GOBIERNO DE ESPAÑA | MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN Centro Criptológico Nacional

ICT Security Guide CCN-STIC 825

ENS - NATIONAL SECURITY FRAMEWORK 27001 CERTIFICATIONS

April 2017

Published by:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CENTRO CRIPTOLÓGICO NACIONAL

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2017.04.27 18:36:00 +02'00'

NIPO:785-17-030-4

Publication date: april 2017
Translation funded by the Ministry of Finance and Public Function - Secretariat General of Digital Administration and done by ISDEFE.

LIMITATION OF RESPONSIBILITY
This document is provided in accordance with the terms compiled in it, expressly rejecting any type of implicit guarantee that might be related to it. In no case can the National Cryptologic Centre be considered liable for direct, indirect, accidental or extraordinary damage derived from using information and software that are mentioned even when a warning is provided concerning this damage.

LEGAL NOTICE
Without written authorization from the National Cryptologic Centre, it is strictly forbidden, incurring penalties set by law, to partially or totally reproduce this document by any means or procedure, including photocopying and computer processing, or to distribute copies of it by means of rental or public lending.

PROLOGUE

The current national and international scenario is dominated by developments in Information and Communication Technologies (ICT) and by risks emerging from their use. The Administration is fully aware of this scenario and it is necessary for this body to develop, acquire, conserve and secure use of ICTs to guarantee that its services run effectively for citizens' and the country's best interests.

Working from the Centre's knowledge and experience regarding threats and vulnerabilities in terms of emerging risks, Law 11/2002, dated 6th May, regulating the National Intelligence Centre, entrusts the National Intelligence Centre with functions related to information technology security, according to Article 4.e), and to protection of classified information, according to the Article 4.f). Through Article 9.2.f), it also gives its Secretary of State-Director the responsibility of managing the National Cryptologic Centre.

One of the most outstanding functions assigned to it, in Royal Decree 421/2004, dated 12th March, regulating the National Cryptologic Centre is to draw up and disseminate standards, instructions, guides and recommendations to guarantee security for the Administration's information and communication technologies.

Royal Decree 3/2010, dated 8th January, develops the National Security Framework (hereinafter called ENS) in the field of Electronic Administration which is also mentioned in the second section of Article 156 of Law 40/2015, dated 1st October, on the Public Sector Legal System. The National Security Framework establishes the security policy, in matters of use of electronic resources, which ensures the protection of information.

Indeed, Royal Decree 3/2010, dated 8th January, updated by Royal Decree 951/2015, dated 23rd October, sets the basic principles and minimum requirements as well as any protection measures to be introduced in Administration systems. In article 29, it authorizes the CCN to develop CIS guidelines to ease meeting these minimum requirements.

The CCN-STIC documents series was drawn up to comply with this function and the ENS, aware of the importance of establishing a frame of reference on this matter that can be used as support so that Administration staff can carry out their difficult and occasionally thankless task of providing security for ICT systems within their responsibility.

April 2017

Félix Sanz Roldán
Secretary of State
Director of the National Cryptologic Centre

ÍNDICE

1. INTRODUCTION

The National Security Framework (hereinafter ENS) establishes a series of security measures in Annex II that are conditional upon the assessment (Annex I) of the security level in each aspect and the category (Article 43) of the information system in question. At the same time, the system's category is calculated according to the security level in each aspect.

These measures constitute a minimum which must be implemented and, if not, the reasons for not implementing them must be justified or they must be replaced with other security measures that achieve the same protective outcome with regard to information and services, in view of the state of technology, the nature of the services provided, the information handled and the risks to which they are exposed.

2. AIM

In this guide, the relationship between the ENS and information security management regulations and standards is considered over a wide range. This specifically refers to the regulations, ISO/IEC 27001 and ISO/IEC 27002, published in 2005 and revised in 2013.

Please note that the relationship is not one of mathematical equivalence. The first aim of this guide is to explain how to use the 27001 certification as support for complying with the ENS, while the second is to determine which control measures from the 27002 standard are necessary to comply with each measure from Annex II and, where applicable, which additional elements are required. That is to say, if the organization has a 27001 certification and the control measures referred to in the 27002 standard have been covered by incorporating the additional elements, it is considered to have complied with Annex II.

3. SCOPE

This guide establishes some general guidelines that are applicable to entities of varying nature, size and sensitivity. It does not enter into particular cases. It is expected that each organization will tailor them to their particular context.

4. ISO STANDARDS

4.1. ISO/IEC 27001

The 27001 standard is an international management standard that is both voluntary and certifiable. This means that an authorized auditor, having inspected the information security management system, certifies that it complies with the standard.

A management system is certified according to the following definition.

According to ISO/IEC - Annex SL - Proposals for management system standards (2012)

Management system

Set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives.

Note 1: A management system can address a single discipline or several disciplines.

Note 2: The system elements include the organization's structure, roles and responsibilities, planning, operation, etc.

Note 3: The scope of a management system may include the whole organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

According to UNE-ISO/IEC 27000:2016 - Information technologies. Security techniques. Information Security Management Systems (ISMS). Overview and vocabulary.

Management system

Set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives

Information security management system (ISMS)

An Information Security Management System (ISMS) consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. It is based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks.

The 27001 standard was revised in 2013.

4.2. ISO/IEC 27002

The 27002 standard includes a number of control points that can or must be taken into consideration within the management system.

The 27002 standard is not certifiable. The control measures described in the 27002 standard are included in a normative annex of the 27001 standard and must be taken into account during the certification process.

The 27002 standard was revised in 2013.

4.3. EVIDENCE OF COMPLIANCE WITH ISO 27001 AND THE ENS

The 27001 standard is a certifiable and voluntary international standard for any information security management system. Compliance with it is demonstrated *erga omnes* by means of a certificate issued by an authorized auditor, following an audit with a satisfactory result.

In turn, the ENS is a mandatory legal provision applicable to information systems, under Law 40/2015. Compliance with it is demonstrated *erga omnes* by means of a declaration of legal conformity, following an audit with a satisfactory result.

Nevertheless, the two mechanisms are different. As will be demonstrated in the following sections, they can be implemented in tandem.

Summary table

	ISO 27001	**National Security Framework ENS - RD 3/2010**
Ontology	International security standard, lacking legal status.	State regulation under Spanish national law, derived from Law 40/2015.
Nature	Voluntary certification	Mandatory compliance
Scope of application	For any information security management system.	For any public sector information systems falling within the scope of application of Law 40/2015.
Modulation of the measures	According to the auditor's discretion	Regulated according to asset types and the required security levels
Evidence of compliance or conformity	Via certification, issued by an authorized auditor, following an audit with a satisfactory result.	Via a declaration of legal conformity, following an audit with a satisfactory result.

5. COMPLIANCE WITH THE ENS BY MEANS OF 27001 CERTIFICATION

The ENS is a mandatory national regulation for all public sector bodies, enshrined in the legal system under Law 40/2015.

The ENS requires a categorization process (Annex I) and a minimum series of security measures (Annex II) that can be mandatory or optional, depending on the system's category. The most leeway that can be granted is that the organization shows that it has implemented alternative measures that achieve the same level of protection.

The first requirement for using 27001 certification as evidence for ENS compliance is that the scope of the 27001 certification covers what is required by Law 40/2015, from the perspective of both the essential assets (Annex I) and the equipment used.[1]

Also, it should be emphasized that Annex II adapts the requirements according to the information system's category while with 27001 certification, the requirement level is at the discretion of the auditor and his/her opinion of what is “sufficient control”. The tables in this guide make it clear that the 27001 auditor’s opinion is in line with the proportionality established in the ENS in order to be able to determine that a 27002 control measure is covered satisfactorily.

The ENS requires a management system in:

- Annex II (Security measures), Operational framework [op], Planning [op.pl], Security architecture [op.pl.2]
- Annex III (Security Audit), Aim of the audit; although an audit is only required for MEDIUM and HIGH category systems.

The following sections relate the security measures included in Annex II with the control measures in the 27001 and 27002 standards, which can be used to substantiate compliance, indicating whenever the ENS requires additional measures to the 27002 standard.

It is important to bear in mind that measure structuring is not the same in the ENS as in the 27001 and 27002 standards. Some aspects are examined in several sections. When one or more sections of the 27002 standard are cited, we are referring to the main part, yet we are aware that other sections could be relevant in terms of the details.

5.1. SUMMARY TABLE

The following table summarizes the differences which may reasonably be expected between 27001 certification and compliance with the ENS. It should be noted that the 27002 standard is more descriptive than it is imperative; meaning details regarding whatever was implemented depends on the auditor's good judgement. Consequently, an aspect that is required by the ENS may be cited in the relevant section of the 27002 standard and yet ignored for whatever reason. It is, therefore, always essential to verify compliance with the ENS for the relevant aspects and category.

The last column estimates the additional effort that may be necessary to complete ENS requirements. The following levels are applied:

[1] Note that the scope of 27001 certification is determined by the client. It is sufficient to clearly specify which part of the management system is being certified.

Level	comments
0	covered It is always advisable to confirm that the specific details of the ENS have been provided for
1	probably covered It is necessary to check that every aspect provided for in the ENS in terms of the security levels required for the system in question and its category are covered; nevertheless, the additional effort may reasonably be expected to be marginal
2	probably needs to be completed It is necessary to check that every aspect provided for in the ENS in terms of the security levels required for the system in question and its category are covered; the additional effort may reasonably be expected to be significant
3	not covered These are aspects that are not covered in the control measures of the 27002 standard, nor in the requirements of the 27001 standard, and they should, therefore, undergo a specific audit

SECURITY MEASURES

org	Organizational Framework	
org.1	Security policies	1
org.2	Security standards	1
org.3	Security procedures	1
org.4	Authorization process	1

op	Operational Framework	
op.pl	Planning	
op.pl.1	Risk analysis	1
op.pl.2	Security architecture	1
op.pl.3	Acquisition of new components	2
op.pl.4	Capacity measurement / management	1
op.pl.5	Certified components	3

op.acc	Access Control	
op.acc.1	Identification	1
op.acc.2	Access requirements	1
op.acc.3	Separation of functions and tasks	0
op.acc.4	Access rights management process	1
op.acc.5	Authentication mechanism	3
op.acc.6	Local access (local login)	1
op.acc.7	Remote access (remote login)	1
op.exp	Operation	
op.exp.1	Asset inventory	0
op.exp.2	Security configuration	3
op.exp.3	Configuration management	3
op.exp.4	Maintenance	1
op.exp.5	Change management	1
op.exp.6	Protection against malicious code	0
op.exp.7	Incident management	0
op.exp.8	User activity log	0
op.exp.9	Incident management log	0
op.exp.10	Activity log protection	0
op.exp.11	Protection of cryptographic keys	1
op.ext	External Services	
op.ext.1	Contracting and service-level agreements	1
op.ext.2	Daily management	1
op.ext.9	Alternative resources	2
op.cont	Continuity of Service	
op.cont.1	Impact analysis	0
op.cont.2	Continuity plan	0
op.cont.3	Regular testing	0
op.mon	System monitoring	
op.mon.1	Intrusion detection	2
op.mon.2	Metrics system	1

mp	**Protective Measures**	
mp.if	Protection of facilities and infrastructure	
mp.if.1	Separate areas with access control	0
mp.if.2	Identification of individuals	0

mp.if.3	Fitting-out of sites	0
mp.if.4	Electrical power	0
mp.if.5	Fire protection	0
mp.if.6	Flood protection	0
mp.if.7	Logs for equipment entry and exit	0
mp.if.9	Alternative facilities	1
mp.per	Personnel management	
mp.per.1	Job description	0
mp.per.2	Duties and obligations	0
mp.per.3	Awareness-raising	0
mp.per.4	Training	0
mp.per.9	Alternative personnel	1
mp.eq	Equipment protection	
mp.eq.1	Tidy work stations	0
mp.eq.2	Blocking of work stations	0
mp.eq.3	Portable device protection	1
mp.eq.9	Alternative resources	1
mp.com	Communications protection	
mp.com.1	Safe perimeter	2
mp.com.2	Confidentiality protection	1
mp.com.3	Protection of authenticity and integrity	1
mp.com.4	Separation of networks	0
mp.com.9	Alternative resources	1
mp.si	Protection of information storage media	
mp.si.1	Labelling	0
mp.si.2	Cryptography	1
mp.si.3	Custody	0
mp.si.4	Transport	0
mp.si.5	Erasure and destruction	0
mp.sw	Protection of software applications	
mp.sw.1	Development	0
mp.sw.2	Acceptance and commissioning	1
mp.info	Information protection	
mp.info.1	Personal data	0
mp.info.2	Information classification	0

mp.info.3	Information encryption	2
mp.info.4	Electronic signature	3
mp.info.5	Time stamping	3
mp.info.6	Document cleaning	3
mp.info.9	Backup copies	0
mp.s	Services protection	
mp.s.1	Email protection	0
mp.s.2	Protection of web services and applications	3
mp.s.8	Protection against denial of service	3
mp.s.9	Alternative resources	2

5.2. ASPECTS OF CONTINUITY

In the ENS, continuity of service is covered by adding various measures.

Some are operational measures

- [op.cont] Continuity of service
- [op.cont.1] Impact analysis
- [op.cont.2] Continuity plan
- [op.cont.3] Periodic testing

Others are specific measures regarding specific types of assets

- [mp.if.9] Alternative facilities
- [mp.per.9] Alternative personnel
- [mp.eq.9] Alternative resources (equipment)
- [mp.com.9] Alternative resources (communications)
- [mp.info.9] Backup copies
- [mp.s.9] Alternative resources (services)

The underlying idea is that the 27001 and 27002 standards are not continuity standards; that function is delegated to the ISO/IEC 27031, ISO 22313 and ISO 22301 standards.

Although the ENS requirements can be satisfied with the 27001 processes and the 27002 control measures, it is advisable to check the points above from a holistic perspective.

6. [ORG] ORGANIZATIONAL FRAMEWORK

6.1. [ORG.1] SECURITY POLICY

- 27001:2013
  - 4 – Context of the organization
  - 5.2 – Policy
  - 5.3 – Roles, responsibilities and authorities
- 27002:2013
  - 6.1.1 - Information security roles and responsibilities
  - 18.1.1 - Identification of applicable legislation and contractual requirements

The ENS distinguishes between an [Information] Security Policy and multiple safety regulations. The Policy is a unique, high-level and long-lasting document which establishes the fundamental principles on which an organization's security is based. The regulations implement specific aspects, in a dynamic manner, according to the circumstances at the time.

The 27002 standard covered Policy in its 2005 version, but it did not in its 2013 version. This is due to the fact that the Policy has been removed from the detailed control measures in the 27002 standard and transferred to the management framework in the 27001 standard.It is recommended to review the requirements described in the ENS in order to comply with them.

6.2. [ORG.2] SECURITY REGULATIONS

- 27002:2013
  - 5.1.1 – Policies for information security
  - 5.1.2 - Review of the policies for information security
  - 6.1.4 - Contact with special interest groups
  - 8.1.3 - Acceptable use of assets
  - 13.2.1 - Information transfer policies and procedures
  - 15.1.1 - Information security policy for supplier relationships
  - 16.1.1 - Responsibilities and procedures
  - 18.2.2 - Compliance with security policies and standards

Broadly speaking, the term "regulations" in the ENS corresponds to the term "policies" in the 27002 standard. The different standards are distributed throughout the sections of the 27002 standard, alongside the corresponding technical elements.

It is recommended to review the requirements described in the ENS in order to comply with them.

6.3. [ORG.3] SECURITY PROCEDURES

- 27002:2013
  - 6.1.3 - Contact with authorities
  - 12.1.1 - Documented operating procedures
  - 13.2.1 – Information transfer policies and procedures
  - 16.1.1 - Responsibilities and procedures
  - 18.1.2 - Intellectual Property Rights (IPR)
  - 18.2.3 - Technical compliance review

The different procedures are distributed throughout the different sections of the 27002 standard, alongside the corresponding technical elements.

It is recommended to review the requirements described in the ENS in order to comply with them.

6.4. [ORG.4] AUTHORIZATION PROCESS

- 27002:2013
  - 6.1.1 - Information security roles and responsibilities
  - 6.2.1 - Mobile device policy
  - 8.2.3 – Handling of assets
  - 8.3.1 - Management of removable media
  - 12.5.1 - Installation of software on operational systems
  - 12.6.2 - Restrictions on software installation
  - 13.1.1 - Network controls
  - 13.1.2 - Security of network services
  - 14.2.4 - Restrictions on changes to software packages

The “authorization process” concept has disappeared from the 2013 version of the 27002 standard. Part of its content can be found in [6.1.1] and some of the authorization tasks are distributed throughout the different sections of the 27002 standard, near the corresponding technical elements. The points to be reviewed appear in the preceding table according to this criterion.

The ENS requires an integrated authorization process. It is recommended to review the requirements described in the ENS in order to satisfy their compliance.

7. [OP] OPERATIONAL FRAMEWORK

7.1. [OP.PL] PLANNING

7.1.1. [OP.PL.1] RISK ANALYSIS

- 27001:2013
  - 6.1 – Actions to address risks and opportunities
  - 6.1.1 - General

  - 6.1.2 – Information security risk assessment
  - 6.1.3 – Information security risk treatment
  - 8.2 – Information security risk assessment
  - 8.3 – Information security risk assessment

Risk analysis is not a protective measure per se, but rather part of the risk management process that must be applied to all security management.

In this sense, it is included in the ENS as a fundamental principle (Chapter II, Article 6).

Following similar reasoning, risk analysis and management fall within the 27001 management standard.

It is recommended to review the requirements described in the ENS in order to comply with them.

7.1.2. [OP.PL.2] SECURITY ARCHITECTURE

- 27002:2013
  - 8.1.1 - Inventory of assets
  - 8.1.2 - Ownership of assets
  - 13.1.1 - Network controls
  - 14.2.5 - Secure system engineering principles

The ENS centralizes, in an organizational measure, what is dispersed throughout the 27001 and 27002 standards. It is recommended to review the requirements described in the ENS in order to comply with them.

In particular, the ENS requirement of having a management system can be considered satisfied if there is an available PDCA system (27001: 2005 standard) or a 27001 certified management system (versions 2005 or 2013), provided that the entire scope required by the ENS is covered (see Law 40/2015).

7.1.3. [OP.PL.3] ACQUISITION OF NEW COMPONENTS

- 27002:2013
  - 14.1.1 - Analysis and specification of security requirements

The ENS centralizes, in an organizational measure, what is dispersed throughout the 27001 and 27002 standards. It is recommended to review the requirements described in the ENS in order to comply with them.

7.1.4. [OP.PL.4] CAPACITY MEASUREMENT / MANAGEMENT

- 27002:2013
  - 12.1.3 - Capacity management

7.1.5. [OP.PL.5] CERTIFIED COMPONENTS

- 27002:2013
  - Not applicable

This aspect is hardly provided for in the 27001 or 27002 standards. Whatever is specifically required by the ENS must be covered.

7.2. [OP.ACC] ACCESS CONTROL

7.2.1. [OP.ACC.1] IDENTIFICATION

- 27002:2013
  - 9.2.1 – H
  - User registration and de-registration

It is recommended to review the requirements described in the ENS in order to satisfy their compliance.

7.2.2. [OP.ACC.2] ACCESS REQUIREMENTS

- 27002:2013
  - 9.1.1 - Access control policy
  - 9.1.2 - Access to networks and network services
  - 9.4.1 - Information access restriction
  - 9.4.4 - Use of privileged utility programs
  - 9.4.5 - Access control to program source code

It is recommended to review the requirements described in the ENS in order to comply with them.

7.2.3. [OP.ACC.3] SEPARATION OF FUNCTIONS AND TASKS

- 27002:2013
  - 6.1.2 – Segregation of duties

It is recommended to review the requirements described in the ENS in order to comply with them.

7.2.4. [OP.ACC.4] ACCESS RIGHTS MANAGEMENT PROCESS

- 27002:2013
  - 9.2.2 - User access provisioning
  - 9.2.3 - Management of privileged access rights
  - 9.2.5 - Review of user access rights

- 9.2.6 - Removal or adjustment of access rights

It is recommended to review the requirements described in the ENS in order to comply with them.

7.2.5. [OP.ACC.5] AUTHENTICATION MECHANISM

- 27002:2013
  - 9.2.4 - Management of users' secret authentication information
  - 9.3.1 - Use of secret authentication information
  - 9.4.3 - Password management system

The 27002 standard almost exclusively deals with passwords and shared secrets in general.

The ENS establishes several authentication methods and adapts their use according to the system's category. It is necessary to check that the ENS requirements are covered beyond what is certified in relation to the 27002 standard.

7.2.6. [OP.ACC.6] LOCAL ACCESS (LOCAL LOGON)

- 27002:2013
  - 9.4.2 – Secure log-on procedures

It is recommended to review the requirements described in the ENS in order to comply with them.

7.2.7. [OP.ACC.7] REMOTE ACCESS (REMOTE LOGIN)

- 27002:2013
  - 9.4.2 - Secure log-on procedures
  - 10.1.1 - Policy on the use of cryptographic controls
  - 13.1.1 - Network controls
  - 13.1.2 - Security of network services
  - 18.1.5 - Regulation of cryptographic controls

It is recommended to review the requirements described in the ENS in order to comply with them.

7.3. [OP.EXP] OPERATION

7.3.1. [OP.EXP.1] ASSET INVENTORY

- 27002:2013
  - 8.1.1 - Inventory of assets

    - 8.1.2 - Ownership of assets

It is recommended to review the requirements described in the ENS in order to comply with them.

7.3.2. [OP.EXP.2] SECURITY CONFIGURATION

- 27002:2013
    - Not explicitly examined

ENS requirements are not explicitly provided for in the 27002 standards. It is advisable to check that ENS requirements are satisfied.

7.3.3. [OP.EXP.3] CONFIGURATION MANAGEMENT

- 27002:2013
    - Not explicitly examined

ENS requirements are not explicitly examined within the 27002 standards. It is advisable to check that ENS requirements are satisfied.

7.3.4. [OP.EXP.4] MAINTENANCE

- 27002:2013
    - 11.2.4 - Equipment maintenance

It is recommended to review the requirements described in the ENS in order to comply with them.

7.3.5. [OP.EXP.5] CHANGE MANAGEMENT

- 27002:2013
    - 12.1.2 - Change management
    - 14.2.2 - System change control procedures
    - 14.2.3 - Technical review of applications after operating platform changes

It is recommended to review the requirements described in the ENS in order to comply with them.

7.3.6. [OP.EXP.6] PROTECTION AGAINST MALICIOUS CODE

- 27002:2013
    - 12.2.1 – Controls against malware

It is recommended to review the requirements described in the ENS in order to comply with them.

7.3.7. [OP.EXP.7] INCIDENT MANAGEMENT

- 27002:2013
  - 6.1.3 - Contact with authorities
  - 6.1.4 - Contact with special interest groups
  - 16.1.2 – Reporting information security events
  - 16.1.3 - Reporting security weaknesses
  - 16.1.4 – Assessment of and decision on information security events
  - 16.1.5 - Response to information security incidents
  - 16.1.6 - Learning from information security incidents
  - 16.1.7 - Evidence collection

It is recommended to review the requirements described in the ENS in order to comply with them.

7.3.8. [OP.EXP.8] USER ACTIVITY LOG

- 27002:2013
  - 12.4.1 - Event logging
  - 12.4.3 – Administrator and operator logs

It is recommended to review the requirements described in the ENS in order to comply with them.

7.3.9. [OP.EXP.9] INCIDENT MANAGEMENT LOG

- 27002:2013
  - 16.1.5 - Response to information security incidents
  - 16.1.7 - Collection of evidence

It is recommended to review the requirements described in the ENS in order to comply with them.

7.3.10. [OP.EXP.10] PROTECTION OF ACTIVITY LOGS

- 27002:2013
  - 12.4.2 - Protection of log information
  - 12.4.4 – Clock synchronisation

It is recommended to review the requirements described in the ENS in order to comply with them.

7.3.11. [OP.EXP.11] PROTECTION OF CRYPTOGRAPHIC KEYS

- 27002:2013
  - 10.1.2 - Key management

It is recommended to review the requirements described in the ENS in order to comply with them.

7.4. [OP.EXT] EXTERNAL SERVICES

7.4.1. [OP.EXT.1] CONTRACTING AND SERVICE-LEVEL AGREEMENTS

- 27002:2013
  - 13.2.2 - Agreements on information transfer
  - 15.1.1 - Information security policy for supplier relationships
  - 15.1.2 - Addressing security within supplier agreements
  - 15.1.3 - Information and communication technology supply chain

It is recommended to review the requirements described in the ENS in order to comply with them.

7.4.2. [OP.EXT.2] DAILY MANAGEMENT

- 27002:2013
  - 15.2.1 - Monitoring and review of supplier services
  - 15.2.2 - Managing changes to supplier services

It is recommended to review the requirements described in the ENS in order to comply with them.

7.4.3. [OP.EXT.9] ALTERNATIVE RESOURCES

- 27002:2013
  - Not applicable

ENS requirements must be reviewed in order to ensure compliance. Although not explicitly addressed in the 27002 standards, this is probably part of the business continuity control measures.

7.5. [OP.CONT] CONTINUITY OF SERVICE

7.5.1. [OP.CONT.1] IMPACT ANALYSIS

- 27002:2013
  - 17.1.1 - Planning information security continuity

ENS requirements must be reviewed in order to comply with them.

7.5.2. [OP.CONT.2] CONTINUITY PLAN

- 27002:2013
  - 17.1.2 - Implementing information security continuity

ENS requirements must be reviewed in order to comply with them.

7.5.3. [OP.CONT.3] PERIODIC TESTS

- 27002:2013
  - 17.1.3 - Verify, review and evaluate information security continuity

ENS requirements must be reviewed in order to comply with them.

7.6. [OP.MON] SYSTEM MONITORING

7.6.1. [OP.MON.1] INTRUSION DETECTION

- 27002:2013
  - Not explicitly examined

The 27002:2013 standard mentions the detection system in several places, appearing to take the following for granted:

- 12.4.1 - Event logging
- 12.4.3 - Administrator and operator logs
- 13.1.2 - Security of network services

It is recommended to review the requirements described in the ENS in order to comply with them.

7.6.2. [OP.MON.2] METRICS SYSTEM

- 27001:2013
  - 9 – Performance evaluation
  - 9.1 – Monitoring, measurement, analysis and evaluation

The ENS requires several very specific points. ENS requirements must be checked to ensure that they are satisfied, especially any related to Article 35.

8. [MP] PROTECTIVE MEASURES

8.1. [MP.IF] PROTECTION OF FACILITIES AND INFRASTRUCTURE

8.1.1. [MP.IF.1] SEPARATE AREAS WITH ACCESS CONTROL

- 27002:2013
  - 11.1.1 - Physical security perimeter
  - 11.1.2 - Physical entry controls
  - 11.1.3 - Securing offices, rooms and facilities
  - 11.1.4 - Protection against external and environmental threats
  - 11.1.5 - Working in secure areas
  - 11.1.6 - Delivery and loading areas
  - 11.2.1 - Equipment positioning and protection

ENS requirements are addressed at intervals throughout the 27002 standards. A review of ENS requirements must be carried out to ensure that they are satisfied.

8.1.2. [MP.IF.2] IDENTIFICATION OF INDIVIDUALS

- 27002:2013
  - 11.1.2 - Physical entry controls

It is recommended to review the requirements described in the ENS in order to comply with them.

8.1.3. [MP.IF.3] FITTING-OUT OF SITES

- 27002:2013
  - 11.2.2 - Supporting utilities
  - 11.2.3 - Cabling security

It is recommended to review the requirements described in the ENS in order to comply with them.

8.1.4. [MP.IF.4] ELECTRICAL POWER

- 27002:2013
  - 11.2.2 - Supporting utilities

It is recommended to review the requirements described in the ENS in order to comply with them.

8.1.5. [MP.IF.5] FIRE PROTECTION

- 27002:2013
  - 11.1.4 - Protection against external and environmental threats

It is recommended to review the requirements described in the ENS in order to comply with them.

8.1.6. [MP.IF.6] FLOOD PROTECTION

- 27002:2013
  - 11.1.4 - Protection against external and environmental threats

It is recommended to review the requirements described in the ENS in order to comply with them.

8.1.7. [MP.IF.7] RECORD OF EQUIPMENT ENTRY AND EXIT

- 27002:2013
  - 11.2.5 - Removal of assets
  - 11.2.6 – Security of equipment and assets off-premises

It is recommended to review the requirements described in the ENS in order to comply with them.

8.1.8. [MP.IF.9] ALTERNATIVE FACILITIES

- 27002:2013
  - 17.2.1 - Availability of information processing facilities

Requirements of the ENS must be checked to ensure that they are satisfied.

8.2. [MP.PER] PERSONNEL MANAGEMENT

8.2.1. [MP.PER.1] JOB DESCRIPTION

- 27002:2013
  - 7.1.1 - Screening

It is recommended to review the requirements described in the ENS in order to comply with them.

8.2.2. [MP.PER.2] DUTIES AND OBLIGATIONS

- 27002:2013

  - 7.1.2 - Terms and conditions of employment
  - 7.2.1 - Management responsibilities
  - 7.2.3 - Disciplinary process
  - 7.3.1 - Termination or change of employment responsibilities
  - 8.1.4 - Return of assets
  - 13.2.4 - Confidentiality or non-disclosure agreements

ENS requirements are addressed at intervals throughout the 27002 standards. A review of ENS requirements should be carried out to ensure that they are satisfied.

8.2.3. [MP.PER.3] AWARENESS-RAISING

- 27001:2013
  - 7.3 - Awareness
- 27002:2013
  - 7.2.2 - Information security awareness, education and training

ENS requirements are addressed at intervals throughout the 27002 standards. A review of ENS requirements should be carried out to ensure that they are satisfied.

8.2.4. [MP.PER.4] TRAINING

- 27001:2013
  - 7.2 - Competence
- 27002:2013
  - 7.2.2 - Information security awareness, education and training

It is recommended to review the requirements described in the ENS in order to comply with them.

8.2.5. [MP.PER.9] ALTERNATIVE PERSONNEL

- 27002:2013
  - 17.2.1 - Availability of information processing facilities

Requirements of the ENS must be checked to ensure that they are satisfied.

8.3. [MP.EQ] EQUIPMENT PROTECTION

8.3.1. [MP.EQ.1] TIDY WORK STATION

- 27002:2013
  - 11.2.9 - Clear desk and clear screen policy

It is recommended to review the requirements described in the ENS in order to comply with them.

8.3.2. [MP.EQ.2] BLOCKING OF WORK STATIONS

- 27002:2013
  - 11.2.8 - Unattended user equipment

ENS requirements must be checked to ensure that they are satisfied.

8.3.3. [MP.EQ.3] PROTECTION OF PORTABLE DEVICES

- 27002:2013
  - 6.2.1 - Mobile device policy

ENS requirements must be checked to ensure that they are satisfied.

8.3.4. [MP.EQ.9] ALTERNATIVE RESOURCES

- 27002:2013
  - 17.2.1 - Availability of information processing facilities

Requirements of the ENS must be checked to ensure that they are satisfied.

8.4. [MP.COM] COMMUNICATIONS PROTECTION

8.4.1. [MP.COM.1] SECURE PERIMETER

- 27002:2013
  - 13.1.2 - Security of network services

The ENS requires several very specific points. Requirements of the ENS must be checked to ensure that they are satisfied.

8.4.2. [MP.COM.2] PROTECTION OF CONFIDENTIALITY

- 27002:2013
  - 10.1.1 - Policy on the use of cryptographic controls
  - 13.1.1 - Network controls
  - 13.1.2 - Security of network services
  - 14.1.2 - Securing application services on public networks
  - 18.1.5 - Regulation of cryptographic controls

The ENS requires several very specific points. Requirements of the ENS must be checked to ensure that they are satisfied.

8.4.3. [MP.COM.3] PROTECTION OF AUTHENTICITY AND INTEGRITY

- 27002:2013
  - 10.1.1 - Policy on the use of cryptographic controls
  - 13.1.1 - Network controls
  - 13.1.2 - Security of network services
  - 14.1.2 - Securing application services on public networks

The ENS requires several very specific points. Requirements of the ENS must be checked to ensure that they are satisfied.

8.4.4. [MP.COM.4] SEPARATION OF NETWORKS

- 27002:2013
  - 13.1.3 – Segregation in networks

ENS requirements must be checked to ensure that they are satisfied.

8.4.5. [MP.COM.9] ALTERNATIVE RESOURCES

- 27002:2013
  - 17.2.1 - Availability of information processing facilities

Requirements of the ENS must be checked to ensure that they are satisfied.

8.5. [MP.SI] PROTECTION OF INFORMATION STORAGE MEDIA

8.5.1. [MP.SI.1] LABELLING

- 27002:2013
  - 8.2.2 - Labelling of information
  - 8.3.1 - Management of removable media

It is recommended to review the requirements described in the ENS in order to comply with them.

8.5.2. [MP.SI.2] CRYPTOGRAPHY

- 27002:2013
  - 8.3.1 - Management of removable media
  - 10.1.1 - Policy on the use of cryptographic controls

It is recommended to review the requirements described in the ENS in order to comply with them.

8.5.3. [MP.SI.3] CUSTODY

- 27002:2013
  - 8.3.1 - Management of removable media

It is recommended to review the requirements described in the ENS in order to comply with them.

8.5.4. [MP.SI.4] TRANSPORT

- 27002:2013
  - 8.3.3 - Physical media transfer
  - 11.2.5 - Removal of assets

It is recommended to review the requirements described in the ENS in order to comply with them.

8.5.5. [MP.SI.5] DELETION AND DESTRUCTION

- 27002:2013
  - 8.3.2 – Disposal of media
  - 11.2.7 - Secure disposal or re-use of equipment

It is recommended to review the requirements described in the ENS in order to comply with them.

8.6. [MP.SW] PROTECTION OF SOFTWARE APPLICATIONS (SW)

8.6.1. [MP.SW.1] APPLICATION DEVELOPMENT

- 27002:2013
  - 9.4.5 - Access control to program source code
  - 12.1.4 - Separation of development, testing and operational environments
  - 14.2.1 - Secure development policy
  - 14.2.5 - Secure system engineering principles
  - 14.2.6 - Secure development environment
  - 14.2.7 - Outsourced development
  - 14.3.1 - Protection of test data

ENS requirements are addressed at intervals throughout the 27002 standards. A review of ENS requirements should be carried out to ensure that they are satisfied.

8.6.2. [MP.SW.2] ACCEPTANCE AND COMMISSIONING

- 27002:2013
  - 12.1.4 - Separation of development, testing and operational environments
  - 12.5.1 - Installation of software on operational systems
  - 12.6.1 - Management of technical vulnerabilities
  - 14.2.8 - System security testing
  - 14.2.9 - System acceptance testing
  - 14.3.1 - Protection of test data
  - 14.2.7 - Outsourced development

ENS requirements are addressed at intervals throughout the 27002 standards. A review of ENS requirements should be carried out to ensure that they are satisfied.

8.7. [MP.INFO] INFORMATION PROTECTION

8.7.1. [MP.INFO.1] PERSONAL DATA

- 27002:2013
  - 18.1.4 - Privacy and protection of personally identifiable information

It is recommended to review the requirements described in the ENS in order to comply with them.

8.7.2. [MP.INFO.2] INFORMATION CLASSIFICATION

- 27002:2013
  - 8.1.2 - Ownership of assets
  - 8.2.1 - Classification of information

It is recommended to review the requirements described in the ENS in order to comply with them.

8.7.3. [MP.INFO.3] INFORMATION ENCRYPTION

- 27002:2013
  - 10.1.1 - Policy on the use of cryptographic controls
  - 8.3.3 - Physical media transfer
  - 13.1.1 - Network controls
  - 13.1.2 - Security of network services
  - 18.1.5 - Regulation of cryptographic controls

ENS requirements are addressed at intervals throughout the 27002 standards. A review of ENS requirements should be carried out to ensure that they are satisfied.

8.7.4. [MP.INFO.4] ELECTRONIC SIGNATURE

- 27002:2013
    - 10.1.1 - Policy on the use of cryptographic controls
    - 14.1.3 - Protecting application service transactions
    - 18.1.5 - Regulation of cryptographic controls

In the ENS, these aspects are highly related to the proper guarantees in the administrative process and the legislation on electronic signatures. Whatever is specifically required by the ENS should be covered.

8.7.5. [MP.INFO.5] TIME STAMPING

- 27002:2013
    - 14.1.3 - Protecting application services transactions

This aspect is not provided for in the 27001 or 27002 standards. Whatever is specifically required by the ENS should be covered.

8.7.6. [MP.INFO.6] DOCUMENT CLEANING

- 27002:2013
    - Not applicable

This aspect is not examined in the 27001 or 27002 standards. Whatever is specifically required by the ENS should be covered.

8.7.7. [MP.INFO.9] BACKUP COPIES

- 27002:2013
    - 12.3.1 - Information backup

It is recommended to review the requirements described in the ENS in order to comply with them.

8.8. [MP.S] SERVICES PROTECTION

8.8.1. [MP.S.1] EMAIL PROTECTION

- 27002:2013
    - 13.2.3 - Electronic messaging

It is recommended to review the requirements described in the ENS in order to comply with them.

8.8.2. [MP.S.2] PROTECTION OF WEB SERVICES AND APPLICATIONS

- 27002:2013
  - Not applicable

This aspect is not examined in the 27001 or 27002 standards. Whatever is specifically required by the ENS should be covered.

8.8.3. [MP.S.8] PROTECTION AGAINST DENIAL OF SERVICE

- 27002:2013
  - 12.1.3 – Capacity management

This aspect is not examined in the 27001 or 27002 standards. Whatever is specifically required by the ENS should be covered.

8.8.4. [MP.S.9] ALTERNATIVE RESOURCES

- 27002:2013
  - 17.2.1 - Availability of information processing facilities

ENS requirements must be checked to ensure that they are satisfied.

9. OTHER CONTROL MEASURES

Some control measures from the 27002 standard are not reflected in the ENS.

[27002:2013] 6.1.5 - Information security in project management

This refers to the standard requiring that all projects undertaken by an organization take information security into account. This aspect may be said to appear implicitly in the ENS, given that it must be applied to all information and services related to Law 40/2015.

[27002:2013] 6.2.2 – Teleworking

This is not explicitly covered by the ENS; however, given that all information must be protected at all times and in all places, the relevant measures apply to people, facilities and ICT methods.

[27002:2013] 12.7.1 - Information systems audit controls

This standard describes how to carry out auditing tasks, ensuring that access from the auditor does not impair the confidentiality, integrity and availability required by the system.

[27002:2013] 18.1.3 - Protection of records

This standard refers to the documents that support the organization's activities. In a public sector body, we understand these documents to all be information whose integrity and availability must be guaranteed in the long term.

The ENS sees this as part of the information that must be protected under the mandate of Law 40/2015 and, therefore, the appropriate protective measures apply.

[27002:2013] 18.2.1 - Independent review of information security

See Annex III - Security Audit.

Explained in the CCN-STIC 802 guide - Audit Guide.

APPENDIX A. GLOSSARY

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

APPENDIX B. REFERENCES

- ENS
  RD 3/2010, dated 8 January, regulating the National Security Framework in the field of Electronic Administration. BOE 29 January 2010.

  Royal Decree 951/2015, dated 23rd October, modifying Royal Decree 3/2010, dated 8th January, regulating the National Security Framework in the field of Electronic Administration.

  https://www.ccn-cert.cni.es/publico/ens/ens/index.html
- ISO/IEC 27000:2016
  Information technology – Security techniques – Information security management systems – Overview and vocabulary
- ISO/IEC 27001:2013
  Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27002:2013
  Information technology – Security techniques – Code of practice for information security management
- Ley 11/2007
  Law 11/2007, dated 22 June, Citizens' electronic access to Public Services.
- Ley 39/2015
  Law 39/2015 of October 1, on Common Administrative Procedure of Public Administrations
- Ley 40/2015
  Law 40/2015, of October 1st, on the Legal Regime of the Public Sector
- CCN-STIC. 800 Series. National Security Framework.