NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Docun Secure Controls Framework (SCF) version 2025.2
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

| Focal Document | Spain - 80E-A-2022-7191 | https://www.boe.as/diario_boe/txt.php?id=80E-A-2022-7191 | Published STRM URL: https://www.boe.as/diario_boe/txt.php?id=80E-A-2022-7191 | https://securecontrolsframework.com/content/strm/scf-strm-emea-spain-boe-a-2022-7191.pdf

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 3	Information systems that	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
741000	process personal data.	When an information system processes personal data, the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April. 72, 2016. reliate to the protection of natural persons in what concerns the	Tunctional	no roadions.	NA.		Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	107	o o o o o o o o o o o o o o o o o o o
Article 3.1	N/A	27, 20 6, relating to the protection of nation persons in wince circles and which repeals Directive 95/46/EC (General Data Protection Regulation) and Organic Law 3/2018, of December 5, on Protection of Personal Data and quarantee of digital rights, or, where applicable, Organic Law 7/2021, of May 28, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal and enforcement infractions of criminal sanctions, the rest of the applicable regulations, as well as the criteria stabilished by the Spanish Data Protection Agency or in its area of competence, by the autonomous data protection automities, without prejudice to the requirements established herein royal decree.	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01		5	
Article 3.2	N/A	In these cases, the person responsible or in charge of the treatment, advised by the data protection delegate, will carry out a risk analysis in accordance with article 24 of the General Data Protection Regulation and, in the cases of its article 35, a data protection impact assessment.	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
Article 3.2	N/A	In these cases, the person responsible or in charge of the treatment, advised by the data protection delegate, will carry out a risk analysis in accordance with article 24 of the General Data Protection Regulation and, in the cases of its article 35, a data protection impact assessment.	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
Article 3.3	N/A	In any case, the measures to be implemented as a consequence of the risk analysis and, where appropriate, the impact evaluation referred to in the previous section will prevail, if they are aggravated with respect to those provided for in this document. decree. In any case, the measures to be implemented as a consequence of the risk	Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service under their control. Mechanisms exist to compel data and/or process owners to	5	
Article 3.3	N/A	analysis and, where appropriate, the impact evaluation referred to in the previous section will prevail, if they are aggravated with respect to those provided for in this document, decree.	Functional	intersects with	Implement Controls	GOV-15.2	implement required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
Article 4	Definitions	(see definitions section)	Functional	intersects with	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5	
Article 5	Basic principles of the National Security Scheme.	The ultimate objective of information security is to guarantee that an organization will be able to meet its objectives, develop its functions and exercise its powers using information systems. Therefore, in terms of information security, the following basic principles must be taken into account:	Functional	intersects with	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	5	
Article 5	Basic principles of the National Security Scheme.	The ultimate objective of information security is to guarantee that an organization will be able to meet its objectives, develop its functions and exercise its powers using information systems. Therefore, in terms of information security, the following basic principles must be taken into account:	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
Article 5	Basic principles of the National Security Scheme.	The ultimate objective of information security is to guarantee that an organization will be able to meet its objectives, develop its functions and exercise its powers using information systems. Therefore, in terms of information security, the following basic principles must be taken into account:	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
Article 5(a)	N/A	Security as an integral process.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
Article 5(b)	N/A	Risk-based security management.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
Article 5(c)	N/A	Prevention, detection, response and conservation.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
Article 5(d)	N/A	Existence of lines of defense.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
Article 5(e)	N/A	Continuous surveillance.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
Article 5(f)	N/A	Periodic reevaluation.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
Article 5(g)	N/A	Differentiation of responsibilities.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
Article 6	Security as a comprehensive process.	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 6.1	N/A	Security is understood as a comprehensive process made up of all human, material, technical, legal and organizational elements related to the information system. The application of the ENS will be governed by this principle, which excludes any specific action or short-term treatment.	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
Article 6.2	N/A	Maximum attention will be paid to raising the awareness of the people involved in the process and that of the hierarchical managers, to prevent ignorance, lack of organization and coordination or adequate instructions from constituting sources of risk for the security. Maximum attention will be paid to raising the awareness of the people involved in	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of security	10	
Article 6.2	N/A Risk-based	the process and that of the hierarchical managers, to prevent ignorance, lack of organization and coordination or adequate instructions from constituting sources of risk for the security.	Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	workforce development and awareness controls.	10	
Article 7	security management.	N/A Risk analysis and management is an essential part of the security process, and	Functional	no relationship	N/A Risk Management	N/A	N/A Mechanisms exist to facilitate the implementation of strategic,	N/A	No requirements to map to.
Article 7.1	N/A	Hisk analysis and management is an essential part of the security process, and must constitute a continuous and permanently updated activity. Risk management will allow the maintenance of a controlled environment,	Functional	subset of	Program Program	RSK-01	operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic,	10	
Article 7.2	N/A	minimizing risks to acceptable levels. The reduction to these levels will be carried out through an appropriate application of security measures, in a balanced manner and proportionate to the nature of the information processed, the services to be provided and the risks to which they are exposed.	Functional	subset of	Risk Management Program	RSK-01	operational and tactical risk management controls.	10	
Article 8	Prevention, detection, response and conservation.	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 8.1	N/A	The security of the system must contemplate actions related to aspects of prevention, detection and response, in order to minimize its vulneralitities and ansure that threats to it do not materialize or, if they do, do not seriously affect the system, to the information it handles or the services it provides. The security of the system must contemplate actions related to aspects of	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control. Mechanisms exist to facilitate the implementation of operational	5	
Article 8.1	N/A	prevention, detection and response, in order to minimize its vulnerabilities and ensure that threats to it do not materialize or, if they do, do not seriously affect the system. to the information it handles or the services it provides.	Functional	subset of	Operations Security Operationalizing	OPS-01	recriminants exist to laborate the imperientation or operational security controls. Mechanisms exist to compel data and/or process owners to	10	
Article 8.2	N/A	Prevention measures, which may incorporate components aimed at deterrence or reducing the exposure surface, must eliminate or reduce the possibility of threats materializing.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
Article 8.2	N/A	Prevention measures, which may incorporate components aimed at deterrence or reducing the exposure surface, must eliminate or reduce the possibility of threats materializing.	Functional	subset of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	
Article 8.3	N/A	Detection measures will be aimed at discovering the presence of a cyber incident.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
Article 8.3	N/A	Detection measures will be aimed at discovering the presence of a cyber incident.	Functional	subset of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
Article 8.4	N/A	Response measures, which will be managed in a timely manner, will be aimed at			Operationalizing	00//15	Mechanisms exist to compel data and/or process owners to	(optional)	
Article 8.4	N/A	restoring information and services that may have been affected by a security incident. Response measures, which will be managed in a timely manner, will be aimed at	Functional	intersects with	Cybersecurity & Data Protection Practices	GOV-15	operationalize cybersecurity & data privacy practices for each system, application and/or service under their control. Mechanisms exist to facilitate the implementation of operational	5	
Article 8.4	N/A	restoring information and services that may have been affected by a security incident.	Functional	subset of	Operations Security	OPS-01	security controls.	10	
Article 8.5	N/A	Without compromising the remaining basic principles and minimum requirements established, the information system will guarantee the conservation of data and information in electronic format.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
Article 8.5	N/A	Without compromising the remaining basic principles and minimum requirements established, the information system will guarantee the conservation of data and information in electronic format.	Functional	subset of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	
Article 8 (end)	N/A	Likewise, the system will keep services available throughout the life cycle of digital information, through a conception and procedures that are the basis for	Functional	intersects with	Secure Development Life Cycle (SDLC)	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal	5	
Article 9	Prevention, detection, response and	the preservation of digital heritage. N/A	Functional	no relationship	Management N/A	N/A	change control procedures. N/A	N/A	No requirements to map to.
Article 9.1	conservation.	The information system must have a protection strategy made up of multiple security layers, arranged in such a way that, when one of the layers is	Functional	intersects with	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or	5	
Article 9.1(a)	N/A	compromised, it allows: Develop an appropriate reaction to incidents that could not be avoided, reducing the probability that the system as a whole will be compromised.	Functional	intersects with	Defense-In-Depth (DiD) Architecture	SEA-03	correctness of higher layers. Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or	5	
							correctness of higher layers. Mechanisms exist to implement security functions as a layered		
Article 9.1(b)	N/A	Minimize the final impact on it.	Functional	intersects with	Defense-In-Depth (DiD) Architecture	SEA-03	structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers. Mechanisms exist to implement security functions as a layered	5	
Article 9.2	N/A	The lines of defense must be made up of measures of an organizational, physical and logical nature.	Functional	intersects with	Defense-In-Depth (DiD) Architecture	SEA-03	structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5	
Article 10	Continuous surveillance and periodic reevaluation.	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 10.1	N/A	Continuous surveillance will allow the detection of anomalous activities or behaviors and their timely response.	Functional	intersects with	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
Article 10.1	N/A	Continuous surveillance will allow the detection of anomalous activities or behaviors and their timely response.	Functional	subset of	Oversight Continuous Monitoring	MON-01	executive leadership. Mechanisms exist to facilitate the implementation of enterprise- wide monitoring controls.	10	
Article 10.1	N/A	Continuous surveillance will allow the detection of anomalous activities or behaviors and their timely response.	Functional	intersects with	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious	5	
Article 10.2	N/A	The permanent evaluation of the security status of the assets will allow measuring their evolution, detecting vulnerabilities and identifying configuration	Functional	intersects with	Cybersecurity & Data Protection Controls	CPL-02	activities. Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's	5	
Article 10.3	N/A	deficiencies. Security measures will be periodically re-evaluated and updated, adapting their effectiveness to the evolution of risks and protection systems, leading to a	Functional	intersects with	Oversight Cybersecurity & Data Protection Controls	CPL-02	executive leadership. Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's	5	
Article 11	Differentiation of	rethinking of security, if necessary. N/A	Functional	no relationship	Oversight N/A	N/A	executive leadership.	N/A	No requirements to map to.
	responsibilities.	In information systems, the person responsible for the information, the person			Defined Roles &		Mechanisms exist to define cybersecurity roles & responsibilities	5	No requirements to map to.
Article 11.1		responsible for the service, the person responsible for security and the person responsible for the system will be differentiated. Responsibility for the security of information systems will be differentiated from	Functional	intersects with	Responsibilities Defined Roles &	HRS-03	for all personnel. Mechanisms exist to define cybersecurity roles & responsibilities		
Article 11.2	N/A N/A	responsibility for the exploitation of the information systems concerned. Responsibility for the security of information systems will be differentiated from	Functional Functional	intersects with	Responsibilities Terms of Employment	HRS-03 HRS-05	for all personnel. Mechanisms exist to require all employees and contractors to apply	5	
Article 11.2	N/A	responsibility for the exploitation of the information systems concerned. Responsibility for the security of information systems will be differentiated from responsibility for the exploitation of the information systems concerned.	Functional	intersects with	Rules of Behavior	HRS-05.1	cybersecurity & data privacy principles in their daily work. Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
Article 11.3	N/A	The organization's security policy will detail the responsibilities of each person responsible and the coordination and conflict resolution mechanisms.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
Article 11.3	N/A	The organization's security policy will detail the responsibilities of each person responsible and the coordination and conflict resolution mechanisms.	Functional	intersects with	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity & data privacy principles in their daily work.	5	
Article 11.3	N/A	The organization's security policy will detail the responsibilities of each person responsible and the coordination and conflict resolution mechanisms.	Functional	intersects with	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for	5	
Article 12	Security policy and minimum security	N/A	Functional	no relationship	N/A	N/A	unacceptable behavior. N/A	N/A	No requirements to map to.
Article 12.1	requirements.	The information security policy is the set of guidelines that govern the way in which an organization manages and protects the information it processes and the services it provides. To this end, the instrument that approves said security	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.1(a)	N/A	policy must include, at a minimum, the following points: The objectives or mission of the organization.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.1(b)	N/A	The regulatory framework in which the activities will be carried out.	Functional	intersects with	Publishing Cybersecurity & Data Protection	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.1(c)	N/A	The security roles or functions, defining for each one, their duties and responsibilities, as well as the procedure for their appointment and renewal.	Functional	intersects with	Publishing Cybersecurity & Data Protection	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.1(d)	N/A	The structure and composition of the committee or committees for security management and coordination, detailing their scope of responsibility and the	Functional	intersects with	Documentation Publishing Cybersecurity & Data Protection	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and	5	
		management and coordination, detailing their scope or responsibility and the relationship with other elements of the organization. The guidelines for structuring the system's security documentation, its			Documentation Publishing Cybersecurity		procedures. Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and		
Article 12.1(e)	N/A	menagement and access.	Functional	intersects with	& Data Protection Documentation Publishing Cybersecurity	GOV-02	procedures. Mechanisms exist to establish, maintain and disseminate	5	
Article 12.1(f)	N/A	The risks arising from the processing of personal data. Each public administration will have a security policy formally approved by the	Functional	intersects with	& Data Protection Documentation	GOV-02	cybersecurity & data protection policies, standards and procedures. Mechanisms exist to establish, maintain and disseminate	5	
Article 12.2	N/A	competent body. Likewise, each body or entity with its own legal personality included in the subjective scope of article 2 must have a security policy formally approved by the competent body. However, all or part of the subjects of an institutional public sector may be included in the subjective scope of the security policy approved by the	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	recurrence exist to establish, mannar and uses mixed copy of the c	5	
Article 12.3	N/A	Administration with which they have a relationship, dependence or affiliation, when so determined by the bodies, competent in the exercise of organizational powers. In the General Administration of the State, each ministry will have its security policy, which will be approved by the head of the Department, Public organizations and entities belonging to the state institutional public sector may have their own security policy, approved by the competent body, which will be consistent with that of the Department with which they maintain the relationship of connection, dependency or affiliation, or be included in the subjective scope of its security policy. The management centers of the General Administration of the State that manage services under the declaration of shared services may also have their own security policy, approved by the competent body, consistent	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
		with that of the Department to which they depend or to which they are attached.							



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 12.4	N/A	The General Secretariat of Digital Administration of the Ministry of Economic Affairs and Digital Transformation will have its own security policy, which will be	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 12.5	N/A	approved by the person in charge of it. Municipalities may have a common security policy prepared by the local regional or provincial entity that assumes responsibility for the information security of municipal systems.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 12.6	N/A	The security policy will be established in accordance with the basic principles indicated in chapter II and will be developed applying the following minimum requirements:	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.6(a)	N/A	Organization and implementation of the security process.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.6(b)	N/A	Risk analysis and management.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.6(c)	N/A	Personnel management.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.6(d)	N/A	Professionalism.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.6(e)	N/A	Authorization and access control.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.6(f)	N/A	Protection of facilities.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.6(g)	N/A	Acquisition of security products and contracting of security services.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.6(h)	N/A	Minimum privilege.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.6(i)	N/A	Integrity and updating of the system.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.6(j)	N/A	Protection of information stored and in transit.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.6(k)	N/A	Prevention against other interconnected information systems.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.6(l)	N/A	Recording of activity and detection of harmful code.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.6(m)	N/A	Security incidents.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.6(n)	N/A	Continuity of activity.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.6(ñ)	N/A	Continuous improvement of the security process.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 12.7	N/A	The minimum requirements will be required in proportion to the risks identified in each system, in accordance with the provisions of article 28, some of which may be ignored in systems without significant risks.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 13	Organization and implementation of the security process.	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 13.1	N/A	The security of information systems must involve all members of the organization.	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
Article 13.1	N/A	The security of information systems must involve all members of the organization.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
Article 13.1	N/A	The security of information systems must involve all members of the organization.	Functional	intersects with	User Awareness	HRS-03.1		5	
Article 13.2	N/A	The security policy, in application of the principle of differentiation of responsibilities referred to in article 11 and as detailed in section 3.1 of annex II, must be known by all people who are part of the organization and clearly identify unaquivocally to those responsible for ensuring compliance, who will have the following functions:	Functional	intersects with	Position Categorization	HRS-02	environment. Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
Article 13.2	N/A	The security policy, in application of the principle of differentiation of responsibilities referred to in article 11 and as detailed in section 3.1 of annex II, must be known by all people who are part of the organization and clearly identify unequivocally to those responsible for ensuring compliance, who will have the following functions:	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
Article 13.2	N/A	The security policy, in application of the principle of differentiation of responsibilities referred to in article 11 and as detailed in section 3.1 of annex II, must be known by all people who are part of the organization and clearly identify unequivocally to those responsible for ensuring compliance, who will have the following functions:	Functional	intersects with	Formal Indoctrination	HRS-04.2	Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.	5	
Article 13.2	N/A	The security policy, in application of the principle of differentiation of responsibilities referred to in article 11 and as detailed in section 3.1 of annex II, must be known by all people who are part of the organization and clearly identify unequivocally to those responsible for ensuring compliance, who will have the following functions:	Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
Article 13.2(a)	N/A	The person responsible for the information will determine the requirements of the information processed	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
Article 13.2(b)	N/A	The person responsible for the service will determine the requirements of the services provided.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
Article 13.2(c)	N/A	The person responsible for security will determine decisions to satisfy the information and service security requirements, supervise the implementation of the necessary measures to ensure that the requirements are satisfied and report on these issues. The person responsible for security will determine decisions to satisfy the	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
Article 13.2(d)	N/A	The person responsible for security will determine decisions to satisfy the information and service security requirements, supervise the implementation of the necessary measures to ensure that the requirements are satisfied and report on these issues.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
Article 13.2(d)	N/A	The person responsible for the system, by himself or through his own or contracted resources, will be in charge of developing the specific way of implementing security in the system and supervising its daily operation, and may delegate to administrators or operators under his control. responsibility.	Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		The person responsible for security will be different from the person responsible	nationale	netationship			Mechanisms exist to define cybersecurity roles & responsibilities	(optional)	
Article 13.3	N/A	for the system, and there should be no hierarchical dependency between the two. In those exceptional situations in which the justified absence of resources makes it necessary for both functions to fall to the same person or to different people between whom there is a hierarchical relationship, compensatory measures must be applied to guarantee the purpose of the principle of differentiation of responsibilities provided for in the article 11.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	for all personnel.	5	
Article 13.3	N/A	The person responsible for security will be different from the person responsible for the system, and there should be no hieractriculal dependency between the two. In those exceptional situations in which the justified absence of resources makes it necessary for both functions to fall to the same person or to different people between whom there is a hierarchical relationship, compensatory measures must be applied to guarantee the purpose of the principle of differentiation of responsibilities provided for in the article 11.	Functional	intersects with	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	
Article 13.4	N/A	A Technical Safety Instruction will regulate the Certification Scheme of Persons Responsible for Safety, which will include the conditions and requirements applicable to this figure.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
Article 13.4	N/A	A Technical Safety Instruction will regulate the Certification Scheme of Persons Responsible for Safety, which will include the conditions and requirements applicable to this figure.	Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
Article 13.5	N/A	In the case of outsourced services, except for justified and documented cause, the organization providing said services must designate a POC (Point or Contact Person) for the security of the information processed and the service provided, who has the support of the management bodies, and that channels and supervises both compliance with the security requirements of the service it provides or solution it provides, as well as communications related to information security and incident management for the scope of said service. Said security POC will be the Security Manager of the contracted organization, will be part of its area or will have direct communication with it. All this without prejudice to the fact that the ultimate responsibility resides with the public sector entity receiving the aforementioned services.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
Article 13.5	N/A	In the case of outsourced services, except for justified and documented cause, the organization providing said services must designate a POC Point or Contact Person) for the security of the information processed and the service provided, who has the support of the management bodies, and that channels and supervises both compliance with the security requirements of the service it provides or solution it provides, as well as communications related to information security and incident management for the scope of said service. Said security POC will be the Security Manager of the contracted organization, will be part of its area or will have direct communication with it. All this without prejudice to the fact that the ultimate responsibility resides with the public sector entity receiving the aforementioned services.	Functional	intersects with	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data.	5	
Article 13.5	N/A	In the case of outsourced services, except for justified and documented cause, the organization providing said services must designate a POC (Point or Contact Person) for the security of the information processed and the service provided, who has the support of the management bodies, and that channels and supervises both compliance with the security requirements of the service it provides or solution it provides, as well as communications related to information security and incident management for the scope of said service. Said security POC will be the Security Manager of the contracted organization, will be part of its area or will have direct communication with it. All this without projudice to the fact that the tilturate responsibility resides with the public	Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for opersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
Article 14	Risk analysis and	sector entity receiving the aforementioned services.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7000 14	management.	Each organization that develops and implements systems for the processing of	ranotonat	no readonship	TVA	1071	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized		To requirements to map to.
Article 14.1	N/A	information or the provision of services will carry out its own risk management. This management will be carried out through the analysis and treatment of the	Functional	intersects with	Risk Assessment	RSK-04	access, use, disclosure, disruption, modification or destruction of the organization's systems and data. Mechanisms exist to conduct recurring assessments of risk that	5	
Article 14.2	N/A	risks to which the system is exposed. Without prejudice to the provisions of Annex II, some internationally recognized methodology will be used. This management will be carried out through the analysis and treatment of the	Functional	intersects with	Risk Assessment	RSK-04	includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data. Mechanisms exist to remediate risks to an acceptable level.	5	
Article 14.2	N/A	risks to which the system is exposed. Without prejudice to the provisions of Annex II, some internationally recognized methodology will be used. This management will be carried out through the analysis and treatment of the	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to respond to findings from cybersecurity & data	5	
Article 14.2	N/A	risks to which the system is exposed. Without prejudice to the provisions of Annex II, some internationally recognized methodology will be used. The measures adopted to mitigate or eliminate risks must be justified and, in any	Functional	intersects with	Risk Response	RSK-06.1	privacy assessments, incidents and audits to ensure proper remediation has been performed. Mechanisms exist to remediate risks to an acceptable level.	5	
Article 14.3	N/A N/A	case, there will be proportionality between them and the risks. The measures adopted to mitigate or eliminate risks must be justified and, in any	Functional	intersects with	Risk Remediation	RSK-06 RSK-06.1	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper	5	
	Personnel	case, there will be proportionality between them and the risks.					remediation has been performed.		
Article 15	management.	N/A Personnel, whether their own or others, related to the information systems	Functional	no relationship	N/A	N/A	N/A Mechanisms exist to facilitate the implementation of personnel	N/A	No requirements to map to.
Article 15.1	N/A	subject to the provisions of this royal decree, must be trained and informed of their duties, obligations and responsibilities in matters of security. Their actions, which must be supervised to verify that established procedures are followed, will apply the approved safety standards and operating procedures in the performance of their duties.	Functional	subset of	Human Resources Security Management	HRS-01	security controls.	10	
Article 15.1	N/A	Personnel, whether their own or others, related to the information systems subject to the provisions of this royal decree, must be trained and informed of their duties, obligations and responsibilities in matters of security. Their actions, which must be supervised to verify that established procedures are followed, will apply the approved safety standards and operating procedures in the performance of their duties.	Functional	intersects with	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	
Article 15.1	N/A	Personnel, whether their own or others, related to the information systems subject to the provisions of this royal decree, must be trained and informed of their duties, obligations and responsibilities in matters of security. Their actions, which must be supervised to verify that established procedures are followed, will apply the approved safety standards and operating procedures in the performance of their duties.	Functional	intersects with	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
Article 15.1	N/A	Personnel, whether their own or others, related to the information systems subject to the provisions of this royal decree, must be trained and informed of their duties, obligations and responsibilities in matters of security. Their actions, which must be supervised to verify that established procedures are followed, will apply the approved safety standards and operating procedures in the performance of their duties.	Functional	intersects with	Formal Indoctrination	HRS-04.2	Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.	5	
Article 15.2	N/A	The meaning and scope of the safe use of the system will be specified and reflected in security standards that will be approved by the management or the corresponding higher body.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 16	Professionalism	N/A The security of information systems will be attended to and will be reviewed and	Functional	no relationship	N/A Competency	N/A	N/A Mechanisms exist to ensure that all security-related positions are	N/A	No requirements to map to.
Article 16.1	N/A	audited by qualified, declicated and instructed personnel in all phases of their life cycle: planning, design, acquisition, construction, deployment, exploitation, maintenance, incident management and dismanting. The entities within the scope of application of this royal decree will require, in an	Functional	intersects with	Requirements for Security-Related Positions Competency	HRS-03.2	staffed by qualified individuals who have the necessary skill set. Mechanisms exist to ensure that all security-related positions are	5	
Article 16.2	N/A	The entities within the scope or approach of the first the organizations that provide them with security services have qualified professionals with suitable levels of management and maturity in the services provided.	Functional	intersects with	Requirements for Security-Related Positions	HRS-03.2	staffed by qualified individuals who have the necessary skill set.	5	
Article 16.3	N/A	Organizations will determine the training and experience requirements necessary for personnel to perform their job.	Functional	intersects with	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
Article 17	Authorization and access control.	Controlled access to the information systems included in the scope of application of this royal decree must be limited to duly authorized users, processes, devices or other information systems, and exclusively to the permitted functions.	Functional	intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine- grained access control for sensitive/regulated data access.	5	



March Marc	FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Part	Anti-l- 17		application of this royal decree must be limited to duly authorized users,	Frankingel		Laura Debilara	140.01		(=,=======	
	Article 17	access control.	permitted functions.	Functional	intersects with	Least Privilege	IAC-21	assigned tasks in accordance with organizational business functions.	5	
			must remain in controlled areas and have adequate and proportional access							
	Article 18		Law 8/2011, of April 28, by which establishes measures for the protection of	Functional	intersects with	Asset Governance	AST-01		5	
			the Regulation for the protection of critical infrastructures.					Mechanisms exist to facilitate the implementation of identification		
March Marc	Article 18		mechanisms based on the risk analysis, without prejudice to the provisions of	Functional	intersects with		IAC-01	and access management controls.	5	
Part	Article 10	facilities.	critical infrastructures and in Royal Decree 704/2011, of May 20, which approves	Tunctional	iliteraecta with	Management (IAM)	IAC-01			
			The information systems and their associated communications infrastructure							
	Article 18		mechanisms based on the risk analysis, without prejudice to the provisions of	Functional	intersects with		PES-01	environmental protection controls.	5	
Author Column C		identice.	critical infrastructures and in Royal Decree 704/2011, of May 20, which approves			Trottodions				
	Article 19	and contracting	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
			In the acquisition of security products or contracting of information and					Machanisms exist to facilitate the implementation of tailored		
March Marc			communication technology security services that are going to be used in the			Technology Development		development and acquisition strategies, contract tools and		
Part	Article 19.1	N/A	be used, in a manner proportionate to the category of the system and the level of	Functional	subset of		TDA-01		10	
Auto			The Certification Body of the National Information Technology Security							
March 100 Service Approximation from the control of control of the control			(hereinafter, CCN), established under the provisions of article 2.2.c) of Royal					8,		
No.	Article 19.2	N/A	Center, taking into account the national and international evaluation criteria and	Functional	intersects with		TDA-01		5	
According Company Co			the specific product or service within its powers, will determine the following							
No. 1.00 1.00 1.00	Article 19.2(a)	N/A		Functional	intersects with		TDA-01		5	
Second column Second colum								procurement methods to meet unique business needs.		
March 13	Article 19.2(b)	N/A	Other additional security certifications that are required by regulations.	Functional	intersects with		TDA-01	procurement methods to meet unique business needs.	5	
Act 1.5	Article 19.2(c)	N/A		Functional	intersects with		TDA-01	development and acquisition strategies, contract tools and	5	
Management Man	Article 19 3	N/A		Functional	intersects with	Technology Development	TD4-01	Mechanisms exist to facilitate the implementation of tailored	5	
Ministry	Article 19.3	IWA		Tunctional	iliter sects with	& Acquisition	IDA-01	procurement methods to meet unique business needs.	,	
Action 2009 IN No. 10 Action and provided the control action of the completion for the control action of the completion of the control action of the completion of the complet	Article 20		privileges necessary for their correct performance, which implies incorporating	Functional	intersects with	Least Privilege	IAC-21	only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business	5	
Arise 200 No. Secretary and the secretary and th								Mechanisms exist to configure systems to provide only essential	_	
Anticus 2010 An	Article 20(a)	N/A		Functional	intersects with	Least Functionality	CFG-03	ports, protocols, and/or services.	5	
Article 200 INA contractions are contributed foundation of the Particular depoted on the Particu	Article 20/b)	N/A		Functional	intersects with	Least Functionality	CEG-03	capabilities by specifically prohibiting or restricting the use of	5	
Action 2009 NA Manual configuration of the contribution of contribution of the contrib						,				
Article 200 NA adjustment to the sergiculation of the potential for definition of the potential of the poten	Article 20(c)	N/A	eliminated or deactivated by controlling the configuration. Ordinary use of the	Eupational	intercepts with	Loast Eupstionality	CEG 03	capabilities by specifically prohibiting or restricting the use of	-	
Articl 200 NA sequence to the configuration of the respective in modern or internate or whole the configuration of	Article 20(c)	IWA	the part of the user.	Tunctional	iliteraecta with		C1 G-03		,	
Article 2012 MA Article 211 MA Article 212 MA Article 211 MA Article 213 MA Article 213 MA Article 214 MA Article 215 MA Artic	Article 20(d)	N/A	adapted to the categorization of the system, in order to eliminate or deactivate	Functional	intersects with	Through Baseline	CFG-02	baseline configurations for technology platforms that are	5	
Action 2.1. NA Action	Article 20(d)	N/A	Security configuration guides will be applied for the different technologies,	Functional	intersects with		CFG-03	Mechanisms exist to configure systems to provide only essential	5	
Article 2.1 No. No. The inclusion of any physicial or logical determinent in the upplicate critation of years and process. And the 2.1 No. No. The inclusion of any physicial or logical determinent in the upplicate critation of years and process. And the 2.1 No. No. The inclusion of any physicial or logical determinent in the upplication of the physicial process. And the 2.1 No. No. The inclusion of the inclu		Integrity and				,				
Article 21.1 NA assets, or its modification, will require prior formal authorization. Article 21.2 NA Article	Article 21			Functional	no relationship		N/A		N/A	No requirements to map to.
Article 21.1 N/A seath, or its modification, will require gript formal authorization. An inclination of the production and monitoring will allow the security status of the production of the p	Article 21.1	N/A	assets, or its modification, will require prior formal authorization.	Functional	intersects with	Program	CHG-01	management program.	5	
Acticle 21.2 NA operations to be adjusted based on configuration deficiencies, desiriding of the course on them. Acticle 21.2 NA Acticle 22.3 NA Acticle 22.5 NA Acticle 22.	Article 21.1	N/A	assets, or its modification, will require prior formal authorization.	Functional	intersects with		CHG-02	control processes.	5	
Article 21.2 N/A Separater evaluation and monitoring will allow the socurity status of the systems to be adjusted based on configuration efficiencies, identified with respect to the systems to be adjusted based on configuration efficiencies, identified without a feet furth, an way that a feet furth, and will allow the security status of the systems to be adjusted based on configuration efficiencies, identified without and monitoring will allow the security status of the systems to be adjusted based on configuration efficiencies, identified without and monitoring will allow the security status of the systems to be adjusted based on configuration efficiencies, identified without and monitoring will allow the security status of the systems to be adjusted based on configuration efficiencies, identified on the systems of the	Article 21.2	N/A	systems to be adjusted based on configuration deficiencies, identified	Functional	intersects with	Management &	CFG-02.2	configurations of systems through Continuous Diagnostics and	5	
Article 21.2 N/A Article 21.2 N/A Article 22.1			incident that occurs on them.			Verification		Mechanisms exist to periodically review system configurations to		
Permanent evaluation and monitoring will allow the security status of the system to be adjusted send non-disprisation deficiencies, indentified varierabilities and updates that affect them, as well as early detection of any intersects with intersects with status of the system of th	Article 21.2	N/A	systems to be adjusted based on configuration deficiencies, identified vulnerabilities and updates that affect them, as well as early detection of any	Functional	intersects with	Periodic Review	CFG-03.1		5	
Article 21.2 N/A vulnerabilities and updates that affect them, as well as early detection of any information attored and in the copy of the information attored and in the copy of the information and implementation of security, special attention will be paid to the information and implementation of security, special attention will be paid to the information and implementation of security, special attention will be paid to the information and implementation of security, special attention will be paid to the information and implementation of security, special attention will be paid to the information and implementation of security, special attention will be paid to the information and implementation of security, special attention will be paid to the information and implementation of security, special attention will be paid to the information stored or in transit through portable or mobile equipment or devices, peripheral devices, information media and communications over open networks, which must be analyzed, especially to achieve adequate protection. Article 22.1 N/A Procedures will be applied to guarantee the recovery and long-term conservation of electronic documents produced by the information systems included in the soops of application of this royal decree, when this is required. Article 22.3 N/A A N/A Procedures will be applied to guarantee the recovery and long-term conservation of electronic documents produced by the information systems included in the soops of application of this royal decree, when this is required. Article 22.3 N/A A protection of the electronic information referred to in this royal decree must be that correspond to the nature of the support will be applied, in accordance with the popicability with the application in non-electronic importance of referred to in this royal decree must be that correspond to the nature of the support will be applied, in accordance with the popicability with the application in non-electronic importance of referred to in this royal decree must be the corre			Permanent evaluation and monitoring will allow the security status of the							
Protection of information stored and in trumant. In the organization and implementation of security, special attention will be paid to the information stored or in trainst through protein or mobile equipment or devices, peripheral devices, information media and communications over open networks, which must be analyzed, especially to achieve adequate protection. Article 22.1 Article 22.1 Article 22.1 Article 22.1 Article 22.1 Article 22.1 Article 22.2 Article 22.3 Article 22.5	Article 21.2	N/A	vulnerabilities and updates that affect them, as well as early detection of any	Functional	intersects with	Continuous Monitoring	MON-01	wide monitoring controls.	5	
Article 22.1 N/A Article 22.2 N/A Article 22.2 N/A Article 22.2 N/A Article 22.3										
In the organization and implementation of security, special attention will be paid to the information stored or in transit through portable or mobile equipment or devices, peripheral devices, information stored or in transit through portable or mobile equipment or devices, specially to achieve adequate protection. Article 22.1 N/A Article 22.2 N/A Article 22.2 N/A Article 22.3 N/A A	Article 22	stored and in	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 22.1 N/A devices, peripheral devices, information media and communications over open networks, which must be analyzed. especially to achieve adequate protection. Article 22.1 N/A Tricle 22.2 N/A Procedures will be applied to guarantee the recovery and long-term conservation of electronic documents produced by the information systems included in the special procedures (SOP) Article 22.3 N/A Deprotection of this royal decree, when this is required. Article 22.3 N/A Deprotection of the common of the common of electronic appointment or the special procedure in the proper execution of day to day a saigned tasks. Department of the special procedure in the s										
Article 22.1 N/A Article 22.2 N/A Article 22.3	Article 22.1	N/A	devices, peripheral devices, information media and communications over open	Functional	intersects with	Data Protection	DCH-01		5	
Article 22.1 N/A by the information actived or in transit through portable or mobile equipment or devices, peripheral devices, information media and communications over open networks, which must be analyzed, especially to achieve adequate protection. Article 22.2 N/A procedures will be applied to guarantee the recovery and long-term conservation of electronic documents produced by the information systems included in the scope of application of this royal decree, when this is required. Article 22.3 N/A linformation in non-electronic support that has been the direct cause or consequence of the electronic information in this royal decree must the applications. Article 22.3 N/A by the information system included in the sort of the support will be applied, in accordance with the applications. Article 22.3 N/A by the information in non-electronic support that has been the direct cause or consequence of the electronic information referred to in this royal decree must the applications. Article 22.3 N/A by the consequence of the electronic information referred to in this royal decree must be applied, in accordance with the applications. Article 22.3 N/A by the consequence of the electronic information referred to in this royal decree must be protected with the among the electronic information referred to in this royal decree must be protected with the same degree of security as this. To do this, the measures that corresponds to the electronic information referred to in this royal decree must be protected with the among the electronic information referred to in this royal decree must be protected with the same degree of security as this. To do this, the measures that corresponds to the electronic information referred to in this royal decree must be protected with the among the electronic information referred to in this royal decree must be protected with the among the electronic information referred to in this royal decree must be protected with the among the electronic information referred to in this royal decree										
Article 22.2 N/A Procedures will be applied to guarantee the recovery and long-term conservation of electronic documents produced by the information systems included in the scope of application of this royal decree, when this is required. Article 22.3 N/A be protected with the same degree of security as this. To do this, the measures that correspond to the nature of the support with eapplicable regulations. Article 22.3 N/A be protected with the same degree of security as this. To do this, the measures that correspond to the nature of the support will be applied, in accordance with faculty of the description information referred to in this royal decree must be protected with the same degree of security as this. To do this, the measures that correspond to the nature of the support will be applied to guarantee the recovery and long-term conservation of electronic support that has been the direct cause or consequence of the electronic information referred to a time to report that the support will be applied to regulate down the same degree of security as this. To do this, the measures that correspond to the nature of the support will be applied, in accordance with a same degree of security as this. To do this, the measures that correspond to the nature of the support will be applied, in accordance with a same degree of security as this. To do this, the measures that correspond to the nature of the support will be applied, in accordance with a same degree of security as this. To do this, the measures that correspond to the nature of the support will be applied, in accordance with a same degree of security as this. To do this, the measures that correspond to the nature of the support will be applied, in accordance with a same degree of security as this. To do this, the measures that correspond to the nature of the support will be applied, in accordance with a same degree of security as this. To do this, the measures that correspond to the nature of the support will be applied, in accordance with a same degree of s	Article 22.1	N/A	devices, peripheral devices, information media and communications over open	Functional	intersects with		DCH-01.2	atored.	5	
Article 22.2 N/A of electronic documents produced by the information systems included in the scope of application of this royal decree, when this is required. All information in non-electronic support that has been the direct cause or consequence of the electronic clumpost that has been the direct cause or the protected with the same degree of security as this. To do this, the measures that applicable regulations. Article 22.3 N/A by the protected with the same degree of security as this. To do this, the measures that applicable regulations. All information in non-electronic support that has been the direct cause or consequence of the electronic information referred to in this royal decree must be protected with the same degree of security as this. To do this, the measures that applicable regulations. Article 22.3 N/A by the same degree of security as the same degree of security as this. To do this, the measures that the applicable regulation of the electronic information referred to in this royal decree must be protected with the same degree of security as this. To do this, the measures that correspond to the nature of the support will be applicable in secondary as signed tasks. 10 Operating Procedures (SOP), or similar documentation, to enable the protection of day-to-day/a assigned tasks. 10 DCH-01 Testing Procedures (SOP) are similar documentation, to enable the protection of day-to-day/a signed tasks. 10 DCH-01 Testing Procedures (SOP) are similar documentation, to enable the protection of day-to-day/a signed tasks. 10 DCH-01 Testing Procedures (SOP) are similar documentation, to enable the protection of day-to-day/a signed tasks. 10 DCH-01 Testing Procedures (SOP) are similar documentation, to enable the protection of day-to-day/a signed tasks. 10 DCH-01 Testing Procedures (SOP) are similar documentation of day-to-day/a passigned tasks. 10 DCH-01 Testing Procedures (SOP) are similar documentation of day-to-day/a passigned tasks. 10 DCH-01 Testing Procedures (SOP) are similar documentation of d								Mechanisms exist to identify and document Standardized		
Article 22.3 N/A Article 22.3	Article 22.2		of electronic documents produced by the information systems included in the	Functional	subset of		OPS-01.1	Operating Procedures (SOP), or similar documentation, to enable	10	
Article 22.3 N/A be protected with the same degree of security as this. To do this, the measures that correspond to the nature of the support will be applied, in accordance with the spoilcable regulations. All information in non-electronic support that has been the direct cause or consequence of the electronic information referred to in this royal docree must be protected with the same degree of security as this. To do this, the measures that correspond to the nature of the support will be applied, in accordance with functional intersects with Data Protection DCH-01 Mechanisms exist to protect sensitive/regulated data wherever it is stored. Sensitive / Regulated Data Protection DCH-01.2			All information in non-electronic support that has been the direct cause or							
the applicable regulations. All information in non-electronic support that has been the direct cause or consequence of the electronic information referred to in this royal decree must be protected with the same degree of security as this. To do this, the measures that correspond to the nature of the support will be applied, in accordance with	Article 22.3	N/A	be protected with the same degree of security as this. To do this, the measures	Functional	intersects with	Data Protection	DCH-01	protection controls.	5	
consequence of the electronic information referred to in this royal decree must be protected with the same degree of security as this. To do this, the measures functional that correspond to the nature of the support will be applied, in accordance with Sensitive / Regulated Data Protection DCH-01.2 School CH-01.2			the applicable regulations.					Mechanisms exist to protect sensitive/regulated data wherever it is		
that correspond to the nature of the support will be applied, in accordance with	Article 22.3		consequence of the electronic information referred to in this royal decree must	Functional	intersects with		DCH-01.2	stored.		
			that correspond to the nature of the support will be applied, in accordance with			Data Protection				



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		The perimeter of the information system will be protected, especially if it is connected to public networks, as defined in Law 9/2014, of May 9, General					Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	(optional)	
	Prevention against other	Telecommunications, reinforcing the tasks of prevention, detection and response to incidents. of security.			Network Security		,		
Article 23	interconnected information	In any case, the risks derived from the interconnection of the system with other	Functional	intersects with	Controls (NSC)	NET-01		5	
	systems.	systems will be analyzed and their connection point will be controlled. For adequate interconnection between systems, the provisions of the corresponding							
	Activity log and	Technical Safety Instruction will be followed.							
Article 24	detection of harmful code.	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
		With the purpose of satisfying the purpose of this royal decree, with full guarantees of the right to honor, personal and family privacy and the self-image					Mechanisms exist to facilitate the implementation of enterprise- wide monitoring controls.		
Article 24.1	N/A	of those affected, and in accordance with the regulations on the protection of personal data, of function public or labor, and other provisions that may be	Functional	intersects with	Continuous Monitoring	MON-01		5	
		applicable, the activities of the users will be recorded, retaining the information strictly necessary to monitor, analyze, investigate and document improper or							
		unauthorized activities, allowing the person acting to be identified at all times.					Mechanisms exist to configure systems to produce event logs that		
		With the purpose of satisfying the purpose of this royal decree, with full guarantees of the right to honor, personal and family privacy and the self-image of those affected, and in accordance with the regulations on the protection of					contain sufficient information to, at a minimum: (1) Establish what type of event occurred;		
Article 24.1	N/A	personal data, of function public or labor, and other provisions that may be applicable, the activities of the users will be recorded, retaining the information	Functional	intersects with	Content of Event Logs	MON-03	(2) When (date and time) the event occurred; (3) Where the event occurred;	5	
		strictly necessary to monitor, analyze, investigate and document improper or unauthorized activities, allowing the person acting to be identified at all times.					(4) The source of the event; (5) The outcome (success or failure) of the event; and		
		In order to preserve the security of information systems, guaranteeing rigorous					(6) The identity of any user/subject associated with the event. Mechanisms exist to minimize sensitive/regulated data that is		
		observance of the principles of action of public Administrations, and in accordance with the provisions of the General Data Protection Regulation and respect for the principles of limitation of the purpose, minimization of data and					collected, received, processed, stored and/or transmitted throughout the information lifecycle to only those elements necessary to support necessary business processes.		
Article 24.2	N/A	imitation of the conservation period stated therein, the subjects included in article 2 may, to the extent strictly necessary and proportionate, analyze	Functional	intersects with	Minimize Sensitive /	DCH-18.1	necessary to support necessary business processes.	5	
74 4010 24.2	1075	incoming or outgoing communications, and only for the purposes of security of the information, so that it is possible to prevent unauthorized access to networks	ranotona	micropoto with	Regulated Data	5011 10.1			
		and information systems, stop denial of service attacks, prevent malicious distribution of harmful code as well as other damage to the aforementioned							
		networks and information systems. To correct or, where appropriate, demand responsibilities, each user who			Identification &		Mechanisms exist to uniquely identify and centrally Authenticate,		
Article 24.3	N/A	accesses the information system must be uniquely identified, so that it is known, at all times, who receives access rights, what type they are, and who has carried out a certain activity.	Functional	intersects with	Authentication for Organizational Users	IAC-02	Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
		out a certain activity. To correct or, where appropriate, demand responsibilities, each user who accesses the information system must be uniquely identified, so that it is known,			Identification &		Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that		
Article 24.3	N/A	at all times, who receives access rights, what type they are, and who has carried out a certain activity.	Functional	intersects with	Authentication for Non- Organizational Users	IAC-03	provide services to the organization.	5	
Article 25	Security incidents.	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
		The entity that owns the information systems within the scope of this royal decree will have security incident management procedures in accordance with					Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response		
Article 25.1	N/A	the provisions of article 33, the corresponding Technical Security Instruction and, in the case of an operator of essential services or a digital service provider, in accordance with the provisions of the annex to Royal Decree 43/2021, of	Functional	intersects with	Incident Response Operations	IRO-01	capability for cybersecurity & data privacy-related incidents.	5	
		January 26, which implements Royal Decree-Law 12/2018, of September 7, security of networks and information systems.							
		The entity that owns the information systems within the scope of this royal decree will have security incident management procedures in accordance with					Mechanisms exist to cover: (1) Preparation;		
Article 25.1	N/A	the provisions of article 33, the corresponding Technical Security Instruction and, in the case of an operator of essential services or a digital service provider,	Functional	intersects with	Incident Handling	IRO-02	(2) Automated event detection or manual incident report intake; (3) Analysis;	5	
		in accordance with the provisions of the annex to Royal Decree 43/2021, of January 26, which implements Royal Decree-Law 12/2018, of September 7,					(4) Containment; (5) Eradication; and		
		security of networks and information systems. The entity that owns the information systems within the scope of this royal					(6) Recovery. Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.		
Article 25.1	N/A	decree will have security incident management procedures in accordance with the provisions of article 33, the corresponding Technical Security Instruction and, in the case of an operator of essential services or a digital service provider.	Functional	intersects with	Incident Response Plan	IRO-04	wable incluent response run (IRF) to all stakeholders.	5	
Article 23.1	N/A	in accordance with the provisions of the annex to Royal Decree 43/2021, of January 26, which implements Royal Decree-Law 12/2018, of September 7.	Tunctional	iliteraecta with	(IRP)	1110-04		,	
		security of networks and information systems.					Mechanisms exist to cover:		
		Likewise, there will be detection mechanisms, classification criteria, analysis and resolution procedures. as well as communication channels to interested					(1) Preparation; (2) Automated event detection or manual incident report intake;		
Article 25.2	N/A	parties and a record of actions. This log will be used for continuous improvement of system security.	Functional	intersects with	Incident Handling	IRO-02	(3) Analysis; (4) Containment;	5	
		Likewise, there will be detection mechanisms, classification criteria, analysis					(5) Eradication; and (6) Recovery. Mechanisms exist to maintain and make available a current and		
Article 25.2	N/A	and resolution procedures, as well as communication criteria, analysis and resolution procedures, as well as communication channels to interested parties and a record of actions. This log will be used for continuous improvement	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	viable Incident Response Plan (IRP) to all stakeholders.	5	
		of system security. Likewise, there will be detection mechanisms, classification criteria, analysis					Mechanisms exist to document, monitor and report the status of		
Article 25.2	N/A	and resolution procedures, as well as communication channels to interested parties and a record of actions. This log will be used for continuous improvement	Functional	intersects with	Situational Awareness For Incidents	IRO-09	cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	5	
		of system security. Likewise, there will be detection mechanisms, classification criteria, analysis and resolution procedures, as well as communication channels to interested			Incident Stakeholder		Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders;		
Article 25.2	N/A	and resolution procedures, as well as communication channels to interested parties and a record of actions. This log will be used for continuous improvement of system security.	Functional	intersects with	Reporting	IRO-10	(1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
A-41-1- 00	Continuity of	The systems will have backup copies and the necessary mechanisms will be	Europia 1	griberi 1	Business Continuity	BCD **	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g.,	10	
Article 26	activity.	established to guarantee the continuity of operations in the event of loss of the usual means.	Functional	subset of	Management System (BCMS)	BCD-01	Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
A-4: 1 00	Continuity of	The systems will have backup copies and the necessary mechanisms will be established to guarantee the continuity of operations in the event of loss of the	Franci II		D-1- R .	non	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these	5	
Article 26	activity.	established to guarantee the continuity of operations in the event of loss of the usual means.	Functional	intersects with	Data Backups	BCD-11	backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
	Continuous	The comprehensive security process implemented must be continually updated					Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory		
Article 27	improvement of the security process.	and improved. To this end, the criteria and methods recognized in national and international practice relating to information technology security management will be applied.	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1		5	
	Continuous	The comprehensive security process implemented must be continually updated			Periodic Review &		Mechanisms exist to review the cybersecurity & data protection		
Article 27	improvement of the security process.	and improved. To this end, the criteria and methods recognized in national and international practice relating to information technology security management will be applied.	Functional	intersects with	Update of Cybersecurity & Data Protection Program	GOV-03	program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
Article 28	Compliance with the minimum	Will be applied. N/A	Functional	no relationship	N/A	N/A	suitability, adequacy and effectiveness. N/A	N/A	No requirements to map to.
	requirements.	To comply with the minimum requirements established in this royal decree, the			Operationalizing		Mechanisms exist to compel data and/or process owners to		
Article 28.1	N/A	entities included in its scope of application will adopt the corresponding security measures and reinforcements indicated in Annex II, taking into account:	Functional	intersects with	Cybersecurity & Data Protection Practices	GOV-15	operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
Article 28.1(a)	N/A	The assets that constitute the information systems concerned.	Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity & data privacy controls for each system,	5	
A-41 1 00 111			For S. 1		C-la 10 min	00111	application and/or service under their control. Mechanisms exist to compel data and/or process owners to select	_	
Article 28.1(b)	N/A	The category of the system, as provided for in article 40 and Annex I.	Functional	intersects with	Select Controls	GOV-15.1	required cybersecurity & data privacy controls for each system, application and/or service under their control. Mechanisms exist to compel data and/or process owners to select	5	
Article 28.1(c)	N/A	The decisions taken to manage the identified risks.	Functional	intersects with	Select Controls	GOV-15.1	required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
							and and an		



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
Article 28.2	N/A	The measures referred to in section 1 will have the status of minimum requirements, being expandable at the discretion of the person responsible for security, who may include additional measures, taking into account the state of the technology, the nature of the information processed or the services provided and the risks to which the affected information systems are exposed. The list of selected security measures will be formalized in a document called Declaration of Applicability, signed by the person responsible for security.	Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service under their control.	(optional)	
Article 28.3	N/A	The security measures referenced in Annex II may be replaced by other compensatory measures, as long as it is documented that they protect, equally or better, from the risk on assets (Annex I) and the basic principles and minimum requirements are satisfied, provided for in chapters II and III. As an integral part of the Declaration of Applicability, the correspondence between the compensatory measures implemented and the measures in Annex II that compensate will be indicated in detail. The set will be subject to formal approval by the person responsible for security. A Con-STIC Guide of those provided for in the second additional provision will guide the selection of said measures, as well as their registration and inclusion in the Declaration of Applicability.	Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cyberseurity & data princy controls for each system, application and/or service under their control.	5	
Article 29	Common infrastructure and services.	The use of common infrastructure and services of public administrations, including shared or transversal ones, will facilitate compliance with the provisions of this royal decree. The specific cases of use of these infrastructures and services will be determined by each public administration.	Functional	intersects with	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry- recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	5	
Article 29	Common infrastructure and services.	The use of common infrastructure and services of public administrations, including shared or transversal ones, will facilitate compliance with the provisions of this royal decree. The specific cases of use of these infrastructures and services will be determined by each public administration.	Functional	intersects with	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
Article 30	Specific compliance profiles and accreditation of secure configuration implementation entities.	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 30.1	N/A	By virtue of the principle of proportionality and seeking an effective and efficient application of the ISN to certain entities or specific sectors of activity, specific compliance profiles may be implemented that will include that set of security measures that, resutting from the mandatory risk analysis, are suitable for a specific security category.	Functional	intersects with	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	5	
Article 30.2	N/A	In a manner analogous to what is provided in the previous section, to enable the adequate implementation and configuration of solutions or platforms supplied by third parties, which are going to be used by the entities included in the scope of application of this royal decree, they may be implemented accreditation schemes for entities and validation of people, which guarantee the security of said solutions or platforms and compliance with the provisions of this royal decree.	Functional	intersects with	Configuration Management Program	CFG-01	Machanisms exist to facilitate the implementation of configuration management controls.	5	
Article 30.3	N/A	The CCN, in the exercise of its powers, will validate and publish the corresponding specific compliance profiles that are defined and the aforementioned accreditation and validation schemes, in accordance with the technical security instructions and security guides approved as planned. in the second additional provision.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 30.4	N/A	The corresponding technical security instructions or, where applicable, the CCN- STIC Security guides, will specify the conditions to which local implementations of products, systems or services originally provided in the cloud or remotally must be subject., as well as the specific conditions for its evaluation and audit. N/A	Functional	no relationship	N/A	N/A	N/A N/A	N/A	No requirements to map to.
Article 31	Security audit.	The information systems included in the scope of application of this royal decree will be subject to a regular audit, at least every two years, to verify compliance with the requirements of the ENS. On an extraordinary basis, said audit must be carried out whenever substantial changes occur in the information systems, which may impact the required security measures. The completion of the extraordinary audit will determine the calculation date for the calculation of the two years, established for the completion of the next regular ordinary audit, indicated in the previous paragraph. The two-year period indicated in the previous paragraphs may be extended for three months when force majeure impediments occur that are not attributable to the entity that owns the information system or systems concerned.	Functional	no relationship	Internal Audit Function	N/A CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	No requirements to map to.
Article 31.1	N/A	The information systems included in the scope of application of this royal decree will be subject to a regular audit, at least every two years, to verify compliance with the requirements of the EN. On an extraordinary basis, said audit must be carried out whenever substantial changes occur in the information systems, which may impact the required security measures. The completion of the extraordinary audit will determine the calculation date for the calculation of the two years, established for the completion of the next regular ordinary audit, indicated in the previous paragraph. The two-year period indicated in the previous paragraphs may be extended for three months when force majeure impediments occur that are not attributable to the entity that owns the information system or systems concerned.	Functional	intersects with	Cybersecurity & Data Protection Assessments	CPL-03	Machanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity & data protection policies, standards and other applicable requirements.	5	
Article 31.1	N/A	The information systems included in the scope of application of this royal decree will be subject to a regular audit, at least every two years, to verify compliance with the requirements of the EMS. On an extraordinary basis, said audit must be carried out whenever substantial changes occur in the information systems, which may impact the required security measures. The completion of the extraordinary audit will determine the calculation date for the calculation of the two years, established for the completion of the next regular ordinary audit, indicated in the previous paragraph. The two-year period indicated in the previous paragraphs may be extended for three months when force majeure impediments occur that are not attributable to the entity that owns the information system or systems concerned.	Functional	intersects with	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology, assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	
Article 31.2	N/A	The audit will be carried out based on the category of the system and, where applicable, the corresponding specific compliance profile, as provided in Annexes I and II and in a coordinance with the provisions of the Audit Security Technical Instruction. of Information Systems Security.	Functional	intersects with	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
Article 31.2	N/A	The audit will be carried out based on the category of the system and, where applicable, the corresponding specific compliance profile, as provided in Annexes I and III and in accordance with the provisions of the Audit Security Technical Instruction. of Information Systems Security. The audit will be carried out based on the category of the system and, where	Functional	intersects with	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity & data protection policies, standards and other applicable requirements. Mechanisms exist to regularly review technology assets for	5	
Article 31.2	N/A	applicable, the corresponding specific compliance profile, as provided in Annexes I and III and in accordance with the provisions of the Audit Security Technical Instruction. of Information Systems Security.	Functional	intersects with	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards. Mechanisms exist to implement an internal audit function that is	5	
Article 31.3	N/A	When carrying out security audits, generally recognized criteria, work methods and conduct wilb useed, as well as national and international standardization applicable to this type of activities. When carrying out security audits, generally recognized criteria, work methods	Functional	intersects with	Internal Audit Function	CPL-02.1	capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes. Mechanisms exist to regularly review processes and documented	5	
Article 31.3	N/A	when carrying out security audits, generally recognized criteria, work methods and conduct will be used, as well as national and international standardization applicable to this type of activities. When carrying out security audits, generally recognized criteria, work methods	Functional	intersects with	Cybersecurity & Data Protection Assessments Functional Review Of	CPL-03	procedures to ensure conformity with the organization's cybersecurity & data protection policies, standards and other applicable requirements. Mechanisms exist to regularly review technology assets for	5	
Article 31.3	N/A	and conduct will be used, as well as national and international standardization applicable to this type of activities.	Functional	intersects with	Cybersecurity & Data Protection Controls	CPL-03.2		5	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
Article 31.4	N/A	The audit report must rule on the degree of compliance with this royal decree, identifying the findings of compliance and non-compliance detected. It must also include the audit methodological criteria used, the scope and objective of the audit, and the data, facts and observations on which the conclusions formulated are based, all in accordance with the aforementioned Technical Instruction on Audit Security, in Security of Information Systems.	Functional	intersects with	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	(optional)	
Article 31.4	N/A	The audit report must rule on the degree of compliance with this royal decree, identifying the findings of compliance and non-compliance detected. It must also include the sudit methodological criteria used, the scope and objective of the audit, and the data, facts and observations on which the conclusions formulated are based, all in accordance with the aforementioned Technical instruction on Audit Security, the Security of Information Systems.	Functional	intersects with	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cycleraecury's data protection policies, standards and other applicable requirements.	5	
Article 31.4	N/A	The audit report must rule on the degree of compliance with this royal decree, identifying the findings of compliance and non-compliance detected. It must also include the audit methodological criteria used, the scope and objective of the audit, and the data, facts and observations on which the conclusions formulated are assed, all in accordance with the aforementioned Technical Instruction on Audit Security, the Security of Information Systems.	Functional	intersects with	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	
Article 31.5	N/A	The audit reports will be presented to the person responsible for the system and the person responsible for security. These reports will be analyzed by the latter who will present their conclusions to the person responsible for the system so that appropriate corrective measures can be taken.	Functional	intersects with	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
Article 31.5	N/A	The audit reports will be presented to the person responsible for the system and the person responsible for security. These reports will be analyzed by the latter who will present their conclusions to the person responsible for the system so that appropriate corrective measures can be taken. The audit reports will be presented to the person responsible for the system and	Functional	intersects with	Cybersecurity & Data Protection Assessments Functional Review Of	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity & data protection policies, standards and other applicable requirements. Mechanisms exist to regularly review technology assets for	5	
Article 31.5	N/A	the person responsible for security. These reports will be analyzed by the latter who will present their conclusions to the person responsible for the system so that appropriate corrective measures can be taken.	Functional	intersects with	Cybersecurity & Data Protection Controls	CPL-03.2	adherence to the organization's cybersecurity & data protection policies and standards. Mechanisms exist to implement an internal audit function that is	5	
Article 31.6	N/A	In the case of HIGH category systems, given the audit opinion and taking into account the eventual seventy of the deficiencies found, the person responsible for the system may temporarily suspend the processing of information, the provision of services or the total operation of the system, until its adequate correction or mitigation. In the case of HIGH category systems, given the audit opinion and taking into	Functional	intersects with	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes. Mechanisms exist to regularly review processes and documented	5	
Article 31.6	N/A	in the case of inthe Category systems, given the aduct opinion and taking into account the eventual seventy of the deficiencies found, the person responsible for the system may temporarily suspend the processing of information, the provision of a services or the total operation of the system, until its adequate correction or mitigation. In the case of HIOH category systems, given the audit opinion and taking into	Functional	intersects with	Cybersecurity & Data Protection Assessments	CPL-03	recontains to regularly review processes and obcumented procedures to ensure conformity with the organization's cybersecurity & data protection policies, standards and other applicable requirements. Mechanisms exist to regularly review technology assets for	5	
Article 31.6	N/A	account the eventual severity of the deficiencies found, the person responsible for the system may temporarily suspend the processing of information, the provision of services or the total operation of the system., until its adequate correction or mitigation.	Functional	intersects with	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	adherence to the organization's cybersecurity & data protection policies and standards.	5	
Article 31.7	N/A	Audit reports may be requested by those responsible for each organization, with powers over information technology security, and by the CCN.	Functional	intersects with	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
Article 31.7	N/A	Audit reports may be requested by those responsible for each organization, with powers over information technology security, and by the CCN.	Functional	intersects with	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity & data protection policies, standards and other applicable requirements.	5	
Article 31.7	N/A	Audit reports may be requested by those responsible for each organization, with powers over information technology security, and by the CCN.	Functional	intersects with	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	
Article 32	Security status report	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 32.1	N/A	The Sectoral Commission for Electronic Administration will collect information related to the state of the main security variables in the information systems referred to in this royal decree, so that it allows the elaboration of a general profile of the state of security in the entities that own the information systems included in the scope of application of article 2, which will be reflected in the corresponding report.	Functional	intersects with	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	5	
Article 32.2	N/A	The CCN will articulate the necessary procedures for the collection and consolidation on information, as well as the methodological aspacts for its treatment and exploitation, through the corresponding working groups that are constituted for this purpose in the Sectoral Commission of Electronic Administration and in the competent collegiate bodies in the field of the General Administration of the State.	Functional	intersects with	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	5	
Article 32.3	N/A	The results of the report will be used by the competent authorities who will promote the appropriate measures that facilitate the continuous improvement of the state of security using, where appropriate, dashboards and indicators that contribute to decision-making through the use of tools, that the CCN provides for this purpose.	Functional	intersects with	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	5	
Article 33	Capacity to respond to security incidents	N/A The CCN will articulate the response to security incidents around the structure	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 33.1	N/A	acided CCN-CERT (for its acronym in English of Computer Emergency Response Team), which will act without prejudice to the security incident response Team), which will act without prejudice to the security incident response capabilities it may have, each public administration and the coordination function at the national and international level of the CCN.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 33.2	N/A	Without prajudice to the provisions of article 19.4 of Royal Decree-Law 122016, of September 7, public sector entities will notify the CCN of those incident that have a significant impact on the security of the information systems concerned. in accordance with the corresponding Technical Safety Instruction.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
Article 33.3	N/A	When an essential operator that has been designated as a critical operator suffers an incident, the reference CSIRTs will coordinate with the Ministry of the Interior, through its Cybersecurity Coordination Office, as provided for in article 11.2 of the Royal Dacree-Law 12/2018, of September 7.	Functional	intersects with	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
Article 33.4	N/A	When an operator with an impact on the National Defense suffers an incident, he must analyze whether, due to its accept, at could have an impact on the functioning of the Ministry of Defense or on the operation of the Armed Forces, he will immediately inform his Reference CSRT, who will imform the response capacity and reference security incidents for the field of national Defense, called ESPDEF-CERT, of the Joint Cyberspace Command (MCCE) through the stabilished channels. In these cases, the ESPDEF-CERT of the Joint Cyberspace Command must be promptly informed of the evolution of the incident management and may collaborate in supervision with the competent authority.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
Article 33.4	N/A	When an operator with an impact on the National Defense suffers an incident, he must analyze whether, due to its scope, it could have an impact on the functioning of the Ministry of Defense or on the operation of the Armed Forces, he will immediately inform his Reference CSIRT, who will inform the response capacity and reference security incidents for the field of national Defense, called ESPDEF-CERT, of the Joint Cyberspace Command (MCCE) through the established channels. In these cases, the ESPDEF-CERT of the Joint Cyberspace Command must be promptly informed of the evolution of the incident management and may collaborate in supervision with the competent authority.	Functional	intersects with	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5	
Article 33.4	N/A	When an operator with an impact on the National Defense suffers an incident, he must analyze whether, due to its scope, it could have an impact on the functioning of the Ministry of Defense or on the operation of the Armed Forces, he will immediately inform his Reference CSIRT, who will inform the response capacity and reference security incidents for the field of national Defense, called ESPDEF-CERT, of the Joint Cyberspace Command (MCCE) through the established channels. In these cases, the ESPDEF-CERT of the Joint Cyberspace Command must be promptly informed of the evolution of the incident management and may collaborate in supervision with the competent authority.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
Article 33.5	N/A	In accordance with the provisions of Royal Decree-Law 12/2018, of September 7, the CCN will exercise the national coordination of the technical response of the response teams to computer security incidents (denominated by its acronym in English Computer Security Incident Response Team, hereinafter, CSIRT) in matters of network security incident Response Team, hereinafter, CSIRT) in matters of network security and public sector information systems.	Functional	no relationship	N/A	N/A	N/A	(optional) N/A	No requirements to map to.
		After a security incident, the CCN-CERT will technically determine the risk of reconnection of the affected system or systems, indicating the procedures to follow and the safeguards to implement in order to reduce the impact and, to the extent possible, avoid that the circumstances that led to it occur again. After a security incident, the General Secretariat of Digital Administration, without prejudice to the regulations that regulate the continuity of information systems involved in public security or the regulations that regulate the continuity or military information systems involved in National Defense that require the							
Article 33.6	N/A	participation of the ESPDEF.CERT of the Joint Cyberspace Command, will authorize reconnection to the common means and services included under its scope of responsibility, including shared or transversal ones, if a CCN-CERT exposure surface report has determined that the risk is acceptable. In the event that it is a security incident that affects a common means or service under the scope of responsibility of the General Intervention of the State	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
		Administration, it will participate in the process of authorization of the reconnection referred to in the previous paragraph.							
Article 33.7	N/A	Private sector organizations that provide services to public entities will notify NIGIE-CERT, a reference security incident response center for citizens and private law entities in Spain operated by the SME National Cybersecurity Institute of Spain MP, SA (MCIBE) dependent on the Ministry of Economic Affairs and Digital Transformation, the incidents that affect them through its computer security incident response team, who, without prejudice to its powers and the provisions of articles 9, 10 and 11 of Royal Decree 43/2021, of January 25, in relation to the Cyberincident Notification and Monitoring Platform, will immediately inform the CCN-CERT.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
Article 34	Provision of response services to security incidents to public sector entities.	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 34.1	N/A	In accordance with the provisions of article 33, the CCN-CERT will provide the following services:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 34.1(a)	N/A	Support and coordination for the treatment of vulnerabilities and the resolution of security incidents experienced by entities within the scope of application of this royal decree. The CCN-CERT, through its technical support and coordination service, will act as quickly as possible in the event of any attack received on the affected information systems. To fulfill the purposes indicated in the previous paragraphs, reports, audit records and configurations of the affected systems and any other information that is considered relevant may be collected, as well as the computer supports that are deemed necessary for the investigation of the incident of the affected systems, without prejudice to the provisions of the applicable data protection regulations, as well as the possible confidentiality of institutional or institutional or regulations, as well as the possible confidentiality of institutional or institution	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 34.1(b)	N/A	organizational data. Research and dissemination of best practices on information security among all members of public sector entities. To this end, the series of CCN-STIC (CCN-Security of Information and Communication Technologies) documents, prepared by the CCN, will offer standards, instructions, guides, recommendations and best practices to apply the ENS and to guarantee security, of information systems within the scope of application of this royal decree.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 34.1(c)	N/A	Training for public sector personnel specialized in the field of information technology security, in order to facilitate the updating of knowledge and to achieve awareness and improvement of their capabilities for the prevention, detection and management of incidents.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 34.1(d)	N/A	Information on vulnerabilities, alerts and warnings of new threats to information systems, compiled from various sources of recognized prestige, including our nwn	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 34.2	N/A	The CCN will develop a program that offers the information, training, recommendations and tools necessary for public sector entities to develop their own capabilities to respond to security incidents, and in which it will be coordinator at the state public level.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 35	Digital administration.	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 35.1	N/A	The security of the information systems that support digital administration will be governed by the provisions of this royal decree.	Functional	intersects with	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	5	
Article 35.2	N/A	The CCN is the competent body to guarantee due interoperability in matters of cybersecurity and cryptography, in relation to the application of Royal Decree 4/2010, of January 8, which regulates the National Interoperability Scheme in the field. of electronic administration.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 36	Life cycle of services and systems	Security specifications will be included in the life cycle of services and systems, accompanied by the corresponding control procedures.	Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
Article 36	Life cycle of services and systems	Security specifications will be included in the life cycle of services and systems, accompanied by the corresponding control procedures.	Functional	intersects with	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.	5	
Article 37	Control mechanisms	Each entity that owns the information systems included in the scope of application of this royal decree and, where appropriate, its agencies, bodies, departments or units, will establish its control mechanisms to truly and effectively guarantee compliance with the ENS.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
Article 37	Control mechanisms	Each entity that owns the information systems included in the scope of application of this royal decree and, where appropriate, its agencies, bodies, departments or units, will establish its control mechanisms to truly and effectively guarantee compliance with the ENS.	Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
Article 37	Control mechanisms	Each entity that owns the information systems included in the scope of application of this royal decree and, where appropriate, its agencies, bodies, departments or units, will establish its control mechanisms to truly and effectively guarantee compliance with the ENS.	Functional	intersects with	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
Article 38	Procedures for determining compliance with the National Security Scheme.	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 38.1	N/A	The information systems included in the scope of article 2 will be subject to a process to determine their conformity with the ENS. To this end, MEDIUM or HIGH category systems will require an audit to certify their conformity, without prejudice to the security audit provided for in Article 31, which may also serve the purposes of certification, while systems BASIC category will only require a self- assessment for their declaration of conformity, without prejudice to the fact that they may also undergo a certification audit. Both the self-assessment procedure and the certification audit will be carried out in accordance with the provisions of article 31 and annex III and in the terms determined in the corresponding Technical Safety Instruction, which will also specify the requirements required of the certifying entities.	Functional	intersects with	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate cybersecurity & data protection controls at planned intervals or when the system, service or project undergoes significant changes.	5	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 38.1	N/A	The information systems included in the scope of article 2 will be subject to a process to determine their conformity with the RN. To this end, McDIUM or HIGH category systems will require an audit to certify their conformity, without prejudice to the security audit provided for in Article 31, which may also serve the purposes of certification, while systems BASIC category will only require a self- assessment for their declaration of conformity, without prejudice to the fact that they may also undergo a certification audit.	Functional	intersects with	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Machanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	
		out in accordance with the provisions of article 31 and annex III and in the terms determined in the corresponding Technical Safety Instruction, which will also specify the requirements required of the certifying entities.							
Article 38.2	N/A	The information systems included in the scope of article 2 will be subject to a process to determine their condrainty with the ENS. To this end, MEDILM or HIGH category systems will require an audit to certify their conformity, without prejudice to the security audit provided for in Article 31, which may also serve the purposes of certification, while systems BASIC category will only require a self- assessment for their declaration of conformity, without prejudice to the fact that they may also undergo a certification audit.	Functional	intersects with	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
		out in accordance with the provisions of article 31 and annex III and in the terms determined in the corresponding Technical Safety Instruction, which will also specify the requirements required of the certifying entities.							
Article 39	Permanent update.	The ENS will remain permanently updated, developing and perfecting itself over time, in parallel with the advancement of the services provided by public sector entities, technological evolution, the emergence or consolidation of new international standards on security and auditing and the risks to which the information systems concerned are exposed.	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
Article 40	Security categories	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 40.1	N/A	The security category of an information system will modulate the balance between the importance of the information it handles and the services it provides and the security effort required, depending on the risks to which it is exposed, under the principle of proportionality.	Functional	intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
Article 40.2	N/A	The determination of the security category will be carried out based on the assessment of the impact that an incident that affects the security of the information or services with detriment to the availability, authenticity, integrity, confidentiality or traceability would have, following the procedure described in Annex I.	Functional	intersects with	Data & Asset Classification		Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
Article 41	Powers	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 41.1	N/A	The power to carry out the assessments referred to in article 40, as well as, where appropriate, its subsequent modification, will correspond to the person responsible or responsible for the information or services affected.	Functional	intersects with	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
Article 41.2	N/A	Based on the assessments indicated in the previous section, the determination of the security category of the system will correspond to the person responsible for security.	Functional	intersects with	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
Article 41.2	N/A	Based on the assessments indicated in the previous section, the determination of the security category of the system will correspond to the person responsible for security.	Functional	intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	

