centro criptológico nacional

Specific Compliance Profile
CCN-STIC 852

Specific Compliance Profile Paying Agencies

March 2023

MINISTERIO DE DEFENSA

General State Administration Publications Catalogue
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional
CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.06.21 17:31:54 +02'00'

ID NO: 083-23-093-X
Date of issue: March 2023

LIMITATION OF LIABILITY

This document is provided in accordance with the terms contained herein, expressly rejecting any type of implicit guarantee that may be related to it. Under no circumstances can the National Cryptologic Centre be held responsible for direct, indirect, fortuitous or extraordinary damage derived from the use of the information and software indicated, even when warned of such a possibility.

LEGAL NOTICE

INDEX

1. INTRODUCTION

By virtue of the principle of proportionality and in order to facilitate compliance with the National Security Framework (ENS) for certain entities or specific sectors of activity, specific compliance profiles may be implemented, comprising that set of security measures which, as a result of the mandatory risk analysis, are applicable to a specific category of security.

The CCN-STIC Guides of the National Cryptologic Centre may establish specific compliance profiles for specific entities or sectors, which will include the list of measures and reinforcements applicable in each case, or the criteria for their determination.

The National Cryptologic Centre, in the exercise of its competences, will validate and publish the corresponding specific compliance profiles that are defined, allowing those entities within its scope of application to achieve a better and more efficient adaptation to the ENS, rationalising the resources required without detriment to the protection pursued and enforceable.

The audits shall be carried out according to the category of the system and, where appropriate, the specific compliance profile that corresponds, in accordance with the provisions of Annex I and Annex III of Royal Decree 311/2022, of 3 May, and in accordance with the provisions of the Technical Security Instruction on Auditing the Security of Information Systems.

To this end, following a study of security needs, resources and a risk analysis of the vulnerabilities and threats to which the Paying Agencies are exposed, and with the aim of guaranteeing maximum security of the information systems, the mandate imposed on the CCN is fulfilled by validating the following Specific Compliance Profile for Paying Agencies, which allows the implementation of the ENS in them, with MEDIUM category security needs.

In the process of drawing up the specific compliance profile of the paying agencies of European funds, an exhaustive analysis was carried out of the regulations involved, the requirements imposed by the European legislator[1], the requirements derived from the National Security Framework [Royal Decree 311/2022], of 3rd May, the implications of third parties in the activities and functions and the particularities of the obliged party. The national coordination agency and representative Agencies have collaborated in this process.

Thanks to their collaboration, the CCN has been able to design and deploy a profile adapted to the legislative reality and particularities of the organisations under analysis.

[1] Mainly Regulation (EU) 2021/2116 of the European Parliament and of the Council of 2 December 2021 on the financing, management and monitoring of the common agricultural policy and repealing Regulation (EU) No 1306/2013 and Commission Delegated Regulation (EU) 2022/127 of 7 December 2021 supplementing Regulation (EU) 2021/2116 of the European Parliament and of the Council with rules on paying agencies and other Agencies, financial management, clearance of accounts, securities and the use of the euro.

As a final element, an Excel tool has been included to help with information related to the application of the profile and synergies of the rules affecting the paying agencies.

2. OBJECT

This guide is the result of the application of article 30 of Royal Decree 311/2022, of 3rd May, on the basis of which and in accordance with the principles of proportionality and efficiency and effectiveness, the Specific Compliance Profile for Paying and Coordination Agencies is presented, specifying and adapting certain requirements of the National Security Framework for these subjects.

Let us not forget that these agencies must comply with the requirements established by the European legislator, which necessarily imply an information security system based on the security standard[2] . By applying this profile, paying agencies will indirectly benefit from the implementation of a single security framework[3] for their information systems. However, certification requirements can be modulated based on the responsibility for the management and control of annual expenditure under the EUR 400 million limit[4].

The CCN has been aware of the significant differences that exist between paying agencies based on their responsibility for managing the amounts of EAFRD and EAGF aid, and the Compliance Profile presented considers different levels of requirements based on this certification obligation that falls on some of them.

Agencies will have to analyse the level of requirements that apply to them under the European legislator and proceed to deploy the requirements set out. [5]

It is not the purpose of this guide to provide a detailed analysis of the standards and to deploy an equivalence of compliance at European level and the differentiated application of ENS controls and reinforcements.[6]

---

[2] Commission Delegated Regulation (EU) 2022/127 of 7 December 2021 supplementing Regulation (EU) 2021/2116 of the European Parliament and of the Council with rules concerning paying agencies and other Agencies, financial management, clearance of accounts, securities and the use of the euro (hereinafter Delegated Regulation (EU) No 2022/127), Annex I, 3 INFORMATION AND COMMUNICATION, point (B), "The security of information systems shall be certified in accordance with ISO 27001: Information Security management systems - Requirements (ISO) (ISO)."

[3] Delegated Regulation (EU) No 2022/127, Annex I, 3 INFORMATION AND COMMUNICATION, point (B), "Member States may, subject to authorisation by the Commission, certify the security of their information systems in accordance with other accepted standards if these standards ensure a level of security at least equivalent to that provided for in ISO 27001".

[4] Delegated Regulation (EU) No 2022/127 Annex I, 3 INFORMATION AND COMMUNICATION, point B), "(...) *shall not apply to paying agencies responsible for the management and control of annual expenditure not exceeding EUR 400 million, if the Member State concerned has informed the Commission of its decision to apply".*

[6] Delegated Regulation (EU) No 2022/127, Annex I, 3 INFORMATION AND COMMUNICATION, point (B), "Member States may, subject to authorisation by the Commission, certify the security of their information

Nor is it the purpose of this guide to analyse the requirement for certification of standards other than the ENS itself, as each agency will have to analyse the need to undergo other certification processes, and specifically those related to the requirements of the European legislator.

3. SCOPE: PAYING AND COORDINATING AGENCIES

This profile applies exclusively to paying agencies and coordinating Agencies for European agricultural funds, in accordance with the provisions of Commission Delegated Regulation (EU) 2022/127 of 7th December 2021 supplementing Regulation (EU) 2021/2116 of the European Parliament and of the Council with rules concerning paying agencies and other agencies, financial management, clearance of accounts, securities and the use of the euro Annex I, 3 Information and Communication, point B), as certification of information systems of national paying agencies is considered possible, with other standards ensuring a level equivalent to ISO 27001.

As provided for in Article 9(1) of Regulation (EU) No 2021/2116 of the European Parliament and of the Council of 2nd December 2021 on the financing, management and monitoring of the common agricultural policy and repealing Regulation (EU) No 1306/2013, the paying agencies shall be the departments or agencies of the Member States and, where appropriate, of the regions responsible for administering and checking expenditure under the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD).

The EU regime allows Member States to authorise the designation of several paying agencies at regional level, in such cases establishing a single[7] national coordinating agency.

In addition, the European legislator has considered the possibility for paying agencies to delegate the performance of tasks, with the exception of payments.[8]

And this is the present situation, so that in Spain there is one Coordinating Agency and several paying agencies.

Therefore, the profile is aimed at; [9]

systems in accordance with other accepted standards if these standards ensure a level of security at least equivalent to that provided for in ISO 27001".

[7] Regulation (EU) 2021/2116; Article 10 "*Member States accrediting more than one paying agency shall also designate a public coordinating body (...)*".

[8] Regulation (EU) 2021/2116; Article 9.1.1 "*With the exception of making payments, the paying agencies may delegate the performance of the tasks referred to in the first subparagraph*".

[9] Royal Decree 92/2018 of 2 March, regulating the system of paying agencies and coordination with European agricultural funds, EAGF and EAFRD.

a) National Coordination Agency; Spanish Agricultural Guarantee Fund, Autonomous Agency (FEGA O.A.). Coordination agency[10], understood as the agency responsible, among other things, for centralising the information to be made available to the European Commission, adopting or coordinating measures aimed at resolving deficiencies, promoting and, where possible, guaranteeing the harmonised application of EU regulations.

b) Paying Agencies; The Autonomous Communities will have a single paying agency for the aids for which they are responsible for the management and control of the payment of expenditure, charged to the European funds; European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD).

   These Agencies, in terms of information security requirements and this profile, are differentiated in the following ways: [11]

   a. 400 million.

   b. 400 million.

c) Delegated Agencies[12]; Paying agencies may delegate the performance of tasks, except for the delegation of payment, in accordance with Regulation (EU) 2021/2116, subject to the conclusion of a written agreement, ensuring that effective systems are in place in advance to ensure the delegated tasks and verification of the fulfilment of obligations.[13]

Considering the differentiation of subjects that may exist in the EAGF and EAFRD aid management ecosystem, for the purposes of Royal Decree 311/2022, of 3rd May, the following should be considered:

[10] Consider the provisions regarding paying agency at national level in Article 9.2.3 of Regulation (EU) 2021/2116; "Where *paying agencies are established at regional level, Member States shall, in addition, accredit a paying agency at national level for aid Frameworkswhich by their nature are to be managed at national level, or shall entrust the management of such Frameworks to their regional paying agencies*".

[11] Difference with significant impact, given that according to Delegated Regulation (EU) No 2022/127, Annex I Authorisation Criteria, Article 1.3 Information and Communication, point B) Security of Information Systems;

"The first and second subparagraphs shall not apply to paying agencies responsible for the management and control of annual expenditure not exceeding EUR 400 million, if the Member State concerned has informed the Commission of its decision to apply one of the following rules instead:

-International Standards Organisation 27002: Code of practice for Information Security management (ISO),

-Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch/IT Baseline Protection Manual (BSI),

-Information Systems Audit and Control Association: Control objectives for Information and related Technology (COBIT)".

[12] The delegation of powers in relation to intervention measures, in accordance with Article 3 of Delegated Regulation (EU) 2022/127, has not been specified.

[13] For further details, see Delegated Regulation (EU) No 2022/127, Annex I, 1.

a) All subjects are Agencies subject to administrative regulations, being subjects of the public sector and therefore being subject to Royal Decree 311/2022, of 3rd May.

b) Paying agencies carrying out acts of delegation should consider the existence of a delegation of functions assimilated to a supply chain [op.ext.3], and in any case remain fully responsible for the legality and regularity of the underlying transactions[14], maintaining due diligence, requiring effective systems in the delegating agencies and verifying regulatory compliance.

c) The coordinating agency can itself be a paying agency and can benefit from the compliance profile, based on the annual expenditure limit of EUR 400 million.

Finally, consideration should be given to the existence of other public entities[15] whose competences and functions are limited to technological services, infrastructure and architecture management, management of communications and system interconnections, coordination of technological services with third parties, system and service redundancies, continuity plans and strategies, and other similar measures. This is even more important for paying agencies, which must focus their efforts on compliance with the internal structure and organisation declared by the European legislator. For this reason, certain security measures may be delegated to these entities, in their execution, but not in their responsibility, since the agency must ensure the execution and verify that the compliance required by the measure is maintained. When a delegation is made, the specific delegation and scope of the delegation, and the agency's measures to ensure and verify compliance by the delegated public agency, should be included in the statement of applicability of the relevant profile.

3.1 METHODOLOGY FOLLOWED FOR THE DEVELOPMENT OF THE PROFILE

This profile has been developed thanks to the interaction of the subject concerned, who has participated through a sample representation, in working meetings, which have served to be able to know the risks present and to adapt the necessary measures that have allowed to present the application of the ENS in a proportional way for the national paying agencies.

These meetings have been held constantly over several months and have made it possible to get to know the subject matter and the differences between them, to analyse the particular legal requirements, to learn about the security trend presented, and to adapt the requirements of the National Framework, in a compliance profile that seeks to guarantee compliance with the ENS and full respect for the provisions of the European legislator.

[14] Annex I Royal Decree 311/2011, External Resources [op.ext] "When the organisation uses external resources (services, products, facilities or personnel), it shall retain full responsibility for the risks to the information processed or services provided, and shall take the necessary measures to exercise its responsibility and maintain control at all times."

[15] Subject in all respects to compliance with Royal Decree 311/2022.

For the elaboration of this profile, the collaboration of the national coordinating agency has been indispensable, as it has been an essential channel for unifying criteria and needs. The European legislator has been respectful of the territorial and jurisdictional distribution of the Member States, insofar as the existence of a national coordinating agency [FEGA] and different paying agencies has been permitted.[16] However, this provision implies 17 differentiated information systems in Spain, under the umbrella of the autonomous regions and their differentiated security strategies, in addition to the system of the national coordinating agency itself.

The main conclusions of this methodology have materialised in the profile presented here, which can be summarised as follows:

a) Paying [and coordinating] agencies have particularities as a public sector subject, both at the functional and competence level, as well as in their own information system, interconnections, dependencies, delegations and supervisions, which make the materialisation of a specific compliance profile desirable.

b) The paying agencies have differences in relation to the security obligations imposed by the European legislator, in that a modulation of the obligations imposed at national level for information security is advisable.

c) At the national level, they have a national coordinating agency that also works to assist and collaborate with all agencies on security issues.

d) At a general level, dependencies of the regional paying agencies with other public entities with technological competences are presented, which will have a significant impact on security compliance and on the evidence that can be presented in audits, especially those carried out to verify compliance with European regulations on agricultural subsidies.[17]

e) Paying agencies are obliged by two standards of direct effect to develop an information security management system, as it is necessary to facilitate compliance with both standards, under the premises that the legislature has given us.[18]

f) There is a common tendency for organisations or their technology managers to study and deploy the CCN's security tools, as many of the security controls could be deployed more easily than initially envisaged.

[16] Consider the provisions regarding paying agency at national level in Article 9.2.3 of Regulation (EU) 2021/2116; "Where paying agencies are established at regional level, Member States shall, in addition, accredit a paying agency at national level for aid Frameworks which by their nature are to be managed at national level, or shall entrust the management of such Frameworks to their regional paying agencies".

[17] Consider those review processes developed under Article 55 of Regulation (EU) 2021/2116, considering the information security system required of paying agencies in Delegated Regulation (EU) 2022/127.

[18] Both at the national level, Royal Decree 311/2022, enabling the development of specific compliance profiles, and at the European level, Delegated Regulation (EU) 2022/127, with its ability to "authorise" information security system certifications equivalent to ISO 27001.

3.2 ANALYSIS OF EUROPEAN LEGISLATIVE REQUIREMENTS

This is why special care has been taken in drawing up this specific compliance profile to integrate the will of the European [and national] legislator. This analysis was necessary in order to understand the nature, purpose, object and, in short, raison d'être of the Paying Agencies. In order to do so, it was necessary to have a detailed knowledge of the European regulations and their connection with the national implementing regulations.

Thanks to this analysis, it was possible to know the services and the information handled by the organisations and to initially draw up a category, in accordance with the requirements and criteria of Royal Decree 311/2022 of 3rd May.

This is not an exhaustive list, but merely an enunciative one based on the importance they have had in the present,[19] has been considered:

Range	Standard	Description	
Standard (EU)	Regulation (EU) 2021/2116	Regulation (EU) 2021/2116 of the European Parliament and of the Council of 2 December 2021 on the financing, management and monitoring of the common agricultural policy and repealing Regulation (EU) No 1306/2013	Repeals the previous one and modifies part of the content. It is subsequently amended by Commission Delegated Regulation (EU) 2022/127 of 7 December 2021 which supplements Regulation (EU) 2021/2116 of the European Parliament and of the Council with rules on paying agencies and other Agencies, financial management, clearance of accounts, securities and the use of the euro.
Standard (EU)	Regulation (EU) 2021/2115 of the European Parliament and of the Council	Regulation (EU) 2021/2115 of the European Parliament and of the Council of 2nd December 2021 laying down rules concerning support for the strategic plans to be drawn up by the Member States under the common agricultural policy (CAP strategic plans), financed by the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD), and repealing Regulations (EU) No 1305/2013 and (EU) No 1307/2013	It sets out guidelines for the definition and conditions of CAP strategic plans, interventions in specific sectors, and points associated with objectives and indicators.
Standard (EU)	**Delegated Regulation (EU) 2022/127**	Commission Delegated Regulation (EU) 2022/127 of 7th December 2021 supplementing Regulation (EU) 2021/2116 of the European Parliament and of the Council with rules on paying agencies and other Agencies, financial management, clearance of accounts, securities and the use of the euro.	Complete information on Regulation (EU) 2021/2016 related to management, accounts and guarantees. Important Related annexes.
Standard (EU)	**Implementing Regulation (EU) No 2022/128**	Commission Implementing Regulation (EU) 2022/128 of 21st December 2021 laying down detailed rules for the implementation of Regulation (EU) 2021/2116 of the European Parliament and of the Council on paying	Develops points of Regulation (EU) 2021/2116 related to authorisations of paying agencies and coordinating Agencies to OOPPs. Establishes guidelines for monitoring and supervision

[19] Although not specifically included, the following have been taken into consideration: Council Regulation (EU/EURATOM) 2020/2093, Regulation (EU/EURATOM) 2018/1046 of the European Parliament and of the Council, Regulation (EU) 1306/2013 of the European Parliament and of the Council, Commission Delegated Regulation (EU) 907/2014, Commission Implementing Regulation (EU) 908/2014, and Commission Implementing Regulation (EU) 2022/128 of 21 December 2021.

Range	Standard	Description	
		agencies and other Agencies, financial management, clearance of accounts, controls, assurances and transparency	
Standard (EU)	Delegated Regulation (EU) 2023/57	Commission Delegated Regulation (EU) 2023/57 of 31 October 2022 amending and correcting Delegated Regulation (EU) 2022/127 supplementing Regulation (EU) 2021/2116 of the European Parliament and of the Council.	Corrigenda Delegated Regulation (EU) 2021/127
Norma (ESP)	Law 30/2022	Law 30/2022 of 23rd December 2002 regulating the management system of the Common Agricultural Policy and other related matters.	Basic and coordination rules for the agricultural support system (CAP) and penalties.
Norma (ESP)	Royal Decree 1046/2022	Royal Decree 1046/2022 of 27th December, which regulates the governance of the Strategic Plan for the Common Agricultural Policy in Spain and the European agricultural funds EAGF and EAFRD.	It establishes the system of paying and coordinating Agencies for the European agricultural funds, EAGF and EAFRD, and establishes FEGA as the coordinating agency. It also establishes the need for each Autonomous Community to have a paying agency for EAGF and EAFRD expenditure and a competent authority responsible both for authorising the aforementioned agency and for supervising and monitoring its proper functioning.
Norma (ESP)	Royal Decree 515/2013	Royal Decree 515/2013 of 5 July 2013, which regulates the criteria and procedure for determining and passing on responsibilities for non-compliance with European Union law.	Regulates the process arising from non-compliance with EU Rights

Of all these standards, one of them was of great impact and should have been analysed in greater detail and attention; Delegated Regulation (EU) 2022/127 in relation to Regulation (EU) 2021/2116. This regulation develops in its Annex I, the security requirements that paying agencies must maintain and deploys requirements associated with services and information security.[20]

Regulation (EU) 2021/2116	
Article	**Reference point**
Art.9	Criteria for the accreditation of paying agencies.
Art.10	Coordinating agency where there is more than one paying agency, a national coordinating agency shall be designated.
Art. 12	Certification Agencies.
Art. 67	Data retention and exchange.
Art. 91	Confidentiality.
Art. 99	Informing beneficiaries of the publication of data concerning them
Art. 101	CHAPTER V Protection of personal data.

[20] The security of information systems must comply with the provisions of Annex I paragraph 3.b) of Commission Delegated Regulation (EU) 2022/127 of 7 December 2021, which supplements Regulation (EU) 2021/2116 of the European Parliament and of the Council with rules on paying agencies and other Agencies, financial management, clearance of accounts, securities and the use of the euro.
All communications between the paying agencies and the coordinating body of paying agencies shall be carried out in compliance with the principles of information security".

Delegated Regulation (EU) 2022/127	
Article	**Reference point**
Art.1	Conditions for the accreditation of paying agencies.
Art.2	Conditions for the authorisation of coordinating Agencies.
Art.3	Obligations of paying agencies with regard to public intervention.

Annex I	3. INFORMATION AND COMMUNICATION
A) Communication	Necessary procedures will be adopted in order to implement the EU regulations (e.g. registers, instructions, databases and checklists).
B) Security of information systems	The security of information systems shall be certified in accordance with ISO 27001.
	Member States may, subject to **authorisation** by the Commission, **certify** the security of their information systems in accordance with other accepted standards, if these standards ensure a level of security at least equivalent to that provided for in ISO 27001.
	It shall not apply to paying agencies responsible for the management and control of annual expenditure **not exceeding EUR 400 million**, if **the Member State concerned has informed the Commission** of its decision to apply one of the following rules instead: a) 27002 b) BSI (c) COBIT
	Agencies entrusted with the management and control of annual Union expenditure not exceeding EUR 400 million may, under the decision of the Member State, not require a certification process.

4. SAFETY STANDARDS.

4.1 ENS RD 311/2022

Royal Decree 311/2022 of 3rd May, which regulates the new National Security Framework, approves our (legal) cybersecurity framework.
The National Security Framework contains the basic principles and minimum requirements necessary for adequate protection of the information processed and the services provided by the entities subject to its application, in order to ensure access, confidentiality, integrity, traceability, authenticity, availability and preservation of data, information and services.
Information systems subject to the application of the ENS will be subject to a process to determine their compliance with the ENS, and for this purpose, MEDIUM or HIGH category systems will require an audit for the certification of their compliance, while BASIC category systems will only require a self-assessment for their declaration of compliance, without prejudice to the possibility that they may also be subject to a certification audit.[21]
From the conclusions drawn during the process of analysing and adapting this profile, it has emerged that the recommended category for paying agencies is the MEDIUM category. However, there are adaptations in relation to specific measures, and on the basis of responsibilities for the management of European expenditure.

4.2 ISO/IEC 27001

The ISO/IEC 27001:2013 / UNE-EN ISO/IEC 27001:2017, Information Security Management Systems, currently coexists with the new version of the ISO /IEC[22] 27001:2022 Information security, cybersecurity and privacy protection standard. This coexistence will last for 36 months, an adaptation period in which entities must adapt their systems to the latest version of the standard.
The ISO 27001 is a voluntary standard that uses the high-level structure of the ISO standards, Annex (L), thus maintaining compatibility with other standards and whose clauses are complemented by an Annex (A) that contains the list of security controls that organisations must deploy in their systems. This international standard specifies the requirements for the establishment, implementation, maintenance and continual improvement of an information security management system in the context of an organisation and includes requirements for the assessment and treatment of information security risks. This standard is certifiable and can be complemented, with

[21] Let us not forget that for the purposes of the provisions of Article 31 of Royal Decree 311/2022, paragraph 2, "The audit will be carried out according to the category of the system and, where appropriate, the specific compliance profile that corresponds, as set out in Annexes I and III and in accordance with the provisions of the Technical Security Instruction on Security Auditing of Information Systems".
[22] ISO (International Organisation for Standardisation) and IEC (the International Electrotechnical Commission) constitute the specialised system for global standardisation.

other sources of controls, by the measures it includes for the security of the organisations' systems[23] .

4.3 EQUIVALENCE ANALYSIS BETWEEN SAFETY STANDARDS.

Throughout the process of developing this profile, a number of changes took place, both at the legislative level and at the level of security standards.

Currently, two ISO 27001 standards coexist (the 2013 version and the 2022 version), both of which are certifiable. For this reason, it was necessary to carry out an equivalence analysis of both standards and, subsequently, of these standards with the ENS.

4.3.1 ISO 27001:2013 - ENS

At a high level, from the analysis carried out, it can be considered that ISO 27001 in its 2013 version requires additional controls in order to be equivalent to the ENS in its entire application, given that it does not consider certain security measures that are contemplated by Annex II of Royal Decree 311/2022, of 3rd May.

However, the ISO standard is flexible in this respect and allows the addition of source systems to its Annex A controls, in that all those measures and/or reinforcements in Annex II of Royal Decree 311/2022 of 3rd May, which are not considered by the 2013 standard, can be added.

On the other hand, at the ENS level, continuity and alternativity controls [op.cont] should be considered to achieve full equivalence, since for the ENS they are not applicable controls in the MEDIUM category.

4.3.2 ISO 27001:2013 - ISO 27001:2022

ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection - Information security management systems - Requirements", heir to the previous ISO/IEC 27001:2013 after the corresponding revision and evolution, presents a significant change in the structure of Annex A, by regrouping the controls in four large blocks; Organisational controls; People controls; Physical controls; Technological controls.

From 114 controls, the number of controls has been reduced to 93, which have been restructured into 4 major domains or chapters and new controls have been added:

5. 7Threat intelligence
5. 23Information security for the use of cloud services

[23] For example, ISO 27017 controls, related to cloud security, can be added. ISO/IEC 27017:2015 Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services

5.30 ICT Preparedness for Business Continuity
7. 4Physical security monitoring
8. 9Configuration management
8.10Deletion of information
8. 11Data masking
8. 12Data leakage prevention
8. 16Follow-up activities
8. 22Web filtering
8. 28Secure coding

The chapters are:

37	Chapter 5	Organisational controls	General security block
8	Chapter 6	Checks on persons	Refers to individuals
14	Chapter 7	Physical checks	Refers to physical objects
34	Chapter 8	Technology controls	Refers to technology

4.3.3 ISO /IEC 27002: 2022: Code of practice for information security management

The ISO/IEC 27002: 2022 is designed to be used as an application guide or reference for determining and implementing controls for the treatment of information security risks in an Information Security Management System (ISMS) based on ISO/IEC 27001. It can also be used as a guidance and implementation document for commonly accepted information security controls, as it can enrich other security frameworks, such as the National Security Framework.

This standard is not certifiable, so systems based on this standard may be eligible for certification under the ISO 27001 requirements standard.

On a general level, the 2022 version of the standard has measures that are more in line with Royal Decree 311/2022 of 3 May, having deployed much needed controls in the new cybersecurity scenario.

4.3.4 ISO 27001: 2022-ENS

A global equivalence of the controls of Annex A of ISO 27001:2022 and Royal Decree 311/2022, of 3 May, has been carried out in order to demonstrate the synergy of the two standards, and to align the specific security profile of paying agencies.[24]

[24] This profile does not aspire to be the ENS reference guide to ISO 27001. See CCN STIC 825 ENS Guide - 27001 Certifications

Identification	Equivalence level	Detail
	Equivalent	In the analysis of control requirements analysed, it has been concluded that there is full equivalence. Both standards have identical requirements or the detailed measures are comparable. The security purposes for the control analysed are equivalent in both standards.
	Partially equivalent	In the requirements analysis of the control analysed, it has been concluded that there is not full equivalence. The standards are not equally demanding in the requirements described. Some of the requirements of the control analysed are equivalent but not all parts of the control can be considered to be covered. The control may need to be supplemented by other controls scattered throughout the standard, or the standard may not have considered the control requirements not covered. Although the purpose may be similar, one of the standards is more demanding and its purpose is more extensive.
	Null	In the requirements analysis of the control analysed, it has been concluded that there is no equivalence. One of the standards does not consider the control analysed. One of the standards has deployed a control for a purpose that is not pursued by the other standard.

See the annex to this profile for details of the analysis carried out. This annex can help the target subjects to align their currently deployed management systems with Royal Decree 311/2022.

4.3.5 Conclusion analysis of security standards

From the above, we can consider:

a) Analysis of Royal Decree 311/2022 and ISO 27001: 2013.

- The level of equivalence of the two standards is low, given that the Royal Decree has evolved in terms of stringency and security, while the standard remains at a discreet security level that does not consider the profile of new security threats and risks.

b) Analysis of Royal Decree 311/2022 and ISO 27001: 2022.

- The level of equivalence is good. Both standards have evolved in terms of security and consideration of new risks, in a cloud and vendor-dependent environment.[25]
- Equivalence can be considered by means of a compliance profile starting from an MEDIUM category and considering the specific modulation;
    i. Reduction of some requirement set in MEDIUM category measures as the ISO standard does not consider the measure as rigorously (e.g. configuration or certified components).

[25] It has been analysed in relation to the direct application on a subject likely to certify its system under the ISO standard.

ii. Apply some reinforcement not initially applicable in a MEDIUM category.

iii. Implement the continuity measures to be considered in a security scenario under ISO.

4.4 ANALYSIS OF PAYING AGENCIES' SYSTEMS AND SCOPES. BASELINE SITUATION: CERTIFICATIONS AND SCOPES

4.4.1 Introduction.

Throughout the profiling process, the differences in paying agencies and specifically, the information systems deployed and alignment processes followed were analysed.

As of the date of information collection, 10 organisations, including FEGA, had developed certification processes based on ISO/IEC 27001:2013. In addition, there are 6 Agencies, including FEGA, that had carried out ENS compliance processes, 5 of which did so in the MEDIUM category and one in the BASIC category. In addition, there is one entity that has carried out a SELF-ASSESSMENT.

The categorisation presented has also been analysed, so that, with some exceptions, all systems are oriented towards an MEDIUM category.

4.4.2 Analysis of Inventories of information and services.

In order to make a proposal for an inventory of services and information on the subjects, the inventory of FEGA and some sample territorial paying agencies were taken into consideration.

In making a proposal it should be considered that each agency has its own particularities, but we should stick to what is required by the ENS without diverting attention from the European regulation.

For this reason, it has been considered useful to present a neutral inventory model, which brings together the requirements of the national and European legislator, and which analyses the required category of the system under the premises of Annex I of Royal Decree 311/2022 of 3rd May.

Cod.	Impact [DP].[26]	INFORMATION	Description	Cod.	Competence Paying Agency - Obligor	SERVICE	Description
Inf.01	Yes	Technical information	Information related to the management of EAGF and EAFRD aid. It includes records and file management, verifications, documentation and requirements to the applicant. Information related to auxiliary registers (animals, farms, etc.).	Ser.01	Yes	Technical Service	It includes activities related to the submitted applications and verification of their requirements, analysis and registration of debts and co-ordination with the national co-ordination agency. Includes actions for consultation of "Auxiliary registers" (register of animals, holding...). They include support actions for citizens and third parties and all the arrangements

[26] Affects Personal data. Consider the impact at the time of valuation.

Cod.	Impact [DP].[26]	INFORMATION	Description	Cod.	Competence Paying Agency - Obligor	SERVICE	Description
			This includes information related to coordination actions with the coordinating agency.				for maintaining the applications and platforms associated with the applications.
Inf.02		**Payment information**	It includes data related to bank accounts, crediting processes, accreditations, underwriting, calculations, monitoring and basic controls.	**Ser.02**	**Yes**	**Payment Service**	This includes regular payments, advances and interest, including the analysis of the conditions and monitoring of these, and settlements.
Inf.03		**Accounting information**	All the information associated with the obligatory accounting and operations of Feaga and EAFRD. Items, expenditure and justifications. Declarations and validated documents.	**Ser.03**	**Yes**	**Accounting Service**	It includes accounting actions, including accounting records and their completeness and accuracy requirements, management of stored products and operations and the required periodic declarations (monthly, quarterly and annual).
Inf.04		**Audit information**	Control information and evidence related to the monitoring of requirements and enforceable controls.	**Ser.04**	**Yes**	**Internal Audit Service**	Activities inherent to the audit process relating to documentary evidence of compliance with the procedures associated with authorisation, accounting, payment, advance payment, guarantee and debts and individual verification assessments.
Inf.05	**Yes**	**Internal control information**	Information related to the agency's internal control, reviews, reports, documents examined, proposals...	**Ser.05**	**Yes**	**Monitoring and Internal Control Service**	Activities related to the examination of applications and requests submitted and activities to prevent fraud and irregularities in the grant process.
Inf.06		**Warehouse and product information**	Information on products and interventions in the warehouse, inventory and traceability, controls, stock, delivery notes and movements, accounting, controls...	**Ser.06**		**Public storage operations**	Activities relating to warehouse operations and interventions, including inventories, contracts, consolidations, accounting activities, channelling of information and control and supervision through annual activities (visits and inspections).
Inf.07		**Human Resources Information**	Information related to the organisation's personnel, profiles, accreditations, preventive and surveillance resources. Training plans, evaluations, approvals. Profile of training personnel. Evaluation and effectiveness. Information related to the actions of people receiving grants and developing vocational training.	**Ser.07**		**Human resources**	Personnel management and risk prevention / health surveillance. All activities related to training grants, traineeships, internships. Non-public sector staff training actions related to information security, security standards, privacy and awareness.
Inf.08		**Information on public activities**	Information related to a public sector entity's own actions, including transparency services (information to be made public, check-in and check-out management, newsletters, activity information). Information related to the annual budget and budget monitoring. Information associated with public procurement processes (minor contracts, specifications, minutes, etc.). Information and supplements submitted to paying agencies related to complaints or non-compliance, suggestions and improvements. Information related to acknowledgements, proposals, award winners, communications, promotional activities and publicity.	**Ser.08**		**Public services**	Activities related to eGovernment (including referrals to portals of other administrations), services to citizens and third parties, actions to comply with transparency requirements, public archiving activities, administrative registration of inputs and outputs, activities to generate public information and subscriptions / newsletters of public activities. Includes budget and economic management / treasury actions. Includes all activities arising from public procurement processes. Complaints, grievances and suggestions Promotional references, acknowledgements, awards and distinctions.
Inf.09	**Yes**	**Judicial information**	Information associated with complaints, court information, appeals, sentences...	**Ser.09**		**Appeals and complaints**	Files and claims. Legal actions, courts and tribunals, appeals, financial responsibility, ...
Inf.10	**Yes**	**Aid information**	Information on other grants and subsidy applications, including forms, documents requested, accreditations, justifications, reports, etc.	**Ser.10**		**Grants and subsidies**	Management of differentiated aid and subsidies, such as general aid for rural and coastal development, aid for people at risk of social exclusion and vulnerable groups, aid from the European Fund for Aid to the Disadvantaged (FEAD)...
Inf.11		**Management system information**	Information related to the management system and its improvement (including assessments,	**Ser.11**	**Yes**	**Management system**	Information security management system. It includes assessment and scoping actions, organisational activities (roles,

Cod.	Impact [DP].[25]	INFORMATION	Description	Cod.	Competence Paying Agency - Obligor	SERVICE	Description
			applicability statements, monitoring reports, audits, procedures, instructions, analyses, reports, minutes, action plans, training plans, evaluations and performances...). Includes information associated with compliance with data protection regulations (exercise of rights, information duties, consents, risk and impact assessments, activity registers, reports, etc.) Information related to the physical security of the facilities (including recordings and maintenance of the security elements involved) Information on visits, access and motivations (person, date, reason and interlocutor).				segregations, committees...), risk and continuity management (risk analysis and impact analysis), configuration management (infrastructure and architecture, applications and platforms), job security, security and data protection training activities, awareness and sensitisation. This includes all activities related to facility security, access control and video surveillance and registration of visitors to facilities. Activities arising from compliance with and diligence of data protection regulations.

4.5 PROPOSAL FOR A UNIFIED SCOPE UNDER A COMPLIANCE PROFILE

In order to facilitate homogenisation in the assessment of services and information and a system model, a MEDIUM categorisation is proposed in accordance with Annex I of Royal Decree 311/2022, of 3 May, assessed on the basis of the provisions of Annex I of this decree and specifying the criteria by means of the provisions of guide CCN-STIC 803.

The following scopes for information systems are also proposed, so that the same scope can be used to evidence an information security management system under the specific paying agency security profile developed under the provisions of Article 30 of Royal Decree 311/2022 [equivalent to ISO 27001].

Proposal A:

The information systems supporting the services provided for the **management of aid and payments of EAGF and EAFRD funds** under the responsibility of the paying agency, in accordance with the Statement of Applicability of the specific compliance profile for paying agencies.

Proposal B[27]:

Information system necessary for the provision of services required for the **management of aid and payments under the responsibility of the paying agency for EAGF and EAFRD funds** (*application, processing, management, payment proposal, authorisation, control, payment execution, management of advances and guarantees, debt management, treasury and accounting*), in accordance with (*the security requirements set out in Royal Decree 311/2022, in accordance with*) the Statement of Applicability of the specific compliance profile for paying agencies.

[27] This proposal is in line with most of the scopes presented by the paying agencies analysed during the work. It details the processes associated with the services covered.

4.6 ENS CONFORMITY FOR THE EU

Given the provision in Delegated Regulation (EU) No 2022/127 that Member States may, subject to authorisation by the Commission, certify the security of their information systems in accordance with other accepted standards if these standards ensure a level of security at least equivalent to that provided for in ISO 27001, consideration should be given to the possibility for the Commission to authorise Spain to certify systems in accordance with the provisions of this profile.

4.7 SPECIFIC COMPLIANCE PROFILE FOR PAYING AGENCIES.

A specific Compliance Profile adapted to Paying Agencies is presented. However, given the particularity that exists, and that the Agencies are subject to differentiated responsibilities based on the management and control of a limited annual expenditure based on the amount of EUR 400 million, the profile is presented in two (2) levels of ENS compliance, namely:

a) Specific Compliance Profile for paying agencies managing aid over 400 million euros.

b) Specific Compliance Profile for paying agencies managing aid of less than EUR 400 million.

This difference in amount means that organisations may be obliged to certify their management systems according to ISO 27001 when they are responsible for the management and control of amounts above EUR 400 million or, on the contrary, when the amount is lower, they are allowed to deploy a management system based on the Code of Best Practice for Information Security Management based on ISO 27002.

And the CCN cannot be oblivious to the differentiation and forces us to accept the lower risk perceived by the European legislator and the lowering of conditions in the deployment of a security standard. For this reason, when designing this specific profile, a difference in the application of some measures has been considered, being stricter or, where appropriate, lowered, based on the requirements of the Delegated Regulation (EU) 2022/127 for an organisation. If ISO certification is required, the compliance profile will be rigorous and stricter, whereas, if ISO 27002 best practices are allowed to be deployed, the profile may have reduced requirements for some measures.

The following shows what the compliance profile looks like:

Dimensions						
Affected	CAT B	CAT M	CAT A	Control	Application PG [28]	PP Application [29]
Category	applies	applies	applies	measure. 1	CATEGORY	CATEGORY
Category	applies	applies	applies	measure. 2	CATEGORY	CATEGORY

4.8 MEASURES SHARED WITH OTHER PUBLIC SECTOR ENTITIES

It has already been pointed out that there are two particularities in relation to paying agencies: on the one hand, the possibility of delegating to other entities and agencies, as recognised by the European legislator[30], always with the express prohibition of delegation of payment.

On the other hand, within the very synergy of the public sector, it may be common the existence of public entities with competence in specific infrastructures or services, affecting the management of security measures, which will coexist with the paying agency's responsibility for them.

Some of the IT assets involved in security fall under the responsibility of Directorates or Autonomous Public Agencies other than the Paying Agency itself. For example, at the network or communications level, network management does not depend on the Paying Agency, or at the infrastructure or Data Processing Centre level, the Agency is not the owner and depends on the Directorate General / Regional Ministry on which it depends organically.

Given this particularity, a distribution of responsibilities for control compliance has been added in Annex I, which may be useful in certification processes or burden sharing and modelling of compliance with the controls present in the specific compliance profile, i.e. greater or lesser stringency in the compliance of a control for the paying agency.

It is important that paying agencies add appropriate justification in their statements of applicability, specify the delegated functions and clearly detail the controls they will put in place to ascertain and verify compliance. These measures may include internal or external audits.

As part of the national strategy to increase security in the public sector, it is recommended that the tools offered by the CCN[31] be deployed.

[28] In the column "PG Application", the category (BASIC, MEDIUM, HIGH) to be applied in case of a general profile of Paying Agency responsible for management and expenditure over EUR 400 million shall be reflected.

[29] In the column "PP Application", the category (BASIC, MEDIUM, HIGH) to be applied in case of a particular profile of Paying Agency responsible for management and expenditure below EUR 400 million shall be reflected.

[30] Regulation (EU) 2021/2116, Article 9

[31] See security solutions section at https://www.ccn-cert.cni.es/soluciones-seguridad.html

Considering the necessary existence of a central coordinating agency (mandated by the European legislator) and considering the existence of a National Authority that monitors and promotes compliance with the security of services and information:

a) The tools and guidelines of the CCN can be a great alliance to unify security criteria, overcoming the differences in regional management and facilitating the understanding of the Commission in the application of security, providing mutual trust, creating synergies between similar subjects, and all this on the basis of the existence of 17 paying agencies to be controlled in a state.

b) The premises given by a national coordination agency can be a great alliance to unify assessment criteria, security tools and services and adequate components for the management of European aid and funds.

5. DECLARATION OF APPLICABILITY OF THE PAYING AGENCY SPECIFIC COMPLIANCE PROFILE

The statement of applicability is the set of measures that are applicable for compliance with the ENS. The set of measures will depend on the levels associated with the security dimensions.

It has been determined that, in order to guarantee security in the systems referred to in this Specific Compliance Profile, the list of measures to be applied and the security level requirement of each measure applied is as indicated in the following table.

As the degree of enforcement may be different for each type of paying agency profile, a separation is presented in the table of applicable measures.

The symbol "*" indicates that the measure concerned has specific implementation criteria, which are detailed in section "6.

Therefore, when a measure is affected, it shall be specified with an asterisk "*" in the table below, above the category. A category change or a reinforcement to be applied (+R) may be referenced.

Dimensions						
Affected	CAT B	CAT M	CAT A	Control	Application PG [32]	PP Application [33]
Category	applies	applies	applies	org.1	MEDIUM	MEDIUM
Category	applies	applies	applies	org.2	MEDIUM	MEDIUM
Category	applies	applies	applies	org.3	MEDIUM	MEDIUM
Category	applies	applies	applies	org.4	MEDIUM	MEDIUM
Category	applies	+ R1	+ R2	op.pl.1	HIGH *	BASICS *
Category	applies	+ R1	+ R1 + R2 + R3	op.pl.2	MEDIUM(+R2) *	MEDIUM
Category	applies	applies	applies	op.pl.3	MEDIUM	MEDIUM
D	applies	+ R1	+ R1	op.pl.4	MEDIUM	MEDIUM *
Category	n.a.	applies	applies	op.pl.5	MEDIUM	NA[34]
T A	applies	+ R1	+ R1	op.acc.1	MEDIUM	MEDIUM (-)
C I T A	applies	applies	+ R1	op.acc.2	HIGH *	MEDIUM
C I T A	n.a.	applies	+ R1	op.acc.3	MEDIUM*	MEDIUM *
C I T A	applies	applies	applies	op.acc.4	MEDIUM	MEDIUM
C I T A	+ [R1 or R2 or R3 or R4]	+ [R2 or R3 or R4] + R5	+ [R2 or R3 or R4] + R5	op.acc.5	MEDIUM	MEDIUM
C I T A	+ [R1 or R2 or R3 or R4] + R8 + R9	+ [R1 or R2 or R3 or R3 or R4] + R5 + R8 + R9	+ [R1 or R2 or R3 or R4] + R5 + R6 + R7 + R8 + R9	op.acc.6	MEDIUM	MEDIUM
Category	applies	applies	applies	op.exp.1	MEDIUM (+R4) *	MEDIUM
Category	applies	applies	applies	op.exp.2	MEDIUM	MEDIUM
Category	applies	+ R1	+ R1 + R2 + R3	op.exp.3	HIGH *	MEDIUM
Category	applies	+ R1	+ R1 + R2	op.exp.4	HIGH *	BASICS *

[32] In the column "PG Application", the category (BASIC, MEDIUM, HIGH) to be applied in case of a general Paying Agency profile shall be reflected.
The category or requirements of the MEDIUM category may be modulated in accordance with the principle of proportionality and with a view to an effective and efficient implementation of the CSA. Where the degree of application of the control is differentiated, it shall be specified by the following references: (PG). An asterisk shall specify the particularity of the application of the category, and a reinforcement to be applied may be referenced (+R).
[33] In the column "PP Application", the category (BASIC, MEDIUM, HIGH) to be applied in case of a particular Paying Agency profile shall be reflected.
The category or requirements of the MEDIUM category may be modulated in accordance with the principle of proportionality and with a view to an effective and efficient implementation of the CSA. Where the degree of application of the control is differentiated, it shall be specified by the following references: (PP) Particular profile. The particularity of the application of the category shall be specified with an asterisk, and a reinforcement to be applied (+R) may be referenced.
[34] Not applicable

Dimensions						
Affected	CAT B	CAT M	CAT A	Control	Application PG [32]	PP Application [33]
Category	n.a.	applies	+ R1	op.exp.5	HIGH *	MEDIUM
Category	applies	+ R1 + R2	+ R1 + R2 + R3 + R4	op.exp.6	MEDIUM	BASICS *
Category	applies	+ R1 + R2	+ R1 + R2 + R3	op.exp.7	MEDIUM	MEDIUM
Category	applies	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R3 + R4 + R5	op.exp.8	MEDIUM	BASIC (+R3) *
Category	applies	applies	applies	op.exp.9	MEDIUM	MEDIUM
Category	applies	+ R1	+ R1	op.exp.10	MEDIUM	MEDIUM
Category	n.a.	applies	applies	op.ext.1	MEDIUM	MEDIUM
Category	n.a.	applies	applies	op.ext.2	MEDIUM	MEDIUM
Category	n.a.	n.a.	applies	op.ext.3	HIGH *	N/A
Category	n.a.	applies	+ R1	op.ext.4	MEDIUM	MEDIUM *
Category	applies	+ R1	+ R1 + R2	op.nub.1	MEDIUM	BASICS *
D	n.a.	applies	applies	op.cont.1	MEDIUM	MEDIUM
D	n.a.	n.a.	applies	op.cont.2	HIGH *	N/A
D	n.a.	n.a.	applies	op.cont.3	HIGH *	N/A
D	n.a.	n.a.	applies	op.cont.4	HIGH *	N/A
Category	applies	+ R1	+ R1 + R2	op.mon.1	MEDIUM	MEDIUM
Category	applies	+ R1 + R2	+ R1 + R2	op.mon.2	MEDIUM	MEDIUM
Category	applies	+ R1 + R2	+ R1 + R2 + R3 + R3 + R4 + R5 + R6	op.mon.3	MEDIUM	BASIC (+R1)*
Category	applies	applies	applies	mp.if.1	MEDIUM	MEDIUM
Category	applies	applies	applies	mp.if.2	MEDIUM	MEDIUM
Category	applies	applies	applies	mp.if.3	MEDIUM	MEDIUM
D	applies	+ R1	+ R1	mp.if.4	MEDIUM	MEDIUM *
D	applies	applies	applies	mp.if.5	MEDIUM	MEDIUM
D	n.a.	applies	applies	mp.if.6	MEDIUM	MEDIUM
Category	applies	applies	applies	mp.if.7	MEDIUM	MEDIUM
Category	n.a.	applies	applies	mp.per.1	MEDIUM	MEDIUM
Category	applies	+ R1	+ R1	mp.per.2	MEDIUM	BASIC*.
Category	applies	applies	applies	mp.per.3	MEDIUM	MEDIUM
Category	applies	applies	applies	mp.per.4	MEDIUM	MEDIUM
Category	applies	+ R1	+ R1	mp.eq.1	MEDIUM	MEDIUM
A	n.a.	applies	+ R1	mp.eq.2	HIGH *	MEDIUM
Category	applies	applies	+ R1 + R2	mp.eq.3	HIGH *	BASIC (+R2)*
C	applies	+ R1	+ R1	mp.eq.4	MEDIUM	BASICS *
Category	applies	applies	applies	mp.com.1	MEDIUM	MEDIUM
C	applies	+ R1	+ R1 + R2 + R3	mp.com.2	MEDIUM	MEDIUM
I A	applies	+ R1 + R2	+ R1 + R2 + R3 + R4	mp.com.3	MEDIUM	MEDIUM
Category	n.a.	+ [R1 or R2 or R3]	+ [R2 or R3] + R4	mp.com.4	MEDIUM	MEDIUM
C	applies	applies	applies	mp.si.1	MEDIUM	MEDIUM
C I	n.a.	applies	+ R1 + R2	mp.si.2	MEDIUM (+R2) *	BASICS *
Category	applies	applies	applies	mp.si.3	MEDIUM	MEDIUM
Category	applies	applies	applies	mp.si.4	MEDIUM	MEDIUM
C	applies	+ R1	+ R1	mp.si.5	MEDIUM	MEDIUM
Category	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4	mp.sw.1	MEDIUM	MEDIUM
Category	applies	+ R1	+ R1	mp.sw.2	MEDIUM	MEDIUM

Dimensions						
Affected	CAT B	CAT M	CAT A			
				Control	Application PG [32]	PP Application [33]
Category	applies	applies	applies	mp.info.1	MEDIUM	MEDIUM
C	n.a.	applies	applies	mp.info.2	MEDIUM	MEDIUM
I A	applies	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4	mp.info.3	MEDIUM	MEDIUM
T	n.a.	n.a.	applies	mp.info.4	HIGH*	NA
C	applies	applies	applies	mp.info.5	MEDIUM	MEDIUM
D	applies	+ R1	+ R1 + R2	mp.info.6	MEDIUM (+R2) *	BASICS *
Category	applies	applies	applies	mp.s.1	MEDIUM	MEDIUM
Category	+ [R1 or R2] + [R1 or R2	+ [R1 or R2] + [R1 or R2	+ R2 + R3	mp.s.2	MEDIUM	MEDIUM
Category	applies	applies	+ R1	mp.s.3	MEDIUM	MEDIUM
D	n.a.	applies	+ R1	mp.s.4	MEDIUM	MEDIUM*

5.1 IMPLEMENTATION MEASURES

Of the 73 security measures defined in Annex II of RD 3/2010, those related to the MEDIUM category will be applicable, with certain appreciations and reinforcements, as well as those of the HIGH category specified in this profile.

Organisational Framework (4):

[org.1] Security policy

[org.2] Security regulations

[org.3] Security procedures

[org.4] Authorisation process

Operational Framework (32):

op.pl] [op.pl Planning

[op.pl.1] Risk analysis

[op.pl.2] Security architecture

[op.pl.3] Acquisition of new components

[op.pl.4] Capacity sizing/management

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

[op.acc] Access control

[op.acc.1] Identification

[op.acc.2] Access requirements

[op.acc.3] Segregation of roles and tasks

[op.acc.4] Access rights management process

[op.acc.5] Authentication Mechanism (external users)

[op.acc.6] Authentication mechanism (users of the organisation).

[op.exp] Exploitation

[exp.op.1] Asset Inventory

[op.exp.2] Security Settings

[op.exp.3] Security configuration management

[op.exp.4] Maintenance and security updates

[op.exp.5] Change management

[op.exp.6] Protection against malicious code

[op.exp.7] Incident management

[op.exp.8] Recording the activity

[op.exp.9] Incident management record

[op.exp.10] Cryptographic key protection

[op.ext] External services

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

[op.ext.2] Day-to-day management

[op.ext.3] Supply Chain Security

[op.ext.4] System Interconnection
[op.nub] Cloud services
[op.nub.1] Protection of cloud services
[op.cont] Continuity of service
[op.cont.1] Impact analysis
[op.cont.2] Continuity plan
[op.cont.3] Periodic testing
[op.cont.4] Alternative means
[op.mon] System monitoring
[op.mon.1] Intrusion detection
[op.mon.2] Metric system
[op.mon.3] Surveillance

Protective Measures (36):

[mp.if] Protection of installations and infrastructures
[mp.if.1] Separate and access-controlled areas
[mp.if.2] Identification of persons
[mp.if.3] Fitting out the premises
[mp.if.4] Electrical energy
[mp.if.5] Fire protection
[mp.if.6] Flood protection
[mp.if.7] Equipment input and output register
[mp.per] Personnel management
[mp.per.1] Job characterisation
[mp.per.2] Duties and obligations
[mp.per.3] Awareness raising
[mp.per.4] Training
[mp.eq] Protection of equipment
[mp.eq.1] Clear workstation
[mp.eq.2] Workplace blocking
[mp.eq.3] Protection of portable equipment
[mp.eq.4] Other devices connected to the network
[mp.com] Protection of communications
[mp.com.1] Secure perimeter
[mp.com.2] Protection of confidentiality
[mp.com.3] Protection of integrity and authenticity
[mp.com.4] Separation of information flows in the network
[mp.si] Protection of information carriers
[mp.si.1] Carrier marking
[mp.si.2] Cryptography
[mp.si.3] Custody
[mp.si.4] Transport
[mp.si.5] Deletion and destruction
[mp.sw] Protection of software applications
[mp.sw.1] Application development
[mp.sw.2] Acceptance and commissioning
[mp.info] Protection of information
[mp.info.1] Personal data
[mp.info.2] Qualification of the information
[mp.info.3] Electronic signature
[mp.info.4] Time Stamps
[mp.info.5] Cleaning of documents
[mp.info.6] Backups
[mp.s] Protection of services
[mp.s.1] E-mail protection
[mp.s.2] Protection of web services and applications
[mp.s.3]Protection of web browsing
[mp.s.4] Denial of service protection

6. CRITERIA FOR THE APPLICATION OF MEASURES

6.1 [op.pl.1] Risk analysis

[PG] General Profile:

The requirements of MEDIUM category shall apply, together with the "R2 Reinforcement" Formal risk analysis.

[PP] Individual Profile:

BASIC category requirements shall apply.

6.2 [OP.PL.2] Security architecture

[PG] General Profile:

The requirements of MEDIUM category shall apply, together with the "R2 Reinforcement - Safety management system with continual improvement".

- [op.pl.2.r2.1] Information security management system, with regular updating and approval.

6.3 [OP.PL.4] Dimensioning/capacity management

[PP] Individual Profile:

The MEDIUM category shall apply, without applying the requirement [op.pl.4.r1.2] of 'R1 Reinforcement - Continuous improvement of capacity management':

- [op.pl.4.r1.2] Tools and resources for capacity monitoring shall be used.

6.4 [OP.PL.5] Certified components

[PP] Individual Profile:

This control shall not apply.

6.5 [OP.ACC.1] Identification

[PP] Individual Profile:

The requirements of MEDIUM category shall apply and the requirement [op.acc.1.r1.3] of "Strengthening R1-Advanced Identification" shall not apply:

- [op.acc.1.r1.3] An up-to-date list of authorised users shall be ensured and maintained by the system/system security administrator.

6.6 [OP.ACC.2] Entry Requirements

[PG] General Profile:

The measure shall be applicable in its HIGH category, "Reinforcement R1-Stringent segregation".

6.7 [OP.ACC.3] Segregation of Duties and Tasks

[PG] General Profile:

The requirements of MEDIUM category shall apply and the requirement may be excluded,

- [op.acc.3.1] Whenever possible, the development and operational capabilities shall not rest with the same person.

[PP] Individual Profile:

The requirements of MEDIUM category shall apply except:

- [op.acc.3.1] Whenever possible, the development and operational capabilities shall not rest with the same person.
- [op.acc.3.2] Whenever possible, the persons authorising and controlling the use shall be different.

6.8 [OP.EXP.1] Inventory of Assets

[PG] General Profile:

The requirements of MEDIUM category shall apply, together with "Strengthening R4-List of software components".

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

This measure shall include the requirement for laptops and devices, incorporating the "asset owner" or assigned user [mp.eq.3.1].

6.9 [OP.EXP.3] Security configuration management

[PG] General Profile:

The requirements of HIGH category with reinforcements shall apply;

"Reinforcement R2-Responsibility for the configuration".

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

"Reinforcement R3-Security copies."

- [op.exp.3.r3.1] The system configuration shall be backed up in such a way that it can be partially or fully reconstructed after an incident.

6.10 [OP.EXP.4] Maintenance and Security Updates

[PG] General Profile:

The requirements of HIGH category shall apply

It is necessary to associate "R2 Reinforcement - Failure Prevention" with the control [op.exp.5] and its appropriate management by means of a reversal plan.

- [op.exp.4.r2.1] Prior to the implementation of security configurations, patches and updates, a mechanism shall be provided to reverse them in case of the occurrence of adverse effects.

[PP] Individual Profile:

BASIC category requirements shall apply.

6.11 [OP.EXP.5] Change Management

[PG] General Profile:

The requirements of HIGH category shall apply.

It is necessary to associate "Reinforcement R1- Failure Prevention" with the control [op.exp.4].

6.12 [OP.EXP.6] Protection against harmful code

[PP] Individual Profile:

The requirements of BASIC category shall apply

6.13 [OP.EXP.8] Registration of the activity

[PP] Individual Profile:

The BASIC category shall apply, requiring "Enforcement 3 Record Retention".

- [op.exp.8.r3.1] The security documentation of the system shall indicate the security events to be audited and the retention time of the logs before deletion. For internal users, active logging of the domain and authorised applications with a base retention of 6 months shall be sufficient.

6.14 [OP.EXT.3] Supply chain security

[PG] General Profile:

HIGH category shall apply.

This control shall relate to the controls in the control block [op.cont].

6.15 [OP.EXT.4] Systems Interconnection [35]

[PG] General Profile:

MEDIUM category shall apply, except for the requirement set out in

- [op.ext.4.1] All exchanges of information and provision of services with other systems shall be subject to prior authorisation. Any flow of information shall be prohibited unless expressly authorised.

For those interconnections with other public entities, they shall be considered authorised by default and as a general rule, unless expressly prohibited by the Security Officer.

[PP] Individual Profile:

The MEDIUM category shall apply, with the exceptions set out in the requirements:

- [op.ext.4.1] All exchanges of information and provision of services with other systems shall be subject to prior authorisation. Any flow of information shall be prohibited unless expressly authorised.

For those interconnections with other public entities, they shall be considered authorised by default and as a general rule, unless expressly prohibited by the Security Officer.

- [op.ext.4.2] For each interconnection, the following shall be explicitly documented: interface characteristics, security and data protection requirements, and the nature of the information exchanged.

Only the general network diagram of the hierarchical superior entity and/or public entity involved in network and interconnection processes shall be considered.

6.16 [OP.NUB.1] Protection of cloud services

[PP] Individual Profile:

The BASIC category shall apply.

6.17 [OP.CONT.2] Continuity plan

[PG] General Profile:

HIGH category shall apply.

6.18 [OP.CONT.3] Periodic testing

[PG] General Profile:

[35] For all purposes, the provisions of the ENS related to the use of services and infrastructures common to the Public Administrations shall be considered.
Article 29 Common infrastructures and services
The use of common infrastructures and services of the public administrations, including shared or transversal services, shall facilitate compliance with the provisions of this Royal Decree. The specific cases of use of these infrastructures and services shall be determined by each public administration.

HIGH category shall apply.

6.19 [OP.CONT.4] Alternative means

[PG] General Profile:

HIGH category shall apply.

6.20 [OP.MON.3] Monitoring.

[PP] Individual Profile:

BASIC category, and "Reinforcement R1-Event Correlation" shall apply.

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

6.21 [MP.IF.4] Electrical Energy

[PP] Individual Profile:

MEDIUM category shall apply, with no R1 Reinforcement-Emergency power supply applied.

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

6.22 [MP.PER.2] Duties and obligations

[PP] Individual Profile:

The BASIC category shall apply.

6.23 [MP.EQ.2] Work center lockout

[PG] General Profile:

The HIGH category will apply, with the application of the R1-Closing of sessions.

- [mp.eq.2.r1.1] After a certain period of time, longer than the above, the sessions opened from this workstation shall be cancelled.

The Agency should monitor the particularisations, which could be deployed in a CCN-STIC Guide, of the security configuration adapted to the Agency and to this profile.

6.24 [MP.EQ.3] Protection of portable devices

[PG] General Profile:

HIGH category shall apply

Consideration should be given to encrypting the hard disk of the laptop, as indicated in "Enforcement R1 - Disk Encryption", if the inventory of information is considered to be of MEDIUM level.

[PP] Individual Profile:

The Basic category will apply with the "R2 Reinforcement - Protected Environments".

- [mp.eq.3.r2.1] The use of handheld devices outside the organisation's premises shall be restricted to secured environments, where access is controlled and safe from theft and prying eyes.

6.25 [MP.EQ.4] Other devices connected to the network

[PG] Individual Profile:

The BASIC category shall apply.

6.26 [MP.SI.2] Cryptography

[PG] General Profile:

MEDIUM category shall apply, together with R2-Security copies.

- [mp.si.2.r2.1] Backups shall be encrypted using algorithms and parameters authorised by the CCN.

[PP] Individual Profile:

The BASIC category shall apply.

6.27 [MP.INFO.4] Time Stamps

[PG] General Profile:

HIGH category shall apply.

6.28 [MP.INFO.6] Back-ups

[PG] General Profile:

MEDIUM category shall apply, together with the requirements of "Strengthening R2-Backup Protection".

- [mp.info.6.r2.1] At least one of the backup copies shall be stored separately in a different location so that an incident cannot affect both the original repository and the copy simultaneously.

This will be associated with the results of the assessment derived from [mp.info.2] and the risks [op.pl.1] and impact [op.cont.1].

This control shall be referenced to "R3-Security copies".

- [op.exp.3.r3.1] The system configuration shall be backed up in such a way that it can be partially or fully reconstructed after an incident.

R2-Protection of backups, for critical items that require storage in a different location, is considered as Reinforcement R2-Protection of backups.

[PP] Individual Profile:

The BASIC category shall apply.

6.29 [MP.S.4] Denial of Service Protection

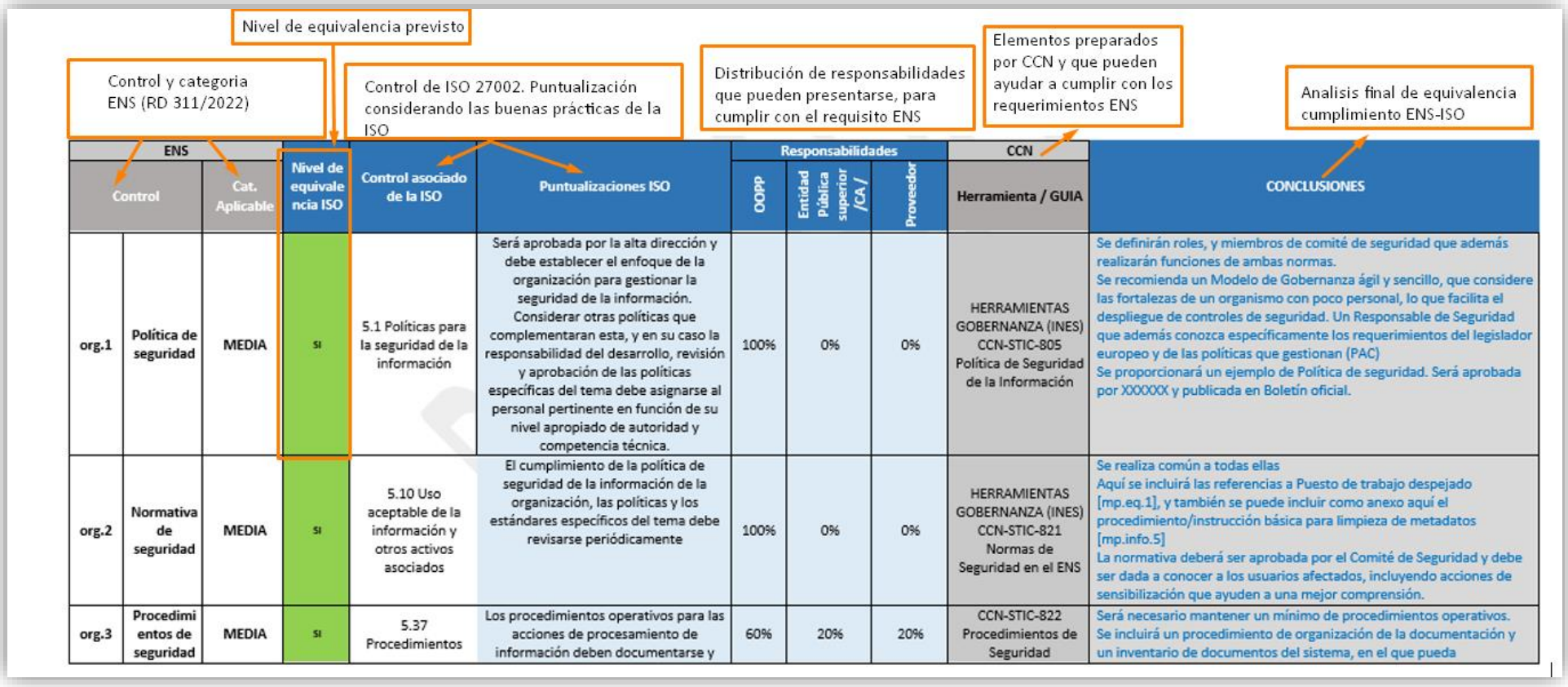
[PP] Individual Profile:

The MEDIUM category shall be applicable with the qualification of the requirement [mp.s 4.1], being associated with the control [OP.PL.4], and compliance with it being sufficient.

7. Annex I - Equivalence and compliance with controls

For a Paying Agency to undergo a single accreditation process, enabling it to be certified according to ENS and ISO 27001, its Information Security Management System must take into account the requirements of both standards.

How to interpret the content of the table presented:



ENS			Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades			CCN	CONCLUSIONES
Control		Cat. Aplicable				OOPP	Entidad Pública superior /CA/	Proveedor	Herramienta / GUIA	
org.1	Política de seguridad	MEDIA	SI	5.1 Políticas para la seguridad de la información	Será aprobada por la alta dirección y debe establecer el enfoque de la organización para gestionar la seguridad de la información. Considerar otras políticas que complementaran esta, y en su caso la responsabilidad del desarrollo, revisión y aprobación de las políticas específicas del tema debe asignarse al personal pertinente en función de su nivel apropiado de autoridad y competencia técnica.	100%	0%	0%	HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-805 Política de Seguridad de la Información	Se definirán roles, y miembros de comité de seguridad que además realizarán funciones de ambas normas. Se recomienda un Modelo de Gobernanza ágil y sencillo, que considere las fortalezas de un organismo con poco personal, lo que facilita el despliegue de controles de seguridad. Un Responsable de Seguridad que además conozca específicamente los requerimientos del legislador europeo y de las políticas que gestionan (PAC) Se proporcionará un ejemplo de Política de seguridad. Será aprobada por XXXXXX y publicada en Boletín oficial.
org.2	Normativa de seguridad	MEDIA	SI	5.10 Uso aceptable de la información y otros activos asociados	El cumplimiento de la política de seguridad de la información de la organización, las políticas y los estándares específicos del tema debe revisarse periódicamente	100%	0%	0%	HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-821 Normas de Seguridad en el ENS	Se realiza común a todas ellas Aquí se incluirá las referencias a Puesto de trabajo despejado [mp.eq.1], y también se puede incluir como anexo aquí el procedimiento/instrucción básica para limpieza de metadatos [mp.info.5] La normativa deberá ser aprobada por el Comité de Seguridad y debe ser dada a conocer a los usuarios afectados, incluyendo acciones de sensibilización que ayuden a una mejor comprensión.
org.3	Procedimientos de seguridad	MEDIA	SI	5.37 Procedimientos	Los procedimientos operativos para las acciones de procesamiento de información deben documentarse y	60%	20%	20%	CCN-STIC-822 Procedimientos de Seguridad	Será necesario mantener un mínimo de procedimientos operativos. Se incluirá un procedimiento de organización de la documentación y un inventario de documentos del sistema, en el que pueda

Therefore, an Agency should consider the following:

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
org.1	Security policy	MEDIUM	MEDIUM	YES	5.1 Information security policies	It shall be approved by top management and shall set out the organisation's approach to managing information security. Consider other policies to complement this one, and where appropriate the responsibility for the development, review and approval of specific policies by relevant staff according to their level of authority and technical competence.	100%		0%	0%	GOVERNANCE TOOLS (INES) CCN-STIC-805 Information Security Policy	Roles will be defined, and security committee members will also perform functions for both standards. An agile and simple Governance Model is recommended, which considers the strengths of the organisation, its functional structure and clear separation, which facilitates the deployment of security controls. A Security Officer who is also specifically aware of the requirements of the European legislator and the policies they manage (CAP). A common Security Policy will be drawn up, approved by the Committee and published in the official Bulletin.
org.2	Safety regulations	MEDIUM	MEDIUM	YES	5.10 Acceptable use of information and associated assets	Compliance with the organisation's information security policy, policies and standards specific to the organisation should be reviewed periodically.	30%	10%	50%	10%	GOVERNANCE TOOLS (INES) CCN-STIC-821 ENS Security Standards	Common to the mandates of both standards, the references to Clear Workplace [mp.eq.1] shall be included here, and the basic procedure/instruction for clearing metadata [mp.info.5] may be included as an annex. The standard shall be approved by the Security Committee and shall be made known to the affected users, including awareness raising actions [mp.per.4] to help understanding.
org.3	Security procedures	MEDIUM	MEDIUM	YES	5.37 Documented operating procedures	Operating procedures for information processing actions should be documented and made available to staff who need them.	40%	10%	20%	30%	CCN-STIC-822 Security Procedures AMPARO	A minimum of operating procedures shall be maintained. This shall include a procedure for the organisation of documentation [7.5 Documented information] and an inventory of system documents, including their creation date, revision date and the sensitivity of the information contained therein.
org.4	Authorisation process	MEDIUM	MEDIUM	PARTIAL	5.2 Information security roles and responsibilities	While ISO is not as specific, it allows for the deployment of a particularised authorisation process. The ENS mandate should therefore be prioritised over ISO.	90%		10%	0%	GOVERNANCE TOOLS (INES) CCN-STIC-801 National Security Framework. Responsibilities and functions	Although the ISO is not as specific, it allows for a particularised authorisation process to be deployed. The requirements of Annex I - Article 1 of Delegated Regulation (EU) 2022/127; Point B) should be considered: "*(iv) appropriate training of staff at all operational levels, including on fraud awareness, and a policy is in place to rotate staff in sensitive positions or to increase supervision,*" and "*(v) appropriate measures are taken to prevent and detect the occurrence of a conflict of interest, within the meaning of Article 61 of Regulation (EU, Euratom) 2018/1046, as regards the performance of functions of the paying agency in relation to persons with influence and holding a position of responsibility within and outside the paying agency. Where there is a risk of conflict of interest, measures shall be taken to ensure the application of that Article.*"
op.pl.1	Risk analysis	HIGH *	BASICS *	YES	6.1 - Actions to address risks and opportunities	The criteria followed for risk acceptance, identifying risk owners, prioritising treatments and assuming residual risks should be documented.	100%		0%	0%	GOVERNANCE TOOLS (INES) Pilar PILLAR CCN-STIC 470-473 CCN-STIC 410 Risk analysis in	Both standards converge and the same risk methodology can be used to deploy this control. It is recommended to use PILAR as a tool and to deploy a statement of shared applicability of both standards. The Security Committee will approve the risks and the treatment plan and receive feedback on risk management.

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
											government systems	The Security Officer must approve the statement of applicability.
op.pl.2	Security Architecture	MEDIUM (+R2*)	MEDIUM	YES	Clause 4.4 Information security management system 8.27 Secure systems architecture and engineering principles	The organisation shall establish, implement, maintain and continually improve an Information Security Management System in accordance with the requirements of the international standard. The principles for designing secure systems shall be established, documented, maintained and applied to any information systems development activity.	40%	10%	20%	30%	GOVERNANCE TOOLS (INES)	Both systems are supported by an Information Security system. However, for a particular profile, a system with an improvement cycle (PDCA) and basic system information will be considered sufficient. Some of the information will be documented by a third party service provider (e.g. network services) and, where appropriate, the service holder (Autonomous Community Agencies on which the OOPP will depend).
op.pl.3	Procurement of new components	MEDIUM	MEDIUM	PARTIAL	5.8 Information security in project management	Procurement processes will be integrated into complete and comprehensive projects, which will cover many elements and should include procurement of components, risks, architecture and requirements. Information security must be integrated into the organisation's project management activities.	80%		10%	10%	GOVERNANCE TOOLS (INES) CCN-STIC Catalogue 105 CCN STIC 140 Guides	It is important to consider the overall process, and in a cross-cutting manner. This will document and include security requirements in procurement processes Specific procurement regulations should be considered.
op.pl.4	Sizing/capacity management	MEDIUM	MEDIUM (*)	YES	8.6 Capacity management	Planning, monitoring and adjustment. A dual strategy should be considered; increasing capacity and/or reducing demand.	50%	10%	20%	20%	GOVERNMENT TOOLS (INES) LORETO CCn-STIC-820 Denial of Service Protection	The two standards can converge perfectly. Automation is recommended, which can be through a provider that helps us to manage measurements, alerts and schedules. Cloud services can help, given their scalability. Consider control [op.nub.1].
op.pl.5	Certified components	MEDIUM	(NA) (*)	No	Not expressly provided for	There is no such control in ISO. However, it can be associated with assets, asset mapping and the risks that may arise. Having accredited products and services can improve the security of the OOPP.	40%	10%	20%	30%	GOVERNANCE TOOLS (INES) PILLAR	This control can be excluded in the Particular Profile [PP], as it is not covered by ISO and does not have a major impact on OOPP services. For General Profile [PG], an inventory of the affected components should be worked out or this feature should be integrated in the asset inventory, including the analysis of inclusion in the CCN STIC 105 catalogue or equivalent certification (e.g. Common Criteria). To be considered in future procurements of new components Consider [op.pl.3]. To be considered for products and for security services.
op.acc.1	Identification	MEDIUM	MEDIUM *	YES	5.16 Identity management	The full lifecycle of identities must be managed.	80%	10%	0%	10%	GOVERNANCE TOOLS (INES)	Both controls allow for the management of identities in a comprehensive manner. It is recommended that the entity maintains an inventory of services (including those provided by cloud services). In this registry, the identification methodology can be controlled. Records or traces can be traced through the active directory and records and holds associated with the activity logs can be maintained.
op.acc.2	Access requirements	HIGH *	MEDIUM	YES	5.15 Access control	Rules for controlling physical and logical access to information and other associated assets must be established and	80%	10%	0%	10%	GOVERNANCE TOOLS (INES)	Service requirements and risk considerations should be the basis for defining access rights, tools and granularity. Access control rules can be implemented at different granularities,

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
						implemented based on business and information security requirements .					EMMA CARLA	ranging from covering entire networks or systems to specific data fields, and can also consider properties such as the location of the user or the type of network connection used for access (will significantly affect costs and resources).
op.acc.3	Segregation of duties and tasks	MEDIUM*	MEDIUM*	YES	5.3 Segregation of duties	Duties and conflicting areas of responsibility should be segregated.	50%	10%	20%	20%	GOVERNANCE TOOLS (INES) EMMA CARLA	Where segregation is difficult, other controls such as activity tracking, audit trails and management oversight should be considered. To maintain control, an inventory of operations should be available, allowing differentiation of segregations and on whom they fall. For example, on change issues; access rights, code and development, system in production, applications, databases, remote access, ... The provisions of Annex I - Article 1.1 of Delegated Regulation (EU) 2022/127 should be considered.
op.acc.4	Access rights management process	MEDIUM	MEDIUM	YES	5.18 Access rights 8.2 Privileged access rights	Granting and revoking access rights Review and change or termination of employment. The allocation and use of privileged access rights must be restricted and managed.	40%	10%	20%	30%	GOVERNANCE TOOLS (INES) EMMA CARLA	Both standards converge, although in the case of ISO provisions contained in several controls must be considered. It is important to consider that this control affects every user, so third party users must be managed.
op.acc.5	Authentication mechanism (external users)	MEDIUM	MEDIUM	PARTIAL	5.18 Access rights 8.5 Secure authentication	Ensure that access rights are activated (e.g. by service providers) only after authorisation procedures are successfully completed.	60%	10%	10%	20%	GOVERNANCE TOOLS (INES)	This is a control that directly affects entities that are owners of published sites and services that allow external users to access them. In this case, the ISO does not specify the control to such an extent, although it does consider the requirements imposed by the ENS. Consider the responsibilities of the provider (developer and maintainer of services) and the owner of the services that may be used by the OOPP.
op.acc.6	Authentication mechanism (organisation's users)	MEDIUM	MEDIUM	YES	8.5 Secure authentication	Secure authentication technologies and procedures shall be implemented according to the information access restrictions and the specific policy on access control.	70%		10%	20%	GOVERNANCE TOOLS (INES)	The ISO control allows authentications to be adapted to ENS requirements and modulated. The reinforcements contained in the High category can improve the security of access and are covered by ISO 27002: (...) k) terminate inactive sessions after a defined period of inactivity, l) restrict connection duration times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorised access. There will be many remote or cloud-based services that can be derived as procedures, password authentication and second factor authentication.
op.exp.1	Inventory of assets	MEDIUM (+R4)	MEDIUM	YES	5.9 Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, should be developed and maintained.	50%	10%	20%	20%	PILAR EMMA GOVERNANCE (INES)	It is important to manage asset inventories, which can be through simple tools or with more complexity depending on the volume of assets and the OOPP budget. Consideration should be given to the owner of the asset, and specifically [mp.eq.3.1] inventory of portable equipment together with an identification of the person responsible for it and a regular check that it is positively under their control. Inventories should ensure that they are kept up to date, therefore regular reviews should be performed; and an update should be

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
												automatically applied following the process of installing, changing or removing an asset. The location of an asset should be included in the inventory as appropriate. It should be noted that this inventory will assist in the case of both standards, risk management, audit activities, vulnerability management and contingency and recovery action planning. Consider control [op.pl.5].
op.exp .2	**Security settings**	**MEDIUM**	**MEDIUM**	**PARTIAL**	8.9 Configuration management	Configurations, including security, hardware, software, service and network configurations must be established, documented, implemented, monitored and reviewed.	50%	10%	10%	30%	CLARA ROCIO EMMA ESE ANA CCN-STIC specific guides GOVERNANCE TOOLS (INES)	The configuration will rely on the different tools deployed in the CCN, and especially CLARA. The system documentation shall consider the basing guidelines and the documentation of those tools that help to manage possible deviations or vulnerabilities. ENS requirements shall be deployed in order to maintain an appropriate configuration. Specifically published guidelines shall be considered. Due to the exposure surface, assets that are only in-house and do not present significant risks can be configured with a generic security template.
op.exp .3	**Security configuration management**	**HIGH***	**MEDIUM**	**PARTIAL**	8.9 Configuration management	Standard templates for hardware, software, services and network security configuration Templates should be periodically reviewed and updated The organisation should define and implement processes and tools to enforce compliance with the configuration	50%	10%	10%	30%	CLARA ROCIO EMMA ESE ANA Specific CCN-STIC guides GOVERNANCE TOOLS (INES)	The organisation must define and implement processes and tools to enforce the configuration. The processes will consider copies of configurations, which will allow us to align both standards. Cloud services shall be bastioned according to the applicable CCN STIC guidelines. System documentation will consider bastioning guidelines and documentation of those tools that help manage potential deviations or vulnerabilities.
op.exp .4	**Maintenance and security updates**	**HIGH***	**BASICS ***	**PARTIAL**	7.13 Equipment Maintenance 8.8 Technical Vulnerabilities	Maintenance process and log Process of identifying technical vulnerabilities, assessing, deploying and controlling. Information on technical vulnerabilities of the information systems in use should be obtained, the organisation's exposure to such vulnerabilities should be assessed, and appropriate measures should be taken.	50%	10%	10%	30%	ANA CLARA ROCIO PILAR GOVERNANCE TOOLS (INES)	Internal procedure for the identification of vulnerabilities in its products and services, considering the asset inventory as a prerequisite, the software supplier, the roles and responsibilities associated with vulnerability management, monitoring, risk assessment - vulnerabilities, updating, tracking and notification, access and disclosure of vulnerabilities including requirements in applicable supplier, support and licensing contracts. An effective technical vulnerability management process should be aligned with incident management, to communicate vulnerability data to incident response and provide technical procedures to be carried out in case an incident occurs. 2.- Vulnerability scanning tools, penetration tests or vulnerability assessments by competent and authorised persons can be used. 3.- The organisation should receive vulnerability reports from internal or external sources; analyse and verify them; develop solutions (updates or patches);

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
												test and deploy to production. 4.- In the case of cloud services, some or even all responsibility is derived to the provider for managing technical vulnerabilities of their services and will include processes for reporting actions to OOPP customers. Change management cannot be isolated in either standard, and the change management cycle itself can be leveraged. If adequate testing of upgrades is not possible, for example due to cost or lack of resources, consideration can be given to delaying deployment to assess the associated risks. 7.- Penetration testing is also a method of identifying vulnerabilities. 8.- When software patches or updates occur, the organisation may consider providing an automated update process where these updates are installed on affected systems or products without the need for end-user intervention.
op.exp.5	**Change management**	**HIGH***	**MEDIUM**	**YES**	8.32 Change management	Changes to the organisation, processes, facilities and information systems should be subject to change management procedures.	50%	10%	10%	30%	GOVERNANCE TOOLS (INES)	In general, both standards require us to have a documented process that will include planning and assessment of the potential impact of changes, communications to stakeholders, testing (in controlled environments) and acceptance of functional and security testing and authorisation of changes. It is undeniable that there will be situations requiring emergency and contingency changes, which will be the exception to the process but will require a full security review afterwards.
op.exp.6	**Protection against malicious code**	**MEDIUM**	**BASICS ***	**YES**	8.7 Protection against malware	Protection against malware must be implemented, including user awareness actions.	10%		0%	90%	µCLAUDIA MARTA MARIA ADA GOVERNANCE TOOLS (INES)	The two standards converge perfectly, although the control needs to be led by the ENS requirements. We must consider the impact of this control on the control [op.exp.4] Maintenance and continuity controls [op.cont]. Consider control [mp.per. 3].
op.exp.7	**Incident management**	**MEDIUM**	**MEDIUM**	**PARTIAL**	5.24 Information security incident management planning and preparation 5.25 Assessment and decision on information security events	In the case of ISO, there are several controls to be considered in order to meet the ENS requirements. 5.24 Information security incident management planning and preparation 5.25 Assessment and decision on information security events 5.26 Responding to information security incidents 5.27 Learning from information security incidents	40%	10%	10%	40%	LUCIA CCN-STIC-817 National Security Framework. Cyber Incident Management GOVERNANCE TOOLS (INES)	Given that there are hierarchical and/or public dependencies, it is necessary to consider the structure of public administrations and central management through the LUCIA platform. We will have to consider different control points to deploy a process that will be aligned with the CCN-STIC 817 Guide and with the National Cyberincident Guide. Consideration should be given to the model of measures to be deployed and especially the resources that may be required. It is advisable that the process be led by ENS in order to comply with both standards.
op.exp.8	**Registration of the activity**	**MEDIUM**	**BASIC (+R3)**	**PARTIAL**	8.15 Registration 8.17	Logs of activities, exceptions, failures, faults and other relevant events must be activated, protected, stored and analysed.	30%	10%	0%	60%	MONICA GLORIA REYES (CARMEN Y LUCIA)	The ENS standard is stricter in terms of requirements than ISO, but it allows us to deploy the process with the security points we need. With regard to events (*), the following should be considered for the General Profile: :

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
					Clock Synchronisation						CCN-STIC-831 Recording of user activity	a) User and administrator authentication events (including access control system alerts and successful and failed logins). b) Events of actions performed on files and objects. c) Upload and download events. d) Events of actions on user accounts.(including creation, modification or deletion of rights or identities) e) Events of actions performed by privileged users. f) All those additional events reflected in the different security policies (including changes in the system configuration; use of utility programs and other applications; activation and deactivation of protection systems, such as antivirus systems and intrusion detection systems). While it is not necessary for the MEDIUM category to automate the review process, it is advisable to have a security information and event management (SIEM) tool or equivalent service to store, correlate, normalise and analyse log information and generate alerts. SIEMs tend to require careful configuration to optimise their benefits. Configurations to consider include identifying and selecting appropriate log sources, tuning and testing rules, and developing use cases. Cloud services should maintain their own activity logging and alert management service. Services dependent on another administration will be the responsibility of that administration. However, it is desirable that they are mapped in the inventory of activity logs. It is recommended that if the OOPP is analysing solutions on the market that cover the requirements of the ENS, it should take into account that they are listed in CCN-STIC-105 ICT Security Products and Services Catalogue 7.2.6 FAMILY: SECURITY EVENT MANAGEMENT SYSTEMS
op.exp.9	**Incident management record**	**MEDIUM**	**MEDIUM**	**PARTIAL**	5.24 Information security incident management planning and preparedness 5.28 Evidence gathering	There shall be a record of incident management activities; as well as guidelines related to the handling of digital evidence (see 5.28) and root cause analysis or post-mortem procedures.	40%		10%	50%	LUCIA CCN-STIC-817 National Security Framework. Cyber Incident Management GOVERNANCE TOOLS (INES)	At a general level ISO is flexible in deploying ENS requirements. To facilitate the recording of accurate information, the use of incident forms is recommended to assist staff in collecting all necessary information. It should be taken into account that for ENS purposes there will be feedback processes with other entities and based on this information the necessary information security events can be reported .
op.exp.10	**Cryptographic key protection**	**MEDIUM**	**MEDIUM**	**PARTIAL**	8.24 Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, must be defined and implemented. The level of protection required derives	40%	10%	10%	40%	CCN-STIC-807 ENS employment cryptology GOVERNANCE TOOLS (INES)	ISO itself refers to legal requirements. In order to implement the organisation's rules for the effective use of cryptography, account must be taken of the legislation and restrictions that may apply to the use of cryptographic techniques and to the problems of transmitting encrypted

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
						from the classification of the information itself both for the type, strength and quality of the cryptographic algorithm required. The organisation will determine the standards to be adopted, as well as the cryptographic algorithms, encryption strength and usage practices, for effective implementation throughout the organisation (which solution is used for which processes).						information. It is therefore necessary for the ENS to address, together with the requirements contained in CCN STIC 807 and CCN STIC 221, the algorithms used. An analysis of the algorithms used should be inventoried and maintained. Services managed by third parties and especially those in the cloud should consider the requirements of this control and the OOPP should check that they are complied with. For the purpose of key managers, CCN-STIC-105 ICT Security Products and Services Catalogue, 7.2.7 FAMILY: CRYPTOGRAPHIC KEY MANAGEMENT DEVICES should be considered.
op.ext.1	**Contracting and service level agreements**	**MEDIUM**	**MEDIUM**	**YES**	5.19 Information security in supplier relationships 5.20 Addressing information security in supplier agreements	Processes and procedures should be identified and implemented to manage information security risks associated with the use of the supplier's products or services. Relevant information security requirements should be established and agreed with each supplier depending on the type of relationship.	70%	10%	10%	10%	GOVERNANCE TOOLS (INES) CCN-STIC-823 Use of cloud services CCN-STIC 821 ENS Guide. Appendix VI. NP 50 Confidentiality agreement for third parties feb-18 ENS. Appendix VII. NP 60 Good practice content template for third parties	At the ENS level, not only the management of security requirements is required, but also the management of service levels and availability, which can have a very direct impact on continuity and service. It is advisable to have a register that traces all affected contracts and allows control of suppliers, their security requirements and access to information and the system. There may be services derived from a higher hierarchical entity and/or public entity. In such a case, the OOPP should consider its needs and document it in order to evidence proper management.
op.ext.2	**Day-to-day management**	**MEDIUM**	**MEDIUM**	**PARTIAL**	5.22 Monitoring, review and change management of supplier services	A process should be in place to manage the relationship between the organisation and the supplier to: monitor and track service performance levels and verify compliance with agreements. Responsibilities for this should be defined.	70%	10%	10%	10%	GOVERNANCE TOOLS (INES) CCN-STIC-844 INES User Manual CCN-STIC-823 Use of cloud services CCN-STIC-815 Indicators and metrics in the ENS CCN-STIC 821 ENS Guide. Appendix VI. NP 50 Confidentiality agreement for third parties feb-18 ENS. Appendix VII.	Their agreements with external parties should be regularly reviewed, validated and updated to ensure that they remain necessary and fit for purpose, and that relevant information security clauses are included. In order to maintain clear compliance with the ENS, regular reports should be required in procurement processes (tender documents and minor contracts) that present indicators and metrics/trends and serve to assess the service, the required agreements and the needs of the given service. These reports should contain general metrics and those that allow reporting through the INES solution.

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
											NP 60 Best practice content model for third parties	
op.ext.3	Supply chain security	HIGH (*)	NA	YES	5.21 Information security management in the ICT supply chain	Processes and procedures should be defined and implemented to address information security risks associated with ICT services and the product supply chain.	70%	10%	10%	10%	GOVERNANCE TOOLS (INES) PILAR INES AMPARO CCN-STIC-823 Use of Cloud Services CCN-STIC 821 ENS Guide. Appendix VI. NP 50 Confidentiality agreement for third parties feb-18 ENS. Appendix VII. NP 60 Good practice content template for third parties	Given the criticality of third-party services and especially the dependencies that can be generated, it is advisable to consider them, at least in the General Profile [GP]. In the entity's risk analysis, services and subcontracting should be considered. The legal requirements involved should be considered. Suppliers [and delegated Agencies or public entities present in the system] should be required to propagate security requirements throughout the supply chain if they subcontract and ICT products should be required to maintain security requirements [op.pl.5] and appropriate security practices throughout the supply chain. Suppliers should be required to provide information on the software components used in the products.
op.ext.4	Interconnection of systems	MEDIUM	MEDIUM *	No	8.23 Segregation in networks	Networks often extend beyond the boundaries of the organisation, as partnerships are formed that require the interconnection or sharing of networks and information, which can increase risk.	50%		10%	40%	GOVERNANCE TOOLS (INES) CCN-STIC-811 Interconnection in ENS	This control is directly required by the ENS and not by ISO. It is referable to other controls to demonstrate compliance. An updated diagram and prior authorisation must be maintained, and analysis of the security and data protection requirements and the nature of the information exchanged.
op.nub.1	Protection of cloud services	MEDIUM	BASIC	PARTIAL	5.23 Information security for the use of cloud services	Processes and procedures should be defined and implemented to address information security risks associated with ICT services and the product supply chain.	60%	10%	0%	30%	GOVERNANCE TOOLS (INES) CCN-STIC-823 Use of Cloud Services	The ISO requirements are closely aligned with the ENS. Information describing the software components should be collected from the provider. Cloud services should consider the requirements derived from the relevant CCN Guidelines. Solicitation documents and minor contracts should be considered for compliance with this control.
op.cont.1	Impact analysis	MEDIUM	MEDIUM	YES	5.29 Information Security during Disruption 5.30 ICT Business Continuity Preparedness	As part of the impact analysis, the consequences of loss of confidentiality and integrity of information must be considered and prioritised, in addition to the need to maintain availability.	70%	10%	10%	10%	GOVERNANCE TOOLS (INES) CCN-STIC 470 User Manual PILAR. Business Impact and Continuity Analysis PILAR.	Services and criticalities must be considered, allowing for the detection of RTOs and RPOs. The consequences of loss of confidentiality and integrity of information must be considered and prioritised, in addition to the need to maintain availability. High impacts and low probability (output of the risk analysis [op.pl.1]) should help in preparing contingency situations.
op.cont.2	Continuity plan	HIGH *	NA	YES	5.29 Information Security during Disruption 5.30 ICT Business	The organisation should plan how to maintain information security at an appropriate level during the disruption.	70%	10%	10%	10%	CCN-STIC 470 User Manual PILAR. Business Impact and	It must be known which information security controls, systems and supporting tools must be prepared for a catastrophic event. Consideration should be given to security controls that will not operate

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
					Continuity Preparedness						Continuity Analysis PILLAR GOVERNANCE TOOLS (INES)	during an outage and compensating controls for information security controls that cannot be maintained during the outage.
op.cont.3	Periodic testing	HIGH *	NA	YES	5.30 ICT Preparedness for Business Continuity	ICT preparedness should be planned, implemented, maintained and tested against business continuity objectives and ICT continuity requirements.	70%	10%	10%	10%	CCN-STIC 470 User Manual PILAR. Business Impact and Continuity Analysis PILLAR GOVERNANCE TOOLS (INES)	The need for ICT preparedness for business continuity can result from risk assessments. The assessment should include all types of scenarios, including those with high impact and low probability, often called extreme but plausible scenarios. It is important to consider the continuity testing associated with OOPP services, to plot timelines and to analyse deviations. Testing can be considered from different perspectives, both mock and paper tests.
op.cont.4	Alternative MEDIUM	HIGH *	NA	PARTIAL	8.14 Redundancy of information processing facilities	Information processing facilities must be implemented with sufficient redundancy to meet availability requirements.	70%	10%	10%	10%	CCN-STIC 470 User Manual PILAR. Business Impact and Continuity Analysis PILLAR GOVERNANCE TOOLS (INES)	The scope of the ENS will be limited to the requirements of the ISO control itself as it will be limited to facilities. The organisation must design and implement a systems architecture with adequate redundancy to meet these requirements. Cloud services enable compliance with this control.
op.mon.1	Intrusion detection	MEDIUM	MEDIUM	PARTIAL	8.21 Security of network services	Network services include the provision of connections, private network services and managed network security solutions such as firewalls and intrusion detection systems. These services can range from simple unmanaged bandwidth to complex measures.	20%		10%	70%	GOVERNANCE TOOLS (INES) CCN-STIC-811 Interconnection in the ENS CCN-STIC-816 Security in Wireless Networks in the ENS	Network services are for the most part covered by the infrastructure manager who will provide these tools to the network. OOPPs should provide evidence of the existence of this infrastructure responsibility. Cloud services include this required item.
op.mon.2	Metrics system	MEDIUM	MEDIUM	PARTIAL	9 - Performance assessment 9.1 - Monitoring, measurement, analysis and evaluation.	The organisation should assess information security performance and the effectiveness of the information security management system. Metrics can be used for both systems, but for the purposes of ISO , they should include the monitoring of security objectives.	80%		10%	10%	GOVERNANCE TOOLS (INES) CCN-STIC-815 Indicators and metrics in the ENS CCN-STIC-844 INES user manual CCN-STIC-808 Verification of compliance with measures in the ENS	ENS criteria should be imposed to collect the metrics required for the INES security report. In addition, it is advisable to take into account the maturity level and implementation level metrics in accordance with CCN-STIC Guide 808. The entity could deploy in the system a catalogue of general metrics associated to a Statement of Applicability and extend measurements to ISO security controls and objectives. To achieve equivalence, appropriate security objectives and metrics should be considered.

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
op.mon.3	**Surveillance**	**MEDIUM**	**BASIC (+R1)***	**YES**	5.7 Threat intelligence 8.16 Monitoring activities	Information related to security threats will be collected and analysed to generate intelligence	20%		10%	70%	GOVERNANCE TOOLS (INES) ANA GLORIA ESE CARMEN Specific CCN-STIC guides	Monitoring solutions will be available to determine the exposure surface in relation to vulnerabilities and configuration deficiencies. This can be done by deploying functions through CCN solutions or, where appropriate, CVE analysis through official sources and lists. For example, vulnerability alerts can be logged and analysed in the system, and impacts and risks can be analysed. Many of the services depend on the superior hierarchical entity and/or public entity, so it is difficult to manage this control directly. In other cases, the information is provided by independent suppliers or consultants, control authorities or threat intelligence expert groups. For ISO we speak of threat intelligence and it requires connection with controls 5 .25 Security events, 8.7 Protection against malware, 8.16 Monitoring or 8.22 Web filtering, to maintain the quality of threat intelligence.
mp.if.1	**Separate and access-controlled areas**	**MEDIUM**	**MEDIUM**	**YES**	7.1 Physical security perimeter	There shall be security perimeters, in areas with protection according to the information and/or assets they contain.	10%	0%	10%	80%	GOVERNANCE TOOLS (INES)	It is more than feasible that the DPC is owned by a higher hierarchical entity and/or another public entity, so these controls for the DPC are not the responsibility of the OOPP. In any case, services contracted to a provider will involve these measures, which will be required in the procurement process. A key management protocol may be considered as a procedure to manage these physical elements or the combination locks of the offices, rooms and facilities involved.
mp.if.2	**Identification of persons**	**MEDIUM**	**MEDIUM**	**YES**	7.2 Physical input controls	Separation of delivery and loading and unloading areas. Visitor control, including supplier personnel, inspection of deliveries and delivery notes. Monitoring of technical access control processes.	30%	0%	0%	70%	GOVERNANCE TOOLS (INES)	It is more than likely that the DPC is owned by a higher hierarchical entity and/or public entity, so these controls are not the responsibility of the OOPP. In any case, services contracted to a provider will involve these measures, which will be required in the contracting process.
mp.if.3	**Fitting out the premises**	**MEDIUM**	**MEDIUM**	**PARTIAL**	7.8 Location and protection of equipment	7.3 Securing of offices, rooms and facilities 7.8 Location and protection of equipment 7.12 Security of cabling	10%	0%	10%	80%	GOVERNANCE TOOLS (INES)	Reliance on higher hierarchical and/or other public entities and key suppliers to fulfil this control should be considered. Compliance with this control through ISO relies on several controls. Thus control 7.8 Location and protection of equipment refers to the need to deploy controls to minimise the risk of potential physical and environmental hazards; for example, theft, fire, explosives, smoke, water or water supply failure, dust, vibration, chemical effects, power supply interference, communications interference, electromagnetic radiation and vandalism; or risks arising from environmental conditions, such as temperature and humidity, which should be monitored to detect conditions that may adversely affect the operation of information processing facilities.
mp.if.4	**Electric power**	**MEDIUM**	**MEDIUM ***	**YES**	7.11 Supporting utilities	Information processing facilities must be protected against power outages and other	10%	0%	10%	80%	GOVERNANCE TOOLS (INES)	Dependence on higher hierarchical entities and/or other public entity and key suppliers to fulfil this control should be considered.

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
						disruptions caused by failures in support services.						With the available information we should deploy the risk analysis and consider the impacts.
mp.if.5	**Fire protection**	**MEDIUM**	**MEDIUM**	**YES**	7.5 Protection against physical and environmental threats	Protection against physical and environmental hazards, such as natural disasters and other intentional or unintentional physical threats to infrastructure, must be designed and implemented.	10%	0%	10%	80%	GOVERNANCE TOOLS (INES)	Dependence on higher hierarchical entities and/or other public entity and key suppliers to fulfil this control should be considered. With the available information we should deploy the risk analysis and consider the impacts.
mp.if.6	**Flood protection**	**MEDIUM**	**MEDIUM**	**YES**	7.5 Protection against physical and environmental threats	Protection against physical and environmental hazards, such as natural disasters and other intentional or unintentional physical threats to infrastructure, must be designed and implemented.	10%	0%	10%	80%	GOVERNANCE TOOLS (INES)	Outside the premises the OOPP may consider having plans that identify downspouts and other similar elements. The OOPP can understand the impact on the position of the office by analysing geographical areas that have been previously flooded by existing official statistics. https://www.miteco.gob.es/es/agua/temas/gestion-de-los-riesgos-de-inundacion/snczi/
mp.if.7	**Check-in and check-out of equipment**	**MEDIUM**	**MEDIUM**	**YES**	7.2 Physical input controls	Secure areas should be protected by appropriate entry controls and access points.	10%	0%	10%	80%	GOVERNANCE TOOLS (INES)	In addition to the registration itself, other complementary measures should be considered, such as controlled access to loading and unloading areas and the design of these areas so that equipment and goods can be loaded and unloaded without delivery personnel gaining unauthorised access to other parts of the building; DPC operators should be required to have OOPP personnel present or incoming deliveries checked against the delivery note, analysed for evidence of package tampering and if necessary inspected for hazardous materials. Entries must be traced to asset management [op.exp.1] and ISO 5.9 and 7.10.
mp.per.1	**Job characterisation**	**MEDIUM**	**MEDIUM**	**YES**	6.1 Screening	Background checks on all candidates to become staff should be carried out prior to joining the organisation and on an ongoing basis in accordance with laws, regulations and code of ethics, and be proportionate to the objectives of the organisation, the classification of information being accessed and the perceived risks. This control should be complemented by 6.2 Terms and Conditions of Employment	10%		90%	0%	GOVERNANCE TOOLS (INES)	All the provisions described above are aligned with Annex I - Article 1.1 of the Delegated Regulation (EU) 2022/127 (Point B)) . In addition, other measures have to be considered such as training actions (fraud), rotation policy, measures against conflict of interest (position of responsibility; sensitive position related to verification, authorisation, payment execution and accounting),...
mp.per.2	**Duties and obligations**	**MEDIUM**	**BASIC**	**PARTIAL**	6.2 Terms and conditions of employment	The agreements should set out the responsibilities of staff and the organisation for information security. This control should be complemented by 6.4 Disciplinary process	60%		40%	0%	GOVERNANCE TOOLS (INES) CCN-STIC Guide 821 National Security Framework. Security standards	An Onboarding or Welcome to users (including supplier personnel) can be prepared which includes all the information required for access and operation of the system, and of the information / services. In relation to the express confirmation, the Particular Profile [PP] will be less strict, with evidence of sending and receiving the relevant e-mails being sufficient. Control [org.2] should be considered. Different means can be deployed to enable compliance with this control (employee portal or system banners informing on equipment start-up, among others).

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
mp.per .3	Awareness-raising	MEDIUM	MEDIUM	YES	6.3 Information security awareness, education and training	Organisational staff and relevant stakeholders should receive appropriate information security awareness, education and training and regular updates of the organisation's policies and procedures, as appropriate to their role. This control should be complemented by control 5.24 Information security incident management planning and preparedness.	80%		10%	10%	GOVERNANCE TOOLS (INES) ATENEA VANESA ELENA	OOPPs should have a plan in place that considers innovative actions for awareness-raising. It can use different means of delivery, including online classroom or webinar based, web-based information, and others. Technical staff should keep their knowledge up to date by subscribing to newsletters and magazines or attending conferences and events aimed at technical and professional improvement. ** The awareness programme should include a range of activities through appropriate channels, such as campaigns, brochures, posters, newsletters, websites, briefings, learning modules and emails. Staff understanding should be assessed at the end of an awareness-raising activity. The CCN has tools that can help with this and so do other security authorities (INCIBE, ENISA...).
mp.per .4	Training	MEDIUM	MEDIUM	YES	6.3 Information security awareness, education and training	Organisational staff and relevant stakeholders should receive appropriate information security awareness, education and training and regular updates on organisational policies and procedures, as appropriate to their job function.	80%		10%	10%	GOVERNANCE TOOLS (INES) ATENEA VANESA ELENA	The OOPPs must have an appropriate training plan and monitor the effectiveness of the actions deployed. The CCN has tools that can help with this and so do other security authorities (INCIBE, ENISA...) The personnel of suppliers or public entities must be trained in security, and it is their responsibility to implement them.
mp.eq. 1	Uncluttered workstation	MEDIUM	MEDIUM	YES	7.7 Uncluttered desktop and clean screen	Clear rules for desk, paper and storage and/or removable MEDIUM, as well as rules for clean screens in the agency's premises should be defined and enforced.	100%		0%	0%	GOVERNANCE TOOLS (INES)	The two standards are clearly synergistic, so the OOPP should consider the protection of information (especially that which, due to the functions performed, must be subject to confidentiality or is considered sensitive or critical). Consideration should be given to the security of information on paper or on storage MEDIUM such as USB or similar, and should seek to archive it in places with operational locks, under lock and key (safe, cabinet or filing cabinet or other security furniture) when the need for its use has ceased and when control over it cannot be maintained (e.g. absences or the office is unoccupied). This measure should be aligned with [org.2] and 5.10 Acceptable use of information and other associated assets and 5.36 Compliance with policies and standards for information security. Awareness raising actions should address this measure.
mp.eq. 2	Workplace blocking	HIGH *	MEDIUM	YES	7.7 Uncluttered desktop and clean screen	Clear rules for desk, paper and storage and/or removable MEDIUM, as well as clear rules for clean screens on the agency's premises should be defined and enforced.	70%		0%	30%	GOVERNANCE TOOLS (INES) CLARA	This necessarily implies that equipment and devices and services must be disconnected or protected with a locking mechanism controlled by a password, token or user authentication mechanism. All equipment and devices and services must be configured with an automatic time-out or log-off function. The OOPP should at least, deploy this policy in the directory and deploy it from the basestate, develop a Technical Instruction that elaborates it on other system elements/devices, and check the effectiveness from time to

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
												time. For example, you can proceed from time to time to test by CLARA the implementation on the equipment. SaaS services should deploy this measure in identical terms, so providers should be required to be present and check its applicability. In any case, users should be aware of the need to block sessions on computers, devices and services when they leave the workstation, even if only for a limited period of time.
mp.eq.3	**Protection of portable devices**	**HIGH**	**BASIC (+R2)**	**PARTIAL**	7.9 Security of off-site assets 8.1 User devices	Off-site assets must be protected taking into account the different risks. Information stored, processed or accessible through user devices must be protected.	70%		0%	30%	GOVERNANCE TOOLS (INES) CLARA CCN-STIC-105 Catalogue of ICT Security Products and Services	This measure connects directly to the controls [op.exp.1]. It is possible that the entire operational inventory is managed or shared by another public asset management agency. In addition, special consideration should be given to security incident management [op.exp.7], (5.24, 5.26) together with access control from outside controlled areas [op.acc.6]. [op.acc.6.r8.1] Access from or through uncontrolled areas shall require two-factor authentication. Reinforcement R9-Remote Access (all levels).[op.acc.6.r9.1] The Information Systems Interconnection ITS shall apply. [op.acc.6.r 9.2] Remote access shall consider the following aspects: a) Be authorised by the appropriate authority. b) Traffic shall be encrypted. c) If usage is not constant, remote access shall be disabled and enabled only when necessary. d) Audit trails shall be collected for such connections. Encryption should be considered, as indicated in R1 - Disk Encryption, if the information inventory indicates that the information is of MEDIUM level. In this case, CCN-STIC-105 ICT Security Products and Services Catalogue 7.5.1 FAMILY: DATA ENCRYPTED STORAGE shall be considered. Likewise, when the equipment contains information that for reasons of the functions performed by the OOPP can be considered critical and HIGH, it shall be kept Reinforcement R2 - Protected environments [mp.eq.3.r1.1] The use of portable equipment outside the organisation's facilities shall be restricted to protected environments, where access is controlled, safe from theft and prying eyes. Good security practices contained in ISO 27002 are of interest, in particular: a) Have a register of user devices with identification of the physical and logical protection requirements for each device. b) Restriction of software installation (e.g. remotely controlled by system administrators); c) Requirements for device software versions and for applying updates (e.g. active automatic update); d) Identification and pre-approval of rules for connection to services,

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
												public networks or any other off-site network (e.g. requiring the use of a personal firewall); e) Encryption of storage devices; f) Protection, detection and response against malware (e.g. use of specific anti-malware); g) Remote deactivation, removal or blocking; h) Full equipment backups, including configuration; i) Encouraging the use of SaaS services and applications; j) Analysis of end-user behaviour; k) Controlled use of removable devices and ability to disable USB ports; i) Use of partitioning capabilities, if supported by the device, that can securely separate organisational information and other associated assets (e.g. software) from other information and other associated assets on the device.
mp.eq.4	**Other devices connected to the network**	**MEDIUM**	**BASICS ***	**PARTIAL**	8.1 User devices	Consider the process of configuration and safe handling by users	60%		40%	0%	GOVERNANCE TOOLS (INES) CCN-STIC-105 Catalogue of ICT Security Products and Services	This control necessarily implies considering these devices in [op.exp.2] and [op.exp.3] and maintaining the necessary checks. R1 will be excluded as it is not covered by the ISO, but when renewal and tendering processes are initiated under the competence of the OOPP, the suitability of the device will be analysed.
mp.com.1	**Secure perimeter**	**MEDIUM**	**MEDIUM**	**PARTIAL**	8.20 Network controls 8.21 Security of network services	Security mechanisms, service levels and network service requirements must be identified, implemented and monitored.	10%		20%	70%	ROCIO EMMA GOVERNANCE TOOLS (INES) CCN-STIC 816 Security in Wireless Networks in the ENS CCN-STIC-811 Interconnection in the ENS	Network services include the provision of connections, private network services and managed network security solutions such as firewalls and intrusion detection systems. These services can range from simple unmanaged bandwidth to complex services. You may be dependent at the network level on a public entity and may not be able to manage this control. It is recalled that all network devices are involved in the bastioning process [op.exp.2][op.exp.3]. At SaaS / IaaS service level (and Cloud in general) the provider must be held responsible for compliance. At equipment level, the firewall shall be deployed in local mode of the user equipment.
mp.com.2	**Protection of confidentiality**	**MEDIUM**	**MEDIUM**	**PARTIAL**	8.20 Network controls 8.21 Security of network services	Security mechanisms, service levels and network service requirements must be identified, implemented and monitored.	10%		20%	70%	EMMA GOVERNANCE TOOLS (INES) CCN-STIC-836 ENS - VPN Security CCN-STIC-807 Cryptology of use in ENS	The organisation must ensure that appropriate security controls are applied to the use of virtualised networks, including SDN, SD-WAN. Different modalities should be considered, VPN TLS, IPSEC, MACSEC, WIREGUARD. Encryption algorithm recommendation 128 symmetric encryption. AES All networks shall be inventoried and VPNs shall be monitored, managed and disabled when no longer needed. The provisions of [op.acc.6] shall be taken into account. Reinforcement R9-Remote access (all levels).[op.acc.6.r9.1] The ITS for Information Systems Interconnection shall apply. [op.acc.6.r 9.2] Remote access shall consider the following aspects: a) Be

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
												authorised by the appropriate authority. b) Traffic shall be encrypted. c) If usage is not constant, remote access shall be disabled and enabled only when necessary. d) Audit logs shall be collected for such connections.
mp.com.3	Protection of integrity and authenticity	MEDIUM	MEDIUM	PARTIAL	8.20 Network controls 8.21 Security of network services	Security mechanisms, service levels and network service requirements must be identified, implemented and monitored.	10%		20%	70%	EMMA GOVERNANCE TOOLS (INES) CCN-STIC-836 ENS - VPN Security CCN-STIC-807 Cryptology of use in ENS	The organisation must ensure that appropriate security controls are applied to the use of virtualised networks, including SDN, SD-WAN. Different modalities should be considered, VPN TLS, IPSEC, MACSEC, WIREGUARD. Since ISO is flexible in incorporating requirements from national regulations, requirements are derived from CCN- STIC Guidelines 836 and 807. 128 symmetric encryption algorithm recommendation. AES All networks shall be inventoried and VPNs shall be monitored, managed and disabled when no longer required. The provisions of [op.acc.6] shall be taken into account. Reinforcement R9-Remote access (all levels).[op.acc.6.r9.1] The ITS for Information Systems Interconnection shall apply. [op.acc.6.r 9.2] Remote access shall consider the following aspects: a) Be authorised by the appropriate authority. b) Traffic shall be encrypted. c) If usage is not constant, remote access shall be disabled and enabled only when necessary. d) Audit logs shall be collected for such connections.
mp.com.4	Separation of information flows in the network	MEDIUM	MEDIUM	PARTIAL	8.23 Segregation in networks	Same security criteria for ISO as ENS, in that networks must be divided into separate network domains and separated from the public network (i.e. Internet). Groupings can be made by trust, criticality, sensitivity, organisation... and by physical or logical network.	10%		20%	70%	EMMA GOVERNANCE TOOLS (INES) CCN-STIC-836 ENS - VPN Security CCN-STIC-807 Cryptology for use in the ENS CCN-STIC-811 Interconnection in the ENS	It is possible that operations and management are dependent at the network level, on a hierarchically superior public entity and/or another public entity and this control cannot be managed by the OOPP. Therefore, the request for segmentation and the precise and updated information shall be stated in the OOPP network diagram [op.pl.2] . When for reasons of size and capacity, segregation for control purposes cannot be managed, VLANs for an administration network and an OOPP internal user network shall be sufficient. See requirements in CCN STIC Guide 836.
mp.si.1	Marking of supports	MEDIUM	MEDIUM	YES	5.13 Labelling of information	An appropriate set of procedures for labelling information in accordance with the information classification Framework adopted by the organisation must be developed and implemented.	100%		0%	0%	GOVERNANCE TOOLS (INES)	The entity shall deploy a process associated with [mp.info.2] and consider the corresponding operating procedures [org.3]. The staff concerned (in-house or external) shall be trained for this purpose [mp.per.4] Consideration shall be given to the necessary labelling and how to place it on paper and digital documents (metadata). This control shall be linked to the control [mp.info.5]. The two standards are perfectly cohesive and controls can be linked to comply with both.
mp.si.2	Cryptography	MEDIUM (+R2)*	BASICS*	PARTIAL	7.10 Storage MEDIUM	Storage MEDIUM should be managed throughout their life cycle; acquisition, use, transport and disposal, in accordance with	50%	10%	0%	40%	GOVERNANCE TOOLS (INES) CCN-STIC-105	The organisation shall establish a specific policy on the management of removable MEDIUM and communicate this policy to anyone using or handling removable MEDIUM. As a general measure, it should be

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
						the organisation's classification Framework and usage requirements.					Catalogue of ICT Security Products and Services CCN-STIC-807 Cryptology for use in the ENS	considered that removable MEDIUM ports, e.g. SD card slots and USB ports, should only be enabled if there is an organisational reason for their use. Devices leaving the premises should be encrypted, especially if they are copies. Given that they may depend on a superior hierarchical entity and/or public entity, this control can be delegated to the same or to the provider that manages this activity in the DPC. This measure can be excluded if there are no affected devices and the OOPP uses cloud storage services that avoid local storage. The requirement given by the CCN-STIC Guide 807 Cryptology for use in the ENS and/or CCN-STIC Guide 221 should be considered.
mp.si.3	**Custody**	**MEDIUM**	**MEDIUM**	**YES**	7.10 Storage MEDIUM	Storage MEDIUM should be managed throughout their life cycle, acquisition, use, transport and disposal, in accordance with the organisation's classification Framework and usage requirements.	70%		20%	10%	GOVERNANCE TOOLS (INES)	The organisation should establish a specific policy on the management of removable MEDIUM and communicate this policy to anyone using or handling removable MEDIUM, require authorisation for the MEDIUM and keep a record. Storage in fireproof boxes may be established and should be mapped against manufacturers' instructions and the retention point that allows for fire resistance. The manufacturers' instructions on temperature and humidity must be taken into consideration, so the corresponding technical data sheets will form part of the system documentation [org.3]. Those good practices described in ISO 27002 that can enrich this control for OOPP shall be deployed. For example; all MEDIUM should be stored in a secure and protected environment according to their information classification and protected against environmental threats (such as heat, humidity, electronic field or ageing), according to manufacturers' specifications; to mitigate the risk of MEDIUM degradation while the stored information is still needed, the information should be transferred to new MEDIUM before it becomes unreadable.
mp.si.4	**Transport**	**MEDIUM**	**MEDIUM**	**YES**	7.10 Storage MEDIUM	Storage MEDIUM must be managed throughout their life cycle, acquisition, use, transport and disposal, in accordance with the organisation's classification Framework and usage requirements.	70%		20%	10%	GOVERNANCE TOOLS (INES)	The organisation must establish a specific policy on the management of removable MEDIUM and communicate this policy to any person who uses or handles removable MEDIUM, requiring authorisation and being supervised by the Systems Manager, who will control the register of entries and exits and analyse the coherence of their entries. In general, elements with information catalogued as OFFICIAL USE shall be protected and subject to encryption if the sensitivity of the information so determines. ENS requirements and ISO best practices can be grouped under a single process. Thus we may consider where

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
												appropriate in the OOPP, the following guidelines; a) use trusted or properly accredited carriers or couriers, creating a list of authorised couriers; b) develop procedures to verify the identification of couriers; c) packaging should be sufficient to protect the contents from any physical damage that may arise during transit, protecting against any environmental factors, such as exposure to heat, moisture or electromagnetic fields; d) use tamper-proof or tamper-evident controls.
mp.si.5	**Deletion and destruction**	**MEDIUM**	**MEDIUM**	**YES**	7.14 Safe disposal or re-use of equipment 8.10 Disposal of information	Items likely to be storage MEDIUM should be reviewed to ensure that all confidential data and licensed software has been securely removed or overwritten prior to disposal or reuse. Information stored on information systems and devices should be deleted when no longer required.	80%		10%	10%	GOVERNANCE TOOLS (INES) OLVIDO CCN-STIC-105 Catalogue of Information and Communication Technologies Security Products CCN-STIC-140 Reference Taxonomy for ICT Security Products (Annex E3 and E3M)	The organisation must establish a specific policy on the management of removable MEDIUM and communicate this policy to anyone using or handling removable MEDIUM. For the use of erasure elements, the recommendations of the CCN and the tools contained in the CCN STIC 105 Catalogue should be considered. Proposals derived from ISO 27040 may be used. Where appropriate, it may be important to bear in mind complementary measures considering the security threats and requirements present in the CCN-STIC-140 Reference Taxonomy for ICT Security Products - Annex E.3: Secure Erasure Tools and Annex E.3M: Secure Erasure Tools. In SaaS (and Cloud services in general), the use of secure erasure processes and accreditations to that effect shall be required. If providers are contracted to carry out deletion and elimination processes, evidence of the security of the service and certification of the effectiveness to that effect must be required. When the MEDIUM is reused, effective erasure must be carried out to prevent access to the information. For secure disposal of MEDIUM, incineration or shredding is an option. The results of disposal and erasure should be recorded as proof and evidence.
mp.sw.1	**Application development**	**MEDIUM**	**MEDIUM**	**YES**	8.25 Secure development lifecycle	Rules for the safe development of software and systems must be established and applied.	20%	20%	20%	40%	GOVERNANCE TOOLS (INES) CCN STIC 422 Secure Web Application Development	At the level of the ENS, control should be considered only in case the OOPP proceeds with development for the own services derived from its nature. Otherwise it does not apply. It is possible that certain electronic services are in SaaS mode or that the responsible party is a superior hierarchical entity and/or public entity, in both cases, the control will derive in its compliance to them. For ISO purposes, this control should be complemented by other controls in more detail. a) separation of development, test and production environments (see 8.31);

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
												b) guidance on security in the software development lifecycle: software development methodology (see 8.28 and 8.27); secure coding guidelines (see 8.28); c) security requirements in the specification and design phase (see 5.8); d) security checkpoints within project milestones (see 5.8); e) system and security testing, such as regression testing, code scanning and penetration testing (see 8.29); f) secure repositories for source code and configuration (see 8.4 and 8.9); g) security in version control (see 8.32); h) required application security knowledge and training (see 8.28); i) developers' ability to prevent, find and fix vulnerabilities (see 8.28); j) licensing requirements and alternatives to ensure cost-effective solutions and avoid future licensing problems (see 5.32).
mp.sw.2	**Acceptance and commissioning**	**MEDIUM**	**MEDIUM**	**PARTIAL**	8.29 Developmental safety and acceptance testing	Security testing processes should be defined and implemented in the development lifecycle. This control should be complemented by the 8.31 Separation of development, test and production environments.	50%		20%	30%	GOVERNANCE TOOLS (INES) CCN STIC 422 Secure Web Application Development	Important to maintain separate test, development and [pre]production environments. Functional and security testing, e.g. user authentication and access restriction and use of cryptography, should be performed. It is possible that certain e-services may be in SaaS mode or the responsible party may be a higher hierarchical entity and/or public entity, as in both cases, control will derive in their compliance to them. In addition, secure coding and secure configurations, including that of operating systems, firewalls and other security components, should be performed . code review activities to test for security flaws, perform vulnerability scans to identify insecure configurations and system vulnerabilities, and perform penetration testing to identify insecure code and design.
mp.info.1	**Personal data**	**MEDIUM**	**MEDIUM**	**YES**	5.34 Privacy and Protection of Personally Identifiable Information (PII)	The organisation shall identify and comply with requirements related to the preservation of privacy and the protection of personal information in accordance with applicable laws and regulations and contractual requirements.	50%	30%	10%	10%	GOVERNANCE TOOLS (INES)	Consideration should be given to the obligations arising from the European legislator and the need for compliance. It is possible that part of these obligations are shared with a hierarchically superior public agency and/or public entity or that it assumes certain roles. Furthermore, it is necessary that processing tasks and co-responsibilities are considered and the obligations are properly regulated.
mp.info.2	**Qualification of information**	**MEDIUM**	**MEDIUM**	**YES**	5.12 Classification of information	It can be mapped to the specific requirements of the ENS and compliance with the two standards can be derived from it.	80%	10%	10%	0%	GOVERNANCE TOOLS (INES)	The qualification policy will determine the criteria that will determine the level of security required, within the operational regulatory framework in OOPP and, where appropriate, considering in general terms the criteria described in Annex I of Royal Decree 311/2022. The sensitivity of the information will be considered and, based on this, the OFFICIAL USE will be assigned. The person responsible for each piece of information will be in charge of assigning the required level of security to each piece of information, and

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
												of its documentation and formal approval. He/she will have the exclusive power to modify the security level at any time. It is important to consider that the entity is going to generate exchanges with other entities and must include the qualification Framework in the agreements, implying the security measures that derive from it. In the case of ISO, it integrates perfectly with the legal requirements deployed by the ENS, so that requirements can be unified.
mp.info.3	**Electronic signature**	**MEDIUM**	**MEDIUM**	**No**	8.24 Use of cryptography 8.26 Application Security Requirements	This is not an ISO specific control, but we associate it with certain controls. When a trusted authority is used (e.g. for the purpose of issuing and maintaining digital signatures or certificates), security is embedded in the whole end-to-end signature or certificate management process.	20%	10%	70%	10%	GOVERNANCE TOOLS (INES) LORETO CCN-STIC-807 Cryptology for use in the ENS CCN-STIC-140 Reference Taxonomy for ICT Security Products	ISO does not consider this control, but it can be associated to controls 8.26 and 8.24. It is important that the OOPP deploys a policy or is attached to that of the superior administrative entity. It is important that the custody and use of the signature is managed. In this environment, special consideration will be given to cloud services and specific agreements with other public entities or third parties may need to be deployed. HSM services may be deployed, which should be ENS-compliant. Within the same, consideration should be given to the processes in which signature verification must be maintained and therefore deploy preservation environments, which allow for such verification. These environments can be in an in-house or third-party service. Although not applicable, the OOPP may deploy certified components according to [op.pl.5].
mp.info.4	**Time stamps**	**HIGH**	**NA**	**No**	8.24 Use of cryptography 8.26 Application Security Requirements	This is not a specific ISO control, but we associate it with certain controls We consider the cryptographic elements and specifically the synchronisation of clocks and time accreditation of acts.	50%		40%	10%	GOVERNANCE TOOLS (INES)	ISO does not consider this control, but it can be associated with the referenced ones. This control only applies to OOPPs managing grants above 400 million, due to their involvement and criticality. Qualified electronic time stamps" shall be used in accordance with the provisions of Regulation (EU) No 910/2014.
mp.info.5	**Cleaning of documents**	**MEDIUM**	**MEDIUM**	**No**	5.13 Labelling of information	This control is not explicitly covered by the standard, but can be considered in the derived control of labelling of digital documents and the use of metadata for this purpose.	80%		0%	20%	GOVERNANCE TOOLS (INES) CCN-STIC Guide 835 Erasure of metadata in the framework of ENS	This control is connected to control [org.2] and [mp.si.1] and [mp.info.2]. Training and awareness-raising actions should be maintained for the purposes of [mp.per.3] and [mp.per.4]. Although ISO does not expressly contemplate this control, references to metadata management can be seen in control 5.13 and as good practices can complement the provisions of ENS.
mp.info.6	**Back-up copies**	**MEDIUM (+R2) ***	**BASICS***	**YES**	8.13 Backing up information	Back-up copies will cover information, software, configuration and overall systems and should be maintained and tested regularly in accordance with the agreed subject-specific backup policy.	30%		10%	60%	GOVERNANCE TOOLS (INES) CCN-STIC-822 ENS Security Procedures . Annex III .PR 30 Procedure for the generation of backup copies and	For ISO purposes there is an appropriate equivalence in that operational control 8.13 aligns with [mp.info.6]. It is important to note that this control is associated with continuity and for ISO this is significant, as OOPPs will need to be aware of this in order to meet the requirements of the standard. The establishment of a backup policy that considers the organisation's information security and data retention requirements is necessary. Backup facilities for information and software should be considered. The copying process and its timing and retention shall be aligned with legal requirements, specifically those specific to the nature of the OOPP and the personal

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
											recovery of information.	information it contains. Information related to the entire copying process, including the software used, processes, reviews... A protocol for simple restores should be available and can be aligned with the control [op.cont.3] and considered as continuity tests. This control may be delegated to a provider or a public entity when there are elements or services for which they are responsible. Certain copy processes associated with elements of the infrastructure/architecture may be the responsibility of a hierarchically superior public entity and/or public entity or even a provider. Cloud services should assume and evidence the copy and restore processes, maintaining the corresponding agreements. In general, it is recommended not to allow the process of local storage, avoiding that information and certain services are excluded from the copy policy.
mp.s.1	**Protection of electronic mail**	**MEDIUM**	**MEDIUM**	**PARTIAL**	5.14 Transfer of information	Information transfer rules, procedures or agreements should be in place, both within the organisation and between the organisation and other parties, for all types of information transfer.	40%	10%	0%	50%	GOVERNANCE TOOLS (INES) CCN-STIC Guide 814 Security in mail CCN-STIC-821 Security Standards in the ENS - ENS. Appendix III. NP 20 Access rules for Electronic Mail (E-Mail)	For ISO it is mostly about exchange or transfer of information, in addition to electronic means which is where the mail service is included, the OOPP should include guidelines related to means of information transmission (not only email, but other means, including physical means and verbal transmission) that will enrich the ENS security guidelines. Consider social engineering actions that can help raise awareness [mp.per.3].
mp.s.2	**Protection of web services and applications**	**MEDIUM**	**MEDIUM**	**PARTIAL**	8.26 Application security requirements	Information security requirements should be identified, specified and approved when developing or acquiring applications.	40%		20%	40%	ANA GOVERNANCE TOOLS (INES) CCN-STIC-812 Security in web services CCN-STIC-823 Use of Cloud Services	This control may be delegated to a hierarchically superior entity and/or public entity or to a service provider with specific services or even to the web service provider. It is recommended to include in the contracts and conditions of the tender documents the requirement to carry out the analysis and the action plans resulting from such analysis. The services contracted to third parties must contain the measures required in this control and specifically the obligation to correct the vulnerabilities detected in the platforms through the security analyses. The OOPP shall have an audit plan reflecting the estimated dates of execution of the audits and the reference of the entity (public or private) in charge of the audit. There is no level of equivalence with respect to the requirements established by the standards, given that the ENS is rigorous and specific. However, ISO allows these requirements to be deployed and the system and the statement of applicability to be adjusted for harmony. It will be traced with the audit and review plan and linked with the management of action plans derived from the

ENS				ISO equivalence level	Associated ISO control	ISO remarks	Responsibilities				CCN	CONCLUSIONS
Control		Cat. Applicable PG	Cat. Applicable PP				OOPP	OODD	Superior Public Entity /CA / OOCC	Supplier	Tool / GUIDE	
												security of web applications/published items. Applications accessible over networks are subject to a variety of threats, so consider security requirements that are scattered throughout the ISO, such as access management through authentication (see 5.17, 8.2, 8.5); resilience against malicious attacks or unintentional interruptions (e.g. buffer overflow protection or SQL injections);
mp.s.3	**Protection of web browsing**	**MEDIUM**	**MEDIUM**	**YES**	8.22 Web filtering	Access to external websites should be managed to reduce exposure to malicious content.	30%	10%	10%	50%	CLAUDIA MARTA HERRAMIENTAS GOVERNANZA (INES) VANESA ATENEA ELENA CCN-STIC-821 Security Standards in the ENS. Appendix II. NP 10 Internet Access Standards	The two standards are closely aligned in this control. Web filtering can include a variety of techniques including signatures, list of acceptable websites or domains, list of banned websites or domains, and custom configuration to help prevent software and other malicious activities from affecting the organisation's network and systems. Actions such as automatic blocking and training and awareness should be considered, always aligned with other controls. However, the OOPP may not manage the network services and so it may be the responsibility of a different entity or vendor to manage and deploy some of the measures described. It is true that the agency can manage some of the control through security tools, such as malware prevention software and monitoring the user's actions on the network. Browser configurations according to [op.exp.2] and [op.exp.3] should be considered.
mp.s.4	**Denial of service protection**	**MEDIUM**	**MEDIUM ***	**PARTIAL**	8.6 Capacity management	Resource use should be monitored and adjusted according to current and expected capacity requirements.	10%			90%	GLORIA REYES GOVERNANCE TOOLS (INES) CCN-STIC-820 Protection against Denial of Service	Cloud services have these measures embedded in them, as their services will be properly protected and balanced in case of need. Detection controls should be put in place to indicate problems in a timely manner. (Cloud services are characterised by elasticity and scalability that allow rapid expansion and reduction on demand of available resources for particular applications and services, which is useful to reduce the demand on the organisation's resources).

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL