centro criptológico nacional

ICT Security Guide
CCN-STIC 825

Independent Annex
Mapping between the ISO 27001:2022 Standard and the RD 311/2022 (ENS)

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

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
2024.01.09 16:27:07 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-289-7
Date of issue: august 2023

INDEX

1. MAPPING BETWEEN THE ISO 27001:2022 STANDARD AND RD 311/2022 (ENS)

ISO 27001 Reference	ISO 27001:2022 Control	Summary description of the ISO 27001:2022 control	ENS Reference	Security measure RD 311/2022
5				
5.1	Information security policies	The ISP and other specific internal policies will be defined, approved by management, communicated to staff and other stakeholders, reviewed at planned intervals and in the event of significant changes.	[org.1] [org.2]	Security Policy Security Regulations
5.2	Roles and responsibilities in information security	Information security roles and responsibilities shall be defined and assigned according to the needs of the organisation.	[org.4]	Authorisation Process
5.3	Segregation of duties	Conflicts of functions and areas of responsibility must be segregated.	[op.acc.3]	Segregation of duties and tasks
5.4	Management responsibilities	Senior management shall require all staff to implement information security in accordance with the ISP, specific regulations and organisational procedures.	[org.1] Art.13	Security Policy Organisation and implementation of the security process.
5.5	Contact with the authorities	The organisation shall establish and maintain contact with the relevant authorities.	Art. 25 [op.exp.7]	Security incidents Incident management
5.6	Contact with special interest groups	The organisation shall establish and maintain contact with special interest groups or other specialised security forums and professional associations.	Article 13 [org.1]	Organisation and implementation of the security process Security Policy
5.7	Threat intelligence	Information related to information security threats will be collected and analysed for threat intelligence.	[op.mon.3]	Surveillance
5.8	Information security in project management	Information security must be integrated into project management.	[op.pl.3]	Procurement of new components
5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including their owners, should be developed and maintained.	[op.exp.1] [op.pl.2]	Inventory of assets Security Architecture
5.10	Acceptable use of information and associated assets	Acceptable use policies and procedures for the handling of information and other associated assets should be identified, documented and implemented.	[org.2] [org.3] [mp.si.3]	Safety regulations Security procedures Custody
5.11	Return of assets	Staff and other third parties, as appropriate, shall return all assets of the organisation in their possession at the time of change or termination of their employment, contract or agreement.	[org.2]	Safety regulations

ISO 27001 Reference	ISO 27001:2022 Control	Summary description of the ISO 27001:2022 control	ENS Reference	Security measure RD 311/2022
5.12	Classification of information	Information should be classified according to the organisation's information security needs, based on confidentiality, integrity, availability and relevant stakeholder requirements.	[mp.info.2]	Qualification of information
5.13	Labelling of information	An appropriate set of procedures for labelling information should be developed and implemented in accordance with the information classification framework adopted by the organisation.	[mp.si.1]	Marking of supports
5.14	Transfer of information	Information transfer rules, procedures or agreements should be in place for all types of transfer services within the organisation and between the organisation and third parties.	[org.2] [org.3] [op.ext.1] [mp.s.1]	Safety regulations Security Procedures Recruitment and NSAs Protection of electronic mail
5.15	Access control	Physical and logical access control rules for information and other associated assets, based on organisational and information security requirements, shall be established and implemented.	[op.acc.2]	Access requirements
5.16	Identity management	The full lifecycle of identities must be managed.	[op.acc.1]	Identification
5.17	Authentication information	The allocation and management of authentication information should be controlled by a management process, including advice to staff on the proper handling of authentication information.	[op.acc.1] [op.acc.2]	Identification Access requirements
5.18	Access rights	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organisation's specific policy and rules on access control.	[op.acc.4]	Access rights management process
5.19	Information security in supplier relations	Processes and procedures should be defined and implemented to manage information security risks associated with the use of supplier products or services.	[op.ext.1]	Contracting and service level agreements
5.20	Addressing information security within supplier agreements	Relevant information security requirements should be established and agreed with each supplier according to the type of relationship established with them.	[op.ext.1]	Contracting and service level agreements
5.21	Managing Information Security in the ICT supply chain	Processes and procedures should be defined and implemented to manage information security risks associated with the supply chain of ICT products and services.	[op.ext.3]	Supply chain security
5.22	Monitoring, review and change management of supplier services	The organisation shall regularly monitor, review, evaluate and manage changes in the provider's information security practices and service delivery.	[op.ext.2]	Day-to-day management
5.23	Information security for the use of cloud services	Processes for the acquisition, use, management and termination of cloud services should be established in accordance with the organisation's information security requirements.	[op.nub.1]	Cloud Services Protection

ISO 27001 Reference	ISO 27001:2022 Control	Summary description of the ISO 27001:2022 control	ENS Reference	Security measure RD 311/2022
5.24	Information security incident management planning and preparation.	The organisation should plan and prepare for managing information security incidents by defining, developing and communicating information security incident management processes, roles and responsibilities.	[op.exp.7]	Incident Management
5.25	Assessment and decision on information security events	The organisation shall evaluate information security events and decide whether they should be categorised as information security incidents.	[op.exp.7]	Incident Management
5.26	Information security incident response	The response to information security incidents should be carried out according to documented procedures.	[op.exp.9]	Incident Management Register
5.27	Learning from information security incidents	Knowledge gained from information security incidents should be used to strengthen and improve information security controls.	[op.exp.7] [op.exp.9]	Incident Management Incident Management Register
5.28	Gathering evidence	The organisation shall establish and implement procedures for the identification, collection, classification and preservation of evidence related to information security events.	[op.exp.7] [op.exp.9]	Incident Management Incident Management Register
5.29	Information security during the outage	The organisation must plan how to maintain information security at an appropriate level during an outage.	[op.cont.1] [op.cont.2]	Impact analysis Continuity Plan
5.30	ICT readiness for business continuity	ICT resilience should be planned, implemented, maintained and verified based on business continuity objectives and ICT continuity requirements.	[op.cont.3]	Periodic Testing
5.31	Identification of legal, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security, together with the organisation's approach to meeting those requirements, should be identified, documented and kept up to date.	[org.1] [mp.info.3]	Security policy Electronic signature
5.32	Intellectual property rights	The organisation should implement appropriate procedures to protect intellectual property rights.	[org.1] [org.2] [op.exp.1]	Security policy Safety regulations Inventory of assets
5.33	Record protection	Records must be protected against loss, destruction, falsification, falsification, unauthorised access and disclosure.	[op.exp.8] [op.mon.3]	Registration of the activity Surveillance
5.34	Privacy and personal data protection (PDP)	The organisation shall identify and comply with privacy and personal data protection (PDP) requirements in accordance with applicable laws, regulations and contractual requirements.	[mp.info.1]	Personal data
5.35	Independent review of information security	The organisation's approach to managing information security and its implementation, including people, processes and technology, should be independently reviewed at planned intervals, or following	Art. 31 Annex III [mp.s.2]	Security Audit Security Audit Securing web services and applications

ISO 27001 Reference	ISO 27001:2022 Control	Summary description of the ISO 27001:2022 control	ENS Reference	Security measure RD 311/2022
		significant changes.		
5.36	Compliance with information security policies and standards	Compliance with the organisation's information security policy, other policies, norms and standards should be regularly reviewed.	Art. 31 Annex III [org.4] [op.exp.3] [op.exp.4]	Security Audit Security Audit Authorisation Process Security configuration management Maintenance and security updates
5.37	Documentation of operational procedures	Operational procedures for information processing facilities should be documented and made available to all users who need them.	[org.3]	Security Procedures
6				
6.1	Check	Background checks should be conducted on an ongoing basis, checking all candidates before they join the organisation, in accordance with applicable legislation, regulations and ethical principles, commensurate with the requirements of the business, the classification of information to be accessed and the perceived risks.	[mp.per.1]	Job characterisation
6.2	Terms and conditions of engagement	Contractual employment agreements should indicate the information security responsibilities of staff and the organisation.	[mp.per.2]	Duties and obligations
6.3	Information security awareness, education and training	Organisational staff and relevant stakeholders should receive appropriate information security awareness, education and training, as well as regular updates on the organisation's ISP, other internal rules and procedures, relevant to their job.	[mp.per.3] [mp.per.4]	Awareness-raising Training
6.4	Disciplinary process	There should be a formal disciplinary process that has been communicated to employees and relevant stakeholders, outlining the actions to be taken against those who have caused a security breach.	[org.1]	Security Policy
6.5	Responsibilities for termination or change	Information security responsibilities and duties, which remain in place after termination or change of employment, should be defined, communicated and enforced to relevant personnel and other stakeholders.	[mp.per.2]	Duties and obligations
6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organisation's information protection needs should be identified, documented, regularly reviewed and signed by staff and other relevant stakeholders.	[org.2] [mp.per.2] [op.ext.1]	Safety regulations Duties and obligations Contracting and service level agreements.

ISO 27001 Reference	ISO 27001:2022 Control	Summary description of the ISO 27001:2022 control	ENS Reference	Security measure RD 311/2022
6.7	Telework	Security measures should be implemented when staff are working remotely, to protect information accessed, processed or stored outside the organisation's premises.	[org.2] [mp.per.2]	Safety regulations Duties and obligations
6.8	Notification of information security events	The organisation shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels.	[op.exp.7]	Incident Management
7				
7.1	Physical security perimeter	Security perimeters should be defined and employed to protect areas containing information and other associated assets.	[mp.if.1]	Separate areas with access control
7.2	Physical input controls	Secure areas should be protected by appropriate entry controls and access points.	[mp.if.2] [mp.if.7]	Identification of persons Check-in and check-out of equipment
7.3	Security of offices, offices and resources	For offices, offices and resources, physical security must be designed and implemented.	[mp.if.1] [mp.if.3]	Separate areas with access control Fitting out of premises
7.4	Physical security monitoring	Facilities must be continuously monitored for unauthorised physical access.	[mp.if.1] [mp.info.1]	Separate and access-controlled areas Personal data
7.5	Protection against external and environmental threats	Protections against physical and environmental hazards, such as natural disasters, or other physical threats to infrastructure, whether intentional or unintentional, must be designed and implemented.	[mp.if.3] [mp.if.5] [mp.if.6]	Separate areas with access control Fire protection Flood protection
7.6	Working in safe areas	Procedures for working in secure areas should be designed and implemented.	[mp.if.1] [org.2]	Fitting out of premises Safety regulations
7.7	Clear workstation and clean screen	Paperless workstation and removable storage media rules should be defined and enforced, as well as clean screen rules for information processing resources.	[mp.eq.1] [mp.eq.2]	Uncluttered workstation Blocking of the workstation
7.8	Location and protection of equipment	Equipment must be securely located and protected.	[mp.if.1] [mp.eq.3]	Separate areas with access control Protection of portable devices
7.9	Safety of off-site equipment	Off-site assets must be protected.	[mp.eq.3]	Protection of portable devices
7.10	Storage media	Storage media should be managed throughout their life cycle, including acquisition, use, transport and disposal, in accordance with the organisation's classification framework and handling requirements.	[mp.si.1] [mp.si.2] [mp.si.3] [mp.si.4] [mp.si.5]	Marking of supports Cryptography Custody Transport Deletion and destruction
7.11	Supply facilities	Data processing equipment must be protected against power failures, and other disturbances caused by failures in the supply	[mp.if.4]	Electric power

ISO 27001 Reference	ISO 27001:2022 Control	Summary description of the ISO 27001:2022 control	ENS Reference	Security measure RD 311/2022
		installations.		
7.12	Wiring safety	Electrical and telecommunications cabling that transmits data or supports information services must be protected against interception, interference or damage.	[mp.if.3]	Fitting out the premises
7.13	Maintenance of equipment	Equipment must be properly maintained to ensure the availability, integrity and confidentiality of information.	[op.exp.4]	Maintenance and upgrades
7.14	Safe disposal or re-use of equipment	All storage media must be verified to ensure that no sensitive information and/or software licences have been securely deleted or overwritten before disposal or reuse.	[mp.si.5]	Deletion and destruction
8				
8.1	User end devices	Information stored, processed or accessible through end-user devices must be protected.	[mp.eq.3] [mp.eq.4]	Protection of portable devices Other devices connected to the network
8.2	Access privilege management	The allocation and use of privileged access rights must be restricted and managed.	[op.acc.1]	Identification
8.3	Restriction of access to information	Access to information and other associated assets must be restricted in accordance with access control regulations.	[op.acc.2] [op.acc.3] [op.acc.4]	Access requirements Segregation of duties and tasks Access rights management process
8.4	Access to source code	Read and write access to source code, development tools and software libraries must be properly managed.	[op.acc.2] [mp.sw.1]	Access requirements Application development
8.5	Secure authentication	Secure authentication technologies and procedures should be implemented based on information access restrictions and access control regulations.	[op.acc.6]	Authentication mechanisms (users of the organisation)
8.6	Capacity management	Resource use should be monitored and adjusted based on current and projected capacity requirements.	[op.pl.4] [mp.s.4]	Capacity Management Denial of service protection
8.7	Controls against malicious code	Protection against malicious code must be implemented and supported by appropriate user awareness.	[op.exp.6]	Protection against malicious code
8.8	Technical vulnerability management	Information on the technical vulnerabilities of the information systems in use should be obtained, the organisation's exposure to these vulnerabilities should be assessed, and appropriate measures should be taken.	[op.mon.3] [op.exp.4]	Surveillance Maintenance and upgrades
8.9	Configuration management	Configurations, including security, hardware, software, services and network configurations, must be established, documented, implemented, monitored and reviewed.	[op.exp.2] [op.exp.3]	Security Settings Configuration Management
8.10	Deletion of information	Information stored in information systems, devices or on any other	[mp.si.5]	Deletion and destruction

ISO 27001 Reference	ISO 27001:2022 Control	Summary description of the ISO 27001:2022 control	ENS Reference	Security measure RD 311/2022
		information carrier should be deleted when no longer required.		
8.11	Data masking	Data masking must be used in accordance with the organisation's access control and other regulations, as well as with business requirements and taking into account applicable legislation.	[mp.info.1]	Personal data
8.12	Preventing data leakage	Measures for the prevention of data leakage to systems, networks and any other devices that process, store or transmit sensitive information must be implemented.	[mp.com.1] [mp.com.2] [mp.si.2] [mp.eq.3]	Secure perimeter Protection of confidentiality Cryptography Protection of portable equipment
8.13	Backing up information	Back-ups of information, software and systems should be maintained and regularly checked in accordance with the specific agreed backup policy.	[mp.info.6]	Back-up copies
8.14	Redundancy of information processing resources	Data processing equipment must be implemented with sufficient redundancies to meet availability requirements.	[op.cont.4]	Alternative media
8.15	Event registration	Records of activities, exceptions, failures and other relevant events must be generated, protected, stored and analysed.	[op.exp.8]	Registration of the activity
8.16	Monitoring of activities	Networks, systems and applications should be monitored for anomalous behaviour, with appropriate actions taken to assess possible information security incidents.	[op.mon.3] [mp.s.4]	Surveillance DoS protection
8.17	Clock synchronisation	The clocks of the information processing systems used by the organisation shall be synchronised with appropriate time sources.	[op.exp.8]	Registration of the activity
8.18	Use of privileged utility programs	The use of utility programs that may be capable of overriding system and application controls should be strictly restricted and controlled.	[op.acc.2]	Access requirements
8.19	Installation of the software in production systems	Procedures and measures must be implemented to securely manage the installation of software in production systems.	[op.exp.2] [op.acc.3] [mp.sw.2]	Security settings Segregation of duties and tasks Acceptance and commissioning
8.20	Network security	Networks and network devices must be secured, managed and controlled to protect information in systems and applications.	[mp.com.1]	Secure perimeter
8.21	Security of network services	Security mechanisms, service levels and service requirements for all network services must be identified, implemented and monitored.	[mp.com.2] [mp.com.3]	Protection of confidentiality Protection Integrity/Authenticity
8.22	Segregation in networks	Groups of information services, users and information systems should be segregated in the organisation's networks.	[op.ext.4] [mp.com.4]	Interconnection of systems Separation of information flows in the network
8.23	Web filtering	Access to external websites should be managed to reduce exposure to malicious content.	[mp.s.3]	Web browsing protection

ISO 27001 Reference	ISO 27001:2022 Control	Summary description of the ISO 27001:2022 control	ENS Reference	Security measure RD 311/2022
8.24	Use of cryptography	Standards for the effective use of cryptography, including cryptographic key management, must be defined and implemented.	[op.exp.10] [mp.si.2] [mp.info.3]	Cryptographic key protection Cryptography Electronic signature
8.25	Security in the development lifecycle	Standards for the secure development of software and systems should be established and implemented.	[mp.sw.1]	Application development
8.26	Application security requirements	Information security requirements should be identified, specified and approved when developing or acquiring applications.	[mp.sw.1] [mp.s.2] [mp.com.3] [mp.sw.2] [mp.info.4]	Application development Protection of web services and applications Protection Integrity/Authenticity Acceptance and commissioning Time stamps
8.27	Secure system architecture and engineering principles	Secure systems engineering principles should be established, documented, maintained and applied to all information systems development activities.	[op.pl.2] [mp.sw.1]	Security Architecture Application development
8.28	Secure coding	Secure coding principles should be applied to software development.	[mp.sw.1]	Application development
8.29	Developmental safety and acceptance testing	Security testing processes must be defined and implemented throughout the development lifecycle.	[mp.sw.2]	Acceptance and commissioning
8.30	Outsourcing development	The organisation should control, monitor and review activities related to the development of outsourced systems.	[op.ext.1] [mp.sw.1] [mp.sw.2] [op.ext.3]	Contracting and service level agreements Application development Acceptance and commissioning Supply chain security
8.31	Separation of development, test and production environments	Development, test and production environments must be separate and protected.	[mp.sw.2]	Acceptance and commissioning
8.32	Change management	Changes to information processing facilities and information systems should be subject to change management procedures.	[op.exp.5]	Change Management
8.33	Test data	Test data must be selected, protected and managed appropriately.	[mp.sw.1] [mp.sw.2]	Application development Acceptance and commissioning

ISO 27001 Reference	ISO 27001:2022 Control	Summary description of the ISO 27001:2022 control	ENS Reference	Security measure RD 311/2022
8.34	Protection of information systems during audit testing	Audit testing and other assurance activities in the assessment of systems in production should be carefully planned and agreed between the assessor and appropriate managers.	[op.exp.2] [op.exp.3] [op.exp.4] [mp.s.2] Article 31	Security settings Security configuration management Maintenance and security updates Protection of web services and applications Security audit

PUBLICACIONES DE DEFENSA

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