SECURITY POLICY

Table of contents

1 Spiral MS Management System Security Policy 6
1.1 Target 6
1.2 The company and its objectives 7
1.3 Regulatory and legal framework 7
1.4 Outreach 8
1.5 Responsibilities 9
1.5.1 Address 9
1.5.2 Security Committee 9
1.5.3 Roles 10
1.6 Commitments 11
2 Information Security Management Policies 14
2.1 Asset management and services 14
2.2 Classification of information 14
2.3 Management and access to Security Documentation 16
2.4 Transmission of information 17
2.5 Physical and Environmental Security 17
2.6 IT Equipment, Communications and Software 17
2.7 Mobile devices 17
2.8 Identification and authentication 17
2.9 Password management 18
2.10 Review of access rights 18
2.11 Access to the Network 18
2.12 Cryptographic Controls and Digital Certificates 19
2.13 Security in the Cloud Environment 19
2.13.1 Cloud Responsibility Matrix 20
2.14 Use of Email 23
2.15 Malicious content filtering 23

2.16 Secure Development 23
2.17 Clean Desk and Clear Work Area 23
2.18 Workplace blocking 24
2.19 Maintenance of archives and equipment and reasonable use of resources 25
2.20 Security of access by third parties 25
2.21 Incident management 25
2.22 Regulations 25
2.23 Licence registration 26
3 Sanctions 27
4 Registers and associated documents 27

Revisions

Revision no.	Date	Description of the change	Author
08	20/02/2025	Modification of section 2.2 (metadata), inclusion of section 2.3, and modification of section 2.22 to include applicable regulations.	Laura Melón Menéndez
07	13/09/2024	Adaptation to ENS. Modification of Clean Desk, and inclusion of Workstation Lockdown.	Óscar Iglesias Touceda
06	30/08/2024	Adaptation to ENS.	José Luis Fernández
05	23/08/2024	Adaptation to ENS.	José Luis Fernández
04	20/08/2024	Adaptation to ENS.	José Luis Fernández
03	19/07/2024	Adaptation to ENS.	Óscar Iglesias Touceda José Luis Fernández
02	11/12/2023	New section "Register of licences".	David Menéndez Cisterna
01	11/09/2023	Initial drafting.	Security Committee Óscar Iglesias Touceda

Approvals

Management Committee	Address
Date 20/02/2025	Date 20/02/2025
Signature José Luis Fernández	Signature Álvaro de Rivera

1 Spiral MS Management System Security Policy

Espiral MS considers that information is one of the relevant assets to offer products and services to our customers and, therefore, requires adequate protection. Therefore, Espiral MS includes Information Security Management within its Management System as a mechanism to establish clear guidelines and security measures for:

- ensure confidentiality[1] , integrity[2] , availability[3] traceability and authenticity of information,
- ensure compliance with the security requirements established by the organisation itself and those agreed with its customers,
- ensure compliance with applicable legislation, regulations and standards,
- guarantee the continuity of the organisation and its business operations.

The infrastructure that supports the services, as well as the information and applications that manage the services provided by Espiral MS are within the scope of the Information Security Management System, which is integrated in the Management System, and therefore the policies, objectives and procedures established therein are applicable.

The application used for asset management and risk analysis makes it possible to assess risk by service. To this end, the services included in the Management System have been defined and the information assets involved in each of them have been identified.

The internal support staff of Espiral MS is responsible for establishing and maintaining the necessary security measures for the correct provision of the services. Any security incident in the systems that support the service must be reported and registered.

1.1 Target

The objective of this Information Security Policy is to establish clear guidelines and security measures to protect the organisation's confidential information, to ensure the availability and reliability of information systems, and to comply with applicable security regulations and standards.

[1] The confidentiality attribute is defined as ensuring that only those actors (entities, persons or processes) authorised to access the information can access it in the manner and form intended.
[2] The integrity attribute is defined as the assurance that information is not inappropriately altered during storage, processing or transit.
[3] The availability attribute is defined as the assurance that information can be accessed, in the manner and form intended, by authorised actors when required.

The Security Policy is mandatory for all staff. It also applies to the entire scope set out in the Framework below.

1.2 The company and its objectives[4]

The Espiral MS Group specialises in software manufacturing and since its inception in 1998 has been committed to offering products and services of the highest quality. The group's companies offer specialised, high value-added software solutions through two products:

- Proactivanet®, a software tool specialised in ITSM.
- Prosafety®, a software tool specialised in corporate Occupational Safety projects.

The Espiral MS Group develops its activity through the knowledge and experience of its employees, providing services to the final customer directly, through the services provided from its own offices, or, in the cases in which it is necessary, with the services provided by its suppliers, partners or commercial partners.

Espiral MS approaches its business activities from three main pillars: the importance of quality, the importance of IT service management, and adequate Information Security. Consequently, it has implemented a Management System for each of the three areas, based on international standards and best practices.

1.3 Regulatory and legal framework

Espiral MS carries out its activities within a legal and regulatory framework that guarantees its adherence to good management practices and information protection and security. This framework includes, among its most important elements, the following.

Standards and Certifications:

- ISO 9001: Quality management system that ensures continuous improvement and customer satisfaction.

[4] See the document "POL - Management System Policy" for further details.

- ISO 20000: IT service management system that ensures the quality of service delivery.
- ISO 27001: Information security management system that ensures the protection of information assets.
- ISO 27017: Extension of ISO 27001 that provides additional guidelines for security in cloud services.
- National Security Scheme (ENS) Medium Level: to ensure compliance with security requirements in e-government.

The scope of the standards under the Management System and the National Security Scheme is described in the document "MAN - Management System Manual".

Laws and regulations:

- General Data Protection Regulation (GDPR): European Union regulation governing the protection of personal data and privacy.
- Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD): Spanish law that adapts and complements the RGPD.
- Law on Information Society Services and Electronic Commerce (LSSICE): Regulates the obligations of information society services and electronic commerce in Spain.
- Intellectual Property Law: Spanish Intellectual Property Law regulates copyright and other related rights on literary, artistic and scientific works, such as those associated with the innovations generated by Espiral MS.

However, a procedure is in place for identifying applicable legislation, and for continuously updating a register[5] where references to these updated rules are kept.

1.4 Outreach

The security policy must be known and accepted by all **Espiral MS** employees. Therefore, it will be available at all times on the Intranet, so that it can be easily accessed and consulted whenever necessary.

Every employee of Espiral MS must read and accept in writing the security policy of **Espiral MS** before performing any professional task that involves the handling of applications, services, systems or information of the company.

[5] Details of the applicable legislation can be found in the document "VIG - Management System Documents in Force".

1.5 Responsibilities[6]

1.5.1 Address

Senior management is responsible for establishing an adequate security environment, allocating resources and authority to implement security measures. In **Espiral MS** there is a clear commitment to Information Security, expressed in the delegation of some of its key functions to the Security Committee.

The security policy shall be disseminated to the **organisation's staff**, who should be aware of and comply with the security policies and procedures, report any security incidents or breaches of which they are aware as soon as possible, and participate in training and awareness programmes when so determined.

1.5.2 Security Committee

Information security is a particularly complex area as it requires knowledge of different disciplines, both technical and legal and management. Being a transversal issue and, aware of its growing importance, Espiral MS has Security Committee that will have, among others, the following functions:

- Manage and maintain the organisation's security policy at planned intervals (annual review, or when significant changes occur that require ad hoc updating).
- It will be the point of communication and reference for internal and external information security and cyber security issues.
- He/she shall have data protection responsibilities and functions (DPO).
- He/she will review the technical-legal issues related to security, cybersecurity and data protection required in different procedures (RFI, tenders, contracts, audits, etc.).
- He/she will be responsible for identifying and appointing people with security responsibilities in the organisation, both at functional level and in relation to customers with specific demands, such as Defence, for example.
- It will lead the Risk Analysis and the elaboration of the Risk Treatment Plan referred to in ISO 27001, involving process owners and asset and service owners in the identification of such risks, and the establishment of mitigation actions, and/or alerting the Management, which, as the ultimate risk management responsible, will assume such risks.
- He/she will promote the establishment of security policies and standards, being responsible for reviewing the organisation's security policies and standards. This involves establishing clear guidelines and security measures to protect the organisation's assets and information.

[6] For more details on responsibilities and roles, please refer to the document "MAN - Management System Manual".

- The committee shall be responsible for promoting and advising on the execution of periodic or extraordinary security risk assessments to identify potential vulnerabilities and threats in the organisation's systems, infrastructure and processes. It shall also encourage the participation of all members of the organisation, especially process owners, in the proactive management and mitigation of identified risks.
- The committee will oversee the implementation of the issues reflected in the security policy and related documents throughout the organisation. This includes ensuring that appropriate security practices are followed and that established standards are met.
- The committee may review and approve changes and projects that affect the security of the organisation. This could include the implementation of new technologies, system upgrades or suggested modifications to existing security processes.
- The committee shall be responsible for promoting security awareness and training programmes for the organisation's personnel, disseminating information on good security practices and promoting a security culture throughout the organisation.
- The organisation shall provide information security training and awareness programmes for all employees, with the aim of promoting good security practices and raising awareness of the risks associated with phishing, malware and other threats.
- The committee can promote periodic assessments of the organisation's security performance and recommend improvements. This may include security reviews, internal audits, and the implementation of additional controls and measures to strengthen the organisation's security posture.

The Security Committee is composed of members from the main areas of the company, such as Customer Operations, Information Systems, Technology, Legal and HR.

1.5.3 Roles

The following are the main roles and responsibilities referred to in the National Security Scheme, in accordance with art. 13 of the ENS.

Responsible for security

Designs, implements and monitors the organisation's security policies and procedures, ensuring compliance with ENS regulations and managing security incidents. Approves the Statement of Applicability.

System Manager

Manages and maintains the technological infrastructure, ensuring that information systems operate correctly and are protected against threats and vulnerabilities.

Responsible for the information

Responsible for determining the value of information and defining protection needs, ensuring that data is handled in accordance with established security and privacy requirements.

Head of Service

It guarantees the continuity and quality of electronic services, ensuring that the necessary security measures are implemented to protect the technological infrastructure and the data it handles.

Data Protection Officer (DPD)

It monitors compliance with data protection regulations, advises on legal obligations and acts as a point of contact with supervisory authorities and data subjects.

In Espiral MS, the security, system and DPD managers are nominal positions. Responsibility for information and services, on the other hand, is assumed collegially by the Security Committee. Appointment and renewal is at the discretion of the company's management, and is not usually updated except in the event of staff turnover (internal or external).

1.6 Commitments

The Security Committee will promote the implementation of all organisational, procedural, physical and logical controls that are necessary to adequately protect the information assets of Espiral MS, by means of what is indicated in this policy or other elements of the regulatory body (derived policies, procedures, baselines, technical instructions, etc.), and channelling them to the different areas and business processes.

In Espiral MS the importance of Information Security is manifested in a more concrete way in:

- Commitment to confidentiality: The company is committed to protecting the confidentiality of information, ensuring that only authorised persons have access to it. Access to systems and data should be restricted and granted only to authorised users based on their role and need-to-know. And appropriate authentication controls must be implemented.
- Commitment to the integrity of information: The company is committed to ensuring the integrity of information, preventing any unauthorised modification or alteration.
- Commitment to the availability of information: The company is committed to ensuring the continuous availability of information to authorised users. This implies the implementation of

measures to protect against interruptions and failures, implementing appropriate business continuity plans.

- Commitment to appropriate security incident response: The company has established an incident management process that includes the reporting, investigation, response and recovery from security incidents. The organisation will seek to implement improvements that can help prevent similar incidents in the future
- Commitment to risk management: The company is committed to identifying, assessing and managing information security risks.
- Commitment to privacy protection: The company is committed to protecting the privacy of individuals' personal information by complying with applicable data protection laws and regulations and obtaining appropriate consent where necessary.
- Commitment to education and awareness: The company is committed to raising awareness and training in information security for all employees, as well as promoting good practices in the use of technological resources.
- Commitment to oversight and compliance: The company is committed to conducting regular internal and external audits to ensure compliance with security policies and standards. In addition, it is committed to taking timely action when security breaches are identified.
- Commitment to continuous improvement: The company is committed to continually review and improve information security controls, taking into account technological advances, new threats and lessons learned from previous incidents.
- Commitment to external collaboration: The company is committed to collaborating with external bodies and entities, such as government agencies and threat intelligence sharing organisations, to share relevant information and assist in the fight against cybercrime.
- Commitment to the protection of personal data: The company expressly recognises the importance of guaranteeing the protection of personal data, both of its employees, collaborators and customers, in compliance with current regulations, such as the General Data Protection Regulation (GDPR) and the National Security Scheme (ENS). The processing of personal data involves a number of inherent risks that may compromise the confidentiality, integrity and availability of such information. Associated risks include, but are not limited to:
  - Unauthorised access to personal data, whether by internal employees, third parties or external agents.
  - Theft, loss or leakage of data through physical or electronic means.
  - Intentional or accidental tampering or alteration of data.
  - Privacy violations through unauthorised publication or disclosure of personal data.

  To mitigate them, a series of controls and safeguards appropriate to the level of risk and based on international standards (ISO) or current legislation (ENS, RGPD, etc.) are implemented.

- Commitment to the ENS principles: in compliance with the National Security Scheme (ENS), the organisation commits to integrate and observe the fundamental principles of the ENS in its internal regulations and in the implementation of security controls.

- Security as an integral process: The organisation ensures that security is considered in all areas, from processes and technologies to personnel. We implement technical and operational controls covering network, system and data security, promoting continuous cybersecurity training for all staff.
- Risk-based security management: Continuous risk analysis is conducted to identify, assess and prioritise threats. Based on these analyses, we implement appropriate controls according to the level of criticality of the assets, such as the application of encryption on sensitive data and role-based access restrictions.
- Prevention, detection, response and preservation: The organisation has in place preventive measures such as regular software updates, intrusion detection systems and continuity plans that ensure operational recovery in case of incidents.
- Existence of lines of defence: A defence in depth strategy is employed, where multiple layers of security have been implemented, such as policies, technical instructions, firewalls, anti-virus, access controls, etc., which act together to protect assets. In addition, the organisation conducts regular audits to ensure the robustness of these defences.
- Continuous monitoring: The organisation has implemented an incident alert system for its systems and networks, using real-time threat detection tools to identify and mitigate risks before they cause significant damage.
- Periodic reassessment: Security policies, configurations and protective measures are regularly reviewed and updated based on evolving threats and identified vulnerabilities. This includes annual security policy reviews and audits in accordance with ISO and ENS standards.
- Differentiation of responsibilities: In the organisation, each member has clearly assigned roles and responsibilities for security. Users have limited access based on their roles, while system administrators manage permissions and controls separately.

This commitment ensures that information security is managed effectively and in accordance with ENS best practices and requirements.

Likewise, the Security Committee shall ensure that the security documentation of the information system is properly structured by developing this Security Policy in the form of various auxiliary policies, technical instructions and registers. They will be located in a centralised document manager and governed by an internal documentation management standard for the preparation, approval, conservation, structure, access, etc., of the documents of the Security Management System applied to the information systems, such as the "MAN - Management System Manual". In addition, the documentation will be indexed in the "VIG - Management System Documents in Force".

2 Information Security Management Policies

2.1 Asset management and services

The Security Committee shall lead and assist the owners of information assets and services in complying with the Security Policy.

2.2 Classification of information

An information classification policy is essential to establish how information is categorised and managed within an organisation

Classification and management on a tiered basis will prevent loss, theft or transfer to unauthorised entities.

All information must be classified. If this is not explicitly done, the information shall be considered confidential by default. In case of doubt, the *data owner* or the Security Committee shall be consulted.

In addition, all employees and external collaborators shall sign a confidentiality agreement prior to performing their duties and having access to any information.

Regardless of the level of classification, files containing metadata shall not be shared with third parties.

Regardless of whether it is electronically labelled or not, Spiral MS employees will handle the information necessary for their work according to the following tiered classification criteria

- Unimportant data

  Definition: Information categorised as non-significant data may be associated with information or documentation of a public nature, i.e. that which does not require any special level of protection and may be disclosed to third parties without restriction.

  Characteristics:

  - It does not contain sensitive or confidential information.
  - It is not subject to privacy or data protection regulations.
  - Disclosure would not represent a significant risk to the organisation.

  Examples: general contact information, information available on the public website.

- Unclassified minor data

Definition: Information categorised as minor unclassified data may be associated with internal company information that does not require any special level of protection and may be disclosed to third parties without restriction, e.g. commercial catalogues.

Characteristics:

- May contain company information.
- Access is not limited to employees and contractors.
- Disclosure would not represent a significant risk to the organisation.

Examples: Marketing documentation, commercial catalogues, etc.

- Internal Information

Definition: Internal information is information that is intended for the internal use of the organisation. It requires certain access controls and protection, but may circulate freely within the company.

Characteristics:

- It may contain internal company information, such as internal policies, procedures and documents.
- Access is limited to employees and contractors.
- Unauthorised disclosure can affect the efficiency and reputation of the organisation.

Examples: Internal memos, internal policies and procedures, internal reports....

- Confidential Information

Definition: Confidential information is information that requires a higher level of protection due to its sensitivity and potential negative impact if disclosed or accessed in an unauthorised manner. Restricted to certain individuals or work teams.

Characteristics:

- It contains sensitive information, such as personal data, trade secrets or confidential financial information.
- Access is restricted to a select group of employees with a legitimate need to know.
- Unauthorised disclosure could result in financial loss, reputational damage or privacy violations.

Examples: Confidential financial information, customer data, confidentiality agreements, research and development, etc.

- Second level sensitive (secret) information

Definition: Second level confidential (secret) information is the highest-level category of classification and covers the most sensitive and critical data for the organisation.

Characteristics:

- It contains highly sensitive information, such as trade secrets, innovative research data or classified information.
- Access is strictly controlled and limited to an extremely small group of people with special authorisation.
- Unauthorised disclosure can have serious consequences for the organisation, such as significant financial loss, legal impact, serious reputational damage or threats to national security. Examples: Future product plans, competitive strategies, highly confidential M&A or research data, classified government information....

2.3 Management and access to Security Documentation

Spiral MS establishes a framework for structuring, managing and controlling access to the system's security documentation, ensuring its availability, integrity and confidentiality.

Structuring the documentation

Safety documentation shall be organised into levels set out in the previous point according to criticality and audience, including:

- Information security policy (regulatory framework and general principles).
- Procedures and technical standards (operational details and specific controls).
- Records and evidence of compliance (audits, incident reports and periodic reviews).

Nomenclature, versioning and traceability standards will be applied to ensure that information is consistent and up to date.

Management and maintenance

Security documentation shall be reviewed and updated periodically or in the event of significant changes in infrastructure, regulations or threat context.

Responsibility for approval, distribution and change control of documentation shall be established.

Obsolete documentation shall be withdrawn from circulation in accordance with established document management procedures.

Access and protection

The principle of least privilege shall apply, ensuring that each user has access only to the documentation necessary for the performance of his or her duties.

Authentication and access control mechanisms will be defined according to company policies.

Secret documents shall be protected in accordance with current regulations and best practices in information security.

This policy will be complemented with specific procedures for document control and access management, ensuring compliance with the National Security Scheme and other applicable regulations.

2.4 Transmission of information

Spiral MS shall implement appropriate security controls and procedures for the secure transmission of information, according to its classification level.

2.5 Physical and Environmental Security

Spiral MS will implement appropriate security controls and procedures to ensure the protection of the company's physical security and environment.

2.6 IT Equipment, Communications and Software

In order to ensure the correct performance of Espiral MS employees in the use and operation of equipment and software programs, Espiral MS will apply the appropriate security controls and procedures to guarantee the proper use of computer equipment and devices

2.7 Mobile devices

Espiral MS may define the type and profile of employee access to the company's information on mobile terminals and, where appropriate, define the responsibilities and obligations corresponding to each of them in derived policies, and shall apply the appropriate security controls and procedures.

2.8 Identification and authentication

The needs for access to information will be defined at functional area level, and employees will be provided with the minimum necessary to carry out their work in good conditions. Espiral MS will apply the

appropriate security controls and procedures that guarantee the correct identification and authentication for access to information by employees according to the classification of the information

2.9 Password management

The password is one of the main elements for employee authentication and access to IT devices, systems and services. Therefore, the recommendations and policies established by the organisation should be observed in the creation, renewal and protection of the password.

Training and awareness will be provided to employees on the importance of choosing secure passwords, protecting them appropriately and following established password guidelines.

2.10 Review of access rights

Access privileges to systems, services, applications and information should always be carried out in accordance with the principle of least privilege. Due to the changes that occur in organisations, such as horizontal and vertical transfers of staff, transfers of personnel, and new staff, there are frequent mismatches in roles and user permissions, usually due to excesses.

At defined intervals, functional managers shall review the appropriateness of the permissions granted to users.

2.11 Access to the Network

Access to the corporate network, whether to its systems, services, applications or information, by unauthorised users is prohibited.

Those individuals outside the organisation who need to connect to the Internet from the Espiral MS offices will do so through the guest WIFI network, which will not provide access to the corporate network, or by their own means.

2.12 Cryptographic Controls and Digital Certificates

Encryption mechanisms shall be used in the following cases:

- Legal or contractual requirements.
- Requirements for business operations

The cryptographic controls and digital certificates will only be available to those employees who need them. Espiral MS shall apply the appropriate security controls and procedures to ensure their correct use

2.13 Security in the Cloud Environment

Espiral MS considers the security elements for the provision of services in cloud mode. Security controls will be used, for risks derived from the type of service, maintaining protection against improper access, data breaches, with appropriate governance.

The organisation will provide information security training and awareness programmes for all employees, with the aim of promoting good security practices and raising awareness of the risks associated with phishing, malware and other threats.

Spiral MS considers risk management in the cloud environment, based on the differentiation of how it is designed, how it operates and how resources are managed and accessed, and especially the change management process. The cloud environment has its own types of risk sources. Consideration will be given to each party's responsibility for shared management of security requirements.

Espiral MS will establish security guidelines to maintain the isolation of the assets and information of the cloud service, and will guarantee adequate management of access and authentication in the cloud environment. In the same way, all relevant technical controls will be applied to achieve a level of security appropriate to the risk.

Espiral MS has a procedure for the return of customer information, including secure disposal after the end of the business relationship and retention periods for such information.

Espiral MS will maintain an adequate management of events, investigations and analysis, carrying out an adequate treatment of security incidents, complying with the highest standards recommended by the best practices of the international market.

For the provision of cloud services, Espiral MS will rely on international benchmark providers, through the evaluation and selection of reliable cloud service providers and secure. This involves considering aspects such as their reputation, the security measures implemented, their security certifications and their ability to comply with applicable regulatory requirements.

2.13.1 Cloud Responsibility Matrix

With specific reference to the Cloud service, ESPIRALMS has established the following matrix of responsibilities that will be applicable to the service offered to customers with this type of licensing:

		SPIRAL MS	CLIENT	SUPPLIER (AWS)
	RESPONSIBILITIES ASSOCIATED WITH CLOUD SERVICES			
Security in services	**Cloud services security policy**	x		x
	Security guidelines for users.	x	x	
	Determination of the security levels required by the INFORMATION involved in the service.		x	
	Determination of the security levels required by the service (IaaS, PaaS, SaaS, DaaS, STaaS, DRaaS and BaaS).	x		
General information on the service	**Security operating procedures for critical service operations.**	x		
	Security documentation of the service.	x		
	Data protection compliance documentation	x	x	
	Standard for the use of administrators	x		
	Software usage rules (users, passwords...)		x	
	Communication channels and contact points	x		
	Backup and Restore Request Rule (all modes)	x		
	Clock synchronisation. Time stamping.	x		
	Network infrastructure security configuration: Network securitisation: Defence in depth techniques (e.g., Deep Packet Analysis, traffic acceleration and holing black) for timely detection and response to network-based attacks associated with anomalous inbound or outbound traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or Distributed Denial of Service (DDoS) attacks.)	x		x
Sizing and capacities	Capacity planning (processing, storage, communication and training)	x		
	Capacity measurement and monitoring. System sizing and performance.	x		

	Availability control	x		
Security planning: security	Security, threat and system vulnerability monitoring (anti-virus, anti-malware and other protocols)	x		
	Intrusion detection. Analysis and logs associated with the network.	x		x
Identity and access planning. Authentication and authorisation mechanism.	Identity management and access control provider protocol	x	x	
	Service / infrastructure access controls. Multiple factors. Identity management.	x	x	
	Service / infrastructure access controls. Identity management.	x	x	
	Access Rights Policy. Access Rights Management. ID, Roles, permissions, revocation, modification, suspension.		x	
	Access to the service. Rights and obligations. Last access. Information provided.	x	x	
	Privileged access. Control, registration and protection	x	x	
	Third party access authorisations.	x	x	
	Authorisation reviews and access to the service.	x	x	
	Interconnections with third parties or platforms.	x	x	
	Key management. Configuration, access control and monitoring.	x	x	
	Key management. Use and custody.	x	x	
Monitoring	Log and traceability management. Configuration.	x		x
	Log and traceability management. Event logging for privileged operations.	x		x
	Log management and traceability. Recording of monitoring actions.	x		x
	Log management and traceability. Reviews.	x		
	Log and traceability management. Client access to logs.		x	
	Log management and traceability. Retentions	x		x
	Log management application. *SaaS: Only on the app*	x		
	Alert and event management. Correlation. *a) IaaS: only for infrastructure (provider). Client machines* *b) SaaS: Only on the app.* *c) PaaS: Only on the platform part.*	x		

Continuity of service	Backup policy. Scope and timing of backups: - backup methods and data formats, including encryption, if applicable; - backup data retention periods; - backup storage location).	x		
	Restore policy - procedures for verifying the integrity of backup data; - procedures and timelines involved in restoring backup data; - procedures for testing backup capabilities;	x		
	Copy retention policy	x		
	Sanitisation. Erasure.	x		
	Continuity plans	x		
	Temporary suspension of service	x		x
Security planning: security	Security, threat and system vulnerability monitoring (anti-virus and other protocols)	x		x
	Cryptographic policy. Appropriate encryption.	x		x
	Restitution of information.	x		
	Metadata and data tagging	x		
	Awareness raising and training plans	x	x	
Change and update management	Service lifecycle: specification, architecture, development, operation, changes	x		
	Interconnection requirements	x		
	System migration procedure	x		
	Protocol for updates, patches and maintenance.	x		
Application protection	Secure development policy	x		
	Acceptance and commissioning testing (vulnerability analysis and penetration testing).	x		
	Acceptance testing and commissioning (consistency analysis and code auditing).	x		
Incident management	Security incident management (preventive)	x		
	Security incident response (reactive). Customer/supplier coordination.	x	x	x
	Security incident tracking	x		x
	Notification of security incidents to competent authorities	x	x	x
	Evidence management and chain of custody.	x	x	x
Supply and	Supply chain management	x		

supplier management	Service level agreements.	x		
	Communication of changes or suspensions of service level agreements.	x		
Audit and reviews	Auditing and monitoring of systems. Monitoring of security measures	x		x
	Auditing and monitoring of systems. Legal, regulatory requirements and needs.	x		x
	Protection of web services and applications	x		x

2.14 Use of Email

Spiral MS will establish an email usage policy to protect confidential information and ensure Information Security, which establishes clear guidelines to properly handle sensitive information, prevents unauthorised disclosure, and promotes security practices that help mitigate cyber-attacks such as phishing or the introduction of malware

2.15 Malicious content filtering

In order to ensure as far as possible the blocking and removal of potentially harmful content, Espiral MS includes the relevant security measures in its operations.

2.16 Secure Development

Spiral MS will implement appropriate security controls and procedures to ensure secure development as part of its business activities.

2.17 Clean Desk and Clear Work Area

Spiral MS will implement appropriate security controls and procedures to ensure that a clean desk and clear work area policy is in place.

- All employees are responsible for keeping their workplaces clear of documents, devices or materials that are not necessary for the performance of ongoing tasks.

- Physical documents and non-essential personal items should be removed from the work area and properly stored when not needed or at the end of the working day.
- All material of a confidential nature, including physical documents and portable electronic devices, should always remain under surveillance, or be stored in locked and secure locations, such as locked filing cabinets, safes or lockers.
- Any confidential documents or materials that are no longer required should be destroyed in accordance with the destruction policy outlined in the guidelines for the use of confidential information in the Security Policy (IT0090.01), or stored securely.
- The organisation will conduct periodic reviews to verify that workplaces comply with defined policies. Failure to do so may result in disciplinary action.
- During regular Information Security awareness and training sessions, specific reminders about the importance of keeping workstations clear and storing confidential materials properly shall be included.

2.18 Workplace blocking

Spiral MS shall implement appropriate security controls and procedures to ensure that a workstation lockdown is established when necessary for security reasons. In this regard:

- All workstations shall be automatically locked after a defined period of inactivity.
- Once locked, a new user authentication shall be required to resume the ongoing activity, ensuring that only the authorised user can access the device and information.
- In the event that a user must be temporarily absent from his or her workstation, even for short periods of time, he or she must manually lock the session in order to prevent identity theft and/or theft of confidential information.
- The organisation will conduct periodic reviews to verify that users of the different workstations comply with the defined policies. Failure to comply with these measures may result in disciplinary sanctions.
- During regular Information Security awareness and training sessions, specific reminders on the importance of keeping workstations locked in case of temporary absence shall be included.

2.19 Maintenance of archives and equipment and reasonable use of resources

Each user is responsible for the professional use of the resources that the organisation makes available to them, and for the conservation and use of the devices assigned to them and owned by Espiral MS, which will apply the appropriate security controls and procedures that allow responsible use, guaranteeing the security of the information stored on them.

2.20 Security of access by third parties

Proper management of the supply chain is crucial today. This concept encompasses hardware and software suppliers, cloud services, development, outsourcing or exchanges of information with third parties (companies or customers). In this sense, Espiral MS will pay special attention to:

- Proper evaluation of suppliers before establishing business relationships.
- At the contractual level, where possible, security clauses should be included in contracts with suppliers to ensure the protection of the company's information and assets
- Espiral MS will apply the appropriate security controls and procedures to guarantee the security of its systems and the information stored by third parties.

2.21 Incident management

Employees are obliged to immediately report a security incident based on the established processes as soon as they become aware of any physical incident (water, fire, etc.), service or supply incident (electricity, water, communications), or software or system incident (loss of data, presence of a virus, being the victim of a phishing attack, etc.) that could have an impact on Information Security.

Espiral MS has a business continuity plan to minimise the impact of disruptive events, communicated to the roles involved, and its employees undertake to inform their managers or the Security Committee through the regulatory channels in the event of any incident.

2.22 Regulations

All personnel shall fulfil their obligations in accordance with the guidelines established in this Policy and the rest of the documents that make up the Management System, and the company undertakes to comply with the applicable legislation, as well as to comply with the contracts in force.

Likewise, employees and collaborators expressly undertake to use and process personal data by adopting the necessary precautions to guarantee the level of security required by the current legal framework on Personal Data Protection, as well as to ensure the rights and freedoms of the data subjects whose data are managed.

The applicable regulations are:

Spanish legislation with link to consolidated and current version	First publication	Last modification
ISO 9001:2015 Standard	2015	See link
ISO 27001:2023	2023	See link
ISO 27017:2021	2021	See link
ISO 20000-1:2018	2018	See link
Workers' Statute	1995	See link
Intellectual property law	2019	See link
Cookie Regulations: Information Society Services Act (LSSI), in combination with the RGPD and the ePrivacy Directive and the AEPD's guide to the use of cookies.	2002 2023	See link
Trademark law	2001	See link
Law on information society services (LSSI)	2002	See link
Sustainable Economy Act	2011	See link
General Telecommunications Law	2014	See link
Penal Code	2015	See link
General Data Protection Regulation (GDPR)	2016	See link
LOPDGDD (Organic Law on Data Protection and Guarantee of Digital Rights).	2018	See link
RDLOPD (Royal Decree implementing the Organic Law on the Protection of Personal Data).	2007	See link
Distance working law	2021	See link
Property Law	1996	See link
National Security Scheme	2022	See link

2.23 Licence registration

Control A.18 Compliance with ISO 27017 requires that a **register of software licences used in the organisation** is kept, so that all licences are inventoried, with their associated status (free or in use), as well as other relevant information or dates for their management.

Since one of the main products offered on the market by Espiral MS is a successful ITAM service (Proactivanet), it is used as a licence control tool. Proactivanet allows the company's software resource inventory to be managed natively.

In addition, it should be noted that the tool itself contains the procedures associated with the management of licences, for example, during the *onboarding* of employee equipment. In this way, an up-to-date and consistent status is always maintained between the platform and the actual plant deployed.

3 Sanctions

Failure to comply with the Information Security Policies and other policies included in the Management system may give rise to disciplinary sanctions, which will be applied in accordance with the provisions of the labour legislation applicable at any given time, and with the provisions of the company's internal policies.

4 Registers and associated documents

- The set of Management System documentation.