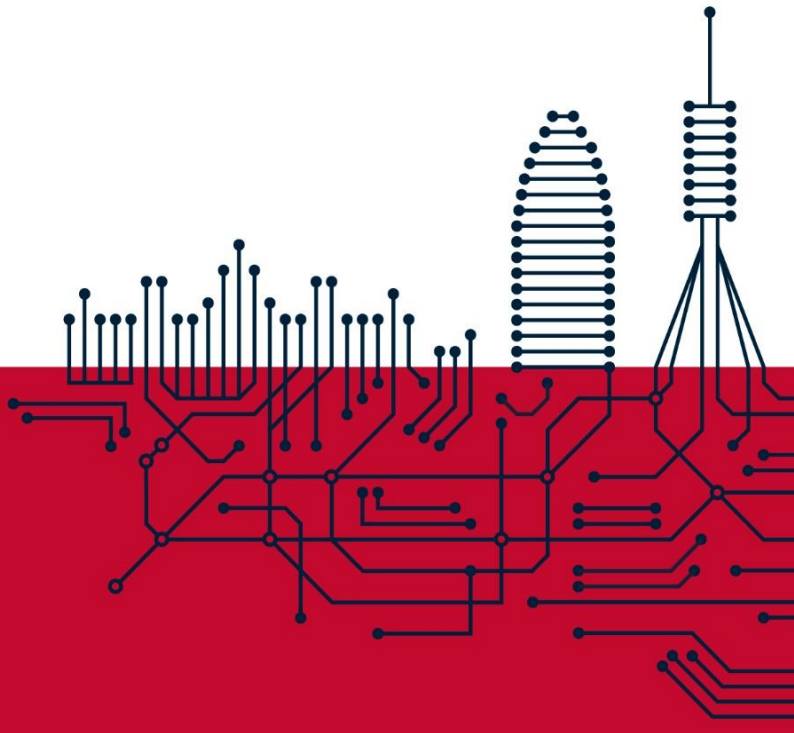
Smarting
ENGINEERING

Information Security Policy



SGSI.PR.01.en

Version	1.0
Date	12/02/2024

> Go beyond

CONTENT

1. SMARTING'S GOALS AND MISSION

Smarting, as a company specializing in the development of digital ticketing solutions for public transportation, recognizes the critical importance of information security in the continued success of its operations and the satisfaction of its stakeholders. This policy establishes the framework for managing information security in the organization in accordance with the principles and requirements of the ISO 27001 standard and the ENS (National Security Scheme).

Information Security Objectives

Smarting**'s information security policy** has the following fundamental objectives:

- Guarantee the confidentiality, integrity and availability of critical information of the company and its customers, as well as ensure traceability and authenticity.
- Comply with laws, regulations, and contractual requirements applicable to information security in the field of public transportation
- Foster a culture of awareness and responsibility in information security management among employees.
- Establish and maintain an information security management system that promotes continuous improvement and adaptability to technological and business changes.

Commitment to Information Security

Smarting**'s senior management**, represented by the CEO and CTO, is committed to:

- Provide adequate resources to implement and maintain an effective information security management system.
- Establish clear roles and responsibilities for information security management at all levels of the organization.
- Encourage employee participation in information protection and provide the necessary training to improve information security skills.
- Periodically evaluate the performance of the information security management system and make adjustments as necessary.

2. LEGAL AND REGULATORY FRAMEWORK

Smarting will carry out its activities in accordance with the legal and regulatory framework in force. You agree to comply with all relevant laws and regulations related to information security, including, but not limited to, those indicated in document SGSI.RG.01.es, in the Legal Framework sheet.

Smarting integrates ENS and ISO 27001 into the organization's security policy to provide a more comprehensive and robust structure to address the specifics of information security, both nationally and internationally. In addition, the adoption of these standards enhances the company's credibility, demonstrating its commitment to security best practices.

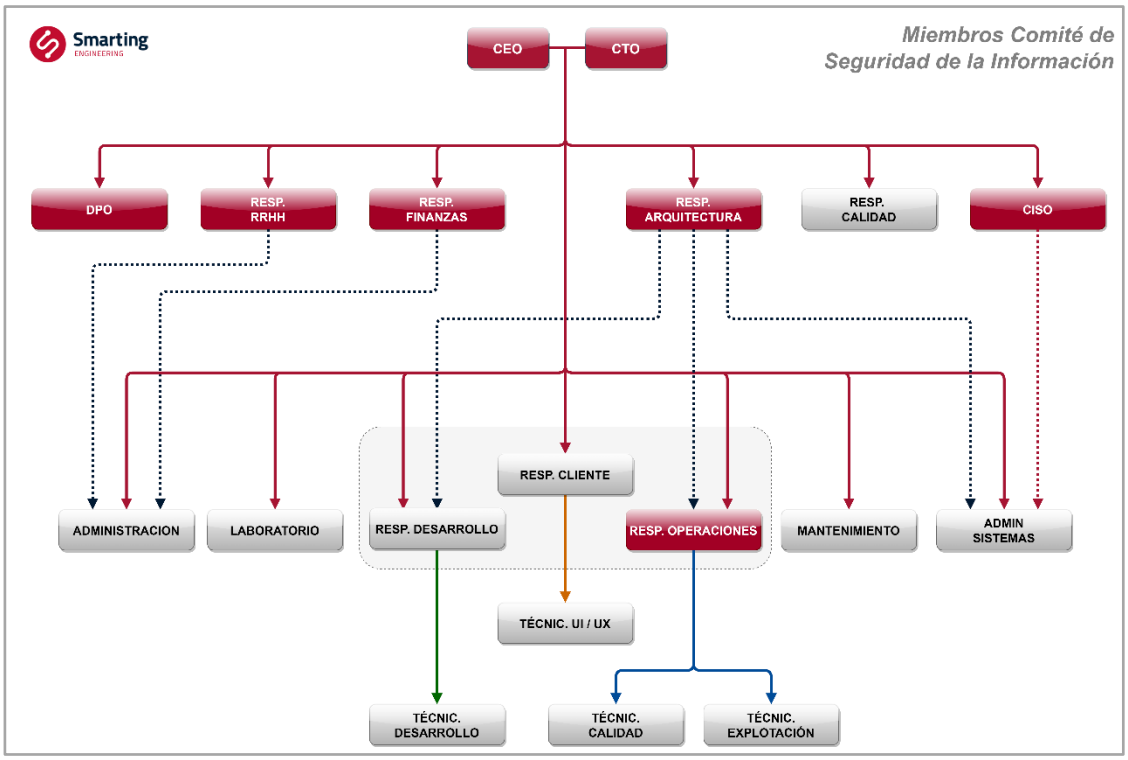
3. SECURITY ORGANIZATIONAL FRAMEWORK

This security policy has been established in accordance with the basic principles set out in Chapter II of Royal Decree 311/2022 and has been developed by applying the following minimum requirements:

Smarting **has identified and defined the security roles and functions necessary** to ensure the protection of information. Each role has clearly defined responsibilities (SGSI.RG.04.es - People).

Smarting **has appointed a Safety Committee** (SGSI.DC.00.es – Minutes of Appointment Committee) that will oversee the monitoring and compliance with the ISMS. The Safety Committee is made up of corporate and responsible positions within the organization. The list of the constituent members of the Safety Committee is defined in the register created for this purpose (SGSI.RG.04.es - People). This ICT Security Committee will have the following functions and responsibilities:

- Coordinate all activities related to ICT security.
- He is responsible for drafting the Security Policy.
- It is responsible for the creation and approval of the rules that frame the use of ICT services.
- It will approve the procedures for action in relation to the use of ICT services.
- It will approve the training and qualification requirements of administrators, operators and users from the point of view of ICT security.

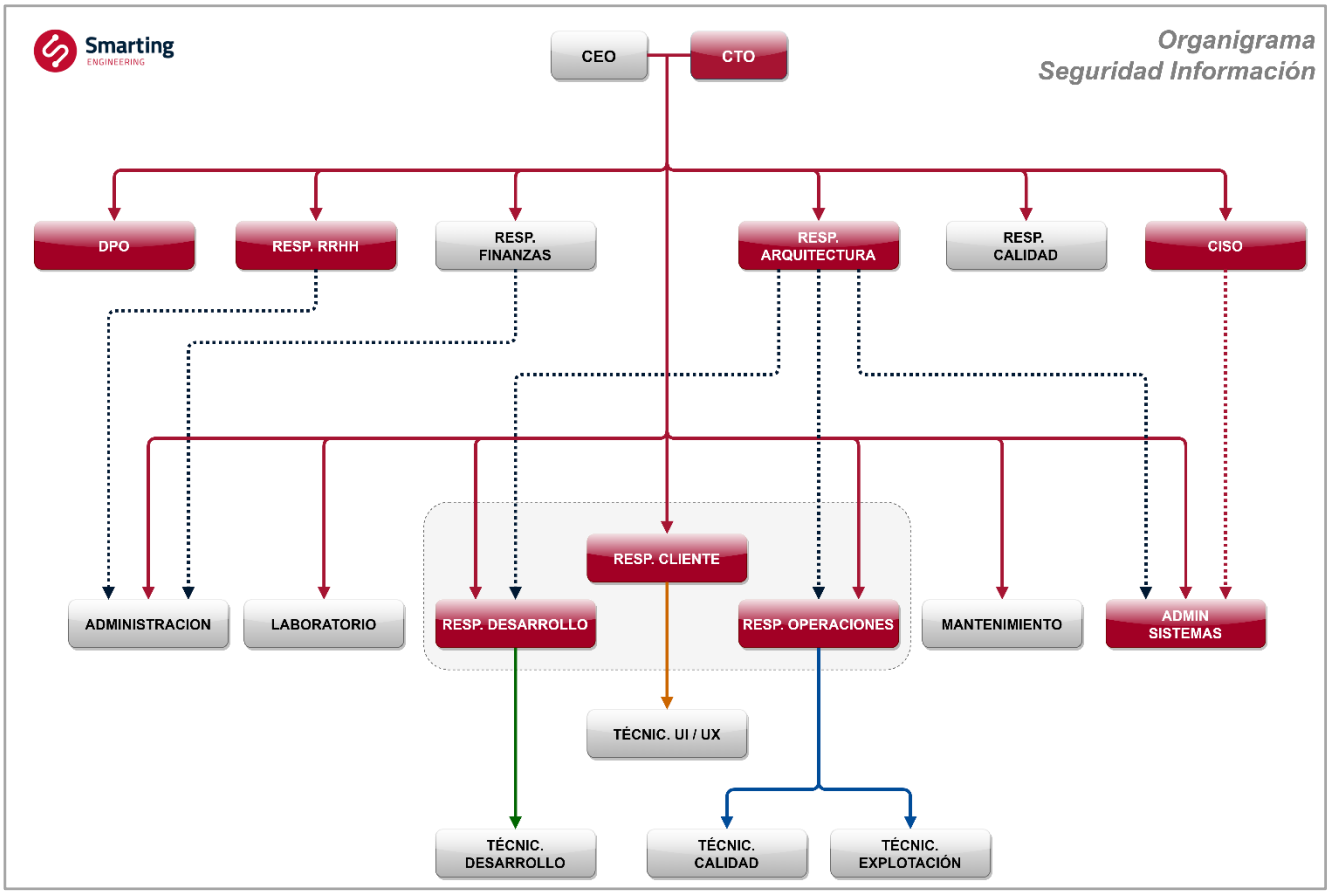


Likewise, the roles and responsibilities of the Security Manager, the Information Manager and the Service Manager have been defined, as well as their relationship with the Security Committee (SGSI.RG.04.es - People).

In order to describe the process and hierarchy for resolving authority conflicts that may occur during the management of the ENS between critical profiles with responsibilities in terms of security, Smarting **has defined the functions for the resolution of conflicts with those responsible** and that applies to all specific ENS management profiles (SGSI.RG.04.es - People).

The Chief Information Security Officer (CISO), the Head of Service (RE) and the Data Protection Officer (DPO) shall be appointed by the Management at the proposal of the Security Committee. Such appointments will be reviewed every 2 years or when the position becomes vacant. The Chief Information Officer (CIO) falls to Smarting in the figure of the Chief Technology Officer (CTO)

The following organizational chart marks the positions with functions or responsibilities related to information security. Escalation in the absence of any of these managers will be carried out according to the hierarchical lines marked in this diagram.



4. RISK ANALYSIS AND MANAGEMENT

All systems subject to this Policy have been assessed using a risk analysis, assessing the threats and risks to which they are exposed. This analysis will be repeated:

- regularly, at least once a year
- when the information handled changes
- when the services provided change
- When a Serious Security Incident Occurs
- when serious vulnerabilities are reported

5. CATEGORIZATION OF SYSTEMS

Smarting has defined the criteria for determining the level of security required in each information system. To this end, the essential elements, information and services are analyzed, pivoting around them the criteria that the person responsible for each type of information and each service may use, considering that the power to determine the category of the system corresponds to the person responsible for it.

The National Security Scheme establishes in its Annex II security measures conditioned on the assessment of the level of security in each dimension and the security category (Article 40) of the respective information system. In turn, the security category of the system is calculated based on the highest security level of the valued dimensions.

The categorization of information systems into Basic, Medium or High according to the criteria of the National Security Scheme (ENS) involves evaluating several factors that affect information security. The following describes the general process for determining the categorization of Smarting's information systems.

- **Identification of Information Systems:**
  - List and classify all the information systems that the organization manages.
- **Assessing the Value of Information:**
  - Analyze the importance and value of the information handled by each system.
  - Consider the confidentiality, integrity, and availability of data.
  - The following are considered **sensitive personal data**:
    - Health data.
    - Genetic and biometric data.
    - Data relating to sexuality or sexual orientation.
    - Personal data revealing racial or ethnic origin, political opinions, and religious or philosophical beliefs.
    - Data on union membership.
  - The information is classified by **its level of confidentiality:** **SGSI.PR.06.es – 4.1.1. Classification levels**
  - The information is classified by its **impact:** **SGSI.PR.06.es – 4.1.2. Information classification**
- **Identification of Critical Assets:**
  - Identify assets critical to business operation and continuity.
  - Determine how the loss or compromise of these assets would affect the organization.
- **Risk Analysis:**
  - Conduct a risk assessment for each system.
  - Identify threats, vulnerabilities, and potential impacts on information security.
- **Compliance:**
  - Assess the compliance of the systems with legal and regulatory requirements, including those established in the ENS.
- **Exposure Level:**
  - Determine the level of exposure to security risks for each system.
  - Assess the likelihood and severity of potential security incidents.
- **Other Systems Dependence:**
  - Consider the interconnection and dependence between different information systems.
  - Assess how the impact on one system could have repercussions on others.
- **Confidentiality, Integrity, and Availability Requirements:**
  - Assess the specific confidentiality, integrity, and availability requirements for each system.
  - Compare these requirements with the levels established in the ENS.
- **Resilience Assessment:**

  - Evaluate the resilience of each system to potential security incidents.
  - Consider the existence of business continuity plans and recovery measures.

- **Category Definition**:
  - Classify each system into one of the categories established by the ENS (**Basic**, **Medium**, **High**) according to the results of the evaluation.
  - When a customer determines a categorization for the information systems that Smarting offers to it, **the category established by the Customer shall prevail**.

- **Documentation and Ongoing Review:**
  - Document the categorization of each information system.
  - Periodically review the categorization to ensure it remains appropriate and adjust it as needed.

6. PERSONNEL MANAGEMENT AND PROFESSIONALISM

All Smarting members are obliged to know and comply with this Information Security Policy and Security Regulations, and it is the responsibility of the Security Committee to apply the necessary measures so that the information reaches those affected.

All employees will receive a security awareness session at least once a year. Likewise, a continuous awareness program will be established to sensitize all Smarting members, particularly new members, which is aligned with other standards implemented.

Personnel engaged in security tasks are appropriately qualified, given the sensitivity and complexity of some of these tasks. This applies to all phases of the safety process lifecycle (installation, maintenance, incident management and decommissioning). To this end, the staff receives the specific training necessary to guarantee the security of the information technologies applicable to the systems and services subject to the ENS.

Logically, the same requirements required internally should be required of any provider providing security-related services. To this end, Smarting has promoted a procedure for the evaluation of suppliers in order to ensure the level of security similar to that required by the entity.

7. AUTHORISATION AND ACCESS CONTROL

The first step in ensuring that information and systems are protected is to limit access to them. For this reason, it has been defined who, and to what extent, will have access to resources, so that each one has the necessary access to perform their tasks, but not to equipment or data that should not be within their reach.

In addition, Smarting's information systems have authorization mechanisms to allow access and deny and revoke it when necessary.

8. FACILITY PROTECTION

The facilities are protected against damage that may affect the systems they house and against access by unauthorized persons. Access to our facilities is secured and is regulated in the procedure set up for this purpose (SGSI.PR.03.es - Procedures).

9. ACQUISITION OF SECURITY PRODUCTS AND CONTRACTING OF SECURITY SERVICES.

Smarting sets the business and information security requirements for your information systems, whether new or existing, and that they are expanded or improved.

Thus, any new acquisition of security products and services that may affect the ISMS must be previously evaluated, from the point of view of functionality and necessary security requirements. After validation, the product will be formally tested to indicate whether it meets the requirements.

All contracted services must be evaluated before they are put into production in order to ensure that they comply with the minimum security requirements defined in this Information Security Policy and the Security Regulations in force.

10. LEAST PRIVILEGE

The Information Security System implemented in **Smarting** follows the Principle of Least Privilege according to which users of the system are granted the minimum levels (or permissions) of access necessary to perform their functions, with the aim of restricting access to information and resources only to what is strictly necessary to fulfill a specific task.

This principle of least privilege ensures that each party (whether a process, a user, or a program) can only access what is essential to its legitimate purpose, not granting unnecessary privileges. However, this principle is not limited to just human user access, it also applies to connected applications, systems, or devices that require privileges to perform necessary tasks.

By limiting privileges, you reduce exposure to cyberattacks and prevent "privilege accumulation."

11. SYSTEM INTEGRITY AND UPDATING.

To ensure the integrity of information systems, any physical and logical changes are always made only after formal approval and through a formal procedure.

To this end, the systems are updated in a controlled manner and according to the security status required at all times. Changes in manufacturers' specifications, the appearance of new vulnerabilities, the issuance of updates and patches that affect systems are analyzed to take the necessary measures so that the systems and their level of security are not degraded, also managing the risks introduced by the changes that will be made.

12. PROTECTING INFORMATION IN TRANSIT AND STORED

A significant part of the information life cycle corresponds to its storage and transport. Information must be protected at all times. To this end, appropriate procedures have been developed, which cover both electronic and paper information, as well as a policy for the handling and processing of information.

13. PREVENTION OF OTHER INTERCONNECTED INFORMATION SYSTEMS.

Prevention against other interconnected information systems is a crucial aspect for **Smarting**. To this end, measures have been established to guarantee security when information systems are connected to each other, taking into account aspects such as perimeter protection, access control or the proper recording of activity with which to detect possible anomalies or unusual behaviour in the interconnection.

Any connection to or from interconnected services will be made following the guidelines defined in the CCN-STIC guides published for this purpose.

14. ACTIVITY LOGGING AND DETECTION OF HARMFUL CODE.

The company supervises its information and processing systems by registering them as security incidents, reviewing the operation and failure records of its systems to identify the problem. Thus, the activities of monitoring the use of **Smarting** systems respect the legal requirements of privacy and are used to verify the effectiveness of the security controls implemented and compliance with the access control policy.

Likewise, corporate teams, through the use of state-of-the-art antivirus (EDR) with centrally managed management, have tools for the protection, detection, recovery and elimination of malicious code.

15. SECURITY INCIDENTS

Smarting**'s management** has established a formal notification procedure whereby all staff must report safety-related incidents through the established channel (security@smarting.es) immediately and without delay. This ensures a quick and effective response to security incidents and weaknesses.

16. BUSINESS CONTINUITY

The company has established a procedure to act against business interruptions and protect critical processes from the effects of major failures in information systems and ensure their immediate restoration. To this end, a business continuity plan (**SGSI.RG.03.es | BIA assessment**) to reduce the impact on Smarting's infrastructure, and consequently on the company, and the recovery of information assets (whether due to accidents, equipment failure, deliberate acts, etc.) so that the department's processes reach an acceptable level of continuity through corrective and preventive recovery measures.

17. CONTINUOUS IMPROVEMENT OF THE SECURITY PROCESS

The Management, for its part, especially values and establishes as the main criterion for the estimation of its risks, the assessment of the confidentiality, integrity and availability of the critical information of the company and its customers, as well as ensuring their traceability and authenticity.

Thus, it undertakes to develop, implement, maintain and continuously improve this **Security Policy** and its **Management System** with the aim of continuous improvement in the way they provide their services and in which they process information.

18. PERSONAL DATA

Smarting processes personal data. In this regard, and in compliance with current data protection legislation, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as risks of varying likelihood and severity for the rights and freedoms of natural persons, **Smarting** has implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, where appropriate, the following:

- pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of treatment systems and services;
- the ability to restore availability and access to personal data quickly in the event of a physical or technical incident;
- a process of regular verification, evaluation and assessment of the effectiveness of technical and organisational measures to ensure the security of the processing.

19. STRUCTURING OF SECURITY DOCUMENTATION

The system's security documentation will follow the guidelines set forth by **Smarting**. Measures will be implemented to structure, manage and control access to security documentation, guaranteeing its integrity and confidentiality. Access will be restricted to authorized personnel and will be carried out in accordance with the defined access policies.

A specific ENS-ISO27001 **channel has been created** in Microsoft Teams, within the general ISO standards team created for Standards management. The necessary permissions will be assigned to the persons who can have access to this documentation: Members of the Information Security Committee, Customer Representatives and Information Security Consultants and Auditors.

The documentation will be divided into folders distinguishing between ISO and ENS. The internal folder structure will follow, when deemed appropriate to facilitate their classification, the sections of the respective rules/regulations.

The documentation generated for Smarting's Information Security Management System will follow the identification structure defined in **SGSI.RG.01.es - System**. This document also keeps the record of documentation and version control.

20. DOCUMENTATION AND COMMUNICATION

This Information Security Policy will be available as documented information and will be communicated within the organization. In addition, it will be shared with relevant stakeholders, such as authorities, operators and public transport users, as appropriate.

21. REVIEW AND UPDATE

This policy will be reviewed annually or sooner if there are significant changes in Smarting's operating or technological environment. Senior management is committed to keeping this policy aligned with the company's objectives and applicable information security requirements.

22. SIGNATURE OF THE DIRECTORATE

By approving this policy, Smarting's Management expresses its determination and commitment to achieve a level of security appropriate to the needs of the business that guarantees the protection of assets in a homogeneous manner.

Note: The documents mentioned in this policy are regularly updated and are available for consultation by interested parties. They can be requested from security@smarting.es