



Information Security Policy

itequia.com



Table of contents

Table of contents.....	2
1. Approval and entry into force.....	3
2. Objectives of the organization.....	3
5. Guiding principles of the policy	4
6. Certification scope	5
7. Regulatory framework	6
8. Security responsibilities and organization.....	7
9. Appointment and renewal of security roles.....	10
10. Conflict resolution	10
11. Risk management.....	10
12. Resources	11
13. Personal data	11
14. Development of the information security policy	12
15. Staff obligations.....	12
16. Third parties / service providers / solution providers.....	12
17. Security incident management.....	13
18. Security category.....	14
19. Approval of the policy and entry into force.....	14



1. Approval and entry into force

Text approved on 20/10/2026 by management, hereinafter the company.

This Information Security Policy is effective from the date of approval (or publication, for entities required to publish it officially) until it is replaced by a new Policy.

This text repeals the previous one, approved on 22/07/2026 by the company's management.

2. Objectives of the organization

The company relies on its information systems to achieve its strategic objectives. Diligent management and protection of these systems are therefore a priority. We must apply appropriate measures, based on a risk assessment, to safeguard them from any incident, whether intentional or accidental, that could compromise the authenticity, traceability, integrity or confidentiality of information, or the availability of services.

The primary goal of information security is to guarantee the company's continuous operation, enabling it to fulfil its functions and deliver high-quality services. To achieve this, it is essential to adopt a preventive approach, actively monitor day-to-day operations and respond swiftly to any incident.

ICT systems are exposed to a dynamic threat landscape that could adversely affect the confidentiality, integrity, availability, intended use and value of information and services. To defend ourselves effectively, we need an adaptable security strategy that adjusts to changes in the environment. This means that each department must implement the mandatory security measures of the Spanish National Security Framework (ENS), continuously monitor service delivery levels, analyse detected vulnerabilities and have incident response plans in place to ensure business continuity.

ICT security must be a fundamental pillar at every stage of a system's life cycle: from its conception and development to its acquisition, operation and eventual decommissioning. Security requirements and funding needs must be identified and included in planning, as well as in requests for proposals and tender specifications for projects that handle personal data, involve the purchase of ICT services or affect our information systems.

3. Scope

This policy applies to all of the company's information systems, to the people who make up the organization and to the company's ICT service and solution providers.



4. Mission

ITEQUIA TECHNOLOGY CONSULTING SL, legally incorporated as a limited liability company with tax ID B75668335, is a PRIVATE entity whose main mission is: development, operation and support of its own software and SaaS services; consulting, development, implementation, operation and support of technology solutions, either custom-built or based on third-party products; and administration and technical support of systems, infrastructure and workplace, in cloud and on-premises environments.

For the purposes of compliance with the Spanish National Security Framework, the entity operates as a private service provider.

The security objectives that the company aims to guarantee through this Policy are:

- Guarantee the confidentiality, integrity and authenticity of information and the continuity of service delivery.
- Implement security measures based on risk.
- Train and raise awareness among the company's members regarding information security. Implement security measures that ensure the traceability of access and respect, among others, the principle of least privilege, also reinforcing users' duty of confidentiality regarding the information they become aware of in the performance of their duties.
- Deploy and control physical security so that information assets are located in secure areas, protected by access controls, according to the risks detected.
- Establish security in communications management through the necessary procedures, so that information transmitted over communication networks is adequately protected.
- Control the acquisition, development and maintenance of information systems at all stages of their life cycle, guaranteeing security by default.
- Monitor compliance with security measures in service delivery, maintaining control over the acquisition and incorporation of new system components.
- Manage security incidents so that they are properly detected, contained, mitigated and resolved, adopting the necessary measures to prevent them from recurring.
- Protect personal information by adopting technical and organizational measures appropriate to the risks arising from processing, in accordance with data protection legislation.
- Continuously supervise the security management system, improving it and correcting any inefficiencies detected.

5. Guiding principles of the policy

- Strategic scope: information security must have the commitment and support of all levels of the company and must be coordinated and integrated consistently with the rest of the strategic initiatives.



- Comprehensive security: security shall be understood as a comprehensive process made up of all the technical, human, material and organizational elements related to information systems, avoiding any one-off actions or ad hoc treatment. Information security must be considered part of normal operations, present and applied from the initial design of ICT systems.
- Risk-based security management: security management based on identified risks will make it possible to maintain a controlled environment, minimizing risks to acceptable levels. Security measures shall be established according to the risks to which information and its systems are exposed, shall be proportionate to the risk they address and must be justified. Risks identified in the processing of personal data shall also be taken into account.
- Prevention, detection, response and preservation: through the implementation of incident prevention actions, minimizing detected vulnerabilities, preventing threats from materializing and, when they do, responding swiftly to restore the information or services provided, while ensuring the secure preservation of information.
- Lines of defence: the company's security strategy is designed and implemented in layers of security.
- Continuous monitoring and periodic reassessment: the company implements means to detect and respond to anomalous activities or behaviour, as well as other means that allow continuous assessment of the security status of assets. There shall also be a continuous improvement process to periodically review and update security measures, according to their effectiveness and the evolution of risks and protection systems.
- Security by default and by design: systems must be designed and configured to guarantee security by default. Systems shall provide the minimum functionality necessary to deliver the service for which they were designed.
- Segregation of responsibilities: in application of this principle, the functions of the Security Officer and the System Officer shall be kept separate.

6. Certification scope

Information system supporting the following services:

- Development, operation and support of own software and SaaS services.
- Consulting, development, implementation, operation and support of technology solutions, either custom-built or based on third-party products.



- Administration and technical support of systems, infrastructure and workplace, in cloud and on-premises environments.

in accordance with the current Statement of Applicability dated 18/09/2026.

7. Regulatory framework

No.	Legislation
1	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
2	Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights.
3	Law 34/2002, of 11 July, on Information Society Services and Electronic Commerce.
4	Royal Decree 311/2022, of 3 May, regulating the National Security Framework
5	Royal Decree 634/2015, of 10 July, approving the Corporate Income Tax Regulations.
6	Royal Legislative Decree 2/2015, of 23 October, approving the consolidated text of the Workers' Statute Law
7	Organic Law 10/1995, of 23 November, of the Criminal Code
8	Law 25/2007, of 18 October, on the retention of data relating to electronic communications and public communications networks
9	Law 6/2020, of 11 November, regulating certain aspects of electronic trust services (repealing Law 59/2003)
10	Royal Legislative Decree 1/1996, of 12 April, approving the consolidated text of the Intellectual Property Law, regularizing, clarifying and harmonizing the legal provisions in force on the matter.
11	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union
12	Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence



8. Security responsibilities and organization

a. ICT Security Committee (STIC)

ICT activities are coordinated through the ICT Security Committee. This committee is made up of technical staff from the different departments for decision-making.

The ICT Security Committee shall consist of:

POSITION
Management
Information Officer (*)
Service Officer (*)
Security Officer (**)
System Officer (**)

(*) These functions may be held by the same person.

(**) These functions may not be held by the same person.

The Director chairs the ICT Security Committee and is primarily responsible for:

- Using the casting vote to agree on the appropriate decisions when no agreement is reached within the team.
- Implementing, maintaining and improving the Information Security Management System (ISMS).
- Allocating the necessary resources and approving the budget.
- Assigning and communicating roles, specifically those of the owners of information security risks and quality risks.

b. Functions and responsibilities

ICT Security Committee

- Establishing, reviewing and approving the scope of the ISMS, as well as the information security policy.
- Ensuring that information security policies, processes, procedures, laws and regulations reflect business requirements and are aligned with the requirements of internal and external stakeholders.



- Establishing, reviewing and approving ISMS objectives and checking whether they are effectively implemented and maintained.
- Monitoring significant changes in information security.
- Reviewing information security incidents and agreeing on the necessary actions, where appropriate.
- Approving the most important initiatives to maintain information security and the established quality level.
- Conducting management reviews at planned intervals.
- Ensuring that staff are aware of the importance of complying with security requirements, legal and regulatory requirements, contractual obligations, quality requirements, quality levels and service level agreements.

Information Officer

- Has the authority to establish the security requirements for the information managed. If this information includes personal data, the requirements arising from the applicable data protection legislation must also be taken into account.
- Determines the security levels of the information.

Service Officer

- Has the authority to establish the security requirements for the services provided.
- Determines the security levels of the service.

Security Officer

Responsible for defining, coordinating and verifying compliance with the information security requirements defined in line with the objectives.

The functions of the Information Security Officer are:

- Coordinating and controlling information security and data protection measures.
- Supervising the implementation, maintaining, controlling and verifying compliance with:
 - The information security strategy defined by the Security Committee.
 - The rules and procedures contained in the Information Security Policy.
 - Supervising security incidents.
 - Communicating to the company's staff the rules and procedures contained in the information security management system, as well as the functions and obligations regarding information security.

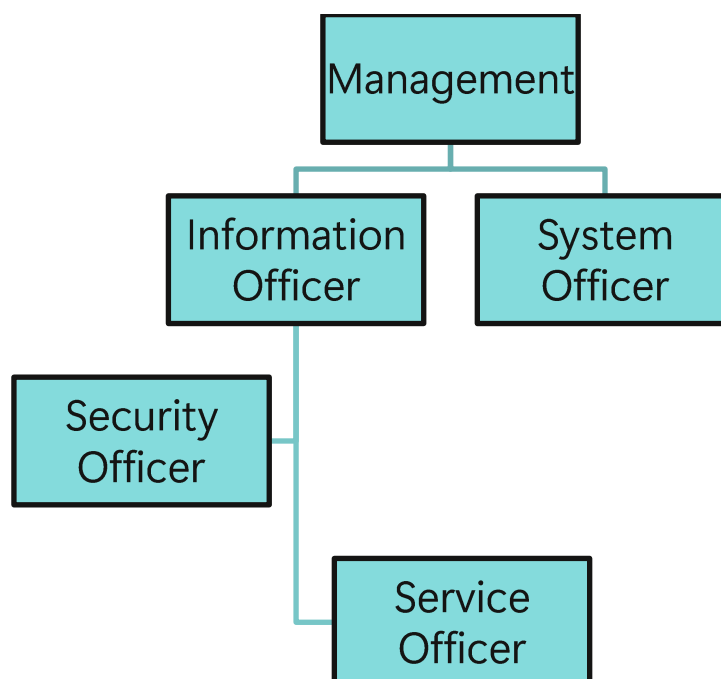


- Supervising and collaborating in the internal or external audits needed to verify the degree of compliance with the Security Policy, its implementing rules and the applicable laws on personal data protection and information security.
- Advising the company's operational areas on information security.

System Officer

- Developing, operating and maintaining the information system throughout its life cycle, including its specifications, installation and verification of its correct operation.
- Defining the topology and management of the information system, establishing the criteria for use and the services available.
- Ensuring that security measures are properly integrated into the overall security framework.

Role dependencies





9. Appointment and renewal of security roles

Management is ultimately responsible for appointing the different security roles. This appointment shall be made formally with the approval of this policy. The original signed by Management shall be filed by the Security Officer.

The established organizational chart shall reflect these appointments.

The appointment shall be renewed in the following cases:

- Medium- or long-term leave of the appointed staff member.
- Permanent departure of the staff member from the company.
- Lack of competence.
- Management decision based on HR management or strategic reasons.

10. Conflict resolution

In the event of conflicts between the different officers, the Information Security Committee may settle the disagreements.

11. Risk management

All systems subject to this Policy must carry out a risk analysis, assessing the threats and risks to which they are exposed. This analysis shall be repeated:

- regularly, at least once a year.
- when there are changes in the information handled.
- when there are changes in the services provided.
- when a serious security incident occurs.
- when serious vulnerabilities are reported.
- when there are changes in the data protection risk analysis or impact assessments.

To harmonize risk analyses, the Information Security Committee shall establish a reference valuation for the different types of information handled and the different services provided. The Security Committee



shall promote the availability of resources to meet the security needs of the different systems, encouraging cross-cutting investments.

Data protection risks shall be taken into account, with the opinion of the Data Protection Officer, if any, and risk treatment plans shall be coordinated.

12. Resources

For the effective application of the Information Security Policy within the company, management shall provide the resources necessary for its proper development, both for implementation activities and for the operation and improvement of the policy and of the information security controls established at any given time.

Protecting the information assets of the company and its clients is vital for proper alignment with business objectives. To this end, an Information Security Management System (ISMS) has been established that implements all the processes and controls necessary to define how information assets are protected.

The Information Security Management System is continuously updated and improved to meet the needs of the business, clients and stakeholders; new objectives are set periodically and business processes are regularly assessed.

13. Personal data

The company processes personal data, as described in the Record of Processing Activities. The company must assess the risks related to the personal data processed and propose an action plan to correct any risks that exceed the authorized threshold.

The risk analysis shall be reassessed periodically and, in any case, when high-risk processing is detected; where appropriate, an impact assessment must be carried out. The implementation of the risk treatment plan shall be coordinated with that of the ENS, and the remaining security procedures or rules with those arising from data protection obligations, especially regarding the control of service providers and the response to incidents or personal data breaches.



14. Development of the information security policy

This Information Security Policy complements and is integrated with other company policies in different areas:

- Security policy (ISO 27001)

This Policy shall be developed through security regulations addressing specific aspects. The security regulations shall be available to all members of the company who need to know them, in particular those who use, operate or administer information and communication systems.

The security regulations shall be available to users through various means on the company intranet.

Users may receive specific training on information security.

Suppliers shall be assessed and should have staff with training appropriate to the services they provide.

15. Staff obligations

All members of the company are obliged to know and comply with this Information Security Policy and the rules, procedures or guidelines that develop it. The company, through the Security Committee and the HR department, is responsible for providing the means necessary for the information to reach those concerned.

All members of the company shall attend an information security awareness session at least once a year. An ongoing awareness programme shall be established for all members of the company, particularly new hires.

People with responsibility for the use, operation or administration of ICT systems shall receive training in the safe handling of systems to the extent they need it to perform their work. Training shall be mandatory before taking on a responsibility, whether it is a first assignment or a change of position or responsibilities.

16. Third parties / service providers / solution providers

When the company provides services to other entities or handles information belonging to others, it shall make them aware of this Information Security Policy, without prejudice to its obligations under data



protection regulations if it acts as a data processor in the provision of those services. Reporting and coordination channels shall be established between the respective Security Committees, together with procedures for responding to security incidents. In addition, the Security Officer (or their delegate) shall be the Point of Contact (POC).

When the company uses third-party services or transfers information to third parties, it shall make them aware of this Security Policy and of the Security Regulations applicable to those services or information, without prejudice to compliance with other data protection obligations. When contracting service providers or purchasing products, the contractor's obligation to comply with the ENS shall be taken into account.

When acquiring rights to use cloud assets, the requirements set out in the security measures of Annex II and the implementation guides shall be taken into account.

Such third party shall be subject to the obligations established in said regulations and may develop its own operating procedures to meet them, so that the company can supervise them or request evidence of compliance, including through second- or third-party audits. Specific procedures shall be established for reporting and resolving incidents, which must be channelled through the POC of the third parties involved and, where personal data are affected, through the Data Protection Officer. Third parties shall ensure that their staff are adequately aware of security matters, at least to the level established in this Policy or as specifically required in the contract.

Where any aspect of the Policy cannot be met by a third party as required in the preceding paragraphs, the Security Officer shall issue a report specifying the risks incurred and how to address them. This report must be approved by the officers responsible for the information and services affected before the contracting process begins or, where applicable, before the contract is awarded. The report shall be forwarded to the company representative, who must authorize the continuation of the third party's contracting process, accepting the risks identified.

When the company acquires, develops or implements an artificial intelligence system, in addition to complying with the applicable regulations, it must obtain a report from the Security Officer, who shall consult the Information Officer and the Service Officer and, where necessary, the System Officer. The Data Protection Officer must also give their opinion.

17. Security incident management

The company shall have a procedure for the agile management of security events and incidents that pose a threat to information and services.

This procedure shall be integrated with other procedures related to security incidents under other sector-specific regulations, such as personal data protection or any other affecting the organization, in order to coordinate the response from the different perspectives and notify the relevant supervisory bodies without undue delay and, where necessary, the State Security Forces or the courts.



18. Security category

The required security category is MEDIUM, within the framework established in Article 40 and the general criteria set out in Annex I of the ENS. Some of the criteria that determine this level are that the process is fully defined and that the process catalogue is kept up to date and ensures consistency of actions across the different parts of the organization.

In addition, there are established regulations and procedures to respond to any security incident, which are updated and maintained regularly. There is also a high level of coordination between departments and the projects carried out.

The ICT Security Committee may modify the required security level.

The principles of the Information Security Policy are adopted and promoted by Management, which provides the necessary means and the resources employees need to comply with them, setting them out and making them public through this Security Policy.

19. Approval of the policy and entry into force

Amendments to this Policy involving changes or adjustments due to inefficiencies shall be made by the Information Security Committee, which must review it annually.

Where the changes involve a substantial modification or affect the principles or the assigned responsibilities, the Security Committee shall propose the changes, which must be approved, where appropriate, by the person or body with the relevant authority.

The replacement of the Policy shall be initiated by the Information Security Committee and ratified by the person or body with the relevant authority, and those concerned shall be duly informed through the same channels used for its dissemination.

Date: 7/10/2026

Approved by Management