centro criptológico nacional

ICT Security Guide
CCN-STIC 825

NATIONAL SECURITY FRAMEWORK.
27001 CERTIFICATIONS

August 2023

MINISTERIO DE DEFENSA

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

Edited by:
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
Pº de la Castellana 109, 28046 Madrid

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
2023.08.09 23:06:43 +02'00'

Date of issue: august 2023
NIPO: pending assignment

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

The reproduction of all or part of this document by any means or process, including reprography and computer processing, and the distribution of copies by public rental or loan, is strictly prohibited without the written authorisation of the National Cryptologic Centre, subject to the penalties established by law.

INDEX

1. INTRODUCTION

The challenges currently presented by the use of technological MEDIUM, as well as the unceasing evolution of so-called disruptive technologies, are posing an enormous challenge for global cybersecurity strategies. The speed of technological evolution and the growing dependence of societies on such MEDIUM is parallel to the increase in the risks and threats associated with their use, requiring more sophisticated responses, adapted to reality and coordinated between the different agents involved.

It has been in this scenario where the most significant cybersecurity frameworks[1] have evolved, thanks to the efforts of the different entities and authorities responsible, which, in many cases, have resulted in legal regulations, with the aim of promoting and homogenising security in the states.

As we have said, in the current context, threats represent a serious problem for the functioning of the social, political and economic activities of states, which has led to the emergence, at the international, European and national levels, of norms that aim to provide an adequate response to these challenges.

The effort to increase cybersecurity levels, through the evolution of regulations and standards on information security, has resulted in the updating of two key standards for cybersecurity in our country: Royal Decree 311/2022, of 3 May, which regulates the National Security Framework (ENS) and the ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements[2]. Both texts have undergone significant modifications to address the challenges arising from new threats, strengthening security programmes and initiatives, and facilitating compatibility between them and their security measures and controls.

The CCN, aware of the existence of different regulatory frameworks, both at European and international level, has developed this document to facilitate the integration and implementation of these standards, pointing out what they have in common'.

As a [legal] framework for cybersecurity, the National Security Framework[3] requires compliance with the minimum principles and requirements established[4], adopting the corresponding security measures and reinforcements, established in Annex II. In order to implement these measures, it is necessary to first consider the category of the system, as provided for in Article 40 and detailed in Annex I, the assets that form part of the information system and the management of information security risks.

The National Security Framework itself recognises the possibility of deploying additional security measures, at the discretion of the Security Officer. Moreover, within this flexibility to adapt to the needs of the information system and the risks detected, the measures themselves can be "modulated" or "replaced" by compensatory or complementary measures, which, while

[1] Such is the case of Royal Decree 311/2022 of 3 May, which regulates the National Security Framework (ENS).
[2] UNE-ISO/IEC 27001:2023 "Information security, cybersecurity and privacy protection. Information security management systems. Requirements"
3 Article 28. Compliance with minimum requirements.
[4] See Chapter II and Chapter III of Royal Decree 311/2022, of 3 May. BOE no. 106, of 4 May 2022. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

fulfilling the same purpose as those replaced, can achieve at least equivalent security and protection.

Cybersecurity framework.

In today's technological and interconnected environment, different [cyber]security frameworks coexist, which strive to develop guidelines for comprehensive risk management, and to reduce, detect, react and recover from any [cyber]security attack. These frameworks certainly coexist and interrelate with the National Security Framework and allow for a holistic view of security in today's entire cyber-technology environment.

The National Security Framework is closely related to ISO/IEC 27001:2022, but there are other frameworks that are of great relevance:

Organisation	Cyber]security framework
NIST National Institute of Standards and Technology https://www.nist.gov	**Cybersecurity Framework (CSF)** A voluntary cybersecurity framework developed by NIST[5], which allows organisations to develop their cybersecurity and risk management programmes, with the characteristic of adaptability and flexibility. It is thus a standard that can be used by organisations of any size and sector. Adherence to it is voluntary. This framework deploys the entire programme on five differentiated functions; identify, protect, detect, respond and recover and a differentiated scale of maturity.
	NIST SP 800-53 A security and privacy framework for information systems and organisations, which includes a catalogue of controls to protect the organisation's operations and assets. Equivalences can be found between different frameworks, such as ISO 27001. NIST 800-53 provides security controls to help deploy NIST CSF[6].
National Cyber Security Centre https://www.ncsc.gov.uk/	The UK's National Cyber Security Centre has developed a certification process[7] with similarities to the National Security Framework, aimed at assessing cyber security expertise, products and services independently according to its own standards. There are different accreditation Frameworks, either for products or for services.
Cloud Security Alliance (CSA) https://cloudsecurityalliance.org/	**Cloud Controls Matrix - CMM v4.**[8] Control framework developed by CSA, consisting of 197 control objectives distributed in 17 domains, related to key elements of cloud security. This framework is aimed at improving the security and implementation of controls for different cloud services. Its equivalence matrices with other security standards, such as ISO 27001/27002/27017/27018, NIST SP 800-53, AICPA TSC, German BSI C5, PCI DSS, ISACA COBIT, NERC CIP, FedRamp, CIS, may be useful.
Center for Internet Security [CIS]. https://www.cisecurity.org	CIS is a non-profit organisation working on cyber security. It has developed the CIS Controls and CIS Benchmarks security standards. It also develops other security work based on global best practices. **CIS Controls** It includes a set of controls[9] that have been prioritised and that, under cybersecurity best practices, present blocks of prevention, protection, response and recovery actions. These controls are distributed in security requirements organised in 3 categories, basic controls, fundamental controls, and organisational controls.

[5] US government agency. https://www.nist.gov/
[6] https://csrc.nist.gov/CSRC/MEDIUM/Publications/sp/800-53/rev-5/final/documents/csf-pf-to-sp800-53r5-mappings.xlsx
[7] https://www.ncsc.gov.uk/section/products-services/introduction
[8] https://cloudsecurityalliance.org/research/cloud-controls-matrix/
[9] https://www.cisecurity.org/controls

	Among the checkpoints that CIS has incorporated are PCI DSS[10], HIPAA[11] and RGPD[12].
ISACA https://www.isaca.org	COBIT[13] Security framework developed by ISACA for IT governance and management, modular and adaptable to organisations. It works on 5 domain blocks in which 40 processes are deployed.

To which ISO/IEC 27001:2022 should be added. ISO[14] 27001 is a voluntary standard that uses the high-level structure of ISO standards, Annex (L), to maintain compatibility with other ISO standards. It has a set of general clauses and an Annex (A) that contains the list of security controls that organisations must deploy in their systems.

2. OBJECT

This document shows the compatible measures between the National Security Framework and the ISO/IEC 27001:2022 standard.

This compatibility should not be interpreted as an arithmetic relation of equivalence, but as an interpretation under a general analysis of the contents of both standards. This analysis includes the minimum requirements set out in the articles of Royal Decree 311/2022 of 3 May and clauses [requirements] of the ISO.

This guide aims to offer an agile tool for those entities that intend to enrich their security framework associated with compliance with the National Security Framework, through the deployment of an information security management system, with complementary sources of ISO 27002:2022 and even capable of supporting an ISO 27001 certification. For the integration of management systems, it is always advisable to carry out a convergence analysis, so the work initiated in this guide is only a general approach that should be particularised for each organisation.

This guide can also be used in reverse, i.e., for those entities that already have information security management systems under ISO 27001 and wish to validate the compliance of their systems with Royal Decree 311/2022 of 3 May.

3. SCOPE

This guide establishes general guidelines that are applicable to organisations of different nature, size and sensitivity, without going into particular cases. It is expected that each organisation will tailor them to suit its unique environment.

4. ISO STANDARDS

ISO[15] is the International Organisation for Standardisation, which develops, through different groups of experts[16], international standards as frameworks of recognised prestige and which make

[10] Payment Card Industry Data Security Standard
[11] Health Insurance Portability and Accountability Act
[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[13] https://www.isaca.org/resources/cobit
[14] ISO (International Organisation for Standardisation) and IEC (International Electrotechnical Commission) constitute the specialised system for worldwide standardisation.
[15] https://www.iso.org/
[16] The expert committees also have development agreements with other organisations such as IEC - International Electrotechnical Commission.

it possible to demonstrate the conformity of processes, products or services to previously established requirements.

ISO enjoys international recognition and prestige, so that globally a system accredited under this standard provides reliability. Thus, for an organisation, presenting an accreditation related to an ISO standard means being able to demonstrate to any third party that it has independently reviewed and verified effective compliance with ISO requirements. An ISO standard implies reliability, which is why they are sometimes adopted by governments and control authorities as a reference of solidity and normative reinforcement[17], which helps to save time, costs and reduce barriers in the international sphere.

And it is here where the importance of this Guide stands out, as a tool for analysing the security measures compatible with the ISO/IEC 2700:2022 standard and the [legal] Royal Decree 311/2022, of 3 May. In such a way that it allows entities that so consider, to take advantage of the synergies of an information security management system under the umbrella of both[18].

It is important to note at this point that the mere fact of having an ISO standard certificate does not automatically lead to equivalence with other standards or frameworks. Entities must submit their management systems to the accreditation and conformity processes required by each framework or standard.

4.1. THE ISO/IEC 2700 SAGA 0

At a general level, there is a complete set of ISO 27000 standards, which encompass different information security practices, elements or requirements that will help to deploy an adequate information security system, and under the dimensions of confidentiality, integrity and availability.

Within the ISO 27000 family[19], we can look at ISO 27000 itself, which describes the overview of security systems and provides key vocabulary and definitions of information security management systems.

They can also be good references for the family of information security management systems;

ISO/IEC 27003 (standard that provides guidelines for deploying an information security management system with the "Plan, Do, Check, Act" improvement cycle).

ISO/IEC 27004 (standard that develops techniques related to metrics and indicators to measure the effectiveness of an information security management system).

ISO/IEC 27005 (standard that includes methodologies for developing the information security risk management process).

ISO /IEC 27017 (standard deploying controls for information security in the cloud)

ISO /IEC 27018 (standard deploying privacy controls for cloud services)

[17] One can consider for example 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 bodies, 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)*."

[18] Led under the [legal] framework of reference, as a compulsory rule for the subjects that fall under its scope of application.

[19] https://www.iso.org/search.html?q=27000

ISO /IEC 27019 (standard related to energy-related process control systems)

ISO/IEC 27701 (standard that develops in parallel to ISO 27001, a Privacy Management System).

4.1.1. ISO/IEC 27001:2022

ISO/IEC 27001 is an international, certifiable information security standard that can be adopted by organisations [public and private] on a voluntary basis. The standard itself is flexible and modular, as its requirements are generic and intended to be applicable to all organisations, regardless of type, size or nature.

The fact that the ISO standard sets out its "requirements"[20] implies that the management system developed under its umbrella is auditable and certifiable. Therefore, accredited certification bodies, after a systematic and methodical audit process, may consider conformity with the standard.

Let us not forget that the purpose of ISO is to provide the *requirements* for establishing, implementing, maintaining and continually improving an information security management system, which will be the one to undergo the certification process.

The information security management systems deployed under this standard seek to maintain the confidentiality, integrity and availability of information through a risk management process.

The **ISO/IEC 27001:2022 "Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements**" has been taken into account for the elaboration of this guide.[21] Heir to ISO/IEC 27001:2013, it has been revised in its entirety, considering certain adaptations and updates in its set of Clauses[22] and in Annex A of controls.

In relation to the clauses, there have been minor modifications, which affect more the drafting part or separation into sub-clauses, rather than significant changes.

Although it is true that specific aspects have been clarified, such as the monitoring and follow-up of security objectives, in general, the requirements of the 2013 standard are maintained, with minor changes.

CLAUSE		CHANGES	
4 Organisational context	**4.1 Understanding the organisation and its context**	**Unchanged**	
	4.2 Understanding stakeholder needs and expectations	**Minor changes**	Stakeholder needs and expectations should be updated so that the organisation is able to demonstrate which relevant requirements will be addressed through the ISMS.
	4.3 Determining the scope of the information security management system	**Unchanged**	

[20] In the framework of ISO standards, only those that consider requirements can be certifiable. ISO/IEC 27001:2022 is a requirements standard "*Information security, cybersecurity and privacy protection - Information security management systems -**Requirements***".

[21] Consider the standard UNE-ISO/IEC 27001:2023 "Information security, cybersecurity and privacy protection. Information security management systems. Requirements"

[22] A new sub-clause, 6.3 Change planning, has been included.

CLAUSE		CHANGES	
	4.4 System management safety information	Minor changes	It focuses on their processes and how they interact in the ISMS.
5 Leadership	5.1 Leadership and commitment	Unchanged	
	5.2 Policy	Unchanged	
	5.3 Organisational roles, responsibilities and authorities	Unchanged	
6 Planning	6.1 Actions to address risks and opportunities	Unchanged	
		Unchanged	It should be noted that the controls are new and need to be taken into account and updated.
		Minor changes	The Statement of Applicability [SOA] should be updated by making the change from the 114 controls to the 93 controls considered in the 2022 version standard.
	6.2 Information security objectives and planning for their achievement	Unchanged	
	6.3 Change planning	New	A change process must be included, which will allow for the control, planning, approval and monitoring of changes associated with the system.
7 Support	7.1 Resources	Unchanged	
	7.2 Competence	Unchanged	
	7.3 Awareness	Unchanged	
	7.4 Communication	Minor changes	The communications plan should be considered as a documented element with clear identification of means. The "who" has been removed and a "how" has been added. The responsible person is no longer required to be documented. (e) processes by which communication must take place are eliminated. They no longer need to be documented.
	7.5 Documented information	Unchanged	
		Unchanged	
		Unchanged	
8 Operation	8.1 Operational planning and control	Minor changes	Greater emphasis is placed on control, especially when third parties are involved.
	8.2 Information security risk assessment	Unchanged	
	8.3 Information security risk treatment	Unchanged	
9 Performance evaluation	9.1 Monitoring, measurement, analysis and evaluation	Minor changes	Work has been done to improve drafting.
	9.2 Internal Audit	Minor changes	The clause has been separated into two sub-points with very similar content. The clause now has two sub-clauses.

CLAUSE		CHANGES	
		Minor changes	The clause has been separated into two sub-points with very similar content. The clause now has two sub-clauses.
	9.3 Management review	**Minor changes**	The clause has been separated into three sub-points with very similar content. The clause now has three sub-clauses.
		Minor changes	The clause has been separated into three sub-clauses with very similar content. The clause now has three sub-clauses. A new point related to stakeholders is added.
		Minor changes	The clause has been separated into three sub-points with very similar content. The clause now has three sub-clauses.
10 Improvement	**10.1 Continuous improvement**	**Unchanged**	The order of the clauses is alerted.
	10.2 Non-conformity and corrective action	**Unchanged**	The order of the clauses is alerted.

Table. Analysis of changes made to clauses [requirements] standard 2022. Following the corresponding revision and evolution in its clauses, the standard underwent a significant change in the structure of Annex A. Thus, the control objectives of Annex A have been regrouped into four large blocks: *organisational controls; people controls; physical controls; technological controls*.

No. Controls	Chapter	Content	Remarks
37	Chapter 5	Organisational controls	General security block
8	Chapter 6	Checks on persons	Refers to individuals
14	Chapter 7	Infrastructure controls	Refers to physical objects
34	Chapter 8	Technology controls	Refers to technology

Table. Controls Block Annex A ISO 27001:2022

In addition to this new distribution of controls under 4 chapters, the number of controls has been reduced from 113 in the 2013 version to 93 in the 2022 version. However, this reduction does not represent a reduction in security, but a restructuring where new controls have been included, others have been merged or integrated with other controls, and some have been modified, while only one of them has been eliminated[23].

New controls have been considered:

New Control			Key point
	5.7	Threat intelligence	Logs
	5.23	Information security for the use of cloud services	Cloud Provider

[23] A.11.2.5 Withdrawal of assets (materials owned by the company)

Chapter 5 Organisational Controls	5.30	ICT readiness for business continuity	Continuity
Chapter 7 Physical controls	7.4	Physical security monitoring	Monitoring and follow-up
Chapter 8 Technology controls	8.9	Configuration management	Bastionados
	8.10	Deletion of information	Elimination process
	8.11	Data masking	Masking
	8.12	Preventing data leakage	Prevention
	8.16	Monitoring of activities	Monitoring
	8.23	Web filtering	Web
	8.28	Secure coding	Code

Table. New controls Annex A ISO 27001:2022

As will be seen below, the new system of controls in Annex A presents a better comparison of the controls compatible with Annex II of Royal Decree 311/2022 of 3 May, given that both standards have taken into account the evolution in cybersecurity required to face new risks and challenges.

4.1.2. ISO/IEC 27002

ISO/IEC 27002 Information Security, Cybersecurity and Privacy Protection - Information Security Control is not a standard of requirements and therefore not certifiable. However, this standard is a code of good practice for information security management and is undoubtedly helpful in deploying information security management systems.

It is intended to serve as an orientation guide for deploying the controls contained in Annex A of ISO 27001. It can also be used as a guidance and implementation document for commonly accepted information security controls.

The standard includes an Annex A[24], which presents five blocks of characteristics, with different attributes that have been assigned to each of the 93 controls in Annex A of ISO 27001:2022.

These attributes should serve to differentiate and separate controls, based on their priority uses and purposes. It allows specific searches and mapping of controls with their associated purposes, key points or dimensions.

Each control is associated with all those attributes that correspond to and/or describe it:

a) Control Type The control type is an attribute to view controls from the perspective of when and how the control modifies the risk with respect to the occurrence of an information security incident. The values of the attribute consist of Preventive (the control aims to prevent the occurrence of an information security incident), Detective (the control acts when an information security incident occurs) and Corrective (the control acts after an information security incident occurs).

[24] Table A.1 - Matrix of controls and attribute values

(b) Safety **properties or dimensions**[25]

The information security dimensions are an attribute to view the controls from the perspective of what characteristics of the information it will help to preserve. The attribute values are Confidentiality, Integrity and Availability.

c) Cybersecurity

Cybersecurity concepts is an attribute to view controls from the perspective of associating controls to cybersecurity concepts defined in the cybersecurity framework described in ISO/IEC TS 27110. The attribute values consist of Identify, Protect, Detect, Respond and Recover.

d) Operational capabilities

Operational Capabilities is an attribute for viewing controls from the perspective of the information security capabilities professional. The attribute values consist of Governance, Asset Management, Information Protection, Human Resource Security, Physical Security, System and Network Security, Application Security, Secure Configuration, Identity and Access Management, Threat and Vulnerability Management, Continuity, Supplier Relationship Security, Legality and Compliance, Information Security Event Management and Information Security Assurance.

e) Security domains

Security domains is an attribute to view controls from the perspective of four information security domains: "Governance and Ecosystem" includes "Information Systems Security Governance and Risk Management" and "Ecosystem Cybersecurity Management" (including internal and external stakeholders); "Protection" includes "Information security architecture", "Information security administration", "Identity and access management", "Information security maintenance" and "Physical and environmental security"; "Defence" includes "Detection" and "Information security incident management"; "Resilience" includes "Continuity of operations" and "Crisis management". The attribute values consist of "Governance and ecosystem", "Protection", "Defence" and "Resilience".

4.2 DIFFERENCES BETWEEN ISO 27001 AND ENS

The good synergy and reciprocity between the National Security Framework [Royal Decree 311/2022 of 3 May] and ISO/IEC 27001:2022, and the possibility of deploying management systems, considering the provisions of both frameworks, has already been highlighted. However, it is also necessary to channel the particularities and differences between the two, without which it will not be possible to maintain a system capable of complying with both.

At the national level, we cannot ignore the fact that according to article 2 of Royal Decree 311/2022, entities subject to compliance with the National Security Framework[26], must deploy management systems in accordance with it. However, these systems may contemplate the

[25] This block can be assimilated to those of the National Security Framework, which also details the dimension(s) in which a security control takes place. However, it should be noted that, for this standard, there are 5 dimensions as opposed to the three classic security dimensions considered by ISO 27001.

[26] The entire public sector, in the terms defined by article 2 of Law 40/2015, of 1 October, and in accordance with the provisions of article 156.2 of the same, as well as private sector entities that provide services or solutions to public sector entities for the exercise by the latter of their competences and administrative powers.

complementary requirements contained in the ISO and may be able to meet its requirements with solvency.

At the global level, we can analyse both frameworks and draw the following conclusions:

	ISO/IEC 27001	National Security Framework (RD 311/2022)
Responsible authority	International Organization of Standardization (ISO)	National Cryptologic Centre (CCN)[27]
Nature	International safety standard	State [legal] framework, derived from Law 40/2015.
Character	Voluntary membership	Subjects subject to compulsory treatment
Scope of application	Information security management system of any organisation.	Public sector information systems. Private sector information systems (*)
Function	Reliability vis-à-vis third parties, evidencing processes for information security.	Legal requirement to promote adequate protection of information processed and services provided by the entities within its scope of application
Modulation of measures	According to context, stakeholders and organisation, in line with risk analysis.	At the discretion of the Security Officer, according to risks, state of technology and services / information. Specific entities or sectors of activity may implement specific compliance profiles[28], with modulation of security measures.
Dimensions	It considers the three classic dimensions of security: Availability, Integrity and Confidentiality.	It considers five dimensions of security. Availability, Integrity, Confidentiality, Traceability and Authenticity.
Source system	Minimum ISO Annex A Total number of controls: 93	Minimum Annex II of the Royal Decree Total number of controls: 73
Risk management	Any methodology can be used, but the focus is on the ISO 31000 methodology. References in ISO/IEC 27005.	Any methodology can be used, but the focus is on MAGERIT[29].
Evidence of compliance or conformity	By means of certification, issued by an accredited certification body, following a satisfactory audit.	By means of a declaration of legal conformity, issued by an accredited certification body, following a satisfactory audit.
Cycle of validity	3-year cycle, subject to a process of annual internal and external reviews or monitoring.	2-year cycle, subject to an annual internal review/monitoring process.
References	Any security framework can be a frame of reference.	There are Instructions, Abstracts, Guidelines[30], and Good Practices. Any security framework can bring improvements to the system.
Certification	Through accredited entities.	Through accredited entities. [31]

Table. Summary of the characteristics of both standards

[27] Attached to the National Intelligence Centre. -Ministry of Defence

[28] See Article 30 of Royal Decree 311/2022 of 3 May.

[29] Methodology developed by Consejo Superior de Administración Electrónica and currently maintained by the Secretaría General de Administración Digital (Ministry of Economic Affairs and Digital Transformation) and CCN. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[30] Second additional provision.

(...) The technical safety instructions shall take into account the applicable EU harmonised standards.

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

[31] https://ens.ccn.cni.es/es/certificacion/entidades-de-certificacion

Although, as can be seen, both standards have differences, they both share their key objective; the management of risks associated with [cyber]security and consider not only the organisation that owns the system, but also extend their requirements to suppliers and supply chains, including those involved in cloud services, which are so common in our current environment.

The deployment of a management system, under the guidelines of these standards, will build confidence with third parties, significantly improve the security and resilience of the system and maintain the recognition of the services and products that are included under the scope of these standards.

Finally, it is worth remembering that at the international level ISO can serve as a "unifying" vehicle for security requirements, acting as a "translator" of security norms or standards. This is reflected, for example, in the requirements imposed by the CAP [Common Agricultural Policy], or in the standards associated with the financial sector, where it is common to make equivalences between ISO/IEC 27001 and the authorities' own guidelines.

Therefore, working with compatible security measures of the National Security Framework and ISO 27001 can be enriching and serve to evidence the requirements imposed in a uniform way and under a common "language".

5. ENS COMPLIANCE THROUGH 27001 CERTIFICATION

An Information Security Management System is a set of policies, procedures and guidelines established in an organisation, together with the resources and processes necessary to protect the assets and especially the information asset. And this is precisely the objective of the National Security Framework, which seeks to increase the security of services and information in the public environment, in an organised manner and in which basic principles and minimum requirements can be combined with technological measures and the necessary security governance.

Establishing and maintaining a management system is a strategic decision that will undoubtedly benefit organisations. Selecting the appropriate standard or framework will depend on the applicable regulations and often on the needs of the organisation, its objectives, internal processes and the size and structure of the organisation.

The National Security Framework is a [legal] framework that is adapted to the environment, which has considered the key points of [cyber]security, and which allows it to be aligned with other security frameworks, including ISO 27001. However, certain differences between the two must be taken into account, which will require adaptations to be made to the organisation's management system.

If an entity develops the processes required by the standards, it will benefit from the advantages of having an Information Security Management System that is legally compliant, comprehensive, capable of evidencing security, and that fosters the ability to detect, react, recover and learn from security incidents and events.

One of the advantages provided by the [legal] framework of the National Security Framework is the efforts made by the Control Authority [CCN]. While it is true that ISO tends to publish different support standards, such as ISO/IEC 27002, a more detailed and rapid analysis is needed, capable of adapting to the needs of the moment, as is being developed within the scope of the National Security Framework. And it is precisely the interest in improving the promotion and

development of security that has led to the constant publication of abstracts, reports, best practices, compliance guides[32] and cybersecurity solutions[33], which make it possible to manage key points, such as technological surveillance, data traceability or network visibility, in a more agile and rapid manner than the ISO standard.

Another improvement that can be obtained by integrating the requirements of the National Security Framework is the consideration of the five dimensions of security, which allows the deployment of controls focused on the two dimensions not initially considered by ISO.

Generally speaking, when an entity is included in the scope of application of the National Security Framework, it must include the conditions established therein in its management system. This does not prevent it from integrating the rest of the points established by the ISO standard, which allow security to be enhanced.

By working on the basis of a strategy in which the management system integrates the common points of both frameworks and, at the same time, considers those where differences can be included without hindering security, we can deploy an Information Security Management System that supports both standards. In order to do so, we will need to consider:

A) Work with the five dimensions of security. Two dimensions should be included in addition to the three classic ISO dimensions. This is not a security problem but can enrich the process of attributes that Annex A of ISO/IEC 27002 has included in its 2022 version.
B) Analyse the scope of each standard and document each of them. A good strategy is to try to unify the scopes where possible, so that the system can comprehensively cover both.
C) Unify statements of applicability, including and describing all applied controls, and giving reasons for exceptions. The standards in their 2022 version have evolved and allow for good compatibility of security measures.
D) Develop a single risk methodology to cover risk management and monitoring. Both standards are permissive in terms of risk methodology, so the institution should adopt the one that best fits its system and its assets.
E) Integrate security roles and management reviews. To include the requirements of both standards, an annual [management] review report can be established, subject to its presentation to the Information Security Committee, with the content required by ISO and also covering those aspects that the National Security Framework establishes.
F) Consider an integrated management system, including all necessary processes, with the records and documentary evidence required by both standards.
G) Analyse the effectiveness and efficiency of the management system, using metrics and indicators to satisfy the analysis and monitoring requirements of both frameworks. At the ISO level, it will be necessary to consider the organisation's security objectives and at the Framework level, the required key indicators should be taken into account[34].
H) Establish a review process, including annual audits against the requirements of both standards. The process shall include the periodic safety reviews to be carried out.

[32] Second additional provision.Development of the National Security Framework.
"(...) For better compliance with the provisions of this Royal Decree, the CCN, in the exercise of its powers, shall draw up and disseminate the corresponding information and communication technology security guides (CCN-STIC guides), particularly the 800 series, which shall be incorporated into the set of documents used to carry out security audits".
[33] https://www.ccn-cert.cni.es/soluciones-seguridad.html
[34] Article 32. Report on the state of security.

I) To pass the certification processes[35], taking into account the differentiated certification Framework of each of the two standards, including the corresponding follow-ups, under the complete cycle required by each standard.

One of the particularities of ISO is that only ISO/IEC 27001 is certifiable, as it is the standard that includes the requirements. However, the organisation may consider not pursuing certification of ISO/IEC 27001 or deploying ISO/IEC 27002 and enriching the system thanks to the security contributions they provide. In any case, the organisation should carry out a cost-benefit analysis and make the decision best suited to its needs.

5.1. ENS ROLL-OUT STRATEGY WITH ADAPTATIONS

The National Security Framework (ENS) is a [legal] framework, the result of national regulation that is mandatory for the public sector and information systems of private sector entities when they provide services or solutions to public sector entities for the exercise of their competences and administrative powers, in accordance with the legal system. [36]

The ENS requires a categorisation process (Annex I) and the deployment of a minimum set of security measures (Annex II) based on it. Royal Decree 311/2002 of 3 May 2002 has introduced novelties in relation to the applicability of the security measures contained in Annex II, from the possibility given by Article 30 related to the publication of specific compliance profiles, to mandatory or optional reinforcements differentiated by the level and category declared.

At a general level, the two standards [ISO/IEC 27001:2022 and Royal Decree 311/2022], have a good Compatible Level, having followed a very similar evolution in relation to new risks, considering the cloud environment and the possible dependence on suppliers.

Therefore, in order to achieve an integrated system with both standards, it is necessary to start from the **ENS category MEDIUM, with a concrete modulation** based on:

A) Implementation of some HIGH category controls for improved deployment of the change and business continuity process.
B) Implementation of category MEDIUM controls to the full extent, even if not provided for by ISO 27001:2022.

It is important to maintain as a strategy, compliance with the ENS under the scope given by Law 40/2015, both from the point of view of essential assets (Annex I) and the components involved[37]. Therefore, the scope must be aligned with legal compliance.

Furthermore, it should be noted that Annex II modulates the requirements according to the categorisation of the system, whereas in ISO/IEC 27001 the level of requirements is limited to the selected scope and motivation of the entity. It will therefore be necessary to consider the principle

[35] The information systems subject to the application of the ENS shall be subject to a process to determine their compliance with the ENS, and to this end, MEDIUM or HIGH category systems shall require an audit for the certification of their compliance, while BASIC category systems shall only require a self-assessment for their declaration of compliance, without prejudice to the fact that they may also be subject to a certification audit, for the purposes of the provisions of article 31 of Royal Decree 311/2022, section 2, "The audit 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 Annexes I and III and in accordance with the provisions of the Technical Security Instruction on Security Auditing of Information Systems".
[36] Consider the provisions derived from Law 40/2015.
[37] Note that a 27001 certification has whatever scope the organisation decides. It is sufficient that it is clearly delimited which part of the management system is being certified.

of proportionality enshrined in the ENS, and to deploy the controls that, under the application of the ENS, are necessary.

An initial map of compatible requirements is presented below, which is intended to help deploy an integrated system for both frameworks.

It should be noted that the structuring of measures is not the same in the ENS as in 27001 and 27002. Some aspects are partially covered by some controls, and in most cases, ENS controls require several ISO 27001 controls to be fully complied with.

Although it has already been mentioned, it is important to bear in mind that neither the National Security Framework nor ISO/IEC 27001:2022 are aimed at business continuity, but that it is part of the block of security measures that "can be deployed". Nevertheless, ISO has developed a set of continuity standards, which include the requirements of a Business Continuity Management System[38].

5.2. SUMMARY TABLE

A global measures analysis has been carried out of both frameworks, both of their general part (articles of the National Security Framework and Annex L of the ISO) and of the measures or controls of Annex A of ISO 27001:2022 and Annex II of Royal Decree 311/2022, of 3 May.

It should be recalled that ISO/IEC 27001 is malleable[39], whereas the ENS requires compliance for the relevant dimensions and categories, so this should always be verified. 5.2.2. Analysis of compatible requirements general part:

Below is a detailed comparison and analysis of the clauses of ISO/IEC 27001:2022 and Royal Decree 311/2022 of 3 May, which must be considered in order to include the requirements given in the management system.

CLAUSE			Article / ENS Measure	Analysis of compatible requirements and differences.
4 Organisational context	4.1 Understanding the organisation and its context		**Royal Decree 311/2022** INTRODUCTION Article 30 Specific compliance profiles and accreditation of secure configuration implementing entities Article 40 Security categories **Annex I** **Annex II** o [org.1] Security policy	For ISO, organisations determine the external and internal issues that are relevant to their purpose and that condition the achievement of the intended outcomes of their ISMS. Such issues may include the political and economic situation, existing regulation, the state of technology, relationships with citizens and suppliers, the functions of any area or department affected by the ISMS, the mission, vision and functions of the organisation, and in general, any factor that impacts on its objectives and operations. The current ENS has taken into account the particularities of public entities and has considered in its Article 30, the specific compliance profiles and accreditation of entities for the implementation of secure configurations. In this way, specific compliance profiles may be implemented for certain entities or sectors of activity, comprising the set of security measures that, based on the mandatory risk analysis, are suitable for a specific security category. For the ENS, when assessing these possible damages in the categorisation phase of the systems, organisations are carrying out an exercise of understanding their context. This categorisation is mandatory for all information systems within the scope of the ENS. However, the organisation should review whether it has a strategy in place where internal and external issues relevant to the ISMS are analysed on a regular basis in order to fulfil its mission and objectives and to achieve further alignment with ISO 27001.

[38] ISO/IEC 27031, ISO 22313 and ISO 22301

[39] Limited to the selected scope and motivation of the entity

CLAUSE		Article / ENS Measure	Analysis of compatible requirements and differences.
	4.2 Understanding stakeholder needs and expectations	**Royal Decree 311/2022** INTRODUCTION Article 30 Specific compliance profiles and accreditation of secure configuration implementing entities Article 40 Safety categories Annex I	For ISO, it requires that the requirements of stakeholders (citizens, suppliers, staff, other public administrations, etc.) that are relevant to information security are identified: legal and regulatory requirements, contractual obligations, etc. The organisation must consider the relevant parties and the associated security requirements. This in turn finds its correspondence in the scope of the ENS in its introduction and in the referenced articles, focusing on the main stakeholders; public and private sector entities, rights and freedoms and the well-being of citizens and to ensure the provision of essential services and resources. The organisation should review whether it has a list of internal and external stakeholders relevant to the ISMS and those who depend on its proper operation and very significantly when analysing impacts and dependencies.
	4.3 Determining the scope of the information security management system	**Law 40/2015:** o Article 2 o Article 156 **Royal Decree 311/2022:** Article 1 Subject matter Article 2 Scope	The ISO standard allows the scopes to be limited, according to the needs of the organisation and the objectives it defines. In any case, it shall be documented. In the ENS, the scope is limited to the electronic MEDIUM used and managed by the entire public sector, for the provision of services to citizens in the exercise of their powers and in their relationship with other Public Administrations, all within the scope of Law 40/2015, to the information systems of private sector entities, in accordance with the applicable regulations and by virtue of a contractual relationship, when they provide services or solutions to public sector entities for the exercise by the latter of their powers and administrative powers.
	4.4 Information security management system	**Royal Decree 311/2022** Article 6 Security as an integral process **Annex II** [org.1] Security policy [op.pl.2] Safety architecture - *Strengthening R1-Management system. Enforcement R2-Safety management system with continuous improvement.* [op.ext.3]. supply chain security Reinforcement R2-Security management system. [op.mon.2] - *Strengthening R2-Efficiency of the safety management system.* **Annex III** Security audit	For ISO, the organisation must establish, implement, maintain and continuously improve an information security management system. For the ENS, security is understood as an integral process consisting of all human, material, technical, legal and organisational elements related to the information system (article 5) and therefore the existence of a documented information security management system with a regular process of approval by the management, based on the Declaration of Applicability regulated in article 28, must be accredited through auditing processes.
5 Leadership	5.1 Leadership and commitment	**Royal Decree 311/2022** Article 11 Differentiation of responsibilities Article 13 Organisation and implementation of the security process **Annex II** [org.1] Security policy	For ISO, top management must demonstrate leadership and commitment to the information security management system, through a number of elements, such as resourcing the system, approving a security policy, promoting continuous improvement… For the ENS, the security of information systems must involve all members of the organisation (article 13), according to the different roles (article 11).
	5.2 Policy	**Royal Decree 311/2022** Article 11 Differentiation of responsibilities Article 12 Security policy and minimum security requirements Article 13 Organisation and implementation of the security process **Annex II** [org.1] Security policy	For ISO, management must establish an information security policy, which must be available as documented, communicated and accessible information. For the ENS, a security policy must be developed and approved which will consider the content outlined (especially by Article 11 and by the control in Annex II [org.1]) and which will articulate the ongoing management of security, and will be approved by the head of the relevant superior body.
	5.3 Organisational roles, responsibilities and authorities	**Royal Decree 311/2022** Article 11 Differentiation of responsibilities **Annex** II [org.1] Security policy	For ISO, management must ensure that responsibilities for information security roles are assigned and communicated within the organisation. For ENS, differentiated roles are established and detailed in the Security Policy, defining for each role the duties and responsibilities of each role, as well as the procedure for their designation and renewal and the mechanisms for coordination and conflict resolution.

CLAUSE				Article / ENS Measure	Analysis of compatible requirements and differences.
6 Planning	6.1 Actions to address risks and opportunities	6.1.1	General considerations	**Royal Decree 311/2022** Article 7 Risk-based security management Article 8 Prevention, detection, response and preservation Article 14 Risk analysis and risk management **Annex II** [op.pl.1] Risk analysis	For ISO, there must be planning to manage risks and opportunities, prevent and reduce impacts and achieve continuous improvement. For the ENS, planning, risk management, preventive and reactive actions, as well as continual improvement is deployed in several articles and controls, as it is further detailed in
		6.1.2	Information security risk assessment	**Royal Decree 311/2022** Article 7 Risk-based security management Article 8 Prevention, detection, response and preservation Article 14 Risk analysis and risk management **Annex II** [op.pl.1] Risk analysis	For ISO, the organisation must define and implement a documented information security risk assessment process, defining the criteria of the process, an objective system, determine the risks (analyse and evaluate) and the owners of these, and manage a treatment plan. For the ENS, the mandate is clear and derives in a global process of the security process, so that the analysis and management of risks is an essential part of security and must constitute a continuous and permanently updated activity. Each organisation that develops and implements systems for information processing or service provision will perform its own risk management.
		6.1.3	Dealing with information security risks	**Royal Decree 311/2022** Article 7 Risk-based security management Article 14 Risk analysis and risk management Article 28 Compliance with minimum requirements Article 30 Specific compliance profiles and accreditation of secure configuration implementing entities **Annex II** paragraph 2.1.3 [op.pl.1] Risk analysis	For ISO, the organisation shall define and perform an information security risk treatment process, which shall be documented. The organisation shall prepare a "Statement of Applicability" which shall contain, the required controls, the justification for inclusions, whether the required controls are implemented or not; and the justification for exclusions from any of the ISO Annex A controls. For the ENS, the measures adopted to mitigate or eliminate risks must be justified and, in any case, there must be proportionality between them and the risks. For ENS, the criticality of the declaration of the controls in Annex II is established in Article 28, which states that the list of security measures selected shall be formalised in a document called the Declaration of Applicability, signed by the person responsible for security. It should be borne in mind that for the ENS, modulations of security measures can be deployed by means of compliance profiles, as specific compliance profiles can be established, according to Article 30, for specific entities or sectors, which will include the list of measures and reinforcements applicable in each case or the criteria for their determination.
	6.2 Information security objectives and planning for their achievement			**Royal Decree 311/2022** Article 2 Subject matter Article 5 Basic principles of the National Security Framework **Annex II** [org.1] Security policy	For ISO, The organisation should establish information security objectives at relevant functions and levels, which shall be consistent, measurable, aligned with security and risks, updated and communicated. For the ENS, the objectives are integrated in the legislator's own mandate and specifically deploy the basic principles and minimum requirements necessary for adequate protection of the information processed and the services provided by the entities within its scope of application, in order to ensure access, confidentiality, integrity, traceability, authenticity, availability and preservation of the data, information and services used by electronic means that they manage in the exercise of their competences. In turn, control [org.1] states that the security policy must specify the objectives or mission of the organisation. However, it does not specify that the information security objectives should be documented, measurable, communicated and updated at regular intervals. Therefore, organisations must have documented information on information security objectives, derived from the organisation's objectives, and supported by security controls and metrics, as well as comply with all other aspects of this ISO 27001 requirement.
	6.3 Change planning			**Royal Decree 311/2022** Article 21. Integrity and updating of the system Article 27. Continuous improvement of the security process. **Annex II** [op.exp.5] Change Management	For ISO until version 2022, changes were a control contained in the control objective A.12 Security of operations [A.12.1.2 Change management]. It is now part of the block of clauses that the system must consider and must be considered globally for the information security management system, so that changes will be planned. For the ENS, changes are maintained in its version 2022, as operational control [op.exp.5], considering not only planning, but also registration, risk analysis, approval, testing, system updates and, if necessary, possible rollback.
7 Support	7.1 Resources			**Royal Decree 311/2022** Article 6 Security as an integral process Article 13 Organisation and implementation of the security process **Annex II**	For ISO, it stipulates that organisations must determine and provide the necessary resources (personnel and financial, generally) for the ISMS. For the ENS, it contains references throughout its articles to the resources that may be necessary for the deployment of security in the system, as can be seen, for example, in Article 13. [op.pl.2.r1.1] Management system, relating to the planning, organisation and control of resources relating to information security,

CLAUSE			Article / ENS Measure	Analysis of compatible requirements and differences.
			[op.pl.2] Security architecture [op.mon.2] Metric system [op.pl.4] Sizing / capacity management	or [op.exp.7.r2.2] Allocation of resources to investigate the causes, analyse the consequences and resolve the incident. In general, the system deployed by ENS requires that the management system, related to the planning, organisation and control of information security resources, is detailed in [op.pl.4] Sizing/capacity management. On this basis, it is necessary to consider a forecast of the resources necessary to correspond to the two standards and associated with measurements or monitoring to check their effectiveness, as proposed in Reinforcement R1 - Effectiveness of the incident management system [op.mon.2.r1.1] and Reinforcement R2 - Efficiency of the security management system [op.mon.2.r2.1].
	7.2 Competence		**Royal Decree 311/2022** Article 15 Personnel management Article 16 Professionalism **Annex II** [mp.per.4] Training	For ISO, organisations must ensure that persons performing work that affects their information security performance are competent, based on appropriate education, training or experience. For the ENS, this requirement is present and is part of the articles, both in its initial part "professionalism" and in its evolution from the point of view of periodic and specific training, especially in critical profiles for security functions. It should be noted that the qualification of personnel is not only required internally, but also for the personnel of suppliers providing security services to the organisation. Specifically, the ENS considers in control [mp.per.4] specific training of critical persons and functions, but further training requirements are also deployed in other controls. In addition, the effectiveness of the training actions carried out will be evaluated. For example, it is stated in [op.pl.3.3] It shall consider technical, training and financing needs together, [op.cont.2.4] The persons affected by the plan shall receive specific training related to their role in the plan, [mp.per.1.2].
	7.3 Awareness		**Royal Decree 311/2022** Article 6 Security as an integral process **Annex II** [mp.per.3] Awareness raising	For ISO, it indicates that individuals should be aware of the information security policy, their contribution to the effectiveness of the ISMS, as well as the implications of not complying with the requirements of the ISMS. For the ENS, awareness is a basic security principle. The *utmost attention shall be paid to the awareness of the persons involved in the process and that of the hierarchy, in order to prevent ignorance, lack of organisation and coordination or lack of appropriate instructions from constituting sources of security risk. In addition, the security measure [mp.per.3] again requires regular awareness-raising activities, in particular on security regulations and on the identification and reporting of security incidents.*
	7.4 Communication		**Royal Decree 311/2022** Article 25 Security incidents **Annex II** [org.1] Security policy [org.2] Security regulations [op.exp.7] Incident management [op.cont.2] Continuity plan	For ISO, organisations must determine the need for internal and external communications related to the ISMS. For ENS, communications are associated with control points in the system, starting with the policy itself, communications to users and stakeholders, regulations, procedures.... and ending with the point of contact associated with incidents or contingencies. This ensures that the system focuses on key communications. Therefore, both standards must be aligned and it will be necessary to have a communications tree associated to each required point of the ENS standard and which is fully integrated in ISO, as well as to maintain the necessary evidence on the communications made regarding the ISMS.
	7.5 Documented information	7.5.1	General considerations	**Royal Decree 311/2022** Article 12 Security policy and minimum security requirements Article 28 Compliance with minimum requirements **Annex II** [org.1] Security policy [org.2] Security regulations [org.3] Security procedures [op.pl.2] Security architecture	For ISO, it must include the documented information required by the standard, and that which is determined to be necessary for the effectiveness of the ISMS. There must also be control over such documentation. For the ENS, managing evidence and deploying the system in a documented manner is important and is reflected in several points. For example, article 12 itself or the policy [org.1] states that it includes guidelines for the structuring of the system's security documentation, its management and access or article 28 when it refers to the measures to be documented. The documentation required by security architecture [op.pl.2], the security documentation associated with [op.acc], configuration documents [op.exp.2], system interconnections [op.ext.4]. However, it does not clearly specify the control of the overall documentary information process as the ISO guidelines should be followed for both systems.
		7.5.2	Creation and updating	**Royal Decree 311/2022** Article 12 Security policy and minimum security requirements Article 28 Compliance with minimum requirements **Annex II** [org.1] Security policy	For ISO, the process of document creation and control is more restrictive, as it establishes points associated with format and description. However, it shares approval with ENS. For the ENS, security-related information considers precise points of creation and approval, scattered throughout the articles and controls, such as [org.1] or [org.4].

CLAUSE				Article / ENS Measure	Analysis of compatible requirements and differences.
				org.2] Security Policy [org.3] Security Procedures [op.pl.2] Security Architecture [op.pl.2] Security Architecture	
		7.5.3	Control of documented information	**Royal Decree 311/2022** Article 12 Security policy and minimum security requirements Article 28 Compliance with minimum requirements **Annex II** [org.3] Security procedures [op.pl.2] Security architecture	For ISO, the information in the system must be controlled and protected. However, for the ENS, this concern is shared and control [org.3] can be observed in a direct manner, by referring to associated points such as access, storage, making copies, labelling of supports, telematic transmission, etc.
8 operation	8.1 Operational planning and control			**Royal Decree 311/2022** Article 6 Article 7 Article 8 Article 37 **Annex II** [op.pl.1] Risk analysis [op.pl.2] Security architecture	For ISO, it requires at a general level that sufficient control information on the ISMS is available to ensure that processes are carried out as planned. This implies the existence of policies, procedures and best practices in information security, risk management, incident management, metrics for monitoring security objectives, management of outsourcing, etc.. For the ENS, system security will be the subject of a holistic approach, with an up-to-date and approved management system and a comprehensive risk management process. This is because risk analysis and management is an essential part of the security process and should be a continuous and continuously updated activity, and the reduction to these levels will be achieved through an appropriate application of security measures, in a balanced and proportionate manner to the nature of the information processed, the services to be provided and the risks to which they are exposed.
	8.2 Information security risk assessment			**Royal Decree 311/2022** Article 7 Article 14 **Annex II** [op.pl.1] Risk analysis	For ISO, at this point, ISO 27001 requires the existence of documented information on the results of information security risk assessments. For the ENS, the requirements of the ENS regarding risk analysis are analogous to those of ISO 27001. For the ENS, risk management shall be carried out by analysing and addressing the risks to which the system is exposed, without prejudice to the provisions of Annex II, an internationally recognised methodology shall be used, and the measures taken to mitigate or eliminate the risks shall be justified and, in any case, there shall be proportionality between them and the risks. Consider also Annex III, which mentions that audits should verify that there is a documented ISMS with a regular management approval process.
	8.3 Information security risk treatment			**Royal Decree 311/2022** Article 7 Article 14 **Annex II** [op.pl.1] Risk analysis	For ISO, the organisation must keep documented information on the results of the treatment of information security risks. For the ENS, in general, risks must be managed and the measures taken to mitigate or eliminate risks must be justified and, in any case, there must be proportionality between them and the risks. Furthermore, the management and coordination of security is part of the responsibility of the committee(s), which is why responsibility for the risks is derived.
9 Performance evaluation	9.1 Monitoring, measurement, analysis and evaluation			**Royal Decree 311/2022** Article 10 Article 21 Article 27 **Annex II** [op.mon.2] Metric system	For ISO, the organisation must assess information security performance and ISMS effectiveness through the implementation of security metrics, and documented evidence of the results of such monitoring and measurement must be available. For ISO, monitoring of safety targets should also be considered. For the ENS, this corresponds to the basic principle of periodic reassessment, which states that security measures shall be reassessed and updated periodically to adapt their effectiveness to the constant evolution of risks and protection systems, including, if necessary, a reassessment of security. Let us not forget that ongoing assessment and monitoring are part of the overall security process and are integrated throughout the ENS security cycle, and it is necessary to collect the necessary data to ascertain the degree of implementation of the applicable security measures. It is also important to take into account the provision of Article 27. Continuous improvement of the security process; "*The implemented comprehensive security process shall be continuously updated and improved. To this end, the criteria and methods recognised in national and international practice relating to IT security management shall be applied*". While it is true that at a global level the system must be "monitored" to analyse possible evolutions and improvements, let us not forget the provision of Article 110, when it states in paragraph 3 "*The security measures shall be reassessed and updated periodically, adapting their effectiveness to the evolution of risks and protection systems, and may lead to a rethinking of security, if necessary*".

CLAUSE				Article / ENS Measure	Analysis of compatible requirements and differences.
	9.2 Internal Audit	9.2.1	General	**Royal Decree 311/2022** Article 31Annex III	For ISO, it involves conducting internal audits at planned intervals to ascertain whether the ISMS meets the organisations' requirements for its ISMS and those of the standard itself, is implemented, and is being effectively maintained. In practice, to renew ISO 27001 certification, this involves an annual follow-up audit for the first two years, and a renewal audit in the third year. For the ENS, and as a result of following a different certification Framework, the audit cycle takes two years, and an internal audit is required annually. Information systems shall be subject to a regular audit, at least every two years, to verify compliance with the requirements of this legislative framework. It also specifies that, on an extraordinary basis, such an audit must be carried out whenever there are substantial modifications to the information system that may have an impact on the required security measures. In general, both systems require the audit process, although each system derives from a different temporary process. The entity must have an audit plan that includes all internal and external reviews. This plan must consider the execution of the internal audit, which will also be considered for ENS (See Resolution of 27 March 2018, of the Secretary of State for Public Function, approving the Technical Security Instruction on Information Systems Security Auditing, when it requires the analysis of "The degree of confidence in the auditee's management reviews and internal audits").
		9.2.2	Internal Audit Programme		
	9.3 Management review	9.3.1	General	**Royal Decree 311/2022** **Annex III**	For ISO, management must review the ISMS at planned intervals to ensure its suitability, adequacy and continuing effectiveness. In practice, this implies management reviews at least on an annual basis. For the ENS, in its Annex III, which mentions that audits should verify that there is a documented ISMS with a regular management approval process. In addition, the Resolution of 27 March 2018, of the Secretary of State for Public Function, which approves the Technical Security Instruction on Auditing the Security of Information Systems, should be referred to when it requires the analysis of "The degree of confidence in the auditee's management reviews and internal audits".
		9.3.2	Management review inputs		
		9.3.3	Results of the management review		
11 Improvement	10.1 Continuous improvement			**Royal Decree 311/2022** Article 12 Article 25 Article 27 **Annex II** [op.pl.2] Security architecture	For ISO, the organisation must continuously improve the suitability, adequacy and effectiveness of the information security management system. For the ENS, the information security policy includes the continuous improvement of the security process as a cross-cutting security principle. Thus, the security implemented must be continuously updated and improved, and to this end, the criteria and methods recognised in national and international practice relating to security management must be applied. In particular, the management of security incidents will include the mandatory register, which will also serve for continuous improvement, together with the rest of the system's security processes. For the ENS this principle is fundamental and to this effect it can be checked as Reinforcement R2-Security management system with continuous improvement. [op.pl.2.r2.1] Information security management system, with regular updating and approval.
	10.2 Non-conformity and corrective action			**Royal Decree 311/2022** Article 8 Article 31 **Annex III**	For ISO, when a non-conformity occurs, organisations must react to it, take actions to control, correct and eliminate its causes, and review the effectiveness of these actions and maintain documented information about them. For the ENS, following an audit process, they will be submitted to the system manager and the security manager, who will analyse them and present their findings to the system manager for appropriate corrective action. The ENS does not explicitly detail the content that a record or similar document of non-conformities and the associated corrective action management should include, and it is therefore recommended that the ISO record requirement be integrated into the system to achieve the compliant level.

5.2.3. ANALYSIS OF COMPATIBLE MEASURES / SECURITY CONTROLS.

A column related to the compatible level of security controls has been included:

Identification	Compatible Level	Detail

	Analogue	In the requirements analysis of the control analysed, it has been concluded that there is full compatibility. Both rules have identical requirements or the detailed measures are comparable. The security purposes for the control analysed are analogous in both standards.
	Partly analogous	In the requirements analysis of the control analysed, it has been concluded that there is not full compatibility. The standards are not equally demanding in the requirements described. Part of the requirements of the control analysed are similar, but not all parts of the control can be considered to be covered. It may be necessary to supplement the control with other controls scattered throughout the standard, or the standard may not have considered the control requirements not covered. While the purpose may be similar, one of the rules 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 compatibility. Some of the standards do not consider the control analysed. One of the rules has deployed a control for a purpose which is not pursued by the other rule.

Table. Compatible measures level matrix.

DIMENSIONS AND CATEGORY			Cod.	Control	ISO/IEC 27001:2022[40]	Compatible level of control ISO 27001:2022 - RD 311/2022.	
Basic	Medium	High			[Main Control]	Category ENS	Compatible level
			org	Organisational framework			
applies	applies	applies	org.1	Security policy	5.1 Information security policies 5.36 Compliance with information security policies and standards	MEDIUM	
applies	applies	applies	org.2	Safety regulations	5.10 Acceptable Use of Information and Associated Assets	MEDIUM	
applies	applies	applies	org.3	Security procedures	5.37 Documentation of operational procedures	MEDIUM	
applies	applies	applies	org.4	Authorisation process	5.2 Roles and responsibilities in information security	MEDIUM	
			op	Operational framework			
			op.pl	Planning			
applies	+ R1	+ R2	op.pl.1	Risk analysis	6.1 - Actions to address risks and opportunities	HIGH *	
applies	+ R1	+ R1 + R2 + R3	op.pl.2	Security architecture	Clause 4.4 Information security management system 8.27 Secure Systems Architecture and Engineering Principles	MEDIUM (+R2*)	

[40] Colour coding:
a) Blue: Organisational controls
b) Yellow: Technical controls.
c) Green: Checks on persons
d) Orange: Physical controls.

DIMENSIONS AND CATEGORY			Cod.	Control	ISO/IEC 27001:2022[40]	Compatible level of control ISO 27001:2022 - RD 311/2022.	
Basic	Medium	High			[Main Control]	Category ENS	Compatible level
applies	applies	applies	op.pl.3	Procurement of new components	5.8 Information Security in Project Management	MEDIUM	
applies	+ R1	+ R1	op.pl.4	Dimensioning/ Capacity management	8.6 Capacity Management	MEDIUM	
n.a.	applies	applies	op.pl.5	Certified components	Level of compatible measures: Not expressly provided for.	MEDIUM	
			op.acc	Access control			
applies	+ R1	+ R1	op.acc.1	Identification	5.16 Identity management	MEDIUM	
applies	applies	+ R1	op.acc.2	Access requirements	5.15 Access control	HIGH	
n.a.	applies	+ R1	op.acc.3	Segregation of duties and tasks	5.3 Segregation of duties	MEDIUM	
applies	applies	applies	op.acc.4	Access rights management process	5.18 Access rights 8.2 Access Privilege Management	MEDIUM	
+ [R1 or R2 or R3 or R4] + [R1 or R2 or R3	+ [R2 or R3 or R4] +R5	+ [R2 or R3 or R4] +R5	op.acc.5	Authentication mechanism (external users)	5.18 Access rights 8.5 Secure authentication	MEDIUM	
+ [R1 or R2 or R3 or R4] + R8 + R9	+ [R1 or R2 or R3 or R4] + R5 + R8	+ [R1 or R2 or R3 or R4] + R5 + R6 + R7 +	op.acc.6	Authentication mechanism (organisation's users)	8.5 Secure authentication	MEDIUM	
			op.exp	Exploitation			
applies	applies	applies	op.exp.1	Inventory of assets	5.9 Inventory of information and other associated assets	MEDIUM (+R4)	
applies	applies	applies	op.exp.2	Security settings	8.9 Configuration management	MEDIUM	
applies	+ R1	+ R1 + R2 + R3	op.exp.3	Configuration management	8.9 Configuration management	HIGH *	
applies	+ R1	+ R1 + R2	op.exp.4	Maintenance and security updates	7.13 Equipment maintenance 8.8 Technical Vulnerability Management	HIGH*	
n.a.	applies	+ R1	op.exp.5	Change management	8.32 Change management	HIGH *	
applies	+ R1 + R2	+ R1 + R2 + R3 + R4	op.exp.6	Protection against malicious code	8.7 Controls against malicious code	MEDIUM	
applies	+ R1 + R2	+ R1 + R2 + R3	op.exp.7	Incident management	5.24 Information Security Incident Management Planning and Preparedness 5.25Assessing and deciding on information security events	MEDIUM	
applies	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R3 + R4 + R5	op.exp.8	Registration of the activity	8.15 Event logs 8.17 Clock synchronisation	MEDIUM	
applies	applies	applies	op.exp.9	Incident management log	5.24 Information Security Incident Management Planning and Preparedness	MEDIUM	

DIMENSIONS AND CATEGORY			Cod.	Control	ISO/IEC 27001:2022[40]	Compatible level of control ISO 27001:2022 - RD 311/2022.	
Basic	Medium	High			[Main Control]	Category ENS	Compatible level
					5.28 Collecting evidence		
applies	+ R1	+ R1	op.exp.10	Cryptographic key protection	8.24 Use of cryptography	MEDIUM	
			op.ext	External services			
n.a.	applies	applies	op.ext.1	Contracting and service level agreements	5.19 Information security in relations with suppliers 5.20 Addressing information security within supplier agreements	MEDIUM	
n.a.	applies	applies	op.ext.2	Daily management	5.22 Monitoring, review and change management of supplier services	MEDIUM	
n.a.	n.a.	applies	op.ext.3	Supply chain security	5.21 Information security management in the ICT supply chain	HIGH *	
n.a.	applies	+ R1	op.ext.4	Interconnection of systems	8.22 Segregation in networks	MEDIUM	
			op.nub	Cloud service			
applies	+ R1	+ R1 + R2	op.nub.1	Protection of cloud services	5.23 Information security for use of cloud services	MEDIUM	
			op.cont	Continuity of service			
n.a.	applies	applies	op.cont.1	Impact analysis	5.29 Information Security During Disruption 5.30 ICT Preparedness for Business Continuity	MEDIUM	
n.a.	n.a.	applies	op.cont.2	Continuity plan	5.29 Information Security During Disruption 5.30 ICT Preparedness for Business Continuity	HIGH *	
n.a.	n.a.	applies	op.cont.3	Periodic testing	5.30 ICT Preparedness for Business Continuity	HIGH *	
n.a.	n.a.	applies	op.cont.4	Alternative MEDIUM	8.14 Redundancy of data processing resources	HIGH *	
			op.mon	System monitoring			
applies	+ R1	+ R1 + R2	op.mon.1	Intrusion detection	8.21 Security of network services	MEDIUM	
applies	+ R1+ R2	+ R1+ R2	op.mon.2	Metrics System	9 - Performance evaluation 9.1 - Monitoring, measurement, analysis and evaluation	MEDIUM	
applies	+ R1 + R2	+ R1 + R2 + R3 + R3 + R4 + R5 + R6	op.mon.3	Surveillance	5.7 Threat intelligence 8.16 Monitoring of activities	MEDIUM	
			mp	Protective measures			
			mp.if	Protection of installations and infrastructures			
applies	applies	applies	mp.if.1	Separate and access-controlled areas	7.1 Physical security perimeter	MEDIUM	

DIMENSIONS AND CATEGORY			Cod.	Control	ISO/IEC 27001:2022[40]	Compatible level of control ISO 27001:2022 - RD 311/2022.	
Basic	Medium	High			[Main Control]	Category ENS	Compatible level
applies	applies	applies	mp.if.2	Identification of persons	7.2 Physical input controls	MEDIUM	
applies	applies	applies	mp.if.3	Fitting out the premises	7.5 Protection from external and environmental threats 7.8 Siting and protection of equipment	MEDIUM	
applies	+ R1	+ R1	mp.if.4	Electric power	7.11 Supply installations	MEDIUM	
applies	applies	applies	mp.if.5	Fire protection	7.5 Protection from external and environmental threats	MEDIUM	
n.a.	applies	applies	mp.if.6	Flood protection	7.5 Protection from external and environmental threats	MEDIUM	
applies	applies	applies	mp.if.7	Check-in and check-out of equipment	7.2 Physical input controls	MEDIUM	
			mp.per	Personnel management			
n.a.	applies	applies	mp.per.1	Job characterisation	6.1 Checking	MEDIUM	
applies	+ R1	+ R1	mp.per.2	Duties and obligations	6.2 Terms and conditions of engagement	MEDIUM	
applies	applies	applies	mp.per.3	Awareness-raising	6.3 Information security awareness, education and training	MEDIUM	
applies	applies	applies	mp.per.4	Training	6.3 Information security awareness, education and training	MEDIUM	
			mp.eq	Protection of equipment			
applies	+ R1	+ R1	mp.eq.1	Uncluttered workstation	7.7 Uncluttered workstation and clean screen	MEDIUM	
n.a.	applies	+ R1	mp.eq.2	Workplace blocking	7.7 Uncluttered workstation and clean screen	MEDIUM	
applies	applies	+R1 + R2	mp.eq.3	Protection of portable devices	7.9 Security of off-site equipment 8.1 User end devices	HIGH *	
applies	+ R1	+ R1	mp.eq.4	Other devices connected to the network	8.1 User end devices	MEDIUM	
			mp.com	Protection of communications			
applies	applies	applies	mp.com.1	Secure perimeter	8.20 Network security 8.21 Security of network services	MEDIUM	
applies	+ R1	+ R1 + R2 + R3	mp.com.2	Protection of confidentiality	8.20 Network security 8.21 Security of network services	MEDIUM	
applies	+ R1 + R2	+ R1 + R2 + R3 + R4	mp.com.3	Protection of authenticity and integrity	8.20 Network security 8.21 Security of network services	MEDIUM	
n.a.	+ [R1 or R2 or R3] + [R1 or	+ [R2 or R3] + R4	mp.com.4	Separation of information flows in the network	8.22 Segregation in networks	MEDIUM	
			mp.si	Protection of information MEDIUM			

DIMENSIONS AND CATEGORY			Cod.	Control	ISO/IEC 27001:2022[40]	Compatible level of control ISO 27001:2022 - RD 311/2022.	
Basic	Medium	High			[Main Control]	Category ENS	Compatible level
applies	applies	applies	mp.si.1	Marking of supports	5.13 Labelling of information	MEDIUM	
n.a.	applies	+ R1 +R2	mp.si.2	Cryptography	8.24 Use of cryptography	MEDIUM (+R2)*	
applies	applies	applies	mp.si.3	Custody	7.10 Storage media	MEDIUM	
applies	applies	applies	mp.si.4	Transport	7.10 Storage media	MEDIUM	
applies	applies	applies	mp.si.5	Deletion and destruction	7.14 Safe disposal or re-use of equipment 8.10 Deletion of information	MEDIUM	
			mp.sw	Protection of computer applications			
n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4	mp.sw.1	Application development	8.25 Security in the development lifecycle	MEDIUM	
applies	+ R1	+ R1	mp.sw.2	Acceptance and commissioning	8.29 Developmental safety and acceptance testing	MEDIUM	
			mp.info	Protection of information			
applies	+ R1 + R2	+ R1 + R2	mp.info.1	Personal data	5.34Privacy and protection of personal data (PDD)	MEDIUM	
n.a.	applies	applies	mp.info.2	Qualification of information	5.12 Classification of information	MEDIUM	
applies	+ R1 + R2 + R3	+ R1 + R2+R2+ R3 +R4	mp.info.3	Electronic signature	8.24 Use of cryptography	MEDIUM	
n.a.	n.a.	applies	mp.info.4	Time stamps	8.24 Use of cryptography 8.26 Application security requirements	HIGH*	
applies	applies	applies	mp.info.5	Cleaning of documents	5.13 Labelling of information	MEDIUM	
applies	+R1	+ R1 + R2	mp.info.6	Back-up copies	8.13 Backing up information	MEDIUM (+R2) *	
			mp.s	Protection of services			
applies	applies	applies	mp.s.1	Protection of electronic mail	5.14 Transfer of information	MEDIUM	
+[R1 or R2]	+[R1 or R2]	+ R2+R3	mp.s.2	Protection of web services and applications	8.26 Application security requirements	MEDIUM	
applies	applies	+ R1	mp.s.3	Web browsing protection	8.2 Web filtering	MEDIUM	
n.a.	applies	+ R1	mp.s.4	Denial of service protection	8.6 Capacity Management	MEDIUM	

6. DEVELOPMENT OF COMPATIBLE SECURITY MEASURES

6.1. [ORG] ORGANISATIONAL FRAMEWORK

[org.1] Security Policy

- **Master Control ISO/IEC 27001:2022**
  - 5.1 Information security policies
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.2 Roles and responsibilities in information security
  - 6.4 Disciplinary proceedings
  - 5.31 Identification of legal, regulatory and contractual requirements

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

It shall be approved by top management and shall set out the organisation's approach to managing information security.

Consideration should be given to other policies that will 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.

Recommendation Implementation:

Roles will be defined, and safety committee members will also perform functions for both standards.

A lean and simple Governance Model is recommended, which considers the organisation's strengths, its functional structure and clear separation, which facilitates the deployment of security controls.

A Common Security Policy shall be drawn up, approved by the Committee and published in the Official Journal.

[org.1.5] Guidelines for the structuring of system security documentation, its management and access should be aligned with clause 7.5 Documented Information of ISO 27001.

It is advisable to review the documented information requirements that have been expressly included in the clauses.

[org.2] Security regulations

- **Master Control ISO/IEC 27001:2022**
  - 5.1 Information security policies
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.6 Contact with special interest groups

- 5.10 Acceptable Use of Information and Associated Assets
- 5.11 Return of assets
- 5.24 Information Security Incident Management Planning and Preparedness
- 5.36 Compliance with information security policies and standards
- 6.7 Teleworking
- 7.7 Uncluttered workstation and clean screen
- 7.9 Security of off-site equipment
- 8.1 User end devices

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Compliance with the organisation's information security policy, policies and specific standards should be reviewed periodically.

Recommendation Implementation:

In general, there will be regulations on the use of equipment, services and facilities, and very specifically, on improper use and, where appropriate, on liability for compliance or violation of the regulations: (disciplinary measures).

To achieve synergy, it is necessary to include the mandates of both standards, with the references to Clear Workplace [mp.eq.1], and the basic procedure/instruction for clearing metadata [mp.info.5] can be included as an annex.

Security documentation shall be available, according to the applicable CCN-STIC guidelines.

The regulations shall be approved by the Security Committee and shall be made known to the users concerned, including awareness-raising actions [mp.per.4] to help improve understanding.

[org.3] Security procedures

- **Master Control ISO/IEC 27001:2022**
  - 5.37 Documentation of operational procedures
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.5 Contact with the authorities
  - 5.37 Documentation of operational procedures
  - 5.14 Transfer of information
  - 5.36 Compliance with information security policies and standards

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Operating procedures for information processing actions should be documented and made available to staff who need them.

Recommendation Implementation:

A minimum of operating procedures will need to be maintained. The organisation should develop the necessary procedures associated with the system, specifying what, who and how to do the operations, manage abnormal activities and information.

Organisations may have suppliers in charge of drawing up the procedures in which they may be involved, and they may therefore be responsible for drawing up specific instructions, under the supervision of the entity's Security Officer.

Information shall be managed in accordance with 7.5 Documented information of ISO 27001:2022.

[org.4] Authorisation process

- **Master Control ISO/IEC 27001:2022**
  - 5.2 Roles and responsibilities in information security
- **Complementary Controls ISO/IEC 27001:2022**
  - Clause 5.3 Information security roles, responsibilities and authorities
  - 8.1 User end devices
  - 5.10 Acceptable Use of Information and Associated Assets
  - 7.10 Storage media
  - 8.19 Installing the software in production systems
  - 8.20 Network security
  - 8.21 Security of network services
  - 8.32 Change management

Category: MEDIUM
Level of measures Compatible: Partially analogue

Particularities of ISO:

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.

Recommendation Implementation:

While ISO is not as specific, it allows for a particularised authorisation process to be deployed.

The entity must maintain an authorisation process, which identifies the different roles and responsibilities, for key actions, including at least for the use of facilities, input of equipment and applications in production, interconnections and communication links, use of MEDIUM and information carriers.

Liability, related to system access, remote and handheld access, should also be considered.

It should be aligned with the change process. Consideration should be given not only to the ISO control but also to Clause 6.3 Change planning, *"Where the organisation determines the need for changes to the information security management system, these changes shall be carried out in a planned manner".*

It is recommended to deploy a responsibility matrix to clearly identify existing roles and their possible functions in relation to the assets and in the system.

6.2. [OP] OPERATIONAL FRAMEWORK

[OP.PL] PLANNING

[op.pl.1] Risk analysis

- **Master Control ISO/IEC 27001:2022**
  - 6.1 - Actions to address risks and opportunities
- **Complementary Controls ISO/IEC 27001:2022**
  - 6.1.1 - General Considerations
  - 6.1.2 - Information security risk assessment
  - 6.1.3 - Dealing with information security risks
  - 8.2 - Information security risk assessment
  - 8.3 - Dealing with information security risks

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

The criteria followed for risk acceptance, identifying risk owners, prioritising treatments and assuming residual risks should be documented.

Recommendation Implementation:

Both standards converge and the same risk methodology can be used to deploy this control. At least a semi-formal risk analysis will be necessary, using specific language, with a basic threat catalogue and tabular presentation, considering qualitative assessments of the system's most valuable assets, quantitative assessments of the most likely threats, assessment of safeguards and assessment of residual risk.

The MAGERIT methodology using the PILAR tool is recommended. However, the ISO 31000 methodology can be used.

A declaration of shared applicability of both rules should be considered.

The Safety Committee shall approve the risks and the treatment plan and receive feedback on risk management.

The Security Officer must approve the statement of applicability.

[op.pl.2] Security architecture

- **Master Control ISO/IEC 27001:2022**
  - 5.9 Inventory of information and other associated assets
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.20 Network security
  - 8.27 Secure Systems Architecture and Engineering Principles

Category: MEDIUM (+R2*)
Compatible measurement level: Analogue
Particularities of ISO:

The organisation shall establish, implement, maintain and continually improve an Information Security Management System in accordance with the requirements of the standard.

The principles for designing secure systems should be established, documented, maintained and applied to any information systems development activity.

Recommendation Implementation:

Both systems are supported by an Information Security and Management System, with an improvement cycle (PDCA). The requirements of category MEDIUM shall apply, together with the "Strengthening R2-Security Management System with continual improvement".

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

It is important to consider the part of documented information that ISO recalls throughout its clauses.

[op.pl.3] Acquisition of new components

- **Master Control ISO/IEC 27001:2022**
  - 5.8 Information security in project management
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.19 Information security in relations with suppliers
  - 5.20 Addressing information security within supplier agreements

Category: MEDIUM
Level of measures Compatible: Partially analogue

Particularities of ISO:

Procurement processes will be integrated into complete and comprehensive projects, which will cover many elements and should include procurement of components, architecture and requirements. Information security must be integrated into the organisation's project management activities.

Recommendation Implementation:

It is important to consider the overall process, and in a cross-cutting manner. This will document and include security requirements in the entity's procurement processes. And it shall be aligned

with capacity; formal process for planning the procurement of new system components, considering capacity [op.pl.4], system risks [op.pl.1], architecture [op.pl.2] and technical, training and funding needs.

This annual capacity plan shall consider forecasts, growth and security needs and resource requirements. It shall be approved by the Information Security Committee.

In any case, entities should consider integration into their procurement processes and full compliance with specific public procurement rules.

[op.pl.4] Dimensioning / Capacity Management

- **Master Control ISO/IEC 27001:2022**
  - 8.6 Capacity Management
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.23 Information security for the use of cloud services

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Planning, monitoring and adjustment. This management involves a dual strategy; increasing capacity and/or reducing demand.

Recommendation Implementation:

The two standards can converge perfectly well. In general, a study should be available at least annually, updated and monitored periodically. Different tools can be used to provide real-time information on the status of capacity and alerts, to see trends for specific periods and to generate alerts under defined thresholds. Automation is recommended, which can be through an ICT provider to help manage measurements, alerts and planning.

Cloud services can be helpful, given their scalability. Consider control [op.nub.1].

[op.pl.5] Certified components

- **Master Control ISO/IEC 27001:2022**
  - No compatible measures.
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.19 Information security in the relationship with suppliers.
  - 5.20 Addressing information security within supplier agreements.

Category: MEDIUM
Level of measures Compatible: Nil
Particularities of ISO:

There is no such control in ISO. However, it can be associated with assets, asset mapping and the risks that may arise. Accredited products and services must be involved, under the premise of improving security.

Recommendation Implementation:

This control is not contemplated in the ISO. It is necessary to include an inventory of the components affected, analysing whether they comply with the established requirements, the particularities provided for in Article 19 of the Royal Decree and specifically whether they are components included in the STIC CCN 105 Catalogue. Where appropriate, similar European accreditations, such as Common Criteria (EU), should be considered.

It is recommended that these requirements be integrated as requirements in the procurement and contracting processes, such as future procurements of new components.

Where components are not listed in the relevant catalogue, other product or service certifications, e.g. from the ISO 27000 family, can be associated.

[OP.ACC] ACCESS CONTROL

[op.acc.1] Identification

- **Master Control ISO/IEC 27001:2022**
  - 5.16 Identity management
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.15 Access control

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

The full lifecycle of identities must be managed.

Recommendation Implementation:

Both standards allow for the management of identities in a comprehensive manner. To this end, users must be identified with a unique identifier and can be aligned with the premises of the standard.

When a user must have different roles in the system, he/she will receive different identifiers. It is important that every entity (entity, user or process) has a unique identifier that allows to know who acts [id] and the actions performed by each entity. In addition, accounts must be disabled for loss of need and associated with the necessary withholdings. Withholdings must be considered based on legal requirements.

Reinforcement R1 - Advanced identification will be considered; it will be possible to single out the person, the associated privileges and a list of users will be maintained.

It is recommended that the entity keeps an inventory of services (including those provided by cloud services) and associates the permissions granted. In this register, the identification methodology can be controlled.

Records or traces can be traced through the active directory and the records and holds associated with the activity records can be maintained.

[op.acc.2] Access requirements

- **Master Control ISO/IEC 27001:2022**
  - 5.15 Access control
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.18 Access rights
  - 8.2 Access Privilege Management
  - 8.3 Restriction of access to information
  - 8.18 Use of privileged utility programs
  - 8.4 Access to source code

Category: HIGH *
Compatible measurement level: Analogue
Particularities of ISO:

Rules for controlling physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.

Various methods can be used for access control, and dynamic elements can be deployed.

Recommendation Implementation:

Access rights for each resource shall be established according to the decisions of the resource manager, in compliance with the security policy and regulations of the system. 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, 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).

In particular, the access to operating system components and their configuration files or registers shall be controlled.

It is necessary to consider Strengthening R1 - Access Privileges, aligning both frameworks and specifically control 8.2. Privileged access rights.

- op.acc.2.r1.1] All authorised users must have a set of security attributes (privileges) that can be individually maintained.

- op.acc.2.r1.2] Access privileges shall be implemented to restrict the type of access a user may have (read, write, modify, delete, etc.).

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

- **Master Control ISO/IEC 27001:2022**
  - 5.3 Segregation of duties
- **Complementary Controls ISO/IEC 27001:2022**

- 5.18 Access rights
- 8.2 Access Privilege Management

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Duties and conflicting areas of responsibility should be segregated.

Recommendation Implementation:

The requirements of the MEDIUM category shall apply. Exceptionally, where entities are limited in terms of "qualified" staff, compensatory measures for the requirement may be considered, [op.acc.3.1] Where possible, development and operational capabilities should not be carried out by the same person, and where segregation is difficult, other controls such as activity monitoring, audit trails and management oversight may be considered.

An inventory of operations should be available, allowing differentiation of segregations and on whom they fall. For example, in change issues; access rights, code and development, system in production, applications, DB remote access…

[op.acc.4] Access rights management process

- **Master Control ISO/IEC 27001:2022**
  - 5.18 Access rights
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.2 Access Privilege Management

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Granting and revoking access rights. Review actions should be taken upon change or termination of employment.

The allocation and use of privileged access rights must be restricted and managed.

Recommendation Implementation:

"Both standards converge, although in the case of ISO, provisions contained in several controls must be considered.

Compliance with the principles of; "*all access shall be prohibited unless expressly authorised"; "ability to authorise, with periodic review of permissions"; [org.4]"Minimal privilege to perform duties or functions"; "need to know and responsibility to share"; and "specific remote access policy, requiring express authorisation*" shall be documented.

It is important to consider that this control affects all users, so third-party users must be managed.

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

- **Master Control ISO/IEC 27001:2022**
  - 5.18 Access rights
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.5 Secure authentication

Category: MEDIUM
Level of measures Compatible: Partially analogue
Particularities of ISO:

Ensure that access rights are activated (e.g. by service providers) only after authorisation procedures are successfully completed.

Recommendation Implementation:

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 in detail, although it does consider the requirements imposed by the ENS.

It is important to consider the Reinforcement R5 Register

[op.acc.5.r5.1] Successful and unsuccessful accesses shall be logged.

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

Third parties may be involved and the responsibilities of the provider (developer and maintainer of services) and the service holder should be considered.

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

- **Master Control ISO/IEC 27001:2022**
  - 8.5 Secure authentication
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.15 Access control

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Secure authentication technologies and procedures shall be implemented according to the information access restrictions and the specific policy on access control.

Recommendation Implementation:

ISO control allows authentications to be adapted to ENS requirements, modulated with the particularities required for ENS control.

Before providing credentials, users shall be aware of and accept the security policy and acknowledge that they have received the access credentials and that they are aware of and accept the obligations involved, including the duty of diligent safekeeping, the protection of their confidentiality and the duty of immediate notification in the event of loss.

The system will only provide the information necessary for the user to authenticate, and if the user is rejected, the reason for the rejection will not be given.

The number of attempts allowed shall be limited, and the user shall be informed of his rights or obligations immediately after gaining access, as well as of the last access made with his identifier. Accesses and attempts shall be logged.

Physical accesses to the facilities may be considered as accesses to controlled areas provided that the requirement set out in the control [op.acc.6] is fulfilled. The controlled area shall be considered as a differentiating element to require greater robustness in authentication:

a) Controlled area; considered as an area that is not publicly accessible and the user, before having access to the equipment, has been authenticated in some way (facility access control), but with a different mechanism than the logical authentication against the system.

b) Uncontrolled area, e.g. Internet. Reinforcement of the authentication process is required.

As authentication mechanisms in controlled areas, you can choose between:

(a) Password when access is from controlled areas and not through uncontrolled areas

b) Password and Other factor

(c) Certificate

Double factor for access from or through uncontrolled areas.

a) Password and Other factor

(b) Certificate

By default, a remote access policy shall be documented for authorised users and situations. Remote access shall:

a) Be authorised.

b) Its traffic shall be encrypted.

c) To be disabled when not necessary, if the use is not constant.

d) Have audit trails of such connections.

The reinforcements (+R6) and (+R7) may be of interest based on the criticality of the information it can process and aligns with the practices set out in ISO 27002.

Access from a provider may be authorised, access via tunnels, with source IP and prior access control by the provider.

Finally, the reinforcements contained in the High category can be considered, as they can improve access security and are covered by ISO 27002:

- end inactive sessions after a defined period of inactivity,

- 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] EXPLOITATION

[op.exp.1] Inventory of assets

- **Master Control ISO/IEC 27001:2022**
  - 5.9 Inventory of information and other associated assets
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.11 Return of assets
  - 7.8 Siting and protection of equipment
  - 7.9 Security of off-site assets

Category: MEDIUM (+R4)
Compatible measurement level: Analogue
Particularities of ISO:

An inventory of information and other associated assets should be developed and maintained, including their owners.

Recommendation Implementation:

The BASIC category requirements apply. It should be recommended to consider the reinforcements present in this control, which although not directly applicable may help to manage the assets in a more complete way. As an example, see "Enforcement 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 analogous to that required in [mp.sw.1.r5].

It is important to manage asset inventories, which can be simple tools or more complex depending on the volume of assets and the organisation's budget. Ideally, however, the inventory should be traceable to key points such as security incidents or change management.

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, so periodic reviews should be carried out; and an update should be automatically applied after 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 planning.

Finally, it may enrich the inventory information to include the corresponding control information [op.pl.5].

[op.exp.2] Security Settings

- **Master Control ISO/IEC 27001:2022**

- 8.9 Configuration management

- **Complementary Controls ISO/IEC 27001:2022**
  - 8.8 Technical vulnerability management
  - 8.12 Data leakage prevention
  - 8.19 Installing software in production systems
  - 8.20 Network security
  - 8.21 Security of network services.

Category: MEDIUM
Level of measures Compatible: Partially analogue
Particularities of ISO:

Configurations, including security, hardware, software, services and network configurations must be established, documented, implemented, monitored and reviewed.

Recommendation Implementation:

The equipment shall be configured prior to its entry into operation so that:

- Standard accounts and passwords are withdrawn.

- The "minimum functionality" rule shall apply, it shall be a safe use.

Virtual machines shall be configured and managed in a secure manner in the same way as physical machines are managed.

Many functions may be managed by the service provider, who will consider the necessary security requirements and specifically, those CCN- STIC guidelines[41] and/or CCN tools that may be useful. The system documentation will consider basing guidelines and documentation of those tools that help to manage possible deviations or vulnerabilities. ENS requirements should be deployed in order to maintain an appropriate configuration.

Because of the area of exposure, assets that are only in-house and do not present significant risks may be configured with a generic security template, lowering certain security requirements.

[op.exp.3] Configuration management

- **Master Control ISO/IEC 27001:2022**
  - 8.9 Configuration management
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.8 Technical vulnerability management
  - 8.12 Data leakage prevention
  - 8.13 Backing up information
  - 8.19 Installing software in production systems

[41] https://www.ccn-cert.cni.es/guias.html

- 8.20 Network security
- 8.21 Security of network services.

Category: HIGH*
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

Configurations, including security, hardware, software, services and network configurations must be established, documented, implemented, monitored and reviewed.

Recommendation Implementation:

The organisation should define and implement processes and tools to enforce configuration. In addition to maintaining a set of standard templates for hardware, software, services and network security configuration, they should be periodically reviewed and, where necessary, updated. The need to enforce security configuration should be defined and implemented in processes and tools.

The requirements of category HIGH with the enhancements; "Enhancement R2-Configuration Responsibility" [op.exp.3.r2.1] shall apply. [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 and, in addition, the processes shall consider copies of the configurations, which will allow us to align both standards; "Enforcement R3-Backups". [op.exp.3.r3.1] The system configuration shall be backed up in such a way that it is possible to rebuild part or all of the system after an incident.

Cloud services shall be based on the applicable CCN STIC guidelines.

System documentation shall consider basing guidelines and documentation of tools that help to manage possible deviations or vulnerabilities.

[op.exp.4] Maintenance and security updates

- **Master Control ISO/IEC 27001:2022**
  - 7.13 Equipment maintenance

Complementary Controls ISO/IEC 27001:2022

- 8.8 Technical vulnerability management
- 8.31 Separation of development, test and production environments
- 8.32 Change management

Category: HIGH*
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

Equipment must be properly maintained. This entails a maintenance process and maintenance record.

Recommendation Implementation:

The ENS is stricter in its requirements, and the application of this control is recommended in its HIGH category, although it can be considered in its MEDIUM category. Compatibility can be achieved through the controls identified and deployed in the system:

1.- 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 the requirements in the applicable supplier, support and licensing contracts.

An effective process for technical vulnerability management 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.

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); test and deploy in production.

4.- In the case of cloud services, part or even all of the responsibility for managing technical vulnerabilities of their services is shifted to the provider, and processes for reporting actions to customers will be included.

5.- Change management cannot be isolated in either standard, and the change management cycle itself can be leveraged. 6. If adequate testing of updates is not possible, e.g. 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 to identify vulnerabilities.

8.- When software patches or updates occur, the organisation may consider providing an automated update process in which these updates are installed on affected systems or products without the need for end-user intervention.

[op.exp.5] Change management

- **Master Control ISO/IEC 27001:2022**
  - 8.32 Change management
- **Complementary Controls ISO/IEC 27001:2022**
  - 7.13 Maintenance of equipment
  - 8.8 Technical Vulnerability Management
  - 8.31 Separation of development, test and production environments

Category: HIGH*
Compatible measurement level: Analogue
Particularities of ISO:

Changes to the organisation, processes, facilities and information systems should be subject to change management procedures.

Recommendation Implementation:

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.

The requirements of category HIGH shall apply. It is necessary to associate "Reinforcement R1-Failure prevention" with the control [op.exp.4].

It is undeniable that there will be situations requiring emergency and contingency changes, which will be the exception to the process but which will require a full security review afterwards.

[op.exp.6] Protection against malicious code

- **Master Control ISO/IEC 27001:2022**
  - 8.7 Controls against malicious code
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.8 Technical vulnerability management
  - 8.9 Configuration management

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Protection against malware must be implemented, including user awareness actions.

Recommendation Implementation:

Both standards converge perfectly, although it is necessary for control to be led by the ENS requirements for the MEDIUM category. This will provide solutions for detecting malicious code on all equipment and devices in the system, updating databases and analysing any external files. The solution will analyse the systems at start-up.

We must consider the impact of this control on control [op.exp.4] Maintenance and continuity controls [op.cont] and consider control [mp.per. 3].

.. op.exp.7 Incident Management

- **Master Control ISO/IEC 27001:2022**
  - 5.24 Information Security Incident Management Planning and Preparedness
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.24 Information Security Incident Management Planning and Preparedness
  - 5.25 Assessing and deciding on information security events
  - 5.26 Information security incident response
  - 5.27 Learning from information security incidents
  - 5.28 Gathering evidence
  - 6.8 Notification of Information Security Events

Category: MEDIUM
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

Security incident management will be carried out, defining and establishing a process, with the roles involved and responsibilities.

Recommendation Implementation:

In the case of ISO, there are several controls to be considered in order to meet the requirements of the ENS in its MEDIUM category. 5.24 Information security incident management planning and preparation, 5.25 Assessment and decision on information security events, 5.26 Information security incident response, 5.27 Learning from information security incidents.

It is desirable that entities tend to comply with the requirements as detailed in the ENS, given that the Royal Decree is aligned with European regulations and outlines the cybersecurity strategy. Consideration should be given to deploying a process that will be aligned with the CCN-STIC Guide 817 and the National Cyber Incident Guide and work under the single window, the LUCIA platform (Strengthening R1 - Notification [op.exp.7.r1.1] public sector entities).

The entity shall develop a comprehensive process for dealing with security incidents, including classification criteria and escalation of notification. A process for the reporting of lost or stolen devices and laptops [mp.eq.3.2] shall be included and the necessary measures and sufficient resources for incident management shall be deployed.

[op.exp.8] Logging of user activity

- **Master Control ISO/IEC 27001:2022**
  - 8.15 Event registration
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.17 Clock synchronisation

Category: MEDIUM
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

Logs of activities, exceptions, failures, faults and other relevant events must be activated, protected, stored and analysed.

Recommendation Implementation:

The ENS standard is stricter in terms of requirements than ISO, but the latter allows the process to be deployed with the security points we need. Thus, an audit log will be kept operational, which will include at least the user or entity identifier, date and time, what information is affected, type of event (*) and its result (failure or success). It is necessary to activate the logs on the servers.

An informal review process shall be maintained, maintaining strict control over access to records and their configuration; clock synchronisation shall be maintained for evidence of recording; and a register or inventory shall be prepared with operational records, third parties involved and retention times established.

With regard to events (*), they should be considered [recommended]:

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 additional events reflected in the different security policies (including changes in system configuration; use of utility programs and other applications; activation and deactivation of protection systems, such as anti-virus systems and intrusion detection systems).

While it is not necessary to automate the review process for the MEDIUM category, it is advisable to have a security information and event management (SIEM) tool or an analogous service to store, correlate, normalise and analyse log information and generate alerts.

SIEMs tend to require careful configuration to optimise their benefits. Settings to consider include identifying and selecting appropriate logging sources, tuning and testing rules, and developing use cases.

Cloud services should maintain their own activity logging and alert management service.

It is recommended that, if you are analysing solutions on the market that cover the ENS requirements, you take into account that these 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

- **Master Control ISO/IEC 27001:2022**
  - 5.26 Information security incident response
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.24 Information Security Incident Management Planning and Preparedness
  - 5.25 Assessing and deciding on information security events
  - 5.26 Information security incident response
  - 5.27 Learning from information security incidents
  - 5.28 Gathering evidence
  - 6.8 Notification of information security events

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

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 postmortem procedures.

Recommendation Implementation:

On a general level ISO is flexible in deploying ENS requirements. All actions derived from [op.exp.7] must be documented. The Register may be managed by a manual file, but it must be mapped to the requirements set out in CCN STIC Guide 817 and, where access is available, the LUCIA solution itself.

Evidence will be managed for use in any jurisdictional setting, (disciplinary purposes and/or diversion of external suppliers and/or prosecution of crime).

There shall be analysis of incidents and identification of auditable events [op.exp.8].

To facilitate the recording of accurate information, the use of incident forms is recommended to assist staff in collecting all necessary information.

For the purposes of the ENS, there will be feedback processes with other entities and, based on this information, it will be possible to report the necessary information security events. It is interesting for the organisation to receive regular information on the global trend of incidents and attacks, both within the organisation's sphere of activity and in its own area of activity. This can help the entity to calibrate prevention measures and even train and raise awareness among its users.

[op.exp.10] Cryptographic key protection

- **Master Control ISO/IEC 27001:2022**
  - 8.24 Use of cryptography
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.17 Authentication Information

Category: MEDIUM
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

Rules for the effective use of cryptography, including cryptographic key management, must be defined and implemented.

The level of protection required derives from the classification of the information itself both for the type, strength and quality of the cryptographic algorithm required.

The organisation shall 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). The ICT Security Guide CCN-STIC 807 shall be taken into account.

Recommendation Implementation:

ISO itself derives from legal requirements, in the fulfilment of this control. In order to implement the organisation's rules for the effective use of cryptography, account must be taken of legislation and restrictions that may apply to the use of cryptographic techniques and the problems of encrypted information transmissions.

It is therefore necessary for the NSS to lead the requirements.

Cryptographic keys shall be protected throughout their life cycle and the entity shall maintain processes and tools for this purpose. An inventory and analysis of the algorithms used shall be kept.

The means of generation and operation shall be isolated.

There shall be a retention of the keys to be archived and the retention of these keys shall be monitored.

Key management, algorithm requirements (see CCN STIC Guide 807 and CCN STIC Guide 221), corresponding certificates and qualified signatures are considered.

Services managed by third parties and especially those in the cloud should consider the requirements of this control. However, the entity should verify compliance with this control.

For key managers, CCN-STIC-105 ICT Security Products and Services Catalogue, 7.2.7 FAMILY: CRYPTOGRAPHIC KEY MANAGEMENT DEVICES" should be considered.

[OP.EXT] EXTERNAL SERVICES

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

- **Master Control ISO/IEC 27001:2022**
  - 5.19 Information security in supplier relations
- **Complementary Controls ISO/IEC 27001:2022**
  - 6.6 Confidentiality or non-disclosure agreements
  - 5.19 Information Security in Supplier Relationships
  - 5.20 Addressing information security within supplier agreements
  - 5.21 Information security management in the ICT supply chain

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

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.

Recommendation Implementation:

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. Service Level Agreements should be included as a requirement in contracts (and specifically in tenders), as well as the characteristics of the "minimum acceptable service", the liability and consequences of non-compliance. Other affected controls [op.cont] and [op.pl.3] [op.pl.4] and especially those services derived from a third party shall be taken into account. Cloud services [op.nub] shall be considered here.

It is advisable to have a register that traces all contracts concerned and allows control of suppliers, their security requirements and access to information and the system.

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

- **Master Control ISO/IEC 27001:2022**
  - 5.22 Monitoring, Review and Change Management of Supplier Services
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.19 Information Security in Supplier Relationships
  - 5.20 Addressing information security within supplier agreements
  - 5.21 Information security management in the ICT supply chain

Category: MEDIUM
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

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 must be defined.

Recommendation Implementation:

Its 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, periodic reports should be required in procurement processes (tender documents and minor contracts) that present indicators and measurements/trends and serve to assess the service, the required agreements and the needs of the given service. It is recommended that suppliers be required to issue reports (with a certain frequency and at least annually) on compliance and/or deviations, especially for cloud services. Public entities should consider the measurements required annually in the national INES survey.

[op.ext.3] Supply Chain Security

- **Master Control ISO/IEC 27001:2022**
  - 5.21 Information security management in the ICT supply chain
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.29 Information Security During Disruption

Category: HIGH *
Compatible measurement level: Analogue
Particularities of ISO:

The relationship between the organisation and the supplier must be managed to: monitor and track service performance levels and verify compliance with agreements.

Responsibilities for this must be defined.

Processes and procedures should be defined and implemented to address information security risks associated with ICT services and the product supply chain.

Recommendation Implementation:

This control should be considered to align both standards, so that the category HIGH, related to the controls in the block of controls [op.cont], will apply.

It is appropriate to consider the requirement of the provision contained in Article 2 of Royal Decree 311/2022 of 3 May;

"The administrative or technical specifications for contracts entered into by public sector entities (...) shall include all those requirements necessary to ensure compliance with the ENS (...)".

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

In the entity's risk analysis, services and outsourcing should be considered, irrespective of the methodology used.

The legal requirements involved must be considered.

Suppliers should be required to propagate security requirements throughout the supply chain if they outsource 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] System Interconnection

- **Master Control ISO/IEC 27001:2022**
  - 8.22 Segregation in networks
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.20 Network security
  - 8.21 Security of network services.

Category: MEDIUM
Level of measures Compatible: **Nil**
Particularities of ISO:

Networks often extend beyond organisational boundaries, as partnerships are formed that require interconnection or sharing of networks and information, which can increase risk.

Recommendation Implementation:

This control is a direct requirement of the ENS, the ICT Security Guide CCN-STIC 811 will be taken into account.

For ISO purposes it is perceived in some controls. The MEDIUM category shall apply and attention shall be paid to 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 associated with public requirements (e.g. SARA NETWORK or IRIS NETWORK), the provision contained in

Article 29 Common infrastructures and services must be considered. "The use of common infrastructures and services of the public administrations, including shared or transversal ones, 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."

An up-to-date diagram and prior authorisation must be maintained, and analysis of the security and data protection requirements and the nature of the information exchanged must be maintained".

[OP.NUB] CLOUD SERVICE

[op.nub.1] Protection of cloud services

- **Master Control ISO/IEC 27001:2022**
  - 5.23 Information security for the use of cloud services
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.19 Information Security in Supplier Relationships
  - 5.20 Addressing information security within supplier agreements
  - 5.21 Information security management in the ICT supply chain
  - 5.22 Monitoring, review and change management of supplier services

Category: MEDIUM
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

Processes and procedures should be defined and implemented to address information security risks associated with ICT services and the product supply chain.

Recommendation Implementation:

ISO requirements are closely aligned with the ENS. Services will require compliance with ENS measures and will be maintained during the service.

The corresponding certification in the MEDIUM category will be required. However, the entity should consider the R2 Strengthening - Specific Security Configuration Guidelines and associate this to the control related to [org.3] and [op.exp.2].

With reference to [op.nub.1.r1.2]; if the cloud service is a security service it shall comply with the requirements set out in [op.pl.5].

Where there are suppliers or services lacking this, a complementary measure identifying the applicable controls may be deployed. Certification to ISO 27001 may be accepted as a complementary measure. Where appropriate, a measure derived from CCN STIC Guide 819 may be considered.

[OP.CONT] CONTINUITY OF SERVICE

[op.cont.1] Impact analysis

- **Master Control ISO/IEC 27001:2022**
  - 5.29 Information Security During Disruption
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.30 ICT Preparedness for Business Continuity

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

The organisation should plan how to maintain information security at an appropriate level during the disruption.

Recommendation Implementation:

Both frameworks highlight the key element of resilience and contingency: planning. Planning should consider the scope, the impact of disruptions and prioritise the consequences of loss of confidentiality and integrity of information, as well as the need to maintain availability. Services and criticalities must be considered, allowing RTOs and RPOs to be detected.

It is recommended that identified risks (output of the risk analysis [op.pl.1]), which have the particularity of having a high impact and low probability, be analysed. These risks can be considered as scenarios associated with disruptions and should be used to assist in the preparation of contingency situations.

[op.cont.2] Continuity plan

- **Master Control ISO/IEC 27001:2022**
  - 5.29 Information Security During Disruption
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.30 ICT Preparedness for Business Continuity
  - 8.14 Redundancy of data processing resources

Category: HIGH *
Compatible measurement level: Analogue
Particularities of ISO:

The organisation should plan how to maintain information security at an appropriate level during the disruption.

Recommendation Implementation:

"The entity should consider the deployment of control in its HIGH category. There are situations in which the dependencies and the needs associated with the availability of services require the deployment of continuity strategies. But also, when we carry out a process of integration of the

National Security Framework and ISO 27001, the controls associated with continuity and alternativity must be promoted.

A comprehensive plan must be designed that necessarily includes the entity's contingency strategy, information, systems, assets, personnel, facilities, collaborators and support tools. It is necessary to plan and maintain preparedness for the hypothetical materialisation of a catastrophic event.

Within the organisation's strategy, consideration should be given to those security controls that will not operate during a total outage or shutdown of the organisation, and where appropriate, to propose compensating controls for those information security controls that cannot be maintained during the outage. A good strategy for this may be to consider an applicability statement with complementary sources to ISO 27001 and the ENS, identifying those controls that will be temporarily disabled and those that will be temporarily enabled as an alternative or compensatory measure. ".

[op.cont.3] Periodic tests

- **Master Control ISO/IEC 27001:2022**
  - 5.30 ICT Preparedness for Business Continuity
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.29 Information Security During Disruption
  - 8.13 Backing up information

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

ICT preparedness should be planned, implemented, maintained and tested against business continuity objectives and ICT continuity requirements.

Recommendation Implementation:

This control shall be included as a HIGH category control. As part of the continuity strategy, the entity should analyse the most appropriate tests to check that its planning is correct and that the estimated resources are sufficient. The need for ICT preparedness for business continuity can be enriched by also considering identified high impact, low probability risks.

The entity should establish a test plan, with schedules and responsible persons, and document the results for detailed analysis and study. Different modalities and different perspectives can be considered for testing, both mock and paper tests.

Planning 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 tests associated with the most critical services, plot timelines and analyse deviations.

[op.cont.4] Alternative means

- **Master Control ISO/IEC 27001:2022**
  - 8.14 Redundancy of information processing resources

- **Complementary Controls ISO/IEC 27001:2022**
  - 5.29 Information Security During Disruption
  - 8.13 Backing up information

Category: HIGH *
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

Information processing facilities must be implemented with sufficient redundancy to meet availability requirements.

Recommendation Implementation:

In order to have a management system aligned with the two standards, this HIGH category control shall be included. The scope of the control can be aligned to the main ISO requirement, but in any case, the organisation must align its capacity plan [op.pl.4] with this control, given that there are (classic) contingency scenarios associated with "unavailability" of key resources on a day-to-day basis.

It is recommended that the organisation design and implement a system architecture with adequate redundancy to meet these requirements.

Cloud services enable compliance with this control, provided they are considered as an alternative or contracted with the key redundancy service.

[OP.MON] SYSTEM MONITORING

[op.mon.1] Intrusion Detection

- **Master Control ISO/IEC 27001:2022**
  - 8.20 Network security
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.21 Security of network services.
  - 8.23 Filtering of Websites

Category: MEDIUM
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

Networks and network devices will be secured, managed and controlled to protect information in systems and applications. 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.

Recommendation Implementation:

Although ISO monitoring includes the protection of IDS/IPS services themselves, specific consideration should be given to the deployment of rule-based intrusion detection and/or prevention tools and/or functionalities, whereby it is sufficient to have network devices configured

for monitoring purposes. SaaS services will necessarily include these measures as part of the service.

[op.mon.2] Metric system

- **Master Control ISO/IEC 27001:2022**
  - 9 - Performance evaluation
- **Complementary Controls ISO/IEC 27001:2022**
  - 9.1 Monitoring, measurement, analysis and evaluation

Category: MEDIUM
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

The organisation shall assess the information security performance and the effectiveness of the information security management system. The organisation shall determine who, when, what, and how, should be monitored.

Metrics can be used for both systems, but for ISO purposes, they must include the monitoring of safety targets.

Recommendation Implementation:

The ENS criteria should be imposed to compile the required metrics, taking into account what is indicated in the ICT Security Guide CCN-STIC 817. The entity should maintain a measurement related to the degree of implementation of security measures and, where appropriate, in those public entities should make the annual report on the state of security, using the INES platform. In addition, it is advisable to take into account the measurements of maturity levels and implementation levels in accordance with CCN-STIC Guide 808.

Measurements derived from [op.exp.9] and analysis of resources, hours and budget for security are considered.

The entity could deploy in the system a catalogue of general metrics associated with a Statement of Applicability and extend measurements to ISO security controls and objectives, considering Clause 6.2 Information security objectives and planning for their achievement; these should be measurable (if possible). To achieve compatible measures, appropriate security objectives and metrics should be considered.

[op.mon.3] Surveillance

- **Master Control ISO/IEC 27001:2022**
  - 5.7 Threat intelligence
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.8 Technical vulnerability management
  - 8.16 Monitoring of activities

Category: MEDIUM

Compatible measurement level: Analogue
Particularities of ISO:

Information related to security threats will be collected and analysed to generate information.

Recommendation Implementation:

An automatic system for collecting and correlating security events, services/architecture will be available. This service may be developed directly by the entity or it may be contracted to a third party. Sometimes cloud services will include this service as an added element.

The entity shall also have monitoring solutions in place to determine the exposure surface in relation to vulnerabilities and configuration deficiencies. This security functionality may also be an outsourced service managed by a third party. These monitoring solutions shall allow the determination of the exposure surface in relation to vulnerabilities and configuration deficiencies. It is advisable to consult the solutions of the CCN and in any case to consider CVE analysis through official sources and lists. The organisation could consider vulnerability warnings and consider them for risk analysis and analyse the impacts derived from them. In any case, it is advisable to maintain a broad system of sources, through information provided by different agents, such as suppliers or independent advisors, control authorities or threat intelligence expert groups.

A significant element to consider is the format available for system logs and events, so that they can be stored in a standardised format, which can be exploited by correlators or syslog.

Entities can consult the different tools available in the CCN for the management of this control.

For ISO we talk about threat intelligence and requires connection to controls 5.25 Information security event assessment and decision, 8.7 Controls against malicious code, 8.8 Technical vulnerability management; 8.16 Activity tracking or 8.23 Web filtering, to maintain the quality of threat intelligence.

6.3 [MP] PROTECTIVE MEASURES

[MP.IF] PROTECTION OF INSTALLATIONS AND INFRASTRUCTURES

[mp.if.1] Separate and access-controlled areas

- **Master Control ISO/IEC 27001:2022**
  - 7.1 Physical security perimeter
- **Complementary Controls ISO/IEC 27001:2022**
  - 7.3 Security of offices, offices and resources
  - 7.6 Working in safe areas

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

There shall be security perimeters, in areas with protection according to the information and/or assets they contain.

Recommendation Implementation:

"Data Processing Centre (DPC) shall be installed, as far as possible, in specific separate areas, and access shall be controlled. This facility may not exist at the infrastructure level, either because the entity has outsourced housing/hosting services to a third party, or because it is working with cloud services (IaaS, PaaS, SaaS) or because the infrastructure itself depends on another entity. Entities must analyse the impact of control and maintain the requirements of both standards. In any case, security measures should be considered as extending to data processing centres and communications or interconnection rooms. Compliance should be considered for own infrastructure and, where appropriate, require providers and cloud services to comply with these. In any case, services contracted from a provider will involve these measures, which will be required in the contracting process.

A key management protocol can 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

- **Master Control ISO/IEC 27001:2022**
  - 7.2 Physical input controls
- **Complementary Controls ISO/IEC 27001:2022**
  - 7.1 Physical security perimeter
  - 7.6 Working in safe areas

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Separation of delivery and loading and unloading areas.

Visitor control, including supplier personnel, inspection of deliveries and delivery notes.

Monitoring of technical processes of access controls".

Recommendation Implementation:

Persons accessing the data processing and communications infrastructures shall be identified and the corresponding entries and exits shall be recorded.

In any case, the services contracted to a supplier will involve these measures, which will be required in the contracting process.

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

- **Master Control ISO/IEC 27001:2022**
  - 7.5 Protection against external and environmental threats.
- **Complementary Controls ISO/IEC 27001:2022**
  - 7.3 Security of offices, offices and resources
  - 7.6 Working in safe areas
  - 7.8 Siting and protection of equipment

- 7.12 Cabling safety

Category: MEDIUM
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

For full compatibility, it should be considered, together with other controls.

Protection against external and environmental threats, intentional or unintentional, should be designed and implemented.

Recommendation Implementation:

Consideration shall be given to office conditions themselves and specifically, conditioning arising from prevention, AARR and problems arising from cabling and communications cabinets. Reviews and controls will be carried out with regard to:

[mp.if.3.1] Temperature and humidity conditions.

[mp.if.3.2] Protection against the threats identified in the risk analysis.

[mp.if.3.3] The protection of cabling against accidental or deliberate incidents.

Compliance with this control through ISO relies on a number of controls. Security of offices, offices and resources; 7.8 Siting and protection of equipment; 7.12 Security of cabling; 7.13 Security of equipment; 7.14 Security of equipment.

Thus control 7.8 Site equipment protection refers to the need to deploy controls to minimise the risk from 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] Electrical energy

- **Master Control ISO/IEC 27001:2022**
  - 7.11 Supply installations
- **Complementary Controls ISO/IEC 27001:2022**
  - 7.12 Cabling safety
  - 5.30 ICT Business Continuity Preparedness

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Information processing facilities must be protected against power outages and other disruptions caused by failures in support services.

Recommendation Implementation:

Sufficient power sockets shall be provided and the supply and operation of emergency lighting can be ensured. Surge-prepared power strips or UPS shall be considered at the level of equipment installed in the offices.

With the information available, we will have to deploy the risk analysis and consider the impacts.

It is a good strategy to consider tests associated with [op.cont] in order to demonstrate the redundancy and robustness of the support system. It is advisable to associate maintenance [op.exp.4] and, if necessary, changes [op.exp.5], key elements such as batteries, repairs...

[mp.if.5] Fire protection

- **Master Control ISO/IEC 27001:2022**
  - 7.5 Protection against external and environmental
- **Complementary Controls ISO/IEC 27001:2022**
  - 7.3 Security of offices, offices and resources
  - 7.6 Working in safe areas

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Protection against physical and environmental hazards, such as natural disasters and other intentional or unintentional physical threats to infrastructure, must be designed and implemented.

Recommendation Implementation:

Consideration will be given to the office conditions themselves and specifically, to risk-prevention derived fittings. Such measures are usually documented and "tested" by the risk prevention process.

Available information should enrich the risk analysis and consider impacts.

[mp.if.6] Protection against floods

- **Master Control ISO/IEC 27001:2022**
  - 7.5 Protection against external and environmental
- **Complementary Controls ISO/IEC 27001:2022**
  - 7.3 Security of offices, offices and resources
  - 7.6 Working in safe areas

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Secure areas should be protected by appropriate entry controls and access points.

Recommendation Implementation:

Both standards require in parallel the same obligations and in this respect a register should be required to allow traceability [in and out] of essential equipment (for data processing centres). This shall include the identification of the person authorising the movement. In addition to the register 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.

A cross-checking process should be implemented, so that deliveries are checked against the delivery note, analysed for evidence of tampering with the package and inspected for hazardous materials or tampering.

The entries must be mapped to the asset management [op.exp.1] and control 5.9 and control 7.10 of the ISO.

[mp.if.7] Equipment input and output register

- **Master Control ISO/IEC 27001:2022**
  - 7.2 Physical input controls
- **Complementary Controls ISO/IEC 27001:2022**
  - 7.3 Security of offices, offices and resources
  - 7.6 Working in safe areas

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Secure areas should be protected by appropriate entry controls and access points.

Recommendation Implementation:

Both standards require in parallel the same obligations and in this respect a register should be required to allow traceability [in and out] of essential equipment (for data processing centres). This shall include the identification of the person authorising the movement. In addition to the register 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.

A cross-checking process should be implemented, so that deliveries are checked against the delivery note, analysed for evidence of tampering with the package and inspected for hazardous materials or tampering.

The entries must be mapped to the asset management [op.exp.1] and control 5.9 and control 7.10 of the ISO.

[MP.PER] PERSONNEL MANAGEMENT

[mp.per.1] Job characterisation

- **Master Control ISO/IEC 27001:2022**
  - 6.1 Checking
- **Complementary Controls ISO/IEC 27001:2022**
  - 6.2 Terms and conditions of engagement
  - 5.24 Information Security Incident Management Planning and Preparedness

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Background checks on all candidates to become staff need to be conducted prior to joining the organisation and on an ongoing basis in accordance with laws, regulations and code of ethics, and be proportionate to the organisation's objectives, the classification of information being accessed and the perceived risks.

This control should be complemented by Terms and Conditions of Engagement.

Recommendation Implementation:

The two standards work in tandem, bearing in mind that the ISO requirement may not be applicable to the full extent where there are previous personnel processes [public sector post provisioning] that have already collated the information to be verified. Verifications of suitability for the post and competence in relation to that required to perform the security function that may be involved, and especially confidentiality, should be considered.

At the ENS level, it does not go into assessing the background of users to the system, beyond those referring to security needs. It is important to establish an allocation of human resources (appropriate and trained) in consideration of [op.pl.4], with a clear separation of functions (consider the controls [org.4] and [op.acc.3]), as well as the definition of attributions (and especially for the public sector, through the corresponding RPT administrative processes).

In addition, other measures such as training actions (mp.per.4), problems related to [high] turnover [op.pl.1] must be considered.

[mp.per.2] Duties and obligations

- **Master Control ISO/IEC 27001:2022**
  - Terms and conditions of engagement
- **Complementary Controls ISO/IEC 27001:2022**
  - 6.4 Disciplinary proceedings
  - 6.5 Responsibilities for termination or change
  - 5.11 Return of assets
  - 6.6 Confidentiality or non-disclosure agreements

Category: MEDIUM
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

Agreements should set out the responsibilities of staff and the organisation for information security.

This control should be complemented by 6.4 Disciplinary process.

Recommendation Implementation:

Although the ENS is stricter in this control, both standards can be clearly aligned. Each person with access to the system shall be informed of the duties and responsibilities derived from their position and functions, in terms of security.

The report shall be managed with accurate information and evidence of receipt and access to procedures associated with their functions and access. Responsibility shall be made known in case of deviation from instructions or non-compliance.

Consideration should be given to the provisions derived from the sectoral regulations associated with the personnel of a public entity and due confidentiality. It is advisable to work on the processes for welcoming users [Welcome, Onboarding or Welcome], taking into account "external" users (supplier personnel) in which all the information required for accessing and managing the system and the information/services is included.

The 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).

[mp.per.3] Awareness raising

- **Master Control ISO/IEC 27001:2022**
  - 6.3 Information security awareness, education and training
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.24 Information security incident management planning and preparation.

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

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.

Recommendation Implementation:

Actions will be carried out to raise awareness on a regular basis, on security regulations, incident procedures and social engineering techniques.

Organisations should have a plan in place, including plans for innovative actions to raise awareness. Different means of delivery can be used, 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 journals or attending conferences and events aimed at technical and professional improvement.

**The awareness-raising programme should include a range of activities through appropriate channels, such as campaigns, brochures, posters, newsletters, websites, briefings, learning modules and e-mails.

Staff understanding should be assessed at the end of an awareness-raising activity. These evaluations should consider not only the user's view, but also the view of managers and security-relevant persons. The evolution of awareness should be considered, using certain metrics and indicators.

The CCN regularly updates documents and seminars, and includes its tools (e.g. ELENA and ATENEA) that can help in this process. There are more entities and security authorities that can also help in raising awareness (INCIBE, ENISA...) and effectiveness of this control.

[mp.per.4] Training

- **Master Control ISO/IEC 27001:2022**
  - 6.3 Information security awareness, education and training
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.24 Information Security Incident Management Planning and Preparedness

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

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.

Recommendation Implementation:

Staff with safety-critical functions should maintain up-to-date system configuration training.

Persons with access to the system must be aware of and trained in incident detection and response, as well as in information management (storage, transfer, copying, distribution and destruction).

The effectiveness of the training actions carried out will be evaluated.

An annual training plan should be developed, including the planned actions. Training actions can take different forms and have different agendas. The CCN has tools that can help with this and so do other security authorities (INCIBE, ENISA...). Training actions can be used, which are present on the CCN's platforms, such as VANESA, for example.

Finally, the training responsibility for third party staff with access to the institution's system must not be forgotten, and the corresponding security training action must be agreed and monitored.

[MP.EQ] EQUIPMENT PROTECTION

[mp.eq.1] Clear workstation

- **Master Control ISO/IEC 27001:2022**
  - 7.7 Uncluttered workstation and clean screen
- **Complementary Controls ISO/IEC 27001:2022**
  - 7.3 Security of offices, offices and resources
  - 7.8 Siting and protection of equipment
  - 5.10 Acceptable Use of Information and Associated Assets

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Clear rules for desk, paper and storage and/or removable media, as well as rules for clean screens on the organisation's premises should be defined and enforced.

Recommendation Implementation:

The two rules are clearly synergistic, so that the protection of information (especially information that must be kept confidential or is considered sensitive or critical due to the functions performed, in any case considering control [mp.info.2]) must be considered.

Workstations shall remain uncluttered, keeping in use only such information as is always necessary, and which shall be stored in a secure location whenever possible.

Consideration should be given to the security of information on paper or on Storage media 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 associated assets and 5.36 Compliance with information security policies and standards.

Awareness-raising actions should build on this measure.

[mp.eq.2] Locking of the workstation

- **Master Control ISO/IEC 27001:2022**
  - 7.7 Uncluttered workstation and clean screen
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.9 Configuration management

- Configurations, including security, hardware, software, service and network configurations shall be established, documented, implemented, monitored and reviewed.

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Clear rules for desk, paper and storage and/or removable media, as well as clear rules for clean screens on the organisation's premises should be defined and enforced.

Recommendation Implementation:

At the level of both standards, at least the MEDIUM category will be considered. This necessarily implies to draw technical measures for equipment and devices and services to 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.

At the very least, this policy should be deployed in the directory and deployed from the initial basing of the component [op.exp.2], with a Technical Instruction [org.3] developing it, and the effectiveness will be checked from time to time [op.exp.3].

For example, the application on the equipment can be checked from time to time by means of CLARA.

SaaS services should deploy this measure in identical terms, so providers should be required to do so and to check its applicability.

Users should in any case be aware of the need to lock sessions on computers, devices and services when they leave the workstation, even if only for a limited period of time.

Based on the risks detected, it may be advisable to deploy the R1-Session Closure Enforcement. -mp.eq.2.r1.1] After a certain period of time, longer than the previous one, the sessions opened from that workstation shall be cancelled.

[mp.eq.3] Portable equipment protection

- **Master Control ISO/IEC 27001:2022**
  - 8.1 User end devices
- **Complementary Controls ISO/IEC 27001:2022**
  - 7.9 Security of off-site equipment
  - 5.9 Inventory of information and other associated assets.
  - 5.12 Classification of information
  - 5.24 Information Security Incident Management Planning and Preparedness
  - 5.25 Assessing and deciding on information security events

Category: HIGH*
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

Off-site assets must be protected taking into account the different risks. Information stored, processed or accessible through user devices must be protected.

Recommendation Implementation:

Both standards converge on the security of this type of device, although the HIGH category should be considered, based on the derivation of the control [mp.info.2] Reinforcement R2 - Protected environments [mp.eq.3.r1.1] The use of portable equipment outside the organisation's premises shall be restricted to protected environments, where access is controlled, safe from theft and prying eyes. This point shall be associated with control [mp.info.2]. The risks identified shall also be taken into account [op.pl.1].

Reinforcement R1 - Disk encryption, [mp.eq.3.r2.1]; if the information inventory shows that the information has a MEDIUM level. The valuation of the information with its information officers must be considered very precisely.

In addition, special consideration shall be given to security incident management [op.exp.7], ISO controls 5.24, 5.26 and access control from outside trusted areas [op.acc.6]; [op.acc.6.r8.1] For access from or through uncontrolled areas, a two-factor authentication shall be required. In the case of remote access, R9-Remote Access (all levels) shall be considered. [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 does not occur on an ongoing basis, remote access shall be disabled and enabled only when necessary.

(d) Audit trails of such connections shall be collected.

For the encryption process, encryption should be considered as indicated in Reinforcement R1 - Disk Encryption, if the inventory of information is considered to have a MEDIUM level. In this case, CCN-STIC-105 ICT Security Products and Services Catalogue 7.5.1 FAMILY: DATA ENCRYPTION STORAGE

The best security practices contained in ISO 27002 are of interest and especially:

(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 auto-update);

(d) Identification and prior approval of rules for connection to services, public networks or any other off-site network (e.g. requiring the use of a personal firewall);

(e) Encryption of storage devices;

(f) Malware protection, detection and response (e.g. use of specific anti-malware);

(g) Remote deactivation, deletion or blocking;

(h) Back-up copies of the complete equipment, including configuration;

i) Encouraging the use of SaaS services and applications;

j) Analysis of end-user behaviour;

k) Controlled use of removable devices and possibility 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 network connected devices

- **Master Control ISO/IEC 27001:2022**
  - 8.1 User end devices
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.9 Inventory of information and other associated assets.
  - 5.12 Classification of information
  - 8.9 Configuration management

Category: MEDIUM
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

Consider the configuration process and safe handling by users.

Recommendation Implementation:

This control necessarily involves considering these devices in [op.exp.2] and [op.exp.3] and maintaining accurate checks. Devices connected to the network and which may at some point have access to information (multifunction and multimedia devices, and [IoT] devices, BYOD, etc.) in accordance with [op.exp.2 and 3] shall be included as securely configured components and, where they allow storage of information, shall provide the functionality to securely [mp.si.5] erase and destroy.

As the renewal of the fleet of devices affected by this control is initiated, products contained in the CCN STIC 105 catalogue or, where appropriate, similar security certification will be acquired.

The R1 should be included which, although not covered by ISO, should be applied for the ENS. Component-by-component checks should be performed [op.pl.5].

[MP.COM] PROTECTION OF COMMUNICATIONS

[mp.com.1] Secure perimeter

- **Master Control ISO/IEC 27001:2022**
  - 8.20 Network security
- **Complementary Controls ISO/IEC 27001:2022**

- 8.21 Security of network services
- 8.9 Configuration management

Category: MEDIUM
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

Networks must be managed and controlled to protect information in systems and applications.

Recommendation Implementation:

Firewall protection shall be provided [see op.pl.5], flows shall be authorised [org.4] and the requirements contained in the Technical Instruction on Security of Information Systems Interconnection [op.ext.4] shall be taken into consideration. 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.

It is important that all network devices are involved in the basing process [op.exp.2][op.exp.3].

At the level of SaaS / IaaS services (and Cloud in general) the provider must be held responsible for compliance.

At the machine level, the firewall will be deployed in local mode on the user machines.

[mp.com.2] Protection of confidentiality

- **Master Control ISO/IEC 27001:2022**
  - 8.21 Security of network services
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.20 Network security
  - 8.24 Use of cryptography
  - 8.9 Configuration management
  - 8.26 Application security requirements

Category: MEDIUM
Level of measures Compatible: **Partially analogue**
Particularities of ISO:

Security mechanisms, service levels and network service requirements must be identified, implemented and monitored.

Recommendation Implementation:

VPNs with CCN-authorised algorithms and parameters shall be used (See CCN STIC Guide 807 and CCN STIC Guide 221). The organisation shall ensure that appropriate security controls are applied to the use of virtualised networks, including SDN, SD-WAN. Different modalities can be considered, VPN TLS, IPSEC, MACSEC, WIREGUARD. All networks shall be inventoried, and VPNs shall be monitored, managed and disabled when they are no longer needed.

Since ISO is flexible in incorporating requirements from national regulations, the requirements are derived from the CCN-STIC Guidelines 836 and 807 and the recommended encryption algorithm AES 128 symmetric encryption.

The provisions of [op.acc.6] shall be taken into account. Reinforcement R9-Remote access (all levels).

[op.acc.6.r9.1] The Information Systems Interconnection ITS shall apply.

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

(a) be authorised by the appropriate authority.

b) Traffic shall be encrypted.

(c) If usage does not occur on an ongoing basis, remote access shall be disabled and enabled only when necessary.

(d) Audit trails of such connections shall be collected.

The requirements can be considered in the CCN-STIC-836 ENS Guide - VPN Security.

[mp.com.3] Authenticity and integrity protection

- **Master Control ISO/IEC 27001:2022**
  - 8.21 Security of network services
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.20 Network security
  - 8.24 Use of cryptography
  - 8.9 Configuration management
  - 8.26 Application security requirements

Category: MEDIUM
Level of measures Compatible: **Partially analogue**
Particularities of ISO:

Security mechanisms, service levels and network service requirements must be identified, implemented and monitored.

Recommendation Implementation:

In communications with points outside the own security domain, the authenticity of the other end shall be ensured, [op.acc.5] and shall include authentication mechanism (external users), which entails using passwords and other element (OTP/certificate) and keeping the log operational. VPNs shall be used according to CCN-authorised algorithms and parameters (see CCN STIC Guide 807 and CCN STIC Guide 221). The organisation must ensure that appropriate security controls are applied to the use of virtualised networks, including SDN, SD-WAN. Different modalities can be considered, VPN TLS, IPSEC, MACSEC, WIREGUARD.

Since ISO is flexible in incorporating requirements from national regulations, the requirements are derived from the CCN-STIC Guidelines 836 and 807 and the recommended encryption algorithm AES 128 symmetric encryption.

All networks shall be inventoried and VPNs shall be monitored, managed and disabled when they are no longer needed. They should be periodically reviewed, checked for necessity and in any case restricted when they are 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 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 does not occur on an ongoing basis, remote access shall be disabled and enabled only when necessary.

(d) Audit trails of such connections shall be collected.

The requirements can be considered in the CCN-STIC-836 ENS Guide "VPN Security".

[mp.com.4] Separation of information flows in the network

- **Master Control ISO/IEC 27001:2022**
  - 8.22 Segregation in networks
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.20 Network security
  - 8.27 Secure Systems Architecture and Engineering Principles
  - 5.9 Inventory of information and other associated assets

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Networks should be divided into domains and "separated" from the public network (i.e. the Internet).

Groupings can be made by trust, criticality, sensitivity, organisation, etc., and by physical or logical network.

Recommendation Implementation:

Network segmentation will be carried out, limiting access and propagation risks, by means of logical means, virtual local area networks (Virtual Local Area Network VLAN), virtual private networks (Virtual Private Network VPN) or separate physical means.

Wireless networks shall be in a separate segment. The system network shall be segregated into at least a user network, a service network and an administration network.

The diagram allowing visualisation of the segmentation and precise network information shall be documented and updated in the architecture information [op.pl.2].

Where for reasons of size and capacity, segregation for control purposes cannot be managed, the feasibility of segregating networks into fewer points, e.g. VLANs for an administration network and an internal user VLAN, may be considered.

The wifi network should be segregated or overridden.

Requirements can be considered in CCN-STIC-836 ENS Guide - VPN Security and CCN-STIC-816 Wireless Network Security in the ENS.

[MP.SI] PROTECTION OF INFORMATION CARRIERS

[mp.si.1] Carrier marking

- **Master Control ISO/IEC 27001:2022**
  - 5.13 Labelling of information
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.12 Classification of information
  - 7.10 Storage media
  - 8.12 Data leakage prevention

Category: MEDIUM
Compatible measurement level: **Analogue**
Particularities of ISO:

An appropriate set of procedures for labelling information in accordance with the information classification Framework adopted by the organisation should be developed and implemented.

Recommendation Implementation:

Given the flexibility granted by ISO, the premises given by the ENS should be adopted, deploying the Framework derived from the information and assessment carried out. Consideration will be given to the necessary labelling and how to place it on paper and digital documents (metadata). This control shall be connected to the metadata clean-up control [mp.info.5]. Watermarks shall be placed on documentation, referring to the qualification of these as OFFICIAL USE [mp.info.2]. The entity shall deploy a process associated with [mp.info.2] and consider the corresponding operational procedures [org.3].

Staff and other stakeholders should be aware of labelling procedures, so all staff should be trained to ensure that information is correctly labelled and handled accordingly. This should be linked to awareness [mp.per.3] and training [mp.per.4].

[mp.si.2] Cryptography

- **Master Control ISO/IEC 27001:2022**
  - 8.24 Use of cryptography
- **Complementary Controls ISO/IEC 27001:2022**

- 8.13 Backing up information
- 8.12 Preventing data leakage
- 7.9 Security of off-site equipment
- 7.10 Storage media

Category: MEDIUM (+R2) *
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

Storage media should be managed throughout their life cycle; acquisition, use, transport and disposal, in accordance with the organisation's classification Framework and usage requirements.

Recommendation Implementation:

The MEDIUM category shall apply, together with Strengthening R2-Backup. [mp.si.2.r2.1] Backups shall be encrypted using CCN-authorised algorithms and parameters (see CCN STIC Guide 807 and CCN STIC Guide 221). Devices leaving the premises shall be encrypted, especially if they are copies.

The organisation should establish a specific policy on the management of removable media and communicate this policy to anyone using or handling removable media.

As a general measure, it shall be considered that removable media ports, e.g. SD card slots and USB ports, should only be enabled if there is an organisational reason for their use.

The control [op.pl.5] that will lead to a collateral application of R1 Reinforcement - Certified products [mp.si.2.r1.1] Certified products according to [op.pl.5] shall be used.

[mp.si.3] Custody

- **Master Control ISO/IEC 27001:2022**
  - 7.10 Storage media
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.9 Inventory of information and other associated assets
  - 5.10 Acceptable Use of Information and Associated Assets
  - 5.11 Return of assets
  - 6.3 Information security awareness, education and training
  - 8.12 Preventing data leakage

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Storage media should be managed throughout their life cycle, acquisition, use, transport and disposal, in accordance with the organisation's classification Framework and usage requirements.

Recommendation Implementation:

The organisation should establish a specific policy on the management of removable media and communicate that policy to anyone using or handling removable media, require authorisation for the media and maintain a record. The media should be stored in a secure and protected environment in accordance with the rating of the information and protected against environmental threats (such as heat, humidity, electronic field or ageing) in accordance with manufacturers' specifications.

Physical and logical measures will be deployed to prevent misuse.

It is possible that storage may be established in fireproof boxes, so they must be traced with the manufacturer's indications and the conservation point that allows them to withstand fire.

The manufacturer's instructions on temperature and humidity must be taken into consideration and the corresponding data sheets [org.3] and 7.13 Maintenance of equipment (Equipment shall be properly maintained to ensure the availability, integrity and confidentiality of information.)

It is advisable to take into account the best practices described in ISO 27002, as they can enrich compliance with this control. For example, all media 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 media degradation while the stored information is still needed, information should be transferred to new media before it becomes unreadable.

[mp.si.4] Transport

- **Master Control ISO/IEC 27001:2022**
  - 7.10 Storage media
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.24 Use of cryptography
  - 8.12 Preventing data leakage
  - 7.2 Physical input controls

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Storage media should be managed throughout their life cycle, acquisition, use, transport and disposal, in accordance with the organisation's classification Framework and usage requirements.

Recommendation Implementation:

The organisation must establish a specific policy on the management of removable media and communicate this policy to any person using or handling removable media, requiring authorisation and being supervised by the CIO, who will control the input/output log and analyse the consistency of its entries.

This management procedure shall be considered, under the guidance of the System Manager, and a register of inputs and outputs shall be considered, where the movement of items shall be collated. This register has a special connection with the register associated with [mp.if.7].

Where required because of the information it contains [mp.si.2], encryption shall be used and keys shall be managed [op.exp.10].

This point shall take full account of Reinforcement R2 - Back-up copies - [mp.si.2.r2.1] Back-up copies shall be encrypted using algorithms and parameters authorised by the CCN. Information considered confidential by European regulations shall benefit from this presumption.

In general, elements with information classified as OFFICIAL USE will be protected and subject to encryption if the sensitivity of the information so determines.

ENS requirements and ISO best practices can be brought together under a single process with the following guidelines;

(a) use trusted or duly accredited carriers or couriers, by creating a list of authorised couriers;

b) develop procedures to verify the identification of couriers;

(c) the packaging must 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-resistant controls.

[mp.si.5] Deletion and destruction

- **Master Control ISO/IEC 27001:2022**
  - 7.10 Storage media
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.10 Deletion of information
  - 8.12 Preventing data leakage
  - 7.10 Storage media

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Items likely to be storage media should be reviewed to ensure that all confidential data and licensed software have been securely removed or overwritten prior to disposal or reuse.

Information stored in information systems and devices should be deleted when no longer needed.

Recommendation Implementation:

Both standards converge and require at a general level, that the organisation establishes a specific policy on the management of removable media and communicate this policy to anyone using or handling removable media.

For the use of erasure elements, the recommendations of the CCN and the tools contained in the CCN STIC 105 Catalogue should be taken into account.

In your case it may be important to keep in mind complementary measures considering the threats and security requirements present in the CCN-STIC-140 Reference Taxonomy for ICT Security Products - Annex E.3: Secure Erasure Tools.

In SaaS (and Cloud services in general), the use of secure deletion processes and accreditations to this effect will be required.

If suppliers are contracted to carry out erasure and disposal processes, evidence of the security of the service and certification of the effectiveness of the service should be required.

When the medium is reused, the information must be effectively erased to prevent access to the information.

For safe disposal of media, shredding may be an option. The results of disposal and erasure should be recorded as proof and evidence.

[MP.SW] SOFTWARE APPLICATION PROTECTION (SW)

[mp.sw.1] Application development

- **Master Control ISO/IEC 27001:2022**
  - 8.25 Security in the development lifecycle
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.28 Secure coding
  - 8.29 Developmental Safety and Acceptance Testing.
  - 8.31 Separation of development, testing and production environments
  - 8.32 Change management
  - 8.4 Access to source code
  - 8.30 Outsourcing development
  - 8.27 Secure Systems Architecture and Engineering Principles
  - 5.8 Information Security in Project Management

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Rules for the safe development of software and systems must be established and applied.

Recommendation Implementation:

Keep development and production environments separate and comply with the principle of least privilege and avoid using real data for testing.

Where an entity does not carry out development directly, it should consider requiring software suppliers, their compliance and, where appropriate, the tests that can be carried out.

Tests prior to the implementation or modification of information systems will preferably not be carried out with real data; in the event that it is necessary to use real data, the corresponding level

of security will be guaranteed. It is possible that certain e-services may be in SaaS mode and should therefore be considered as a provider. [see op.nub.1].

For the enrichment of this control, the following will be considered;

a) separation of development, test and production environments (see 8.31);

b) guidance on safety in the software development life cycle: software development methodology (see 8.28 and 8.27); secure coding guidelines (see 8.28);

(c) safety requirements at the specification and design stage (see 5.8);

(d) security checkpoints within the 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) version control security (see 8.32);

h) required application security knowledge and training (see 8.28);

i) the ability of developers 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 entry into service

- **Master Control ISO/IEC 27001:2022**
  - 8.29 Developmental safety and acceptance testing
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.31 Separation of development, test and production environments
  - 8.32 Change management
  - 8.33 Test Data
  - 8.11 Data masking
  - 8.30 Outsourcing development
  - 8.27 Secure Systems Architecture and Engineering Principles
  - 5.8 Information security in project management

Category: MEDIUM
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

Security testing processes should be defined and implemented in the development lifecycle.

This control should be complemented by 8.31 Separation of development, test and production environments.

Recommendation Implementation:

Both standards require separate test, development and [pre]production environments. Before going into production, the correct functioning of the application and other elements shall be checked, while maintaining security criteria.

For this purpose, basic testing can be considered by means of a validation checklist, presenting the results to the Security Officer and associated Change Management [op.exp.5]. Testing will be considered for versioning and patching, which will be tested in a controlled environment. Functional and security testing should be considered, e.g. user authentication and access restriction and use of cryptography.

It is possible that certain e-services may be in SaaS mode or at the level of public entity or subsidiaries depending on another entity, in both cases, the control will derive its compliance to them.

In addition, encryption and secure configurations, including that of operating systems, firewalls and other security components, must be carried out.

Code review activities shall be considered to detect security flaws, perform vulnerability analysis to identify insecure configurations and system vulnerabilities, and perform penetration testing to identify insecure code and design. Consideration should be given to [annual] plans for conducting audits and reviews in this regard.

[MP.INFO] PROTECTION OF INFORMATION

[mp.info.1] Personal data

- **Master Control ISO/IEC 27001:2022**
  - 5.34 Privacy and Personal Data Protection (PDP)
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.31 Identification of legal, regulatory and contractual requirements

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

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.

Recommendation Implementation:

Consideration should be given to the obligations derived from the European legislator and the need for compliance. Consideration should be given to the figure of the Data Protection Officer, which may be shared with other public entities.

It is possible that third parties may be involved in the processing or data processing operations, and they must provide proof of compliance with the relevant regulations. Likewise, it is necessary that processing orders and co-responsibilities are contemplated and that the obligations are correctly regulated.

[mp.info.2] Qualification of information

- **Master Control ISO/IEC 27001:2022**
  - 5.12 Classification of information
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.13 Labelling of information
  - 5.14 Transfer of information
  - 5.15 Access control
  - 5.9 Inventory of information and other associated assets.
  - 5.10 Acceptable Use of Information and Associated Assets
  - 8.12 Preventing data leakage

Category: MEDIUM
Compatible measurement level: Analogue
Particularities of ISO:

Information shall be classified according to the organisation's information security needs, based on confidentiality, integrity, availability and stakeholder requirements.

Recommendation Implementation:

Given the flexibility of the ISO, the ENS criteria will be imposed. The qualification policy will determine the criteria that will determine the level of security required, within the regulatory framework 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.

It is important to designate an information manager and to outline in the policy the assessment criteria in accordance with the regulations involved. The person responsible for each piece of information will be in charge of assigning the required security level to each piece of information, and of its documentation and formal approval. He/she shall have the exclusive power to modify the security level at any time.

Marking of carriers [mp.si.1] and the impact of this control should be considered.

It is important to consider that the entity will generate exchanges with other entities and should include the rating Framework in the agreements, implying the security measures that derive from it.

[mp.info.3] Electronic signature

- **Master Control ISO/IEC 27001:2022**
  - 8.24 Use of cryptography
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.26 Application security requirements
  - 5.31 Identification of legal, regulatory and contractual requirements

Category: MEDIUM
Level of measures Compatible: Nil
Particularities of ISO:

This is not a specific ISO control, but we associate it with certain controls, considering cryptographic elements. 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.

Recommendation Implementation:

ISO does not consider this control, but it can be associated with controls 8.26 and 8.24. The measure is considered to be complied with when any signature valid in the current regulations is used. Controls on the same and the acceptable use must be managed.

It is important to consider the following reinforcements:

Reinforcement R1 - Qualified certificates: When advanced electronic signatures based on certificates are used, these shall be qualified. Qualified providers will be those who issue them, in accordance with the European regulations in force.

Strengthening R2 - Authorised algorithms and parameters: The CCN shall determine the cryptographic algorithms that have been authorised.

Reinforcement R3 - Signature verification and validation: Verification and validation of the signature shall be ensured for the required time.

A policy should be deployed or attached to that of the higher administrative body. It is important that the custody and use of the signature is managed. In this regard, 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.

It should consider the processes in which signature verification must be maintained and therefore deploy preservation environments that allow for such verification. These environments can be in an in-house or third-party service.

Certified components can be taken into account by direct application of control [op.pl.5].

[mp.info.4] Time Stamps

- **Master Control ISO/IEC 27001:2022**
  - 8.26 Application security requirements
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.17 Clock synchronisation
  - 8.24 Use of cryptography

Category: HIGH*
Level of measures Compatible: Nil
Particularities of ISO:

This is not a specific ISO control, but we associate it with certain controls. We consider cryptographic elements and specifically the synchronisation of clocks and time accreditation of events.

Recommendation Implementation:

This control has the particularity of not being present in the case of ISO and of not being required in those entities whose category is MEDIUM. However, in the event that the entity has declared a HIGH category or the application of the control has been considered (especially for the purposes of the administrative procedures involved), this control will be considered.

Time stamps shall be renewed regularly until the protected information is no longer required by the administrative process it supports.

- mp.info.4.4] "Qualified electronic time stamps" shall be used in accordance with Regulation (EU) No 910/2014.

Complementary consideration shall be given to site/website certificates, which must be issued by qualified entities in accordance with Regulation (EU) No 910/2014.

[mp.info.5] Cleaning of documents

- **Master Control ISO/IEC 27001:2022**
  - It is not envisaged
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.13 Labelling of information
  - 8.12 Preventing data leakage

Category: MEDIUM
Level of measures Compatible: **Nil**
Particularities of ISO:

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.

Recommendation Implementation:

This control is connected to control [org.2] and [mp.si.1] and [mp.info.2]. It is important to deploy a metadata policy for the control of information that will be actively incorporated into the entity's processes. Information that needs to be removed, prior to publication/dissemination, should be "processed" to remove unnecessary metadata.

Training and awareness-raising actions shall be maintained for the purposes of [mp.per.3] and [mp.per.4].

Although ISO does not expressly contemplate control, there are references to metadata management in control 5.13 and as best practices they can complement the provisions of ENS.

[mp.info.6] Backups

- **Master Control ISO/IEC 27001:2022**

- 8.13 Backing up information

- **Complementary Controls ISO/IEC 27001:2022**
  - 8.14 Redundancy of information processing resources
  - 7.14 Safe disposal or re-use of equipment
  - 7.10 Storage media
  - 5.37 Documentation of operational procedures
  - 5.29 Information Security During Disruption
  - 5.30 ICT preparedness for business continuity
  - 5.31 Identification of legal, regulatory and contractual requirements

Category: MEDIUM (+R2) *
Compatible measurement level: Analogue
Particularities of ISO:

Backups will cover information, software, configuration and overall systems should be maintained and tested regularly in accordance with the agreed subject-specific backup policy.

Recommendation Implementation:

For ISO purposes there is a compatible level of security measures as the operational control 8.13, aligns with the [mp.info.6].

The MEDIUM category shall apply, together with the requirements of "R2 Hardening-Protection of backups". [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.

- Reinforcement R2-Protection of backups is considered, for critical items that require storage in a different location. This shall be associated with the results of the assessment derived from [mp.info.2] and the risks [op.pl.1] and impact [op.cont.1] and consideration of 8.14 Redundancy of information processing facilities and 5.31 Identification of legal, regulatory and contractual requirements.

This control shall be referenced to "R3-Backup R3.1. [op.exp.3.r3.1] The configuration of the system shall be backed up in such a way that it is possible to rebuild part or all of the system after an incident.

It is important to note that this control is associated with continuity and for ISO this is significant, as it must be taken into account in order to comply with ISO requirements. It is necessary to establish a backup policy that considers the organisation's information security and data retention requirements. Consideration should be given to backup facilities for information and software. The copying process and its timing and retention shall be aligned with legal requirements and the personal information it contains.

Information related to the whole copying process must be controlled, including software used, processes, revisions... A protocol [org.3] for simple restores should be available and can be aligned with the control [op.cont.3] and considered as continuity testing.

Consideration should be given to the media used, if any, and the manufacturer's instructions and storage specifications. The safe disposal of copies and their media should be considered within the process. [mp.si.5].

[MP.S] PROTECTION OF SERVICES

[mp.s.1] E-mail protection

- **Master Control ISO/IEC 27001:2022**
  - 5.14 Transfer of information
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.12 Preventing data leakage
  - 5.10 Acceptable Use of Information and Associated Assets
  - 5.23 Information security for use of cloud services
  - 6.2 Terms and conditions of engagement
  - 6.3 Information security awareness, education and training

Category: MEDIUM
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

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.

Recommendation Implementation:

For ISO this is mainly about information exchange or transfer, as well as electronic means, which is where the mail service is included. This control may be delegated to the mail provider and control [org.2] shall be considered for the specification of instructions for use.

This monitoring will consider guidelines related to more means of information transmission (not only e-mail, 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

- **Master Control ISO/IEC 27001:2022**
  - 8.26 Application security requirements
- **Complementary Controls ISO/IEC 27001:2022**
  - 5.35 Independent review of information security.
  - 5.8 Information security in project management
  - 5.17 Authentication Information
  - 8.2 Access Privilege Management

- 8.5 Secure authentication

Category: MEDIUM
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

Information security requirements should be identified, specified and approved when developing or acquiring applications.

Recommendation Implementation:

By default, all published services will consider access controls (where required), protections against tampering and code injection attacks, privilege escalation and cross site scripting.

An audit plan should be in place that provides for the actions of automatic vulnerability reviews, similar tools and black box/white box audits.

It is common to deploy services through a service provider (specific services or web services). It is recommended to include in contracts and tender conditions the requirement for the execution of the analysis and the action plans resulting from the analysis.

Services contracted to third parties shall contain the measures required in this control and specifically the obligation to correct vulnerabilities detected in the platforms through security scans.

At least one annual black box test with a report and action plan shall be required. The audit plan shall reflect 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 compatible measures with respect to the requirements set by the standards since the ENS is rigorous and specific. ISO, however, allows to deploy these requirements and to adjust the system and the statement of applicability for harmony.

It will be mapped against the audit and review plan and linked to the management of action plans arising from the security of web applications / published items.

Applications accessible over networks are subject to a variety of threats, therefore security requirements scattered throughout the ISO will be considered, such as access management through authentication (see 5.17, 8.2, 8.5); resilience against malicious attacks or unintentional disruptions (e.g. buffer overflow protection or SQL injections).

[mp.s.3] Web browsing protection

- **Master Control ISO/IEC 27001:2022**
  - 8.23 Web filtering
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.9 Configuration management
  - 8.12 Preventing data leakage
  - 6.3 Information security awareness, education and training

Category: MEDIUM

Compatible measurement level: Analogue
Particularities of ISO:

Access to external websites should be managed to reduce exposure to malicious content.

Recommendation Implementation:

The two standards are closely aligned in this control.

Rules of use and limitations of personal use shall be established [org.2]. Awareness-raising activities [mp.per.3] will be carried out regularly, on hygiene in web browsing, encouraging safe use and warning of incorrect use, by means of informative mailings, posters or session banners.

Training [mp.per.4] shall be provided to system administration, service monitoring and incident response personnel.

Measures shall be deployed to protect web address resolution and connection establishment information from malicious software and a cookie control policy shall be in place, in particular to avoid contamination between personal and organisational use and shall be made known to users through awareness actions [mp.per.3]. Web filtering may 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 should be considered.

Browser configurations according to [op.exp.2] and [op.exp.3] should be considered.

[mp.s.4] Denial of service protection

- **Master Control ISO/IEC 27001:2022**
  - 8.6 Capacity Management
- **Complementary Controls ISO/IEC 27001:2022**
  - 8.16 Monitoring of activities

Category: MEDIUM
Level of measures Compatible: **Partially analogue**

Particularities of ISO:

Resource use should be monitored and adjusted according to current and expected capacity requirements.

Recommendation Implementation:

Forecasting analyses shall be performed in the annual capacity plan [op.pl4], with a special emphasis on needs analysis, and tools shall be deployed to monitor system behaviour, whereby trends can be extracted and adaptations can be made according to the needs presented. Detection controls should be put in place to indicate problems in a timely manner.

Network management services will be considered, through firewall services and appropriate configuration to consider this type of DoS incidents. Tools to assist in the prevention of such incidents will be considered in addition to managed services.

It is desirable to review and include as a requirement in supply contracts / solutions and denial of service management.

Cloud services have these measures embedded in them, as their services will be properly protected and balanced in case of need. [op.nub.1]

It would be a good alternative measure to consider cloud services with deployment of measures associated with capacity and availability (Cloud services are characterised by elasticity and scalability that allow for rapid expansion and reduction on demand of available resources for particular applications and services, which is useful for reducing the demand on organisational resources).

7. OTHER CONTROLS OF THE ISO

As can be seen, it is necessary in some cases to deploy several ISO controls in order to provide full coverage of the requirement established in the ENS. However, there are some of them, which have not been included because they have less impact.

Some ISO controls have been highlighted here, as an exemplification of their consideration within some aspect of Royal Decree 311/2022.

5.4 Management responsibilities

Top management should ensure that all employees and contractors are aware of and follow the organisation's information security policy.

Consideration in the CSA:

Article 13. Organisation and implementation of the security process.

org.1 Security policy

5.5 Contact with the authorities

It should be clear who is responsible for contacting authorities (e.g. law enforcement agencies, regulators, supervisory authorities), which authorities should be contacted (e.g. which region/country) and in which cases this is necessary. A rapid and appropriate response to incidents can greatly lessen the impact and may even be required by law.

Consideration in the CSA:

Article 25. Security incidents.

op.exp.7 Incident management

5.6 Contact with special interest groups

To ensure that the latest information security trends and best practices are maintained, staff with ISMS tasks should maintain good contact with special interest groups. These groups can be asked for expert advice in certain cases and can be a great source for improving one's own knowledge.

Consideration in the CSA:

Article 13. Organisation and implementation of the security process.

org.1 Security policy

5.11 Return of assets

When an employee or outsider can no longer access an asset, e.g. at the end of the contract, the asset must be returned to the organisation. There should be a clear policy for this, which should be known to all involved.

Consideration in the CSA:

org.2 Safety regulations

5.17 Authentication information

Secret authentication, such as passwords and access keys, should be managed in a formal process. In addition, among other security actions, users should be prohibited from sharing secret authentication information.

Consideration in the CSA:

op.acc.1 Identification

op.acc.2 Access requirements

5.32 Intellectual Property Rights (IPR)

Intellectual property rights are also part of legal compliance. Intellectual property can be of great value. Misuse can result in great harm and loss.

Consideration in the CSA:

org.1 Security policy

op.exp.1 Inventory of assets

org.2 Safety regulations

5.33 Protection of registers

All records must be protected. Records have the added risk of loss, compromise or unauthorised access. Requirements for the protection of records may come from the organisation itself or from other sources, such as legislation. For this, strict guidelines must be created and followed.

Consideration in the ENS

op.exp.8 Registration of the activity

op.mon.3 Surveillance

5.35 Independent Review of Information Security

It is not recommended that organisations review their own information security system. It is therefore advisable to have independent reviews, so that their information security is audited periodically or when significant changes occur. This maintains an objective and transparent view of information security.

Consideration in the ENS

Article 31. Safety audit.

Annex III. Security audit.

mp.s.2 Protection of web services and applications.

5.36 Compliance with information security policies and standards

In relation to security policies, standards and procedures, it is important to periodically review whether the organisation's activities and/or processes fully respect and comply with them.

Information systems should also be regularly reviewed for compliance. Automated tools may be considered.

Consideration in the ENS

Article 31. Safety audit.

Annex III. Security audit.

org.4 Authorisation process

op.exp.3 Security configuration management

op.exp.4 Maintenance and security updates

6.4 Disciplinary proceedings

There should be a disciplinary process for breaches of the company's security policy. The disciplinary procedure should be proportionate and gradual, based on severity, intentionality, recidivism and, most importantly, whether adequate training was received.

Consideration in the ENS

org.1 Security policy

6.5 Responsibilities for termination or change

Security responsibilities do not end when the professional relationship changes or ends. Confidentiality agreements should be included, requiring that the confidentiality of information be respected after leaving the organisation.

Consideration in the ENS

mp.per.2 Duties and obligations

6.6 Confidentiality or non-disclosure agreements

Confidentiality agreements should be used, setting out the information covered, the responsibilities of all parties, the duration of the agreement and the penalties in case of breach of the agreement.

Consideration in the ENS

org.2 Safety regulations

mp.per.2 Duties and obligations

op.ext.1 Contracting and service level agreements

6.7 Teleworking

Remote working has become commonplace and commonplace. However, there are information security implications, which need to be considered and documented. The remote

working policy should describe where and when remote working is allowed, the provision of devices and equipment, authorised access and what information can be accessed remotely.

Consideration in the ENS

org.2 Safety regulations

mp.per.2 Duties and obligations

7.4 Physical security monitoring

Surveillance can deter unauthorised access and detect intrusion. Surveillance personnel, security cameras and alarms monitor and alert to unauthorised access.

The design of any security and surveillance system should be considered confidential.

Periodic testing is required to ensure that the system designed and implemented is functioning properly. Camera and other surveillance systems, which collect personal information or may be used to track and/or geo-locate an individual, may require special data protection consideration.

Consideration in the ENS

mp.if Protection of installations and infrastructure

mp.info.1 Personal data

7.9 Security of off-site equipment

Devices, including personal devices authorised for access, use and processing of organisational information, need protection when they leave the premises. The organisation needs to know which devices are used off-site, by whom and what information is accessed or used off-site.

Consideration in the ENS

mp.eq.3 Portable device protection

8.3 Restriction of access to information

Access to information and other assets should be based on the needs of each user, with access being kept to a minimum and restricted to individual users. Information should not be accessible to anonymous users to avoid untraceable and unauthorised access. This is important to preserve the confidentiality of information, to monitor its use and to prevent unauthorised modification and distribution.

Consideration in the ENS

op.acc.2 Access requirements

op.acc.3 Segregation of roles and tasks

op.acc.4 Access rights management process

8.11 Masking[42] of data

Only the minimum amount of data necessary will be available for the specific function performed in the search results. To achieve this, personal data must be masked (or anonymised or

[42] Understood as a synonym for obfuscation or anonymisation

pseudonymised) to hide the identity of the subjects. This may be required not only for security, but also by current legislation such as the GDPR.

Consideration in the ENS

mp.info.1 Personal data

8.19 Installing software in production systems

The installation of software can introduce vulnerabilities into operating systems. To minimise this risk, software should only be installed by authorised personnel.

Software must come from reliable sources and be maintained or fully tested if developed in-house. Previous versions should be retained and all changes recorded so that they can be reverted if necessary.

Consideration in the ENS

op.exp.2 Security settings

op.acc.3 Segregation of roles and tasks

mp.sw.2 Acceptance and commissioning

8.30 Outsourcing development

Where development is outsourced, information security requirements must be communicated to and accepted by the developer. Licensing and intellectual property, testing and evidence of testing, and contractual rights to audit the development process are examples of security considerations that should be agreed between the parties.

Consideration in the ENS

op.ext.1 Contracting and service level agreements

mp.sw.1 Application development

mp.sw.2 Acceptance and commissioning

op.ext.3 Supply chain protection

8.34 Protection of Information Systems during Audit Tests

Operational systems should not be unduly affected by audits or technical reviews. To avoid excessive disruption, audits should be planned, with an agreed time and scope. Read-only access will prevent accidental changes to systems during an audit. All accesses should be monitored.

Consideration in the ENS

op.exp.2 Security settings

op.exp.3 Security configuration management

op.exp.4 Maintenance and security updates

mp.s.2 Protection of web services and applications

Article 31. Safety audit.

ANNEX A. GLOSSARY AND ABBREVIATIONS

See guide CCN-STIC 800 ENS Glossary of Terms and Abbreviations.

ANNEX B. REFERENCES

- [ENS] Royal Decree 311/2022, of 3 May, which regulates the National Security Framework. BOE of 4 May 2022
- ISO/IEC 27001:2022 Information security, cybersecurity, and privacy protection - Information security management systems - Requirements-.
- ISO/IEC 27002:2022 Information security, cybersecurity, and privacy protection - Information security controls.
- ISO/IEC 27004, Information technology. Security techniques. Information security management. Monitoring, measurement, analysis and evaluation.
- ISO/IEC 27005, Information security, cybersecurity and privacy protection. Guidance on information security risk management.
- ISO 31000:2018, Risk management - Guidelines
- Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations.
- Law 40/2015, of 1 October, on the Legal Regime of the Public Sector.
- CCN-STIC. 800 Series. National Security Framework (ENS).

PUBLICACIONES DE DEFENSA

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