



Information Security and Privacy Policy

15-10-2025
PUBLIC USE



Table of Contents

0.	Approval and version control.....	2
1.	Entry into force.....	3
2.	Mission of the organization	3
3.	Scope	4
4.	Objectives	4
5.	Regulatory framework	4
6.	Development	5
7.	Security Organization	6
8.	Security and Privacy Committee	7
9.	Risk Management.....	7
10.	Personnel Management	8
11.	Professionalism and security and privacy of human resources.....	8
12.	Authorization and control of access to Information Systems.....	9
13.	Facility protection	10
14.	Product Procurement	10
15.	Security and privacy by default.....	11
16.	System integrity and updating.	11
17.	Protecting Information in Transit and Stored	11
18.	Prevention of interconnected information systems	11
19.	Business continuity	12
20.	Continuous improvement of the security and privacy process.....	12



0. Approval and version control

<i>Date</i>	<i>Description</i>	<i>Author</i>	<i>Approved by</i>	<i>Remarks</i>	<i>Version</i>
September 2024	Information Security Policy	Security Manager	Safety Committee	Initial Edit	1.0
October 2025	Information Security and Privacy Policy	Information Security and Privacy Officer	Safety Committee	Adjustment to ISO27701	2.0

PUBLIC USE



1. Entry into force

This Information Security and Privacy Policy is effective from the date of signature and until it is replaced by a new Policy.

2. Mission of the organization

COMPANY MISSION

Offer services to streamline the creation of IT strategies, ensure information security and privacy and systems integration, ensure smooth and effective digital transformation and improve the digital customer experience.

To achieve its objectives, **REACT** assumes its commitment to the security and privacy of information, committing itself to its proper management, to offer all its stakeholders the greatest guarantees regarding the security and privacy of the information used.

These systems must be managed diligently, taking appropriate measures to protect them against accidental or deliberate damage that may affect the availability, integrity, confidentiality, authenticity or traceability of the information processed or the services provided.

The objective of information security is to guarantee the quality of information and the continuous provision of services, acting preventively, monitoring daily activity and reacting promptly to incidents.

IT systems must be protected against rapidly evolving threats with the potential to affect the confidentiality, integrity, availability, authenticity, traceability, intended use and value of information and services. To defend against these threats, a strategy that adapts to changes in environmental conditions is required to ensure the continuous delivery of services. This implies that departments must apply the minimum-security measures required by the National Security Scheme, as well as continuously monitor the levels of service provision, assess and analyze reported vulnerabilities, and prepare an effective response to incidents to ensure the continuity of the services provided.

Different departments must ensure that IT security is an integral part of every stage of the system's lifecycle, from conception to decommissioning, development or acquisition decisions and operational activities. Security and privacy requirements and funding needs should be identified and included in planning, in the request for proposals, and in tender documents for IT projects.

Departments must be prepared to prevent, detect, and react to and recover from incidents, in accordance with Article 8 of the ENS (Article 8. Prevention, detection, response and conservation).

3. Scope

This policy applies to all the entity's IT systems and to all members of the organization involved in Services and Projects aimed at the public sector, which require the application of ENS, without exceptions.

4. Objectives

For all the above, the Management establishes the following information security and privacy objectives:

- Provide a framework to increase resilience or resilience for an effective response.
- Ensure the rapid and efficient recovery of services, in the face of any physical disaster or contingency that may occur and that could put the continuity of operations at risk.
- To prevent information security incidents to the extent technically and economically feasible, as well as to mitigate information security risks generated by our activities.
- Guarantee the confidentiality, integrity, availability, authenticity and traceability of the information.

5. Regulatory framework

One of the objectives must be to comply with applicable legal requirements and with any other requirements that we subscribe to in addition to the commitments made with customers, as well as the continuous updating of them. To this end, the legal and regulatory framework in which we carry out our activities is:

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data.
- Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights.
- Royal Legislative Decree 1/1996, of 12 April, Law on Intellectual Property.
- Law 2/2019, of 1 March, amending the revised text of the Intellectual Property Law, approved by Royal Legislative Decree 1/1996, of 12 April, and incorporating Directive 2014/26/EU of the European Parliament and of the Council, of 26 February 2014, into Spanish law, and Directive (EU) 2017/1564 of the European Parliament and of the Council, of 13 September 2017.
- Royal Decree 311/2022, of 3 May, regulating the National Security Scheme.
- Law 34/2002, of 11 July, on Information Society Services and Electronic Commerce (LSSI).
- Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations.
- Law 40/2015, of 1 October, on the Legal Regime of the Public Sector.

6. Development

To achieve these objectives, it is necessary to:

- Continually improve our information security and privacy system.
- Identify potential threats, as well as the impact on business operations that such threats, if they materialize, may cause.
- Preserve the interests of its key stakeholders (customers, shareholders, employees, and suppliers), reputation, brand, and value-creating activities.
- Work together with our suppliers and subcontractors to improve the delivery of IT services, continuity of services, and information security and privacy, resulting in greater efficiency of our business.
- Evaluate and guarantee the technical competence of the staff, as well as ensure their adequate motivation for their participation in the continuous improvement of our processes, providing training and adequate internal communication so that they develop good practices defined in the system.
- Guarantee the correct condition of the facilities and the appropriate equipment, so that they are in accordance with the activity, objectives and goals of the company.
- Guarantee a continuous analysis of all relevant processes, establishing the relevant improvements in each case, based on the results obtained and the established objectives.
- Structure our management system in a way that is easy to understand. Our management system has the following structure:

The management of our system is entrusted to the IT Systems Manager, and the system will be available in our information system in a repository, which can be accessed according to the access profiles granted in accordance with our current access management procedure.

The documentation referring to the security and privacy of the system is structured in folders within the company's file server, divided into sub-folders named by standard points and operating frameworks, which collect the different procedures, records and evidence, with restricted access for the company's personnel, not being able to access unauthorized external personnel.

The safety documentation is structured in:

- Information Security and Privacy Policy.
- Safety regulations: documents that describe the use of equipment, services and facilities. They describe what is considered misuse, the responsibility of personnel with respect to compliance with or violation of regulations, rights, duties and disciplinary measures in accordance with current legislation.
- Specific documents: safety documentation developed according to the CCN-STIC guidelines that are applicable.
- Security Procedures: Documents that detail how to operate the elements of the system.

This policy is complemented by the rest of the policies, procedures and documents in force to develop our management system.

7. Security Organization

The essential responsibility lies with the General Management of the organization, as it is responsible for organizing the functions and responsibilities and providing adequate resources to achieve the objectives of the ENS. Managers are also responsible for setting a good example by following established safety standards.

These principles are assumed by the General Management, which has the necessary means and provides its employees with sufficient resources to comply with them, and they are reflected and made publicly known through this Integrated Information Security and Privacy Policy.

The defined security roles or functions are:

Function	Duties and responsibilities
Information Officer (RINFO)	<ul style="list-style-type: none"> · Make decisions regarding the information processed
Service Manager (RSER)	<ul style="list-style-type: none"> · Coordinate the implementation of the system · Continuously improve the system
Security Officer (RSEG or CISO)	<ul style="list-style-type: none"> · Determining the adequacy of technical measures · Providing the best technology for service
System Manager (RSIS)	<ul style="list-style-type: none"> · Coordinate the implementation of the system · Continuously improve the system
Address	<ul style="list-style-type: none"> · Provide the necessary resources for the system · Leading the system
Security Administrator (AS)	<ul style="list-style-type: none"> · Implementation, management and maintenance of security measures.



This definition of duties and responsibilities is completed in the job profiles and in the documents of the Register of Managers, Roles and Responsibilities system.

CONFLICT RESOLUTION

Any differences in criteria that could lead to a conflict will be dealt with within the Security and Privacy Committee and the criteria of the General Management will prevail in all cases.

8. Security and Privacy Committee

The procedure for their appointment and renewal will be ratification in the Security and Privacy Committee.

The Committee for the Management and Coordination of Security and Privacy is the body with the greatest responsibility within the information security management system, so that all the most important decisions related to security and privacy are agreed by this committee.

The members of the Information Security and Privacy Committee are:

- **HEAD OF SECURITY AND PRIVACY:** Marcela Pereira M., COO
- **SYSTEM MANAGER:** Bernardo Corrales, CTO
- **SERVICE MANAGER:** Alan Archila L., CEO
- **CHIEF INFORMATION OFFICER:** Alan Archila L., CEO

These members are appointed by the committee, which alone can appoint, renew and dismiss them.

The Security and Privacy Committee is an executive body with autonomy for decision-making and that does not have to subordinate its activity to any other element of our company.

The organization of the Security and Privacy of the information is developed in the complementary document to this Security and Privacy Organization Policy.

This policy is complemented by the rest of the policies, procedures and documents in force to develop our management system.

9. Risk Management

All systems subject to this Policy shall conduct a risk analysis, assessing the threats and risks to which they are exposed. This analysis is reviewed regularly:

- at least once a year;
- when the information handled changes;



- when the services provided change;
- when a serious security or privacy incident occurs;
- when serious vulnerabilities are reported.

For the harmonization of risk analyses, the IT Security and Privacy Committee will establish a benchmark assessment for the different types of information handled and the different services provided. The IT Security and Privacy Committee will boost the availability of resources to meet the security and privacy needs of the different systems, promoting horizontal investments.

To carry out the risk analysis, the risk analysis methodology developed in the Risk Analysis procedure will be taken into account.

10. Personnel Management

All members of REACT have the obligation to know and comply with this Information Security and Privacy Policy and the Security Regulations, being the responsibility of the IT Security and Privacy Committee to provide the necessary means for the information to reach those affected.

All REACT members will attend an IT security and privacy awareness session at least once a year. A continuous awareness program will be established to serve all REACT members, in particular new entrants.

People with responsibility for the use, operation or administration of IT systems shall be trained in the safe handling of the systems to the extent that they need it to carry out their work. Training will be mandatory before assuming a responsibility, whether it is your first assignment or if it is a change of job or responsibilities in it.

11. Professionalism and security and privacy of human resources

This Policy applies to all REACT personnel and external personnel who perform tasks within the company.

HR will include information security and privacy features in employee job descriptions, inform all personnel it engages of its obligations with respect to compliance with the Information Security and Privacy Policy, manage Confidentiality Commitments with staff, and coordinate user training tasks with respect to this Policy.

- The Security Management Officer (RGS) [CISO], is responsible for monitoring, documenting, and analyzing reported security incidents, as well as communicating to the Information Security and Privacy Committee and information owners.
- The Information Security and Privacy Committee will be responsible for implementing the necessary means and channels for the Security Management Officer (RGS) [CISO] to handle reports of system incidents and anomalies. The Committee will also be aware of, overseeing the investigation, monitoring the

evolution of information and promoting the resolution of information security incidents.

- The Security and Privacy Management Officer (RGS) [CISO] will be involved in the preparation of the Confidentiality Pledge to be signed by employees and third parties performing functions at REACT, in advising on the penalties to be applied for non-compliance with this Policy, and in dealing with information security and privacy incidents.
- All REACT staff are responsible for reporting information security and privacy weaknesses and incidents that are detected in a timely manner.
- Professionalism of human resources:
 - Determine the necessary competence of personnel to carry out the work affecting Information Security and Privacy.
 - It is necessary to ensure that people are competent on the basis of appropriate education, training or experience.
 - Demonstrate through documented information that the competence of the staff in matters of Information Security and Privacy is necessary.

The objectives of controlling the safety of personnel are:

- Reduce the risks of human error, implementation of irregularities, improper use of facilities and resources, and unauthorized handling of information.
- Explain the safety responsibilities in the personnel recruitment stage and include them in the agreements to be signed and verify their compliance during the performance of the employee's tasks.
- Ensure that users are aware of information security and privacy threats and concerns and are trained to support the organization's Information Security and Privacy Policy in the course of their normal duties.
- Establish confidentiality commitments with all personnel and users outside the information processing facilities.
- Establish the necessary tools and mechanisms to promote the communication of existing security weaknesses, as well as incidents, in order to minimise their effects and prevent their recurrence.

12. Authorization and control of access to Information Systems

The control of access to information systems aims to:

- Prevent unauthorized access to information systems, databases, and information services.
- Implement security in user access through authentication and authorization techniques.
- Control the security of the connection between the REACT network and other public or private networks.
- Review critical events and activities carried out by users on systems.
- Raise awareness of their responsibility for the use of passwords and equipment.
- Ensure information security when using laptops and personal computers for remote work.

13. Facility protection

The objectives of this policy on the protection of facilities are:

Prevent unauthorized access, damage, and interference to REACT's headquarters, facilities, and information

- Protect REACT's critical information processing equipment, placing it in protected areas and protected by a defined security perimeter, with appropriate security measures and access controls. Likewise, to contemplate the protection of this in its transfer and to remain outside the protected areas, for maintenance or other reasons.
- Control environmental factors that could impair the proper functioning of the computer equipment that houses the REACT information
- Implement measures to protect the information handled by the staff in the offices, within the normal framework of their usual tasks.
- Provide protection proportionate to the risks identified.

This Policy applies to all physical resources related to REACT's information systems: facilities, equipment, wiring, records, storage media, etc.

The Security and Privacy Management Officer (RGS) [CISO], together with the Data Subjects, as appropriate, shall define the physical and environmental security measures for the protection of critical assets, based on a risk analysis, and shall monitor their implementation. It will also verify compliance with physical and environmental security provisions.

The heads of the different departments will define the levels of physical access of REACT personnel to the restricted areas under their responsibility. Information Owners will formally authorize off-site work with information about their business to REACT employees when they deem it appropriate.

All REACT staff are responsible for compliance with the clean screen and desktop policy, for the protection of information related to daily work in the offices.

14. Product Procurement

Different departments must ensure that IT security and privacy is an integral part of every stage of the system's life cycle, from conception to decommissioning, development or acquisition decisions and operational activities. Security and privacy requirements and funding needs should be identified and included in planning, in the request for proposals, and in tender documents for IT projects.

On the other hand, the security and privacy of information will be taken into account in the acquisition and maintenance of information systems, limiting and managing change.

The policy for the development and acquisition of information systems is developed in the document: Policy for the Acquisition, Development and Maintenance of Systems.

15. Security and privacy by default

REACT considers it strategic for the entity that processes integrate information security and privacy as part of its life cycle. Information systems and services must include security and privacy by default from their creation to their retirement, including security in development and/or acquisition decisions and in all operating activities, establishing security and privacy as an integral and transversal process.

16. System integrity and updating.

REACT is committed to ensuring the integrity of the system through a change management process that allows the control of the update of the physical or logical elements through authorization prior to their installation in the system. This assessment will be carried out primarily by IT management, which will assess the impact on the security and privacy of the system before making the changes and will monitor in a documented manner those changes that are assessed as significant or have implications for the security of the systems.

Periodic security reviews will assess the security status of the systems, in relation to the manufacturers' specifications, vulnerabilities and updates affecting them, reacting diligently to manage the risk in view of the security status of the systems.

17. Protecting Information in Transit and Stored

REACT establishes safeguards for the Security and Privacy of Information stored or in transit through insecure environments. Laptops, personal assistants (PDAs), peripheral devices, information carriers and communications over open networks or with weak encryption will be considered insecure environments.

18. Prevention of interconnected information systems

REACT establishes protective measures for Information Security and Privacy especially to protect the perimeter, in particular, if it connects to public networks, especially if they are used in their entirety or mainly, for the provision of electronic communications services available to the public.

In any case, the risks arising from the interconnection of the system, through networks, with other systems will be analysed, and their point of connection will be controlled. Electronic connections available to the public.



19. Business continuity

REACT, with the aim of guaranteeing the continuity of activities, establishes measures so that the systems have backups and establishes the necessary mechanisms to guarantee the continuity of operations, in the event of loss of the usual means of work through the services provided by the AZURE Cloud infrastructure.

20. Continuous improvement of the security and privacy process

REACT establishes a process of continuous improvement of information security and privacy by applying the criteria and methodology established in international standards such as ISO 27001 to adapt to emerging regulations and threats.

In Madrid, Spain, October 15, 2025

Signed: The General Directorate

PUBLIC USE