometric type.

**Reinforcement R4-Certified physical device.**

— [op.acc.6.r4.1] Qualified certificates shall be used as an authentication mechanism, in physical support (card or similar) using algorithms, parameters and devices authorized by the CCN.
— [op.acc.6.r4.2] The use of the certificate shall be protected by a second factor of the PIN type or biometric type.

**Reinforcement R5-Registration.**

— [op.acc.6.r5.1] Successful and failed accesses shall be recorded.
— [op.acc.6.r5.2] The user shall be informed of the last access made with his identity.

**Reinforcement R6-Limitation of the access window.**

— [op.acc.6.r6.1] Points where the system will require a renewal of user authentication by unique identification shall be defined, not enough with the established session.

**Reinforcement R7-Suspension for non-use.**

— [op.acc.6.r7.1] Credentials shall be suspended after a defined period of non-use.

**Reinforcement R8-Double factor for access from or through uncontrolled areas.**

"Controlled zone" is a zone that is not publicly accessible, requiring the user, before having access to the equipment, to have previously authenticated in some way (access control to the facilities), different from the logical authentication mechanism against the system. An example of an uncontrolled area is the Internet.

— [op.acc.6.r8.1] Access from or through uncontrolled areas requires a double authentication factor: R2, R3 or R4.

**Reinforcement R9-Remote Access (all levels).**

— [op.acc.6.r9.1] The Information Systems Interconnection STI shall apply.
— [op.acc.6.r9.2] Remote access shall consider the following aspects:

a) Be authorized by the appropriate authority.
b) Traffic must be encrypted.
c) If use does not occur on a constant basis, remote access shall be disabled and enabled only when necessary.
d) Audit records of such connections shall be collected.

**Application of the measure (by confidentiality, integrity, accountability and authenticity).**

— LOW level: op.acc.6 + [R1 or R2 or R3 or R4] + R8 + R9.
— MEDIUM level: op.acc.6 + [R1 or R2 or R3 or R4] + R5 + R8 + R9.
— HIGH level: op.acc.6 + [R1 or R2 or R3 or R4] + R5 + R6 + R7 + R8 + R9.

### 4.3 Operation [op.exp].

#### 4.3.1 Asset inventory [op.exp.1].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

[op.exp.1.1] An update inventory of all elements of the system shall be maintained, detailing their nature and identifying their controller; that is, the person who makes the decisions regarding it.

**Reinforcement R1-Tagging Inventory.**

– [op.exp.1.r1.1] Labelling of equipment and wiring shall be part of the inventory.

**Reinforcement R2- Periodic Asset Identification.**

– [op.exp.1.r2.1] Tools shall be available to continuously display the status of all computers on the network, in particular servers, network and communications devices.

**Reinforcement R3-Identification of critical assets.**

– [op.exp.1.r3.1] Tools shall be available to categorize critical assets by organization context and security risks.

**Reinforcement R4-List of software components.**

– [op.exp.1.r4.1] A formal list of third party software components used in system deployment shall be kept update. This list shall include software libraries and the services required for its deployment (platform or operational environment). The content of the list of components shall be equivalent to what is required in [mp.sw.1.r5].

**Implementation of the measure.**

– BASIC Category: op.exp.1.
– MEDIUM Category: op.exp.1.
– HIGH Category: op.exp.1.

**4.3.2 Security configuration [op.exp.2].**

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

Computers shall be configured prior to their entry into operation, so that:

– [op.exp.2.1] Standard accounts and passwords are removed.
– [op.exp.2.2] The “minimum functionality” rule shall apply, i.e.:

a) The system must provide the minimum functionality required for the organization to achieve its objectives.
b) It shall not provide unjustified functions (operation, administration or audit) in order to minimize its exposure perimeter by eliminating or deactivating functions that are unnecessary or inappropriate for the intended purpose.

– [op.exp.2.3] The default security rule shall apply, i.e.:

a) Security measures shall be respectful to the user and shall protect the user, unless

he consciously exposes himself to a risk.

b) To reduce security, the user will have to take conscious actions.

c) Natural use, in cases where the user has not consulted the manual, will be safe use.

– [op.exp.2.4] Virtual machines shall be configured and managed in a secure way. Patching management, user accounts, antivirus software, etc. will be performed as if they were physical machines, including the host machine.

**Implementation of the measure.**

– BASIC Category: op.exp.2.
– MEDIUM Category: op.exp.2.
– HIGH Category: op.exp.2.

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | + R1 | +R1+R2+R3 |

### 4.3.3 Security configuration management [op.exp.3].

**Requirements.**

The configuration of the system components shall be continuously managed so that:

– [op.exp.3.1] The “minimum function” rule is maintained at all times ([op.exp.2]).
– [op.exp.3.2] The “minimum privilege” rule is maintained at all times ([op.exp.2]).
– [op.exp.3.3] The system is adapted to new, previously authorized needs. (See [op.acc.4]).
– [op.exp.3.4] The system reacts to reported vulnerabilities. (See [op.exp.4]).
– [op.exp.3.5] The system reacts to incidents. (See [op.exp.7]).
– [op.exp.3.6] The security settings may only be edited by duly authorized personnel.

**Reinforcement R1 -Regular maintenance of the configuration.**

– [op.exp.3.r1.1] There shall be authorized and regularly maintained hardware/software configurations for servers, network elements and workstations.
– [op.exp.3.r1.2] The hardware/software configuration of the system shall be checked periodically to ensure that unauthorized elements have not been introduced or installed.
– [op.exp.3.r1.3] A list of authorized services for servers and workstations shall be maintained.

**Reinforcement R2-Responsibility of configuration.**

– [op.exp.3.r2.1] The security configuration of the operating system and applications, both for stations and servers and for system network electronics, shall be the responsibility of a very limited number of system administrators.

**Reinforcement R3-Security backups.**

– [op.exp.3.r3.1] The system configuration shall be backed up so that it can be rebuilt in part or in full after an incident.

**Reinforcement R4-Application of the configuration.**

– [op.exp.3.r4.1] The security configuration of the operating system and applications shall be kept update through a manual application or procedure allowing the installation of appropriate version modifications and security updates.

**Reinforcement R5-Control of the Security Status of the Settings.**

– [op.exp.3.r5.1] Tools shall be available to enable the security status of the network device configuration to be known on a regular basis and, if it proves deficient, to enable its correction.

**Implementation of the measure.**

– BASIC Category: op.exp.3.
– MEDIUM Category: op.exp.3 + R1.
– HIGH Category: op.exp.3 + R1 + R2 + R3.

### 4.3.4 Security maintenance and updates [op.exp.4].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | + R1 | +R1+R2 |

**Requirements.**

In order to maintain the physical and logical equipment that constitutes the system, the following shall apply:

– [op.exp.4.1] Manufacturers' specifications for the installation and maintenance of systems shall be met, including continuous monitoring of warnings of defects.
– [op.exp.4.2] A procedure shall be available to analyses, prioritize and determine when to apply security updates, patches, upgrades, and new versions. Prioritization shall take into account the change in risk depending on the implementation or not of the update.
– [op.exp.4.3] Maintenance may only be carried out by duly authorized personnel.

**Reinforcement R1-Tests in pre-production.**

– [op.exp.4.r1.1] Before a new or patched version is put into production, it shall be tested in a controlled test environment consistent with configuration to the production environment, that the new installation works properly and does not decrease the efficiency of the functions needed for daily work.

**Reinforcement R2-Failure prevention.**

– [op.exp.4.r2.1] A mechanism to reverse them in the event of adverse effects shall be provided prior to the application of security settings, patches and updates.

**Reinforcement R3-Updates and periodic tests.**

– [op.exp.4.r3.1] The integrity of the firmware used in the hardware devices of the system (network infrastructure, BIOS, etc.) must be checked periodically. The periodicity of these checks will follow the recommendations of the CCN-STIC Guide that is applicable.

**Reinforcement R4 — Continuous monitoring.**

– [op.exp.4.r4.1] A strategy for continuous monitoring of threats and vulnerabilities

shall be deployed at the system level. This strategy shall detail:

1. The critical security indicators to be used.
2. The security patch application policy for related software components in the lists of [op.exp.1.r4], [op.ext.3.r3] and [mp.sw.1.r5]).
3. The criteria for regular and exceptional review of threats to the system.

**Implementation of the measure.**

– BASIC Category: op.exp.4.
– MEDIUM Category: op.exp.4 + R1.
– HIGH Category: op.exp.4 + R1 + R2.

**4.3.5 Change management [op.exp.5].**

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | N.A. | applies | + R1 |

**Requirements.**

Continuous monitoring of changes to the system shall be maintained so that:

– [op.exp.5.1] Changes shall be planned to reduce the impact on the provision of the affected services. To this end, all change request shall be recorded by assigning a reference number for follow-up, in an equivalent way to the recording of incidents.
– [op.exp.5.2] The information to be recorded for each change request shall be sufficient to allow the person to authorize them to have no doubts about it and to manage it until its rejection or implementation.
– [op.exp.5.3] Pre-production tests, whenever possible, shall be carried out on equipment equivalent to production, at least in the specific aspects of the change.
– [op.exp.5.4] A risk analysis shall determine whether the changes are relevant to system security. Changes that involve a risk at HIGH level must be approved, explicitly, prior to their implementation, by the security officer.
– [op.exp.5.5] Once the change is implemented, the appropriate acceptance tests will be performed. If positive, the configuration documentation (network diagrams, manuals, inventory, etc.) shall be updated where appropriate.

**Reinforcement R1-Prevention of failures.**

– [op.exp.5.r1.1] Prior to the application of the changes, consideration should be given to the possibility of reversing them in the event of adverse effects.
– [op.exp.5.r1.2] All software and hardware failures shall be communicated to the designated security organization officer.
– [op.exp.5.r1.3] All system changes shall be documented, including an assessment of the impact of such a change on system security.

**Implementation of the measure.**

– BASIC Category: N.A.
– MEDIUM Category: op.exp.5.
– HIGH Category: op.exp.5+ R1.

**4.3.6 Protection against harmful code [op.exp.6].**

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | + R1+R2 | +R1+R2+R3+R4 |

**Requirements.**

– [op.exp.6.1] Preventive and reaction mechanisms against harmful code shall be available, including maintenance in accordance with the manufacturer's recommendations.

– [op.exp.6.2] Harmful code protection software shall be installed on all equipment: user workstation, servers and perimeter elements.

– [op.exp.6.3] Any file from external sources shall be analyzed before working with it.

– [op.exp.6.4] Harmful code detection databases shall remain permanently updated.

– [op.exp.6.5] The harmful code detection software installed at user workstations shall be properly configured and implement real-time protection according to the manufacturer's recommendations.

**Reinforcement R1- Periodic Scanning.**

– [op.exp.6.r1.1] The entire system shall be scanned regularly to detect harmful code.

**Reinforcement R2-Preventive system review.**

– [op.exp.6.r2.1] Critical functions shall be analyzed when boot the system to prevent unauthorized modifications.

**Reinforcement R3 — Whitelist.**

– [op.exp.6.r3.1] Only those previously authorized applications may be executed. A whitelist shall be implemented to prevent the execution of unauthorized applications.

**Reinforcement R4-Capacity of response in case of incident.**

– [op.exp.6.r4.1] Security tools aimed at detecting, investigating and resolving suspicious activities in user workstations and servers (EDR - *Endpoint Detection and Response*) shall be used.

**Reinforcement R5-Configuration of the harmful code detection tool.**

– [op.exp.6.r5.1] The harmful code detection software shall allow perform advanced configurations and review the system at boot and every time a removable device is connected.

– [op.exp.6.r5.2] The harmful code detection software installed on servers and perimeter elements shall be properly configured and implement real-time protection according to the manufacturer's recommendations.

**Implementation of the measure.**

– BASIC Category: op.exp.6.
– MEDIUM Category: op.exp.6+ R1 + R2.
– HIGH Category: op.exp.6+ R1 + R2 + R3 + R4.

### 4.3.7 Incident management [op.exp.7].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | + R1+R2 | + R1+R2+ R3 |

**Requirements.**

– [op.exp.7.1] A comprehensive process shall be available to address incidents that may have an impact on system security, including the report of security events and weaknesses, detailing the classification criteria and the escalation of the reporting.

– [op.exp.7.2] The management of incidents affecting personal data shall take into account the provisions of the General Data Protection Regulation; organic Law 3/2018 of 5 December 2018, in particular its first additional provision, as well as the other implementing regulations, without prejudice to the requirements laid down in this Royal Decree.

**Reinforcement R1-Notification.**

– [op.exp.7.r1.1] One-stop-shop solutions shall be available for reporting incidents to CCN-CERT, allowing the distribution of notifications to the different entities in a federated manner, using hierarchical administrative units.

**Reinforcement R2 — Detection and Response.**

The comprehensive process for dealing with incidents that may have an impact on system security ([op.exp.7.1]) shall include:

– [op.exp.7.r2.1] Imposition of urgent measures, including detention of services, isolation of the affected system, collection of evidence and protection of records, as appropriate.
– [op.exp.7.r2.2] Allocation of resources to investigate the causes, analyses the consequences and resolve the incident.
– [op.exp.7.r2.3] To inform the information officer and service manager concerned and of the actions taken to resolve the incident.
– [op.exp.7.r2.4] Measures for:

a) Prevent a recurrence of the incident.
b) Include in user procedures the identification and way of dealing with the incident.
c) Update, extend, improve or optimize incident resolution procedures.

**Reinforcement R3-Dynamic Reconfiguration**

Dynamic reconfiguration of the system aims to stop, divert or limit attacks, limiting damage.
– [op.exp.7.r3.1] Dynamic reconfiguration includes, for example, changes in router rules, access control lists, intrusion detection/prevention system parameters and rules on firewalls and gateways, critical element isolation, and backup isolation.
– [op.exp.7.r3.2] The organization shall adapt dynamic reconfiguration procedures by reacting to CCN-CERT announcements concerning sophisticated cyber threats and attack campaigns.

**Reinforcement R4-Prevention and Automatic Response.**

– [op.exp.7.r4.1] Tools shall be available to automate the prevention and response process by detecting and identifying anomalies, dynamic network segmentation to reduce the attack surface, isolation of critical devices, etc.

**Implementation of the measure.**

– BASIC Category: op.exp.7.
– MEDIUM Category: op.exp.7+ R1 + R2.
– HIGH Category: op.exp.7+ R1 + R2 + R3.

**4.3.8 Recording of the activity [op.exp.8].**

| dimensions | Acc | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | applies | +R1+R2+R3+R4 | +R1+R2+R3+R4+R5 |

**Requirements.**

Activities in the system shall be recorded in such a way that:

– [op.exp.8.1] An audit log shall be generated, which shall include at least the identifier of the user or entity associated with the event, date and time, on what information the event takes place, type of event and the outcome of the event (failure or success), according to the security policy and the procedures associated with it.
– [op.exp.8.2] Activity record on servers shall be activated.

**Reinforcement R1-Review of records.**

– [op.exp.8.r1.1] Activity record shall be reviewed informally on a regular basis, looking for abnormal patterns.

**Reinforcement R2-Synchronisation of the clock of the system.**

– [op.exp.8.r2.1] The system shall have a time reference *(timestamp*) to facilitate event logging and auditing functions. The modification of the system time reference shall be an administration function and, in case of synchronization with other devices, authentication and integrity mechanisms shall be used.

**Reinforcement R3-Retention of records.**

– [op.exp.8.r3.1] The system security documentation shall indicate the security events to be audited and the record retention time before being deleted.

**Reinforcement R4-Access Control.**

– [op.exp.8.r4.1] Activity records and, where applicable, backups thereof may only be accessed or deleted by duly authorized personnel.

**Reinforcement R5-Automatic review and correlation of events.**

– [op.exp.8.r5.1] The system shall implement tools to analyses and review system activity and audit information, in search of possible or actual security compromises.
– [op.exp.8.r5.2] An automatic system for collection of records, correlation of events and automatic response to them shall be available.

**Application of the measure (by accountability).**

– LOW level: op.exp.8.
– MEDIUM level: op.exp.8 + R1 + R2 + R3 + R4.
– HIGH level: op.exp.8 + R1 + R2 + R3 + R4 + R5.

### 4.3.9 Incident management record [op.exp.9].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

All actions related to incident management shall be recorded in such a way that:

– [op.exp.9.1] Initial, intermediate and final reports of incidents, emergency actions and system modifications resulting from the incident shall be recorded.
– [op.exp.9.2] Evidence that may be settled in a jurisdictional area shall be recorded, especially where the incident may involve disciplinary action against internal staff, external suppliers or prosecution of crimes. In determining the composition and detail of this evidence, specialized legal advice will be used.
– [op.exp.9.3] As a result of incident analysis, the determination of auditable events

shall be reviewed.

**Implementation of the measure.**

– BASIC Category: op.exp.9.
– MEDIUM Category: op.exp.9.
– HIGH Category: op.exp.9.

### 4.3.10 Cryptographic key protection [op.exp.10].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | + R1 | + R1 |

**Requirements.**

– [op.exp.10.1] Crypto keys shall be protected throughout their life cycle: (1) generation, (2) transport to the point of operation, (3) safekeeping during the operation, (4) archive after decommissioning and (5) final destruction.
– [op.exp.10.2] The means of generation shall be isolated from the means of exploitation.
– [op.exp.10.3] The keys removed from operations to be archived shall be in isolated means of exploitation.

**Reinforcement R1-Algorithms authorized reinforcement.**

– [op.exp.10.r1.1] Algorithms and parameters authorized by the CCN shall be used.

**Reinforcement R2-Advanced cryptographic key protection.**

– [op.exp.10.r2.1] Encryptors that meet the requirements set out in the applicable CCN-STIC guide shall be used.

**Implementation of the measure.**

– BASIC Category: op.exp.10.
– MEDIUM Category: op.exp.10 + R1.
– HIGH Category: op.exp.10 + R1.

## 4.4 External resources [op.ext].

Where the organization uses external resources (services, products, facilities or personnel), it shall maintain full responsibility for the risks to the information processed or services provided, taking the necessary measures to exercise its responsibility and maintain control at all times.

### 4.4.1 Contracting and service level agreements [op.ext.1].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | N.A. | applies | applies |

**Requirements.**

— [op.ext.1.1] A Service Level Agreement shall be contractually established prior to the effective use of external resources, including the characteristics of the service provided, which should be understood as “minimum admissible service”, as well as the liability of the provider and the consequences of any breaches.

**Implementation of the measure.**

– BASIC category: N.A
– MEDIUM Category: op.ext.1.
– HIGH Category: op.ext.1.

### 4.4.2 Daily management [op.ext.2].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | N.A. | applies | applies |

**Requirements.**

The following shall be established:

– [op.ext.2.1] A routine system for measuring compliance with service obligations, including the procedure for neutralizing any deviation outside the agreed tolerance range ([op.ext.1]).
– [op.ext.2.2] The coordination mechanism and procedures for carrying out the maintenance tasks of the systems covered by the agreement, which shall cover incidents and disasters (see [op.exp.7]).

**Implementation of the measure.**

– BASIC Category: N.A
– MEDIUM Category: op.ext.2.
– HIGH Category: op.ext.2.

### 4.4.3 Supply chain protection [op.ext.3].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | N.A. | N.A. | applies |

**Requirements.**

– [op.ext.3.1] The impact of an accidental or deliberate incident originating in the supply chain on the system shall be analyzed.
– [op.ext.3.2] The risk to the system shall be estimated because of the estimated impact in the previous point.
– [op.ext.3.3] Measures shall be taken to contain the impacts estimated in the previous points.

**Reinforcement R1-Contingency plan.**

– [op.ext.3.r1.1] The organizational continuity plan shall take into account the dependency of critical external suppliers.
– [op.ext.3.r1.2] Continuity tests or exercises must be performed, including scenarios

where a supplier fails.

**Reinforcement R2-Security Management System.**

– [op.ext.3.r2.1] A system to protect the processes and information flows in the online relationships (online) between the different components of the supply chain shall be implemented.

**Reinforcement R3-List of software components.**

– [op.ext.3.r3.1] A formal record containing the details and supply chain relationships of the various components used in software construction as specified in [mp.sw.1.r5] shall be kept update. This list shall be provided by the supplier of the application, library or product supplied.

**Implementation of the measure.**

– BASIC Category: N.A.
– MEDIUM Category: N.A.
– HIGH Category: op.ext.3.

### 4.4.4 Interconnection of systems [op.ext.4].

Interconnection is referred to as the establishment of links with other information systems for the exchange of information and services.

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | N.A. | applies | + R1 |

**Requirements.**

– [op.ext.4.1] All exchanges of information and provision of services with other systems shall be subject to prior authorization. Any flow of information shall be prohibited unless expressly authorized.
– [op.ext.4.2] For each interconnection it shall be explicitly documented: the interface characteristics, security and data protection requirements and the nature of the information exchanged.

**Reinforcement R1-Coordination of activities.**

– [op.ext.4.r1.1] Where systems are interconnected where identification, authentication and authorization take place in different security domains, under different responsibilities, local security measures shall be accompanied by appropriate coordination mechanisms and procedures for the effective attribution and exercise of the responsibilities of each system.

**Implementation of the measure.**

– BASIC Category: N.A
– MEDIUM Category: op.ext.4.
– HIGH Category: op.ext.4 + R1.

## 4.5 Cloud services [op.nub].

### 4.5.1 Cloud service protection [op.nub.1].

| dimensions | All |
|---|---|

| category | BASIC | MEDIUM | HIGH |
|---|---|---|---|
| | applies | + R1 | +R1+R2 |

**Requirements.**

— [op.nub.1.1] Systems providing a cloud service to public sector bodies shall comply with the set of security measures depending on the cloud service model they provide: Software as a *Service (SaaS*), Platform as a *Service (PaaS*) and Infrastructure as a Service (*IaaS*) defined in the CCN-STIC guides that are applicable.

— [op.nub.1.2] Where cloud services provided by third parties are used, the information systems supporting them shall comply with the ENS or comply with the measures developed in a CCN-STIC guide which shall include, inter alia, requirements relating to:

a) Audit of penetration tests (*Pentesting*).
b) Transparency.
c) Encryption and key management.
d) Jurisdiction of the data.

**Reinforcement R1- Certified Services.**

— [op.nub.1.r1.1] Where cloud services provided by third parties are used, they shall be certified under a certification methodology recognized by the Certification Body of the National Scheme for Evaluation and Certification of Information Technology Security.

— [op.nub.1.r1.2] If the cloud service is a security service, it shall comply with the requirements set out in [op.pl.5].

**Reinforcement R2-Specific Security Configuration Guides.**

— [op.nub.1.r2.1] The security configuration of the systems providing these services shall be carried out in accordance with the relevant CCN-STIC Guide to Specific Security Configuration, aimed at both the user and the provider.

**Implementation of the measure.**

— BASIC category: op.nub.1.
— MEDIUM category: op.nub.1 + R1.
— HIGH category: op.nub.1+ R1 + R2.

### 4.6 Continuity of service [op.cont].

#### 4.6.1 Impact analysis [op.cont.1].

| dimensions | A | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | N.A. | applies | applies |

**Requirements.**

– [op.cont.1.1] An impact analysis shall be carried out to determine the availability requirements for each service (impact of an interruption over a given period of time), as well as the elements that are critical to the provision of each service.

**Implementation of the measure (by availability).**

– Low level: N.A
– Medium level: op.cont.1.
– High level: op.cont.1.

### 4.6.2 Continuity plan [op.cont.2].

| dimensions | A | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | N.A. | N.A. | applies |

**Requirements.**

A continuity plan shall be developed setting out the actions to be carried out in the event of interruption of the services provided by the usual means. The plan shall cover the following aspects:

– [op.cont.2.1] Functions, responsibilities and activities to be performed shall be identified.
– [op.cont.2.2] There shall be a provision to coordinate the entry into service of alternative means in such a way as to ensure that the essential services of the organization can continue to be provided.
– [op.cont.2.3] All alternative means shall be planned and materialized in agreements or contracts with the relevant suppliers.
– [op.cont.2.4] Persons affected by the plan shall receive specific training regarding their role in the plan.
– [op.cont.2.5] The continuity plan shall be an integral and harmonious part of the organization's continuity plans in other non-security matters.

**Reinforcement R1-Emergency and contingency plan.**

– [op.cont.2.r1.1] Where the need for continuity of systems is identified, there shall be an appropriate contingency and emergency plan. Depending on the impact analysis, the aspects to be covered shall be determined.

**Reinforcement R2-Integrity check.**

– [op.cont.2.r2.1] In the event of a system failure or discontinuity, the integrity of the operating system, firmware and configuration files shall be checked.

**Implementation of the measure (by availability).**

– LOW level: N.A.
– MEDIUM level: N.A.
– HIGH level: op.cont.2.

### 4.6.3 Periodic tests [op.cont.3].

| dimensions | A | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | N.A. | N.A. | applies |

**Requirements.**

– [op.cont.3.1] Periodic tests shall be carried out to identify and, where appropriate, correct any errors or deficiencies that may exist in the continuity plan.

**Implementation of the measure (by availability).**

– LOW level: N.A.
– MEDIUM level: N.A.
– HIGH level: op.cont.3.

#### 4.6.4 Alternative means [op.cont.4].

| dimensions | A | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | N.A. | N.A. | applies |

**Requirements.**

– [op.cont.4.1] Provision shall be made for the availability of alternative means to be able to continue providing service when the usual means are not available. In particular, the following elements of the system shall be covered:

a) Services contracted to third parties.
b) Alternative facilities.
c) Alternative staff.
d) Alternative computer equipment.
e) Alternative media.

– [op.cont.4.2] A maximum time shall be set for alternative means to become operational.

– [op.cont.4.3] Alternative means shall be subject to the same security guarantees as the originals.

**Reinforcement R1-Automation of transition to alternative media.**

– [op.cont.4.r1.1] The system shall have hardware or software elements that allow the services to be automatically transferred to alternative media.

**Implementation of the measure (by availability).**

– LOW level: N.A
– MEDIUM level: N.A.
– HIGH level: op.cont.4.

### 4.7 System monitoring [op.mon].

The system shall be subject to measures to monitor its activity and shall execute pre-determined actions depending on the security compromise situations identified in the risk analysis. This may include generating real-time alarms, ending the process that is causing the alarm, disabling certain services, disconnecting users and blocking accounts.

#### 4.7.1 Intrusion detection [op.mon.1].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | + R1 | +R1+R2 |

**Requirements.**

— [op.mon.1.1] Intrusion detection or prevention tools shall be available.

**Reinforcement R1-Detection based on rules.**

— [op.mon.1.r1.1] The system shall have rules-based intrusion detection or prevention tools.

**Reinforcement R2- Response Procedures.**

— [op.mon.1.r2.1] There shall be procedures for responding to alerts generated by the

intrusion detection or prevention system.

**Reinforcement R3-Default Actions.**

— [op.mon.1.r3.1] The system shall automatically execute default actions to respond to generated alerts. This may include ending the process that is causing the alert, disabling certain services, disconnecting users, and blocking accounts.

**Implementation of the measure.**

— BASIC category: op.mon.1.
— MEDIUM category: op.mon.1 + R1.
— HIGH category: op.mon.1+ R1 + R2.

### 4.7.2 Metrics system [op.mon.2].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | + R1+R2 | + R1+R2 |

**Requirements.**

– [op.mon.2.1] In accordance with the security category of the system, the necessary data shall be collected to determine the degree of implementation of the applicable security measures and, where appropriate, to provide the annual report required by Article 32.

**Reinforcement R1-Effectiveness of the incident management system.**

– [op.mon.2.r1.1] Accurate data to assess the behavior of the incident management system shall be collected in accordance with the Technical Security Instruction for Security Incident Notification and the corresponding CCN-STIC Guide.

**Reinforcement R2-Efficiency of the security management system.**

– [op.mon.2.r2.1] The data required to know the efficiency of the security system, relative to the resources consumed, shall be collected in terms of hours and budget.

**Implementation of the measure.**

– BASIC Category: op.mon.2.
– MEDIUM Category: op.mon.2 + R1+ R2.
– HIGH Category: op.mon.2 + R1 + R2.

### 4.7.3 Monitoring [op.mon.3].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | + R1+R2 | + R1+R2+R3+R4+R5+R6 |

**Requirements.**

– [op.mon.3.1] An automatic security event collection system shall be available.

**Reinforcement R1-Correlation of events.**

– [op.mon.3.r1.1] An automatic security event collection system shall be available to allow the correlation of security events.

**Reinforcement R2-Dynamic analysis.**

— [op.mon.3.r2.1] Monitoring solutions shall be available to determine the exposure area in relation to vulnerabilities and configuration deficiencies.

**Reinforcement R3 -Advanced Cyber Threats.**

— [op.mon.3.r3.1] Systems for detection of advanced threats and abnormal behavior shall be available.
— [op.mon.3.r3.2] *Advanced Persistent Threat (APT*) detection systems shall be available by detecting significant anomalies in network traffic.

**Reinforcement R4-Digital Observatories.**

— [op.mon.3.r4.1] Digital observatories shall be available for cyber-monitoring purposes dedicated to detecting and tracking anomalies that could represent threat indicators in digital content.

**Reinforcement R5 -Data Mining.**

Measures shall be implemented to prevent, detect and react to data mining attempts:

— [op.mon.3.r5.1] Limitation of queries, monitoring volume and frequency.
— [op.mon.3.r5.2] Alerts security administrators of suspicious behaviors in real time.

**Reinforcement R6-Security Inspections.**

Periodically, or following incidents that have revealed new or underestimated system vulnerabilities, the following inspections shall be carried out:

— [op.mon.3.r6.1] Configuration check.
— [op.mon.3.r6.2] Vulnerability analysis.
— [op.mon.3.r6.3] Penetration tests.

**Reinforcement R7-Interconnections.**

— [op.mon.3.r7.1] For interconnections that require it, controls shall apply to information exchange flows through the use of metadata.

**Implementation of the measure.**

— BASIC category: op.mon.3.
— MEDIUM category: op.mon.3 + R1 + R2.
— HIGH category: op.mon.3 + R1 + R2 + R3 + R4 + R5 + R6.

## *5. Protective measures [mp]*

Protective measures shall be aimed at protecting specific assets, according to their nature, with the level required in each security dimension.

### 5.1 Protection of facilities and infrastructure [mp.if].

#### 5.1.1 Separate areas with access control [mp.if.1].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

— [mp.if.1.1] The equipment of the Data Processing Centre (DPC) shall be installed, as far as possible, in separate areas, specific to its function.

– [mp.if.1.2] Access to the indicated areas shall be controlled so that it can only be accessed by the intended entries.

**Implementation of the measure.**

– BASIC Category: mp.if.1.
– MEDIUM Category: mp.if.1.
– HIGH Category: mp.if.1.

### 5.1.2 Identification of persons [mp.if.2].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

[mp.if.2.1] The access control procedure shall identify persons accessing premises where essential equipment is part of the DPC information system, recording the corresponding inputs and exits.

**Implementation of the measure.**

– BASIC Category: mp.if.2.
– MEDIUM Category: mp.if.2.
– HIGH Category: mp.if.2.

### 5.1.3 Fitting-out of premises [mp.if.3].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

The premises where the information systems and their essential components are located shall be equipped with appropriate elements for the efficient operation of the equipment installed there, and in particular to ensure:

– [mp.if.3.1] Temperature and humidity conditions.
– [mp.if.3.2] Protection from threats identified in the risk analysis.
– [mp.if.3.3] Protection of wiring against accidental or deliberate incidents.

**Implementation of the measure.**

– BASIC Category: mp.if.3.
– MEDIUM Category: mp.if.3.
– HIGH Category: mp.if.3.

### 5.1.4 Electrical energy [mp.if.4].

| dimensions | A | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | applies | + R1 | + R1 |

**Requirements.**

– [mp.if.4.1] The premises where the information systems and their essential components are located shall have electrical power outlets in such a way as to ensure the supply and proper operation of emergency lights.

**Reinforcement R1 Emergency Electrical Supply.**

– [mp.if.4.r1.1] In the event of a failure of the main supply, the power supply shall be guaranteed for sufficient time for an orderly completion of the processes and the safeguarding of the information.

**Implementation of the measure (by availability).**

– LOW level: mp.if.4.
– MEDIUM level: mp.if.4 + R1.
– HIGH level: mp.if.4 + R1.

**5.1.5 Fire protection [mp.if.5].**

| dimensions | A | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

– [mp.if.5.1] The premises where the information systems and their essential components are located shall be protected against fires in accordance with at least the applicable industrial regulations.

**Implementation of the measure (by availability).**

– LOW level: mp.if.5.
– MEDIUM level: mp.if.5.
– HIGH level: mp.if.5.

**5.1.6 Flood protection [mp.if.6].**

| dimensions | A | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | N.A. | applies | applies |

**Requirements.**

– [mp.if.6.1] Facilities where information systems and their essential components are located shall be protected against water incidents.

**Implementation of the measure (by availability).**

– LOW level: N.A.
– MEDIUM level: mp.if.6.
– HiIGH level: mp.if.6.

### 5.1.7 Recording of entries and exits of equipment [mp.if.7].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

– [mp.if.7.1] A detailed record of any entry and exit of essential equipment, including identification of the person authorizing the movement, shall be kept.

**Implementation of the measure.**

– BASIC Category: mp.if.7.
– MEDIUM Category: mp.if.7.
– HIGH Category: mp.if.7.

### 5.2 Staff management [mp.per].

### 5.2.1 Job characterization [mp.per.1].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | N.A. | applies | applies |

**Requirements.**

— [mp.per.1.1] For each job, directly related to the handling of information or services, security responsibilities shall be defined and shall be based on risk analysis.

— [mp.per.1.2] The requirements to be met by persons to be employed shall be defined, in particular in terms of confidentiality. Those requirements shall be taken into account in the selection of the person to fill the post, including the verification of its employment history, training and other references, in accordance with the legal system and respect for fundamental rights.

**Reinforcement R1-Personal Security Enabling.**

— [mp.per.1.r1.1] Security/system administrators shall have a Personal Security Clearance (PSC) granted by the competent authority as a consequence of the results of the previous risk analysis or as a security requirement of a specific system.

**Implementation of the measure.**

– BASIC Category: N.A.
– MEDIUM Category: mp.per.1.
– HIGH Category: mp.per.1.

### 5.2.2 Duties and obligations [mp.per.2].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | + R1 | + R1 |

**Requirements.**

Each person working in the system shall be informed of the duties and responsibilities of its job in security matters, including:

– [mp.per.2.1] Disciplinary measures.

– [mp.per.2.2] Considering both the period during which the post is held, and the obligations in the event of termination of the assignment, or transfer to another post.

– [mp.per.2.3] The duty of confidentiality in respect of the data to which it has access, both during the period assigned to the post, and after its termination.

– [mp.per.2.4] In the case of personnel hired through a third party:

- [mp.per.2.4.1] The duties and obligations of each party and of the contracted personnel shall be established.
- [mp.per.2.4.2] The procedure for resolving incidents related to non-compliance with obligations shall be established.

**Reinforcement R1-Express confirmation.**

– [mp.per.2.r1.1] Express confirmation shall be obtained that users are aware of the necessary and mandatory security instructions and their acceptance, as well as the procedures necessary to carry them out properly.

**Implementation of the measure.**

– BASIC Category: mp.per.2.
– MEDIUM Category: mp.per.2 + R1.
– HIGH Category: mp.per.2 + R1.

**5.2.3 Awareness [mp.per.3].**

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

The necessary actions shall be taken to regularly raise the awareness of personnel about their role and responsibility so that the security of the system reaches the required standards. In particular, it shall be recalled periodically:

– [mp.per.3.1] Security regulations relating to the proper use of the most common equipment or systems and social engineering techniques.

– [mp.per.3.2] Identification of suspicious incidents, activities, or behaviors that must be reported for treatment by specialized personnel.

– [mp.per.3.3] The procedure for reporting security incidents, whether real or false alarms.

**Implementation of the measure.**

– BASIC Category: mp.per.3.
– MEDIUM Category: mp.per.3.
– HIGH Category: mp.per.3.

**5.2.4 Training [mp.per.4].**

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

— [mp.per.4.1] Staff shall be regularly trained in matters relating to information security which require the performance of their duties, in particular as regards:

a) Configuration of systems.
b) Detection and response to incidents.
c) Information management in any medium in which it may be located. At least the following activities shall be covered: storage, transfer, copying, distribution and destruction.

In addition, the effectiveness of the training actions carried out shall be assessed.

**Implementation of the measure.**

– BASIC Category: mp.per.4.
– MEDIUM Category: mp.per.4.
– HIGH Category: mp.per.4.

### 5.3 Protection of equipment [mp.eq].

#### 5.3.1 Clear desk [mp.eq.1].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | + R1 | + R1 |

**Requirements.**

— [mp.eq.1.1] Workplaces shall remain clear, without any material other than that required at all times.

**Reinforcement R1-Storage material.**

– [mp.eq.1.r1.1] Once used, and whenever feasible, the material shall be stored in a closed place.

**Implementation of the measure.**

– BASIC Category: mp.eq.1.
– MEDIUM Category: mp.eq.1 + R1.
– HIGH Category: mp.eq.1 + R1.

#### 5.3.2 User session lockout [mp.eq.2].

| dimensions | Auth | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | N.A. | applies | + R1 |

**Requirements.**

– [mp.eq.2.1] The user session will be lock after a reasonable period of inactivity, requiring a new user authentication to resume the ongoing activity.

Reinforcement R1-Closing of sessions.

– [mp.eq.2.r1.1] After a certain period of time, more than the previous one, the sessions opened from that workstation will be cancelled.

A CCN-STIC Guide will specify the implementation of the security configuration adapted to the categorization of the system or associated compliance profile.

**Application of the measure (by authenticity).**

– Low level: N.A
– Medium level: mp.eq.2.
– High level: mp.eq.2 + R1.

### 5.3.3 Protection of portable devices [mp.eq.3].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | +R1+R2 |

**Requirements.**

Equipment (portable computers, tablets, etc.) which are likely to leave the organization's premises and cannot benefit from the corresponding physical protection, with a manifest risk of loss or theft, shall be adequately protected.

Without prejudice to general measures affecting them, the following shall be adopted:

– [mp.eq.3.1] A portable device inventory shall be kept together with an identification of the person responsible for each device and a regular check that it is positively under its control.

– [mp.eq.3.2] A security operational procedure shall be established to inform the loss or subtraction incident management service.

– [mp.eq.3.3] When a portable device connects remotely over networks that are not under the strict control of the organization, the scope of operation of the server shall limit accessible information and services to the minimum required, requiring prior authorization from those responsible for the information and services concerned. This point applies to connections over the internet and other networks that are not trusted.

– [mp.eq.3.4] The portable device shall be prevented, as far as possible, from containing remote access keys to the organization that are not essential. Remote access keys are those that are capable of enabling access to other equipment of the organization or others of a similar nature.

**Reinforcement R1– Encryption of the disc.**

– [mp.eq.3.r1.1] The portable device shall be protected by encryption of the hard drive when the confidentiality level of the information stored on it is MEDIUM level.

**Reinforcement R2– Protected environments.**

– [mp.eq.3.r2.1] The use of portable devices outside the organization's facilities shall be restricted to protected environments, where access is controlled and safe from theft and prying eyes.

**Implementation of the measure.**

– BASIC Category: mp.eq.3.
– MEDIUM Category: mp.eq.3.
– HIGH Category: mp.eq.3 + R1 + R2.

### 5.3.4 Other devices connected to the network [mp.eq.4].

| dimensions | C | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |

| | | | |
|---|---|---|---|
| | applies | + R1 | + R1 |

This measure affects all types of devices connected to the network that may at some point have access to information, such as:

a) Multifunctional devices: printers, scanners, etc.
b) Multimedia devices: projectors, smart speakers, etc.
c) Internet of Things (*IoT*) devices.
d) Guest devices and employees' own personal devices, *Bring Your Own Device* (BYOD).
e) Others.

**Requirements.**

– [mp.eq.4.1] Devices present in the system shall have an appropriate security configuration to ensure the control of the defined flow of information input and output.
– [mp.eq.4.2] Devices present on the network that have some type of temporary or permanent storage of information shall provide the functionality necessary to remove information from information media. (See [mp.si.5]).

**Reinforcement R1-Certified products.**

– [mp.eq.4.r1.1] Products or services that comply with [op.pl.5] shall be used where possible.

**Reinforcement R2-Control of devices connected to the network.**

– [mp.eq.4.r2.1] Solutions will be available to visualize devices present on the network, control their connection/disconnection to the network and verify their security settings.

**Application of the measure (by confidentiality).**

– LOW level: mp.eq.4.
– MEDIUM level: mp.eq.4 + R1.
– HIGH level: mp.eq.4+ R1.

## 5.4 Protection of communications [mp.com].

### 5.4.1 Secure perimeter [mp.com.1].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

– [mp.com.1.1] A perimeter protection system shall be available to separate the internal network from the outside. All traffic must pass through that system.
– [mp.com.1.2] All information flows across the perimeter must be authorized in advance.

The Technical Security Instruction for the Interconnection of Information Systems shall determine the perimeter requirements to be met by all components of the system depending on the category.

**Implementation of the measure.**

– BASIC Category: mp.com.1.
– MEDIUM Category: mp.com.1.

– HIGH Category: mp.com.1.

### 5.4.2 Protection of confidentiality [mp.com.2].

| dimensions | C | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | applies | + R1 | +R1+R2+R3 |

**Requirements.**

— [mp.com.2.1] Encrypted virtual private networks shall be used when communication takes place over networks outside the security domain itself.

**Reinforcement R1-Algorithms and authorized parameters.**

— [mp.com.2.r1.1] Algorithms and parameters authorized by the CCN shall be used.

**Reinforcement R2-Hardware devices.**

— [mp.com.2.r2.1] Hardware devices shall be used in the establishment and use of the virtual private network.

**Reinforcement R3 -Certified Products.**

— [mp.com.2.r3.1] Products or services complying with [op.pl.5] shall be used.

**Reinforcement R4-Encryptors.**

— [mp.com.2.r4.1] Encryptors that meet the requirements set out in the applicable CCN-STIC guide shall be used.

**Reinforcement R5-Encrypt of particularly sensitive information.**

— [mp.com.2.r5.1] All transmitted information shall be encrypted.

**Application of the measure (by confidentiality).**

— LOW level: mp.com.2.
— MEDIUM level: mp.com.2 + R1.
— HIGH level: mp.com.2 + R1 + R2+ R3.

### 5.4.3 Protection of integrity and authenticity [mp.com.3].

| dimensions | I Auth | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | applies | + R1 + R2 | + R1 + R2 + R3 + R4 |

**Requirements.**

— [mp.com.3.1] In communications with points outside the own security domain, the authenticity of the other end of the communication channel shall be ensured before exchanging information. (See [op.acc.5]).
— [mp.com.3.2] Active attacks shall be prevented by ensuring that the envisaged procedures for handling the incident shall be activated upon detection. Active attacks shall be considered as:

a) The alteration of information in transit.
b) The injection of spurious information.
c) The kidnapping of the session by a third party.

— [mp.com.3.3] Any identification and authentication mechanism provided for in the

legal system and in the implementing legislation shall be accepted.

**Reinforcement R1-Virtual private network.**

— [mp.com.3.r1.1] Encrypted virtual private networks shall be used when communication takes place over networks outside the security domain itself.

**Reinforcement R2-Algorithms and authorized parameters.**

— [mp.com.3.r2.1] Algorithms and parameters authorized by the CCN shall be used.

**Reinforcement R3-Hardware devices.**

— [mp.com.3.r3.1] It is recommended to use hardware devices in the establishment and use of the virtual private network.

**Reinforcement R4-Certified products.**

— [mp.com.3.r4.1] Certified products shall be used in accordance with [op.pl.5].

**Reinforcement R5-Encryptors.**

— [mp.com.3.r5.1] Encryptors that meet the requirements set out in the applicable CCN-STIC guide shall be used.

**Application of the measure (by integrity and authenticity).**

— LOW level: mp.com.3.
— MEDIUM level: mp.com.3 + R1 + R2.
— HIGH level: mp.com.3 + R1 + R2 + R3 + R4.

### 5.4.4 Separation of information flows on the network [mp.com.4].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | N.A. | +[R1oR2oR3] | +[R2oR3] +R4 |

Segmentation limits access to information and, consequently, the spread of security incidents, which are restricted to the environment in which they occur.

When the transmission of information over the network is restricted to certain segments, access to information is limited and security incidents are encapsulated in their segment.

**Requirements.**

The information flows shall be separated into segments so that:

– [mp.com.4.1] Network traffic shall be segregated so that each computer only has access to the information it needs.

– [mp.com.4.2] If wireless communications are used, it shall be in a separate segment.

**Reinforcement R1-Basic Logic Segmentation.**

– [mp.com.4.r1.1] Network segments shall be implemented through virtual local area networks *(VLANs)*.

– [mp.com.4.r1.2] The network forming the system shall be segregated into different subnets with at least:

- Users.
- Services.
- Administration.

**Reinforcement R2-Advanced Logic Segmentation.**

– [mp.com.4.r2.1] Network segments will be implemented via virtual private networks (Virtual Private Network, VPN).

**Reinforcement R3-Physical segmentation.**

– [mp.com.4.r3.1] Network segments shall be implemented with separate physical means.

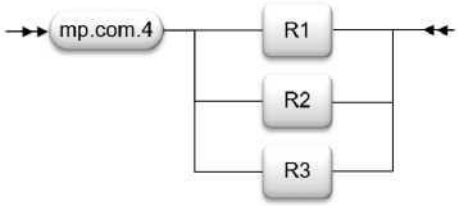
**Reinforcement R4-Interconnection points.**

— [mp.com.4.r4.1] Input control of users who reach each segment and control the input and output of the information available in each segment.
— [mp.com.4.r4.2] The interconnection point shall be particularly secured, maintained and monitored (as in [mp.com.1]).

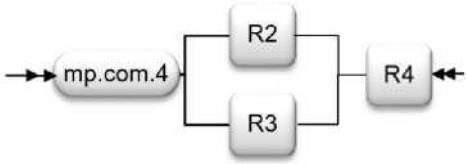
**Implementation of the measure.**

— BASIC category: N.A.

— MEDIUM category: mp.com.4+ [R1° R2 or R3].




— HIGH category: mp.com.4+ [R2 or R3] + R4.




### 5.5 Protection of information media [mp.si].

#### 5.5.1 Marking [mp.si.1].

| dimensions | C | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | N.A. | applies | applies |

**Requirements.**

— [mp.si.1.1] Information media (printed paper, electronic documents, multimedia content — videos, courses, presentations, etc.) containing information that according to [mp.info.2] must be protected by specific security measures, shall bear the corresponding markings or metadata indicating the level of security of the information contained with the highest rating.

**Reinforcement R1-Digital Watermark.**

— [mp.si.1.r1.1] The security policy of the organization shall define watermarks to

ensure proper use of the information being handled.

— [mp.si.1.r1.2] Digital information media (electronic documents, multimedia, etc.) may include a watermark according to the security policy.

– [mp.si.1.r1.3] Computers or devices through which applications, remote or virtual desktops, data, etc. are accessed shall display an on-screen watermark according to the security policy.

**Application of the measure (by confidentiality).**

– Low level: N.A.
– Medium level: mp.si.1.
– High level: mp.si.1.

### 5.5.2 Cryptography [mp.si.2].

| dimensions | C I | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | N.A. | applies | + R1 + R2 |

This measure applies in particular to all removable devices when they leave a controlled area. Removable devices shall be understood to mean CDs, DVDs, removable disks, pen *drives*, USB sticks or other similar devices.

**Requirements.**

– [mp.si.2.1] Cryptographic mechanisms shall be used to ensure the confidentiality and integrity of the information contained.
– [mp.si.2.2] Algorithms and parameters authorized by the CCN shall be used.

**Reinforcement R1– Certified products.**

– [mp.si.2.r1.1] Certified products shall be used in accordance with [op.pl.5].

**Reinforcement R2-Security backups.**

– [mp.si.2.r2.1] Security backups shall be encrypted using algorithms and parameters authorized by the CCN.

**Application of the measure (by confidentiality and integrity).**

– LOW level: N.A.
– MEDIUM level: mp.si.2.
– HIGH level: mp.si.2 + R1 + R2.

### 5.5.3 Custody [mp.si.3].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

– [mp.si.3.1] Due diligence and control shall apply to information media that remain under the responsibility of the organization, ensuring access control with physical measures ([mp.if.1] and [mp.if.7]) or logic ([mp.si.2]).
– [mp.si.3.2] Maintenance requirements of the manufacturer shall be respected, in particular with regard to temperature, humidity and other environmental agents.

**Implementation of the measure.**

– BASIC Category: mp.si.3.
– MEDIUM Category: mp.si.3.
– HIGH Category: mp.si.3.

**5.5.4 Transport [mp.si.4].**

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

The system manager shall ensure that the devices remain under control and meet their security requirements while being moved from one location to another, outside the organization's controlled areas.

**Requirements.**

– [mp.si.4.1] An entry/exit record shall be available identifying the carrier who delivers/receives the support.
– [mp.si.4.2] A routine procedure shall be available to cross-check departures with arrivals and raise relevant alarms when an incident is detected.
– [mp.si.4.3] The cryptographic means of protection ([mp.si.2]) corresponding to the highest level of security of the information contained shall be used.
— [mp.si.4.4] Keys shall be managed according to [op.exp.10].

**Implementation of the measure.**

– BASIC Category: mp.si.4.
– MEDIUM Category: mp.si.4.
– HIGH Category: mp.si.4.

**5.5.5 Erasure and destruction [mp.si.5].**

| dimensions | C | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | applies | + R1 | + R1 |

The measure of erasure and destruction of information media shall apply to all types of equipment and media capable of storing information, including electronic and non-electronic means.

**Requirements.**

– [mp.si.5.1] Media intended to be re-used for other information or released to another organization shall be subject to the secure deletion of its content that does not permit its retrieval. Where the nature of the medium does not allow for secure deletion, the support may not be reused in any other system.

The CCN-STIC guides will specify the criteria for defining a deletion or destruction mechanism as safe, depending on the sensitivity of the information stored on the device.

**Reinforcement R1-Certified products.**

– [mp.si.5.r1.1] Products or services that comply with [op.pl.5] shall be used.

**Reinforcement R2 — Destruction of supports.**

– [mp.si.5.r2.1] Upon completion of the information support lifecycle, it shall be safely

destroyed in accordance with the criteria established by the CCN.

**Application of the measure (by confidentiality).**

– LOW level: mp.si.5.
– MEDIUM level: mp.si.5 + R1.
– HIGH level: mp.si.5 + R1.

### 5.6 Protection of IT applications [mp.sw].

#### 5.6.1 IT Applications development [mp.sw.1].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | N.A. | +R1+R2+R3+R4 | +R1+R2+R3+R4 |

**Requirements.**

– [mp.sw.1.1] Application development shall be carried out on a different and separate system from the production system, with no development tools or data in the production environment, nor production data in the development environment.

**Reinforcement R1-Minimum privilege.**

– [mp.sw.1.r1.1] Applications shall be developed in accordance with the principle of minimum privilege, accessing only the resources essential to their function, and with the privileges that are indispensable.

**Reinforcement R2- Safe Development Methodology.**

– [mp.sw.1.r2.1] A recognized safe development methodology shall be applied which:

a) It shall take into account security aspects throughout the life cycle.
b) It shall include secure programming rules, in particular: control of allocation and release of memory, memory overflow.
c) It shall specifically process data used in testing.
d) It shall allow the inspection of the source code.

**Reinforcement R3-Security from the design.**

— [mp.sw.1.r3.1] The following elements shall be an integral part of the system design:

a) Identification and authentication mechanisms.
b) Mechanisms for the protection of processed information.
c) The generation and treatment of audit trails.

**Reinforcement R4-Test data.**

— [mp.sw.1.r4.1] Preferably, tests prior to the deployment or modification of information systems shall not be carried out with actual data. Where it is necessary to use actual data, the corresponding level of security shall be ensured.

**Reinforcement R5-List of software components.**

— [mp.sw.1.r5.1] The developer shall develop and keep update a formal list of the third party software components used in the application or product. A history of the components used in the different versions of the software shall be maintained. The minimum content of the list of components, which shall contain at least the identification of the component, the manufacturer and the version used, shall be specified in a CCN-STIC

guide.

**Implementation of the measure.**

— BASIC category: N.A.
— MEDIUM category: mp.sw.1 + R1 + R2 + R3 + R4.
— HIGH category: mp.sw.1 + R1 + R2 + R3 + R4.

**5.6.2 Acceptance and commissioning [mp.sw.2].**

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | + R1 | + R1 |

**Requirements.**

Before going into production, the correct operation of the application shall be checked.

— [mp.sw.2.1] It shall be verified that:

a) Security acceptance criteria are met.
b) The security of other components of the service is not impaired.

**Reinforcement R1- Tests.**

— [mp.sw.2.r1.1] Tests shall be carried out in an isolated environment (pre-production).

**Reinforcement R2-Inspection of source code.**

— [mp.sw.2.r2.1] A source code audit shall be performed.

**Implementation of the measure.**

– BASIC Category: mp.sw.2.
– MEDIUM Category: mp.sw.2 + R1.
– HIGH Category: mp.sw.2 + R1.

**5.7 Protection of information [mp.info].**

**5.7.1 Personal data [mp.info.1].**

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

— [mp.info.1.1] When the system processes personal data, the security officer shall collect data protection requirements that are set by the controller or by the processor, with the advice of the DPO, and which are necessary to implement in the systems according to the nature, scope, context and purposes of the data protection, as well as the risks to the rights and freedoms in accordance with Articles 24 and 32 of the GDPR, and according to the data protection impact assessment, if carried out.

**Implementation of the measure.**

— BASIC category: mp.info.1.
— MEDIUM category: mp.info.1.

— HIGH category: mp.info.1.

### 5.7.2 Rating of information [mp.info.2].

| dimensions | C | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | N.A. | applies | applies |

**Requirements.**

– [mp.info.2.1].. In order to classify the information, the legal provisions of the laws and international treaties of which Spain is a member and their applicable regulations shall apply in the case of classified information. The value to be used in the case of non-classified information would be OFFICIAL USE for information with some type of restriction in its handling due to its sensitivity and confidentiality.

– [mp.info.2.2] The security policy shall establish who is responsible for each information handled by the system.

– [mp.info.2.3] The security policy shall set out, directly or indirectly, the criteria which, in each organization, shall determine the level of security required, within the framework set out in Article 40 and the general criteria set out in Annex I.

– [mp.info.2.4] The person responsible for each information shall follow the criteria set out in the previous section to assign to each information the level of security required and shall be responsible for its documentation and formal approval.

– [mp.info.2.5] The person responsible for each information at all times shall have the exclusive power to modify the level of security required, in accordance with the previous sections.

**Application of the measure (by confidentiality).**

– Low level: N.A.
– Medium level: mp.info.2.
– HIGH level: mp.info.2.

### 5.7.3 Electronic signature [mp.info.3].

| dimensions | I Auth | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | applies | +R1+R2+R3 | + R1+R2+R3+R4 |

**Requirements.**

– [mp.info.3.1] Any type of electronic signature provided for in the current legal system shall be used, including the secure verification code systems linked to the Public Administration, public body, body or public law entity, under the terms and conditions established in Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations and Law 40/2015 of 1 October 2015.

**Reinforcement R1-Qualified certificates.**

– [mp.info.3.r1.1] When advanced electronic signature systems based on certificates are used, certificates shall be qualified.

**Reinforcement R2-Algorithms and authorized parameters.**

– [mp.info.3.r2.1] Algorithms and parameters authorized by the CCN or by a national or European scheme that is applicable shall be used.

The CCN shall determine the cryptographic algorithms that have been nominally

authorized for use in the National Security Framework in accordance with the Technical Security Instruction on Cryptology of use in the ENS.

**Reinforcement R3-Verification and validation of signature.**

– [mp.info.3.r3.1] Where appropriate, verification and validation of the electronic signature shall be guaranteed for the time required by the administrative activity that it supports, without prejudice to the possibility of extending this period in accordance with the provision of the applicable Electronic Signature and Certificate Policy. For this purpose, all relevant information for its verification and validation, including certificates or verification and validation data, shall be attached to the signature or referenced.

**Reinforcement R4-Advanced electronic signature based on qualified certificates.**

– [mp.info.3.r4.1] Advanced electronic signature based on qualified certificates shall be used complemented by a second factor of the type “something known” or “something that is”.

**Reinforcement R5-Qualified electronic signature.**

– [mp.info.3.r5.1] Qualified electronic signature shall be used, using certified products as set out in [op.pl.5].

**Application of the measure (by integrity and authenticity).**

– LOW level: mp.info.3.
– MEDIUM level: mp.info.3 + R1 + R2 + R3.
– HIGH level: mp.info.3 + R1 + R2 + R3 + R4.

**5.7.4 Time stamps [mp.info.4].**

| dimensions | Acc | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | N.A. | N.A. | applies |

**Requirements.**

The use of time stamps shall require the following cautions:

– [mp.info.4.1] Time stamps shall apply to information that may be used as electronic evidence in the future.
– [mp.info.4.2] Data relevant to the subsequent verification of the date shall be treated with the same security as the information dated for the purposes of availability, integrity and confidentiality.
– [mp.info.4.3] Time stamps shall be renewed regularly until the protected information is no longer required by the administrative process to which it supports, where applicable.
– [mp.info.4.4] “Qualified electronic time stamps” shall be used in accordance with Regulation (EU) No 910/2014 and implementing legislation.

**Reinforcement R1-Certified products.**

– [mp.info.4.r1.1.] Certified products according to [op.pl.5] shall be used.
– [mp.info.4.r1.2] A date and time shall be assigned to an electronic document, as set out in the CCN-STIC Cryptology Guide of use in the ENS.

**Application of the measure (by accountability).**

– LOW level: N.A

– MEDIUM level: N.A.
– HIGH level: mp.info.4.

**5.7.5 Clean-up of documents [mp.info.5].**

| dimensions | C | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

– [mp.info.5.1] In the document clean-up process, any additional information contained in hidden fields, metadata, comments or previous revisions shall be removed from the document, except where such information is relevant to the recipient of the document.

This measure is particularly relevant when the document is widely disseminated, as is the case when it is offered to the public on a web server or other type of information repository.

**Application of the measure (by confidentiality).**

– LOW level: mp.info.5.
– MEDIUM level: mp.info.5.
– HIGH level: mp.info.5.

**5.7.6 Backups [mp.info.6].**

| dimensions | A | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | applies | + R1 | + R1 + R2 |

**Requirements.**

– [mp.info.6.1] Backups shall be made to recover of accidentally or intentionally lost data. The periodicity and retention periods of these backups shall be determined in the organization's internal rules on backups.
– [mp.info.6.2] The backup procedures established shall indicate:

a) Frequency of copies.
b) On-site storage requirements.
c) Storage requirements elsewhere.
d) Controls for authorized access to backup copies.

**Reinforcement R1-Recovery tests.**

– [mp.info.6.r1.1] Backup and restoration procedures should be tested regularly. Their frequency will depend on the criticality of the data and the impact of the lack of availability.

**Reinforcement R2-Protection of backups.**

– [mp.info.6.r2.1] At least one of the backups shall be stored separately in a different place, so that an incident cannot affect both the original repository and the copy simultaneously.

**Application of the measure (by availability).**

– LOW level: mp.info.6.
– MEDIUM level: mp.info.6+ R1.
– HIGH level: mp.info.6+ R1 + R2.

### 5.8 Protection of services [mp.s].

#### 5.8.1 E-mail protection [mp.s.1].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | applies | applies | applies |

**Requirements.**

The e-mail shall be protected against threats that are specific to it, acting as follows:

– [mp.s.1.1] Information distributed by e-mail shall be protected, both in the body of the messages and in the annexes.
– [mp.s.1.2] Message routing and connecting information shall be protected.

The organization shall be protected against problems that materialize by e-mail, in particular:

– [mp.s.1.3] Unsolicited mail, in the words “spam”.
– [mp.s.1.4] Harmful code consisting of viruses, worms, Trojans, spies, or others of a similar nature.
– [mp.s.1.5] Micro-application mobile code, in the English expression “applet”.

Rules for the use of e-mail shall be established for staff. (See [org.2]). These rules of use shall contain:

– [mp.s.1.6] Limitations to the use of private communications.
– [mp.s.1.7] Awareness and training activities related to the use of e-mail.

**Implementation of the measure.**

– BASIC Category: mp.s.1.
– MEDIUM Category: mp.s.1.
– HIGH Category: mp.s.1.

#### 5.8.2 Protection of web services and applications [mp.s.2].

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |
| | +[R1oR2] | +[R1oR2] | +R2+R3 |

**Requirements.**

Systems providing web services shall be protected against the following threats:

– [mp.s.2.1] Where the information requires access control, it shall be ensured that the information cannot be accessed without authentication, in particular by taking action on the following aspects:

a) The server shall be prevented from providing access to documents by alternative means to the given protocol.

b) Uniform Resource locator (URL) manipulation attacks shall be prevented.

c) Attacks of manipulation of fragments of information that are stored on the hard drive of the visitor of a website through its browser, at the request of the page server, known in English as cookies, shall be prevented.

d) Code injection attacks shall be prevented.

– [mp.s.2.2] Privilege escalation attempts shall be prevented.

– [mp.s.2.3] Cross site scripting attacks shall be prevented.

**Reinforcement R1-Security audits.**

– [mp.s.2.r1.1] Continuous “black box” security audits shall be carried out on web applications during the development phase and before the production phase.

– [mp.s.2.r1.2] The frequency of these security audits shall be defined in the audit procedure.

**Reinforcement R2-Advanced Security Audits.**

– [mp.s.2.r2.1] “White Box” security audits shall be carried out on web applications during the development phase.

– [mp.s.2.r2.2] Defined methodologies and automatic vulnerability detection tools shall be used in conducting security audits on web applications.

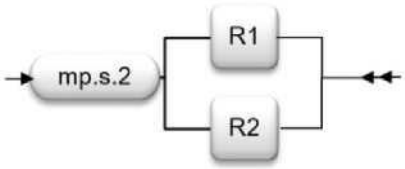
– [mp.s.2.r2.3] Once a security audit has been completed, the results shall be analyzed and the vulnerabilities found shall be resolved using the defined procedures [op.exp.5].

**Reinforcement R3-Caches protection.**

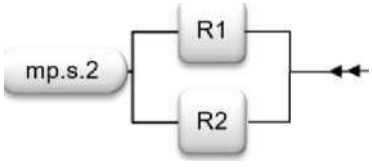
– [mp.s.2.r3.1] Manipulation attacks on programs or devices performing an action on behalf of others, known in English terminology as “*proxies*”, and special high-speed storage systems, known in English terminology as “*caches*”, shall be prevented.

**Implementation of the measure.**

— BASIC category: mp.s.2 + [R1 or R2].




— MEDIUM category: mp.s.2 + [R1 or R2].




— HIGH category: mp.s.2 + R2 + R3.

**5.8.3 Protection of web browsing [mp.s.3].**

| dimensions | All | | |
|---|---|---|---|
| category | BASIC | MEDIUM | HIGH |

| | | | |
|---|---|---|---|
| | applies | applies | + R1 |

**Requirements.**

Internal users' access to internet browsing shall be protected against the threats that are specific to it, acting as follows:

– [mp.s.3.1] Rules of use shall be established, defining the use that is authorized and limitations on personal use. In particular, the permitted use of encrypted connections shall be specified.

– [mp.s.3.2] Hygiene awareness activities in web browsing shall be carried out on a regular basis, promoting safe use and warning of misuse.

– [mp.s.3.3] System administrator(s) shall be trained in service monitoring and incident response.

– [mp.s.3.4] Web address resolution and connection information shall be protected.

– [mp.s.3.5] The organization in general and the workstation in particular shall be protected from problems occurring via web navigation.

– [mp.s.3.6] It shall protect against the action of harmful programs such as active pages, executable code downloads, etc., preventing the system from being exposed to attack vectors such as s pyware, ransomware, etc.

– [mp.s.3.7] An executive cookie control policy shall be established, in particular, to avoid contamination between personal use and organizational use.

**Reinforcement R1 — Monitoring.**

– [mp.s.3.r1.1] The use of web browsing shall be recorded, establishing the elements that are recorded, the retention period of these records and the use that the public body intends to make of them.

– [mp.s.3.r1.2] A function for rupture of encrypted channels shall be established to inspect their contents, indicating what is analyzed, what is recorded, how long records are retained and what use the public body intends to make of these inspections. This is without prejudice to the possibility of allowing unique encrypted access to trusted destinations.

– [mp.s.3.r1.3] A blacklist of closed destinations shall be established.

**Reinforcement R2-Authorized Destinations.**

– [mp.s.3.r2.1] A whitelist of accessible destinations shall be established. All access outside the destination indicated on the whitelist shall be prohibited, unless expressly authorized.

**Implementation of the measure.**

– BASIC Category: mp.s.3.
– MEDIUM Category: mp.s.3.
– HIGH Category: mp.s.3 + R1.

**5.8.4 Protection against denial of service [mp.s.4].**

| dimensions | A | | |
|---|---|---|---|
| level | LOW | MEDIUM | HIGH |
| | N.A. | applies | + R1 |

**Requirements.**

Preventive measures shall be put in place against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. For this purpose:

– [mp.s 4.1] The system shall be planned and equipped with sufficient capacity to accommodate the expected load with slackness.
– [mp.s.4.2] Technologies shall be deployed to prevent known attacks.

**Reinforcement R1-Detection and reaction.**

– [mp.s.4.r1.1] A denial of service attack detection and treatment system (DoS and DDoS) shall be established.
– [mp.s. 4.r1.2] Reaction procedures shall be established, including communication with the communications provider.

**Reinforcement R2-Own Attacks.**

– [mp.s.4.r2.1] Attacks shall be detected and avoided from own facilities, harming third parties.

**Implementation of the measure (by availability).**

– LOW level: N.A.
– MEDIUM level: mp.s.4.
– HIGH level: mp.s.4+ R1.

### *6. Assessment of the implementation of security measures*

Maturity levels are commonly used to characterize the implementation of a process. The Capability Maturity Model (CMM) describes the characteristics that make a process effective, measuring the degree or level of professionalization of the activity.

A process is a collection of related and structured activities or tasks that, in a specific sequence, provides a service for the organization.

For the assessment of the implementation of security measures, these will be analyzed as processes and their maturity level will be estimated using the Capability Maturity Model (CMM).

Five “maturity levels” are identified, so that an organization that has institutionalized all the practices included at a level and its lowers, is considered to have reached that level of maturity:

a) **L0-Not Existing.**

There is no process that supports the required service.

b) **L1 — Initial. Ad hoc.**

Organizations at this level do not have a stable environment for the provision of the required service. Although correct engineering techniques are used, efforts are undermined by lack of planning. The success of the projects is based most of the time on personal effort, although often failures and almost always delays and cost overruns occur. The result is unpredictable. Solutions are often implemented reactively to incidents.

Working procedures, where they exist, are informal, incomplete and not systematically applied.

c) **L2-Reproducible, but intuitive.**

At this level, organizations have institutionalized management practices, basic metrics and reasonable quality monitoring.

Working procedures exist, but they are not sufficiently documented or do not cover all the required aspects.

d) **L3-Defined process.**

In addition to good management, at this level, organizations have detailed and documented rules and procedures for coordination between groups, staff training,

engineering techniques, etc.

e) **L4-Managed and measurable.**

It is characterized by the fact that organizations have a set of effectiveness and efficiency metrics, which are systematically used for decision-making and risk management. The resulting service is of high quality.

f) **L5 — Optimized.**

The complete organization is focused on the continuous improvement of processes. Metrics are used intensively and the innovation process is managed.

A certain level of maturity shall be required for each security measure that applies to the information system. The minimum maturity levels required by the ENS depending on the category of the system are:

| Category of the system | Minimum level of maturity required |
|---|---|
| BASIC | L2-Reproducible, but intuitive. |
| MEDIUM | L3-Defined process. |
| HIGH | L4-Managed and measurable. |

### *7. Development and supplementation of security measures*

The security measures shall be developed and supplemented as set out in the second final provision.

### *8. Interpretation*

The interpretation of this Annex shall be carried out according to the proper meaning of your words, in relation to the context, historical and legislative background, which includes the provisions of the technical security instructions and the CCN-STIC guides that apply to the implementation and to the various application scenarios such as electronic sites, validation services of electronic certificates, electronic dating services and validation of dated documents, taking into account the spirit and purpose of those sites.

## ANNEX III

## Security audit

### *1. Subject of the audit*

1.1 The security of an organization's information systems shall be audited in the following terms in order to verify:

a) That the security policy defines the roles and functions of those responsible for the system, information, services and security of the information system.

b) That procedures exist for the resolution of disputes between those responsible.

c) That persons have been designated for such roles in the light of the principle of "differentiation of responsibilities".

d) That a risk analysis has been carried out, with annual review and approval.

e) That the protection recommendations described in Annex II on Security Measures are complied with, depending on the conditions of implementation in each case.

f) That there is an information security management system, documented and with

a regular approval process by the management, based on the Statement of Applicability regulated in Article 28 of this Royal Decree.

1.2 The audit shall be based on the existence of evidence to support objectively compliance with the following points:

a) Documentation of the procedures.
b) Incident record.
c) Examination of the staff concerned: knowledge and praxis of the measures that affect you.
d) Certified products. The use of products satisfying Article 19 “Procurement of security products and contracting of security services” shall be considered sufficient evidence.

1.3 A documented audit program or plan shall be available. Audit activities involving checks in the operating systems shall be planned and agreed in advance.

### *2. Audit levels*

The audit levels carried out to the information systems shall be as follows:

2.1 Audit of BASIC-category systems.

a) BASIC-category information systems do not require an audit. A self-assessment performed by the same staff that manages the information system or delegated by them shall be sufficient.
The result of the self-assessment must be documented, indicating whether each security measure is implemented and subject to regular review, as well as the evidence supporting the previous assessment.
b) The self-assessment reports shall be analyzed by the security officer, who shall forward the findings to the system manager for appropriate corrective action.

2.2 Audit of MEDIUM or HIGH-category systems.

a) The audit report shall state the degree of compliance with this Royal Decree and identify the findings of conformity and non-compliance. It shall also include the methodological audit criteria used, the scope and purpose of the audit, and the data, facts and observations on which the conclusions are based.
b) The audit reports shall be analyzed by the security officer, who shall submit the findings to the system manager for appropriate corrective action.

### *3. Interpretation*

The interpretation of this annex shall be carried out according to the proper meaning of its words, in relation to the context, historical and legislative background, including the provisions of the Technical Security Instruction on Auditing the Security of Information Systems and the applicable CCN-STIC guide, taking into account the spirit and purpose of those.

## ANNEX IV

## Glossary

— Assets: component or functionality of an information susceptible to deliberate or accidental attack with consequences for the organization. Includes: information, data, services, software, hardware, communications, administrative resources, physical resources and human resources.
— System/system security administrator: person responsible for the installation and maintenance of an information system, implementing the procedures and security configuration established within the framework of the organization’s security policy.

— Risk analysis: study of the foreseeable consequences of a possible security incident, considering its impact on the organization (on the protection of its assets, its mission, its image or reputation, or on its functions) and the likelihood of its occurrence.

— Controlled area: zone or area in which an organization considers the physical and procedural security measures required for the protection of the information and information systems located in it to be complied with.

— Security architecture: a set of physical and logical elements that form part of the system architecture and whose objective is the protection of assets within the system and in interconnections with other systems.

— Security audit: it is a systematic, independent and documented process aimed at obtaining objective evidence and its objective assessment in order to determine the extent to which audit criteria are met in relation to the adequacy of the security controls adopted, compliance with the security policy, rules and operating procedures established and detecting deviations from those criteria.

— Authentication: ratification of the identity of a user, process or device.

— Multifactor authentication: requiring two or more authentication factors to ratify an authentication as valid.

— Authenticator: something, physical or immaterial, that the user possesses under his exclusive control and that distinguishes him from other users.

— Authenticity: property or characteristic consisting of an entity who claims to be or guarantees the source from which the data originates.

— Biometrics (authentication factor): recognition of individuals based on their biological or behavioral characteristics.

— Supply chain: related set of resources and processes that begins with the provision of raw materials and extends through the delivery of products or services to the end user through transport modes. It includes suppliers (first, second and third level), raw material warehouses (direct or indirect), production lines, finished product warehouses and distribution channels (wholesalers and retailers), until they reach the final customer.

— Security category of a system: It is a degree, within the BASIC-MEDIUM-HIGH scale, with which an information system is qualified in order to select the necessary security measures for it. The security category of the system reflects the holistic view of the set of assets as a harmonious whole, oriented to the provision of services.

— Electronic signature certificate (authentication factor): an electronic statement linking the validation data of a signature to a natural or legal person and confirming at least that person's name or pseudonym.

— Qualified electronic signature certificate: an electronic signature certificate which has been issued by a qualified trust service provider and meets the requirements set out in Annex I to Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.

— Cyberthreat: threat to systems and services present in cyberspace or reachable through cyberspace .

— Cyberattack: any willful conduct of individuals or organizations, known or not, developed through cyberspace against information systems, with the purpose of subtracting, altering, abusing, destabilizing, rendering useless, destroying or eliminating assets.

— Cyberspace: global and dynamic domain composed of information technology infrastructures, including the internet, telecommunications networks and information systems that configure a virtual domain.

— Cyber incident: Information and communication technology security incident occurring in cyberspace.

— Cybersecurity (information systems security): the ability of networks and information systems to withstand, with a specified level of reliability, any action that compromises the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed, or related services offered by or accessible through such

networks and information systems.

— Security compromise: security incident in which, due to a breach of technical or organizational security measures, an information or a service is exposed, or potentially exposed, to unauthorized access.

— Confidentiality: property or characteristic consisting of that information is neither made available nor disclosed to unauthorized individuals, entities or processes.

— Password: a secret memorized by the user, composed of several characters according to rules of complexity versus attacks of divination or brute force.

— One-Time Password (OTP): password generated dynamically that can only be used once and for a limited period of time.

— Availability: property or characteristic of assets in that authorized entities or processes have access to them when required.

— Authentication device (*token*): physical authenticator.

— ENS Conformity Certification Stamp: electronic document, in PDF-A format, signed electronically by the Certification Entity responsible for the evaluation of the information systems concerned, including a link to the Certification of Conformity with the ENS, which, while it remain valid, will remain accessible through the electronic side or website of the public or private entity concerned.

— ENS Declaration of Conformity Stamp: electronic document, in PDF-A format, signed or stamped electronically by the entity under whose responsibility the information system in question is located, including a link to the Declaration of Conformity with the ENS, which, for the duration of its validity, will remain accessible through the electronic site or website of the public or private entity concerned.

— Security domain: collection of uniformly protected assets, typically under a single authority. Security domains are used to differentiate between zones in the information system. For example:

a) Central facilities, branches, commercials working with laptops.
b) Central server (host), Unix front and administrative teams.
c) Physical security, logical security.

— Security event: an identified occurrence of a system, service or network state indicating a possible breach of information security policy, a failure of controls or an unknown situation that may be relevant to security.

— Authentication factor: there are 3 types of authentication factors: (1) something you known, a secret; (2) Something you have, an authenticator; and (3) something you are, biometrics.

— Electronic signature: data in electronic form attached to or logically associated with other electronic data used by the signatory to sign .

— Advanced electronic signature: an electronic signature that meets the requirements referred to in Article 26 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.

— Qualified electronic signature: an advanced electronic signature which is created by a qualified electronic signature creation device and is based on a qualified electronic signature certificate.

— Incident management: procedures followed to detect, analyze, limit and respond to an incident.

— Risk management: coordinated activities to direct and control an organization with respect to risks.

— Security incident (cyber incident or incident): unexpected or unwanted event with consequences to the detriment of the security of network and information systems.

— Integrity: property or characteristic that the information asset has not been unauthorized altered.

— Software components list: document detailing the software components used to build something, whether an application or a service.

— Security measures: set of provisions to protect the information system from the risks to which it is subject, in order to ensure its security objectives. These may include prevention, deterrence, protection, detection and reaction, or recovery measures.

— Minimum privilege: principle that determines that the design of the security architecture of a system guarantees the use of the minimum services and permits necessary for its proper functioning.

— Continuous monitoring: a dynamic security management process based on tracking critical security indicators and patching vulnerabilities discovered in information system components.

— Digital Observatory: a digital observatory, in its purpose of knowing realities of the information that is transmitted through digital media, is a set of decision-making capabilities dedicated to the detection and tracking of anomalies in the origin, definition or dissemination of digital content, which could represent indicators of threat.

— Specific compliance profile: a set of security measures, whether or not included in Annex II to this Royal Decree, which, as a result of the mandatory risk analysis, are applicable to a particular entity or sector of activity and for a specific security category, and which has been authorized by the CCN.

— PIN: a user-memorized secret, composed of a few characters, following certain rules against divination attacks.

— Electronic signature policy, electronic seal and certificates: set of security, organization, technical and legal standards to determine how electronic signatures and electronic seals are generated, verified and managed, including the characteristics required for electronic signature certificates or electronic seals.

— Security policy (Information Security Policy): a set of guidelines set out in a document, governing the way in which an organization manages and protects the information it treats and the services it provides.

— Basic security principles: fundamentals that should govern any action aimed at securing information and services.

— Process: organized set of activities carried out to produce a product or provide a service, which has a delimited beginning and end, involves resources and giving rise to a result.

— Security process: method used to achieve the security objectives of the organization. The process is designed to identify, measure, manage and keep under control the security risks the system faces.

— ICT process: a set of activities carried out for the design, development, supply and maintenance of an ICT product or service.

— ICT product: element or group of elements of networks or information systems.

— Minimum security requirements: minimum requirements necessary to ensure the information processed and the services provided.

— Memorized secret (authentication factor): something that only the authorized user knows. Typically, it is specified in a password or a PIN.

— Information system: any of the following:

1º The electronic communications networks used by the entity within the scope of application of this Royal Decree in respect of which it has management capacity.

2° Any device or group of interconnected or related devices, in which one or more of them perform, by means of a program, the automatic processing of digital data.

3º Digital data stored, processed, retrieved or transmitted by means of the items referred to in points 1 and 2 above, including those necessary for the operation, use, protection and maintenance of such elements.

—TEMPEST: term referring to investigations and studies of compromising emanations (unintentional electromagnetic emissions produced by electrical and electronic equipment that, detected and analyzed, may lead to the collection of information) and to the measures applied to the protection against such emanations.

—Accountability: property or characteristic whereby the actions of an entity (person or process) can be traced unquestionably to that entity.

—Official use: designates information with some kind of restriction on its handling due to its sensitivity and confidentiality.

—Users of the organization: staff of the organization, own or contracted, stable or circumstantial, who access the system to carry out the functions or activities entrusted to them by the organization.

—External users: users with access to the system who do not enter the group of users of the organization. In particular, administered citizens.