Information Security Policy

Information security management System (ISMS)

Paseo de la Castellana,79 -28046- Madrid (España)

Phone: 932 661 614 (Calls from Spain)

International +34 933 935 946

Website: www.anf.es

Security Level

Public Document

Important Notice

Address: Paseo de la Castellana, 79 - 28046 - Madrid (Spain)

Phone: 902 902 172 (calls from Spain) International (+34) 933 935 946

Website: www.anf.es

INDEX

Commitment and Leadership of Top Management

Top Management of ANF AC is aware of the importance of protecting information and the assets used to process such information. The organization's business processes largely depend on the existence of this information, and to a great extent, we act merely as custodians of the data.

In order to ensure such protection and to maintain its commitment to information security and to its customers, suppliers, collaborators, employees, and other interested parties, ANF AC has implemented an Information Security Management System (ISMS) based on the international standard ISO/IEC 27001:2013, which has been further strengthened by the implementation of the Spanish National Security Framework (ENS) at the HIGH level. All of this is carried out without disregarding the obligations established by the General Data Protection Regulation (EU), where the primary focus is on preserving the fundamental rights of data subjects.

Top Management of ANF AC has participated in the preparation of this document and approves it, along with all related documentation, for the proper development, implementation, and maintenance of the ISMS / ENS.

ISO/IEC 27001:2022 and the ENS establish the need for Top Management to be aware of the risks associated with the processing and storage of the information handled within the organization.

For this reason, any exclusion of controls considered necessary to meet risk acceptance criteria must be justified by evidence demonstrating that the associated risks have been accepted by the responsible parties. The exclusion of controls shall not affect the organization's ability and/or responsibility to ensure information security in accordance with the security requirements derived from the risk assessment and applicable legal or regulatory requirements.

Top Management of ANF AC declares its full commitment to all objectives set out in this Information Security Policy, as well as in the set of documents published within the framework of the Information Security Management Systems.

Likewise, it is committed to promoting and approving the necessary measures for their effective implementation within the organization.

Excellence requires a commitment to continuous improvement; accordingly, ANF AC Top Management conducts an annual review of its ISMS / ENS to ensure its continued suitability, adequacy, and effectiveness..

Florencio Díaz Vilches

CEO of ANF Autoridad de Certificación

1. Document control

1.1. Name and identification of the document

Document name	Information Security Policy		
Version	1.8.		
OID	1.3.6.1.4.1.18332.101.80.1.		
Approval date	09/07/2025	**Publication date**	09/07/2025

1.2. Reviews

In order to ensure the validity of this regulatory framework, this document will be reviewed at least once a year and, immediately, when relevant changes occur in the organization, in the legal framework or technical standards.

In its review will have to take into account the new developments affecting the future strategy of the business, legal conditions, technical developments, and incidents that have occurred.

The responsibility for the approval of measures that presuppose a modification of the Information Security Policy, is of the PKI Governing Board at the proposal of the Security Committee.

Version	Changes	Author	Approval
1.8.	Regulatory framework update. Minor revisions	Yulier Nuñez	09/07/2025
1.7.	NIS2 regulatory framework update	Yulier Nuñez	19/12/2024
1.6.	Review and adaptation to the National Security Scheme (ENS)	Pablo Díaz	10/07/2023
1.5.	Revisión y actualización	Pablo Díaz	01/02/2022
1.4.	Revisión y actualización	F. Díaz	10/01/2019
1.3.	Revisión y actualización	Álvaro Díaz	01/02/2016
1.2.	Revisión y actualización	Laura Villas	27/04/2015
1.1.	Ampliación y actualización	Moisés Amador	02/04/2014
1.0.	Versión inicial de la Política de seguridad de la información	Isabel Fábregas	24/01/2011

2. Introducción

This Information Security Policy of ANF Autoridad de Certificación (hereinafter, ANF AC) is part of the regulatory body of the Information Security Management System (hereinafter ISMS) of ANF AC.

ANF Certification Authority (hereinafter, ANF AC), for its provision of trustworthy services depends on its human resources, the information it stores and custody, its documentary base, the technology developed by its R & D department, intangible assets and tangible assets, including ICT systems (Information and Communication Technologies), as well as its reputation.

The objective of information security is to guarantee the quality of information and the continuous provision of services, acting preventively, supervising daily activity and reacting quickly to incidents and ultimately, ensuring the continuity of the organization.

ICT systems must be protected against all types of threats, whether fortuitous or intentional. Our sector has a rapid evolution with the potential to influence the confidentiality, integrity, availability, intended use and value of information and services. To defend against these threats, a strategy is required that adapts to changes in the conditions of the environment to ensure the continuous provision of services. This implies that all departments of the organization must apply the minimum-security measures required by the Information Security Management System implemented by ANF AC, as well as continuously monitor levels of service delivery, follow and analyze the reported vulnerabilities, and prepare an effective response to the incidents to ensure the continuity of the services provided. This document defines the Information Security guidelines in accordance with the interests of ANF AC and its interested parties.

Of special incidence for our organization is the legal and technical framework. ANF AC is regulated by specific laws and regulations that we are committed to follow and respect.

The different departments must ensure that ICT security is an integral part of every stage of the system's life cycle, from its conception to its withdrawal from service, through development or acquisition decisions and exploitation activities. Security requirements and funding needs should be identified and included in planning, offers request, and bidding documents for ICT projects.

Departments should be prepared to prevent, detect, react and recover from incidents. Specifically:

1. The system security must include aspects of prevention, detection and correction, to procure threats on the system do not materialize, do not affect seriously the information handled, or the services provided.
2. Preventive measures should eliminate or at least reduce the possibility that threats get to materialize endangering the system. These prevention measures will include, among others, deterrence and reduction of exposure.
3. The detection measures will be accompanied by measures of reaction, so that security incidents be addressed on time.
4. The recovery measures will allow the restoration of information and services, so that they can cope with situations in which a security incident disable the usual means.
5. Without detracting from the other basic principles and minimum requirements established, the system will ensure the preservation of data and information in electronic form.

6. Similarly, the system services remain available throughout the life cycle of digital information, through a conception and procedures that are the basis for the preservation of digital heritage.

3. Purpose

This document aims to establish the guidelines that shall govern information security in accordance with the needs of ANF AC and the applicable legislation. Furthermore, it defines the principles and directives by which ANF AC will manage and protect its information and services through the implementation, maintenance, and continuous improvement of an Information Security Management System (hereinafter, ISMS), applying the requirements of the UNE-ISO/IEC 27001:2022 standard and those of its interested parties, within the current legal and regulatory framework, including Royal Decree 311/2022 of 3 May, which regulates the Spanish National Security Framework (ENS).

The following objectives are defined:

- Define the basic principles of Information Security.
- Detail all aspects related to the Information Security policy of ANF AC (object, scope, approval, entry into force and application, breaches and sanctions, review and improvement).
- Indicate the documentation that develops the Information Security policy of ANF AC.
- Detail the organization of Information Security in ANF AC.
- Describe the actions of ANF AC regarding personal data.
- Promote the continuous improvement of the effectiveness of our system and processes, as a permanent objective of ANF AC, as well as sustain and increase information security and customer satisfaction.

Information security objectives should:

- be consistent with the information security policy
- be measurable (if applicable)
- take into account applicable safety requirements and the results of valuations and risk treatment
- be communicated
- be updated

In general terms, ANF AC shall implement preventive, reactive, and recovery mechanisms in order to minimize the impact of security incidents.

With regard to prevention, measures shall be taken to prevent services and information from being affected by security incidents. To this end, the security measures established in Annex II of the ENS shall be implemented, together with any additional measures identified through the risk analysis process.

With regard to reaction, mechanisms for the detection, communication, and management of security incidents shall be established, so that any incident can be handled within the shortest possible timeframe. Wherever possible, security incidents shall be detected automatically by means of service monitoring components or anomaly detection systems, and incident response procedures shall be initiated as soon as possible. For incidents detected by users, whether internal or external, the appropriate incident reporting communication channels shall be established.

With regard to recovery, for those services considered critical, based on the assessment carried out by their respective owners, plans shall be developed to ensure the continuity of such services in the event that they become unavailable as a result of a security incident.

This Information Security Policy,

- Is signed by the Chief Executive Officer and the Head of Security of ANF AC.
- Is approved by the PKI Governing Board upon proposal of the Security Committee, and is published by the Security Officer.
- Is publicly available within the organization and to external collaborators providing services to ANF AC. A copy of the document is provided during the onboarding procedure.
- Shall serve as the reference for the resolution of conflicts and other matters related to the organization's security.

4. Scope

This document, as well as those that complement, implement or develop it, will be applicable to all information systems of ANF AC and that infrastructure and systems that provide support.

ANF Certification Authority (ANF AC) is accredited and provides the following qualified trust services:

- **Centralized electronic signature solution, including issuance, custody, provisioning, and usage control in the Cloud. Sign to Sign.**
- **Video identification solution for transaction authentication and certificate issuance. Mi eID eSIGN.**
- **Internal information system – Whistleblowing channel in the Cloud. Grattil.Issuance of qualified electronic signature certificates**
- **Issuance of qualified electronic seal certificates *(QSealC)***
- **Issuance of Qualified Website Authentication Certificates *(QWACs)***
- **Qualified electronic time stamping service *(QTimeStamping)***
- **Qualified validation service of electronic signatures and seals**
- **Qualified preservation service for electronic signatures and seals**
- **Qualified certified electronic delivery service *(eDelivery)***

5. Terms and Definitions

- **ISMS** (Information Security Management System): A set of interrelated or interacting elements (organizational structure, policies, activity planning, responsibilities, processes, procedures, and resources) used by an organization to establish an information security policy and objectives and to achieve those objectives, based on a risk management and continuous improvement approach, as defined in the UNE-ISO/IEC 27001 standard.
- **ENS** (National Security Framework): The Spanish National Security Framework, regulated by Royal Decree 311/2022 of 3 May, applicable within the scope of electronic administration in the public sector. Its purpose is to establish the security policy and create the necessary conditions for trust in the use of electronic means, through measures that ensure the security of systems, data, communications, and electronic services, enabling the exercise of rights and the fulfillment of obligations through these means.
- **Interested party**: Person or group that has an interest in the performance or success of the organization.
- **Authenticity**: Property ensuring that a person and/or organization accessing and using information is who it claims to be.
- **Confidentiality**: Property that ensures that information is not made available or disclosed to unauthorized persons and/or organizations.
- **Integrity**: Property or characteristic ensuring that an information asset has not been altered in an unauthorized manner.
- **Traceability**: Capability that allows all actions performed on information or an information processing system to be unequivocally associated with a person and/or organization.
- **Availability**: Property ensuring that information is accessible and usable when required by an authorized person and/or organization.
- **Asset**: In relation to information security, any information or element related to its processing (systems, media, buildings, people, etc.) that has value for the organization.
- **Risk**: The possibility that a specific threat may exploit a vulnerability to cause loss or damage to an information asset. It is usually considered as a combination of the probability of an event and its consequences.
- **Threat**: Potential cause of an unwanted incident, which may result in harm to a system or the organization.
- **Risk analysis**: Process to understand the nature of risk and determine the level of risk.
- **Risk treatment**: Process of modifying risk through the implementation of controls.
- **Personal data**: Any information relating to a person that identifies or can be used to identify that person.

6. Mission

ANF AC is a Qualified Trust Service Provider (QTSP) in accordance with the eIDAS Regulation. ANF AC operates a Public Key Infrastructure (PKI) and is officially accredited to provide, among others, the following qualified services:

- **Centralized electronic signature and authentication service, including issuance, custody, provisioning, and access control.**
- **Remote video identification service, for authentication and the issuance of electronic certificates.**
- **Service of issuance, revocation and renewal of qualified certificates of electronic signature**, in accordance with the eIDAS Regulation.
- **Service of emission, revocation and renewal of qualified certificates of electronic seal**, in accordance with the eIDAS Regulation.
- **Service of issuance, revocation and renewal of qualified SSL secure server certificates**, in accordance with the eIDAS Regulation.
- **Qualified Validation service of electronic signatures and seals**.
- **Electronic time stamp servic**e, which allows its users to obtain a guarantee that determines with total certainty that the information existed at a specific moment in time.
- **Service of electronic signature preservation**, which aims to extend the reliability of electronic signature data beyond the period of technological validity.
- **Certified electronic delivery service**, which allows data to be transmitted between third parties by electronic means.

In addition, ANF AC provides its customers and the market in general with:

- Internal information system – Whistleblowing channel, in compliance with Law 2/2023 of 20 February, on the protection of persons who report regulatory infringements and on the fight against corruption.

ANF AC is officially accredited by:

- Spanish Data Protection Agency (AEPD), as a Certification Body under the AEPD DPO Certification Scheme.
- Spanish Tax Agency (AEAT), for the Certified Digitization service of tax documents.

7. Regulatory Framework

The legal and technical framework to be observed by ANF AC.

ANF AC has been audited and certified in compliance with internationally recognized standards and frameworks, including:

- The set of ETSI standards related to qualified eIDAS trust services
- ISO 9001
- ISO 27001
- ISO 27002
- ISO 27005
- ISO 27024
- ISO 14001
- Royal Decree 311/2022

The applicable legal framework includes:

- Regulation (EU) No 910/2014 of 23 July 2014 of the European Parliament and of the Council (hereinafter, eIDAS),
- Law 6/2020 of 11 November, regulating certain aspects of electronic trust services,
- 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, repealing Directive 95/46/EC (General Data Protection Regulation – GDPR),
- Organic Law 3/2018 of 5 December, on Personal Data Protection and Guarantee of Digital Rights,
- Royal Decree 311/2022 of 3 May, regulating the National Security Framework (ENS), published in the Official State Gazette (BOE) on 4 May 2022,
- Royal Decree 4/2010 of 8 January, regulating the National Interoperability Framework in the field of Electronic Administration,
- Law 34/2002 of 11 July, on Information Society Services and Electronic Commerce,
- Law 10/2021 of 9 July, on remote work,
- Royal Decree-Law 12/2018 of 7 September, on the security of network and information systems,
- Order PCI/487/2019 of 26 April, publishing the National Cybersecurity Strategy 2019 (ENCS 2019),
- Royal Legislative Decree 1/1996 of 12 April, approving the Intellectual Property Law,
- 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,
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022,
- Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024.

Additionally, the following Administrative Resolutions apply mutatis mutandis:

- Resolution of 13 October 2016 of the Secretary of State for Public Administrations, approving the Security Technical Instruction (STI) in accordance with the National Security Framework,

- Resolution of 27 March 2018 of the Secretary of State for Civil Service, approving the Security Technical Instruction on Information Systems Security Audits,
- Resolution of 13 April 2018 of the Secretary of State for Civil Service, approving the Security Technical Instruction on Security Incident Notification,
- Resolution of 7 October 2016 of the Secretary of State for Public Administrations, approving the Security Technical Instruction on Security Status Reporting.

REFERENCE GUIDELINES

Royal Decree 311/2022 of 3 May, which develops the National Security Framework, promotes the preparation and dissemination of information and communication technology security guidelines by the National Cryptologic Centre (CCN), in order to facilitate compliance with the minimum security requirements.

The CCN-STIC document series is developed to fulfil the responsibilities of the National Cryptologic Centre and to support the provisions of the National Security Framework.

1. CCN-STIC 402: Organization and Management for the Security of ICT Systems (2006).
2. CCN-STIC 801: ENS – Responsibilities and Functions (2025).
3. CCN-STIC 805: ENS – Information Security Policy (2025).
4. CCN-STIC 830: ENS – Scope of Application of the National Security Framework (2016).
5. Reports and resolutions of the Spanish Data Protection Agency (AEPD).

8. Security Organization

The security organization is based on the CCN-STIC-402 Guideline: Organization and Management for the Security of ICT Systems from the Spanish National Cryptologic Centre.

The following structures shall be established:

- Supervisory structure, responsible for verifying compliance with security requirements and ensuring continuous alignment with the organization's objectives.
- Operational structure, responsible for implementing the identified security measures.

ANF AC has specific policies in place, namely the "Roles and Responsibilities Policy" (OID 1.3.6.1.4.1.18332.38.1) and the "Assignment of Roles and Responsibilities" (OID 1.3.6.1.4.1.18332.101.10.1).

8.1. Supervisory Structure

The supervisory structure for security is responsible for verifying the correct implementation and operation of established security requirements, with the objective of maintaining alignment with organizational goals and ensuring compliance with applicable standards and legislation.

The following roles within Top Management of ANF AC form part of this structure:

- Chief Executive Officer (Top Management)
- Security Officer
- Legal Director

The functions and responsibilities of each role are described in the following sections.

8.1.1. Top Management

Top Management formally expresses its commitment to supporting the security plans derived from this Policy. Such support shall be reflected in:

- Providing the necessary human and financial resources, within budgetary constraints;
- Assigning roles and responsibilities to individuals involved in security plans;
- Supporting the training of human resources involved in security plans to ensure appropriate awareness and competencies;
- Ensuring compliance with the National Security Framework (ENS);
- Facilitating communication with other organizations regarding Information Security matters;
- Promoting continuous improvement in the field of Information Security.

This commitment is demonstrated through the formal approval of this document.

8.1.2. Security Officer

The Security Officer is responsible for defining, coordinating, disseminating, and verifying the Information Security requirements within the organization.

This role is part of the Security Committee, acting as its Chair and therefore responsible for elevating matters of interest related to information security, as well as for its coordination and composition.

Responsibilities include:

- Determining the members of the Security Committee at any given time;
- Convening and coordinating Security Committee meetings, in which they shall also act as Secretary;
- Establishing security measures in accordance with the requirements defined by Service and Information Owners, the results of risk analysis and risk management, the information obtained from implemented indicators, and the guidelines set out in Annex II of the National Security Framework (ENS);
- Supervising compliance with the Information Security Policy and its derived standards and procedures;
- Planning strategic objectives in cybersecurity, including proposing to Human Resources objectives related to cybersecurity that may be considered for staff promotion and/or special remuneration;
- Coordinating and controlling Information Security measures. Together with the Systems Manager, designing and implementing indicators to measure the effectiveness and efficiency of the implemented measures;
- Maintaining a register of security incidents; investigating and analyzing such incidents, and verifying compliance with monitoring protocols and the execution of resulting actions;
- Supervising and coordinating cybersecurity crisis situations (exceptional situations);
- Promoting, coordinating, and supporting periodic security risk analyses carried out by Service and Information Owners, and presenting the results to the Security Committee as part of the Risk Management plan;
- Planning and coordinating internal and external audits required for ENS, ISMS, and other relevant certifications, collaborating in such audits and supervising the implementation of corrective actions;
- Maintaining security documentation properly organized, updated, and periodically reviewed, ensuring its availability to personnel within the organization;
- Collecting personal data protection requirements defined by the Data Controller or Data Processor, with the advice of the Data Protection Officer (DPO).

The Security Officer shall be appointed by Top Management.

8.1.3. Legal Director

The Legal Director is responsible for defining, coordinating, verifying, and, where applicable, approving the legal requirements within the organization.

This role is part of the Security Committee, acting as its Secretary and therefore responsible for preparing meeting minutes, submitting them for signature, and ensuring their filing and safekeeping.

The Legal Director also assumes the role of Data Protection Officer (DPO). In this capacity, they shall ensure that personal data is processed and protected in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and Organic Law 3/2018 of 5 December on Personal Data Protection and Guarantee of

Digital Rights, working in coordination with the other members of Top Management and the Security Committee.

8.2. Operational Structure

The operational security structure shall assume responsibility for the operational management of information systems security, implementing within such systems the necessary measures to meet the security requirements established by the specification structure.

The following roles form part of this structure:

- Systems Manager
- IT Development and Programming Manager
- Compliance Officer
- Cryptography Manager
- System Users

The functions and responsibilities of the roles associated with the operational structure are described below.

8.2.1. Systems Manager

This role shall be performed by the Head of Systems.

Its functions and responsibilities include:

- Defining, in coordination with the Information Security Officer, the functional security specifications of the organization's Information Systems;
- Ensuring that the design of information systems and communication networks incorporates, from the outset, the necessary information security aspects in terms of availability, integrity, confidentiality, authenticity, and traceability;
- Verifying that the security configuration following the installation of a new system is appropriate;
- Verifying that, after system changes, the security configuration remains appropriate;
- Implementing and verifying the operation of security measures arising from risk treatment plans or corrective action plans derived from information security audits;
- Verifying the proper functioning of information security indicators;
- Carrying out periodic technical audits to verify the effectiveness of the measures and compliance with established security requirements. These audits may be conducted by internal or external personnel.

8.2.2. IT Development and Programming Manager

This role shall be performed by the Head of IT Development.

Its functions and responsibilities include:

- Defining, in coordination with the Information Security Officer, the functional security specifications of the applications designed and developed by the ANF AC technical team;

- Ensuring that application design incorporates, from the outset, the necessary information security aspects in terms of availability, integrity, confidentiality, authenticity, and traceability;
- Analyzing and selecting the technologies and programming languages to be used in development projects;
- Coordinating the technical development team.

8.2.3. Compliance Officer

This role is responsible for supervising the design of systems and the technological platform to ensure compliance with applicable regulatory requirements.

Responsibilities include:

- Attending all meetings related to the design and development of ANF AC technological platforms;
- Supporting external auditors in addressing their requirements;
- Leading internal audits.

8.2.4. Cryptography Manager

This role is responsible for monitoring the state of the art in cryptographic security and determining the algorithms and their usage within ANF AC products and services.

8.2.5. System Users

All personnel and users of ANF AC information systems.

8.2.5.1. Functions and Responsibilities of Personnel

All ANF AC personnel involved in the use, management, maintenance, and operation of information and related services are required to be aware of and comply with the Information Security Policy.

The Security Committee shall ensure that this Policy is communicated to all relevant parties and remains permanently available to them.

All such personnel shall attend security awareness sessions, as established in the annual training and awareness plan.

Individuals responsible for the use, management, maintenance, or operation of ICT-supported services shall receive appropriate training to ensure secure system operation, as required for their roles. This training shall be mandatory prior to assuming responsibilities, whether for an initial assignment or following a change in role or responsibilities.

8.2.5.2. Functions and Responsibilities of Third Parties

Third parties involved in the management, maintenance, or operation of services provided by ANF AC shall be made aware of this Information Security Policy and shall be required to comply with it and with any derived regulations.

Third parties may develop their own operational procedures to meet the requirements of this Policy. Specific incident reporting procedures shall be established to enable affected third parties to report incidents. Third-party personnel shall receive awareness training equivalent to that required for internal staff.

Where a third party is unable to satisfy any aspect of this Policy, the Security Officer shall conduct a risk assessment. The identified risk shall be formally accepted by the Security Committee.

8.3. Rules Governing the Information Security Organizational Structure

Rules addressed to Top Management and members of the supervisory structure:

- Top Management of ANF AC shall review and, where appropriate, approve the regulatory proposals submitted by the Security Committee;
- Where a new ISMS document is approved, Top Management shall ensure its communication to all parties authorized to access it;
- Where an ISMS document is modified or withdrawn, Top Management shall ensure that all authorized parties are informed of the updated version;
- Top Management shall actively promote an information security culture within ANF AC, particularly by supporting training initiatives related to the ISMS;
- Top Management shall inform the Security Committee of:
    - Business strategy-related aspects;
    - Market intelligence, particularly regarding competition;
- Top Management shall estimate and allocate financial resources for the ISMS.

Rules addressed to the Chief Executive Officer:

- Responsible for allocating the resources, physical infrastructure, and personnel necessary for managing the organization's information security;
- Responsible for ensuring that decisions adopted by Top Management are implemented.

Rules addressed to the Information Security Committee:

- The Information Security Committee shall update and submit to Top Management the Information Security Policies, the risk analysis methodology, and the information classification methodology, as appropriate;
- The Information Security Committee shall analyze escalated security incidents and initiate contact with authorities when deemed necessary;
- The Committee is responsible for managing the development, review, and evaluation of the Information Security Policy;
- This Policy shall be reviewed at least annually and whenever new circumstances so require, taking into account business strategy changes, legal requirements, technological developments, and security incidents;
- Reviews shall consider applicable legal frameworks, technical standards, and recommendations published by reference organizations to which ANF AC is committed;
- The Committee shall verify compliance with the Information Security Policies.

Rules addressed to the Security Officer

- The Security Officer shall lead the development of guidelines for managing information security and the establishment of technical, physical, and administrative controls derived from security risk analyses;
- The Security Officer shall periodically validate and monitor the implementation of established security controls.

Rules addressed to the Internal Audit Manager

- The Internal Audit Manager shall plan and perform internal audits of the ISMS to determine whether policies, processes, procedures, and controls comply with institutional, security, and regulatory requirements;
- The Internal Audit Manager shall conduct full or partial reviews of ISMS scope processes or areas to verify the effectiveness of corrective actions;
- The Internal Audit Manager shall report audit findings to area managers and the Security Committee.

Rules addressed to IT Development and Systems Managers

- The Technology Manager shall assign functions, roles, and responsibilities for the operation and administration of the organization's technological platform. These shall be documented and appropriately segregated.

Rules addressed to all employees and third-party collaborators:

Employees of ANF AC and third parties performing activities within or for the organization are responsible for complying with all information security policies, standards, procedures, and requirements.

8.4. Non-compliance

Failure to comply with any obligation or requirement defined in these documents shall, by default, be classified as objective non-compliance. However, the Security Committee, based on the specific circumstances of each case, shall ultimately determine the final classification.

8.5. Sanctions

Any action aimed at reducing or eliminating the effectiveness of the controls implemented to ensure Information Security, altering the properties of Information Security, or hindering or preventing the investigation of any breach of the Information Security Policy and its associated regulations, shall be considered a breach of trust and may be subject to investigation and, where appropriate, to corresponding disciplinary or legal actions against those responsible.

Sanctions shall be classified in accordance with the internal Disciplinary Sanctions Policy OID 1.3.6.1.4.1.18332.101.45.34.

8.6. Conflict Resolution

In the event of a conflict between the different information or service owners within the organizational structure of the Information Security Policy, the matter shall be resolved by their hierarchical superior, with the mediation of the Information Security Officer, and escalated to the Information Security Committee for resolution if no agreement is reached.

In resolving such disputes, requirements arising from the protection of personal data shall always be taken into account.

8.7 Authorized Personnel for the Transport of Information Media

List of personnel authorized to routinely transport information media:

- Security Officer
- Systems Manager

The Security Officer may grant specific authorizations to other members of the organization to transport information media.

8.8 Procedure for the Appointment, Renewal, and Registration of Security Roles

Top Management is the competent authority for the appointment and removal of roles related to information security (e.g. Security Officer, Service Owner, System Owner), upon a reasoned proposal from the Security Officer or the relevant body. Minimum eligibility criteria shall include: adequate technical competence, demonstrated experience in similar roles, absence of conflicts of interest, and compliance with applicable legal requirements.

Appointments shall have a default term of two (2) years, renewable for equal periods following performance evaluation and suitability for the role. Any renewal shall be formally documented and justified in writing. Removal may take place at any time for justified reasons (e.g. non-compliance, loss of trust, incompatibility), applying a documented procedure that includes a hearing and resolution. In case of temporary absence or vacancy, an interim replacement shall be appointed for a maximum period of six (6) months, ensuring the formal handover of responsibilities and operational continuity.

Register: All appointments, renewals, removals, and replacements shall be recorded in the Mandate Register maintained by the Secretariat of the Security Coordination Body, accessible to Top Management and the Security Officer. At a minimum, the register shall include: position, name and identification document, date of appointment, start date of duties, term of office, appointment resolution, required specific training, and date of the last evaluation. Minutes, resolutions, and appointment records shall be archived in accordance with the ISMS document management policy for a minimum period of five (5) years after the end of the mandate.

9. Information Security Assets

ANF AC holds information that must be protected against risks and threats to ensure the proper functioning of its business. This type of information is essential to the organization's objectives and is referred to as an Information Security asset. Its protection is the objective of any Information Security Management System.

Assets may be divided into different groups according to their nature. Following the MAGERIT methodology (used by the Public Administrations) for asset classification, the following asset types are identified:

1. Essential assets: the information processed and the services provided. They define the security requirements for all other system components. These assets depend on more basic assets such as equipment, communications, facilities, and personnel.
2. Services: business processes offered externally (e.g. certificate issuance, time-stamping, OCSP responses) or internally (e.g. payroll, billing).
3. Data and information processed within the organization. These typically form the core of the system, while other assets support their storage and processing.
4. Software applications.
5. IT equipment.
6. Personnel: the main asset, including internal staff, subcontractors, customers' personnel, etc.
7. Communication networks supporting information flow, whether owned or outsourced.
8. Information media: physical media used for long-term data storage.
9. Supporting equipment: auxiliary assets not included in previous groups (e.g. document destruction equipment, environmental control systems).
10. Facilities where information systems are hosted (e.g. offices, buildings, vehicles).

In addition to these assets, intangible elements such as corporate image and reputation must also be considered. To protect information assets, it is necessary to identify and understand them within the organization. For this purpose, an asset inventory has been established, identifying and classifying them. Each asset includes, at a minimum, its description, location, and responsible owner.

The Information Security Management System has conducted a risk analysis by assessing threats and risks affecting the organization. This analysis shall be repeated:

- On a regular basis, at least once per year;
- When the information handled changes;
- When the services provided change;
- When a serious security incident occurs;
- When significant vulnerabilities are reported.

All aspects related to this area are detailed in the published document "Risk Assessment".

9.1. Risk Management

Services and infrastructures within the scope of this Policy shall be subject to a risk analysis to guide protection measures aimed at minimizing risks.

The ISO 27005 methodology shall be used as the baseline approach for conducting risk analyses.

The methodology's threat catalog shall be used as a starting point.

Risk analyses shall be carried out:

- Regularly, once per year;
- When significant changes occur in the information handled;
- When changes affect essential services or the infrastructures that support them;
- When a serious security incident occurs;
- When severe threats or significant vulnerabilities are identified that are not adequately addressed by existing controls.

According to the MAGERIT risk scale, the risk level shall be considered automatically acceptable when below HIGH level (i.e., the maximum acceptable residual risk shall be MEDIUM). Residual risk values above MEDIUM shall require explicit acceptance by the Security Committee, duly justified.

For unacceptable residual risk values, an appropriate Risk Treatment Plan shall be developed to reduce them to acceptable levels.

9.2. Acceptable Use of Assets

General principle: Assets shall be classified according to their value, legal requirements, sensitivity, and criticality for the organization.

Information, together with the processes and systems that use it, constitutes essential assets for achieving ANF AC's objectives. Information security must be ensured regardless of its form or medium (system data, printed documents, etc.). All information classified as an asset shall be properly categorized to ensure its security level, privacy, and long-term preservation.

9.3. Handling of Printed Information after Use

General principles:

- **Destruction**
  - **Paper media**: shall be disposed of in designated containers and subsequently destroyed under controlled conditions.
  - **Electronic media**: prior to disposal or reuse, data shall be securely erased or rendered unreadable.
- **Etiquetado**
  All information (electronic or paper) including the entity's corporate identity shall be automatically classified as Internal Use. Only the Security Officer may assign a different classification (e.g. Public or Confidential).

9.4. External Storage Media and Portable Devices

General principles:

- The use of privately owned external storage devices (e.g. hard drives, USB drives, optical media) is strictly prohibited on the organization's IT systems;

- The use of personal portable computing devices on ANF AC premises is strictly prohibited without explicit authorization from the Security Officer;
- The connection of smartphones, tablets, etc. to the ANF AC communication network is strictly prohibited without explicit authorization from the Security Officer;
- The removal of ANF AC portable equipment from its premises is strictly prohibited without explicit authorization from the Security Officer.

9.5. Workplace

Organizational IT equipment:

- Upon joining the organization, each individual receives the necessary work tools, acknowledging receipt through an onboarding process ("Welcome") and committing to their return through an offboarding process ("Exit").
- Access to such equipment shall be personal and shall use only the resources provided by the organization.
- Users shall ensure that the screen saver is automatically activated and that resuming activity requires proper authentication (unlocking mechanism).
- ANF AC follows a "clean desk policy", requiring documents to be stored in locked drawers and/or filing cabinets. It is strictly prohibited to:
  - Leave documents unattended;
  - Leave visible information such as:
    - Usernames and passwords;
    - IP addresses;
    - Contracts;
    - Invoices;
    - Account numbers;
    - Customer lists;
    - Intellectual property.
- ANF AC maintains a locked storage area with restricted access for authorized personnel, to be used for safeguarding:
  - Employee data / CVs;
  - Personal data of third parties external to the organization.
- ANF AC provides safes that shall be used for storing high-value information.
- ANF AC also maintains bank safety deposit boxes for the storage and custody of critical information.
- Each user identifier shall have associated privileges based on the user's role and responsibilities, allowing access to specific types of information.
- The use of a unique identifier enables traceability of user activities, ensuring individual accountability.
- Hardware and software modifications shall only be performed by authorized technical personnel or by third parties explicitly approved by the Security Officer.
- The use of corporate IT equipment for personal activities is prohibited.
- Access to internet websites not strictly required for organizational purposes is prohibited.

Printers, scanners, and photocopiers:

- Devices and operations shall not be left unattended, especially when printing or processing confidential information.

Email and other communication channels:

- Users shall be responsible for avoiding practices that may compromise information security.
  - Corporate email services are provided exclusively for operational and administrative purposes related to the organization.
  - All emails processed through corporate systems and networks are considered organizational property and do not guarantee privacy; therefore, corporate email accounts shall not be used for personal matters.
  - IMPORTANT NOTICE: ANF AC periodically monitors incoming and outgoing emails to improve quality management processes and security controls. The organization also maintains email recovery systems.
- It is prohibited to use email for:
  - Sending confidential or sensitive information via the Internet unless it is previously encrypted using a Security Officer-approved encryption system;
  - Creating, sending, forwarding, or storing emails with content that could be illegal or offensive (e.g. sexually explicit, racist, defamatory, abusive, obscene, discriminatory, or otherwise inappropriate);
  - Sending messages on behalf of another person or using falsified sender information.
  - Exceptionally, and only when authorized by Top Management, a secretary may send emails on behalf of management, clearly identifying themselves in the signature.
  - Users shall be reasonable regarding the volume and size of emails sent and stored.
  - Deleted or spam emails shall be permanently removed periodically.
  - Messages should be properly classified and stored in appropriate folders.
- Corporate communication channels shall not be used for private communications.
- IMPORTANT NOTICE:
- ANF AC records communications to improve management quality and security controls. A private communication line is available for urgent personal calls.

9.6. Incident Management

Potential incidents or events that must be recorded (this list is non-exhaustive and shall be extended as necessary, with particular emphasis on reporting even suspected anomalies) include:
General examples:

- Loss of service, equipment, or facilities
- System failures or overloads
- Human error
- Breaches of policies or guidelines

- Physical security breaches
- Uncontrolled system changes
- Software or hardware failures
- Unauthorized access attempts
- Events affecting user identification and authentication
- Events affecting access rights to data
- Incidents affecting media management
- Events affecting backup and recovery procedures

Incident prioritization according to impact

Critical: Emergency incidents requiring immediate resolution. Multiple incidents shall be handled in parallel, using all available resources. Examples include risks to human life, critical Internet infrastructure, or core certification services (e.g. CRL, OCSP, TSU, RA).

High: Incidents requiring priority handling over others, even if detected later. Managed in a dedicated queue and processed sequentially. Examples include privileged account compromise or denial of service incidents.

Medium: Incidents processed sequentially in order of arrival unless higher priority incidents arise. May escalate if unattended. Includes general system compromise or persistent network scanning.

Low: Incidents processed sequentially. May be automatically closed if not addressed within a prolonged period.

DENIAL OF SERVICE (DOS/DDOS)

Prevention:

- Systems shall be designed with sufficient capacity to handle expected loads;
- Technologies shall be deployed to prevent known attack types.

Detection and response:

- Mechanisms for detecting and managing DoS/DDoS attacks shall be implemented;
- Incident response procedures shall include communication with service providers.

Internal misuse:

- Measures shall be implemented to prevent the organization from being used as a source of attacks against third parties.

9.7. Confidentiality Commitment for Personnel

All personnel shall sign a confidentiality commitment during the onboarding process. This commitment shall remain valid even after termination of the employment relationship.

9.8. Certified Components

Criteria and controls shall be established for the selection, acquisition, integration, and verification of security products and services forming part of the system architecture. This applies to all security components, including hardware, software, managed services, and cloud-based solutions supplied by third parties.

9.8.1. Minimum Requirements

1. As a general rule, the Catalogue of ICT Security Products and Services (CPSTIC) of the Spanish National Cryptologic Centre (CCN) shall be used for the selection of products and services forming part of the security architecture.
2. If no product or service within the CPSTIC implements the required functionalities, a product certified in accordance with the provisions set out in Article 19 of Royal Decree 311/2022 shall be acquired.
3. Where the system provides security services to third parties within the scope of the ENS, the products supporting such services shall:
    a. Be included in the CPSTIC following the qualification process, or
    b. Provide certification demonstrating compliance with the functional and assurance requirements defined in Article 19.

10. Tools for Implementing the Security Policy

Since the Security Policy is written at a high level, it must be complemented by more detailed documents that support the implementation of its provisions:

- **Security Standards**: Standards standardize the use of specific aspects of the system. They define proper usage and user responsibilities and are mandatory in nature.
- **Security Guides**: Guides have a training-oriented purpose and aim to help users correctly apply security measures by providing explanations where precise procedures do not exist. They help prevent important security aspects from being overlooked, even when these may manifest in different ways. ANF AC provides various training programs tailored to each organizational area.
- **Security Procedures**: Security procedures address specific tasks, providing step-by-step instructions on what must be done. They are particularly useful for repetitive tasks.

For functional reasons, these elements are not always clearly separated; manuals, training courses, and security regulations may combine elements of all the above, with the objective of achieving greater effectiveness in user awareness and training.

Although mixed-format manuals and regulations can serve as important tools, it is often useful to clearly distinguish between the policy (abstract level) and its practical implementation. This approach provides greater flexibility and ensures consistency of results even when technologies or mechanisms change. Therefore, whenever possible, a clear distinction shall be maintained between these elements.

All documents published by ANF AC within the framework of its Security Policy are detailed in the document “Scope and Document Structure of the ISMS”.

Within the framework of the Information Security Management System, and in accordance with Clause 12.6.1 – Technical Vulnerability Management, the following shall be carried out:

- Maintaining up-to-date information from manufacturers and suppliers

Updates, whether security- or functionality-related, of control systems shall be governed by a patch management process that properly identifies their lifecycle and defines their frequency. Effective patch management in control systems must address two traditional challenges: the reluctance to introduce changes into systems that are operating correctly, and the limited tendency of some manufacturers to release patches addressing security issues. Fortunately, both limitations are increasingly becoming less significant.

11. Establishment, Implementation, Maintenance and Improvement of the ISMS / ENS

The deployment of the ISMS/ENS is initiated through the Risk Analysis, which makes it possible to determine the level of information security risk affecting the organization and to identify the necessary security controls and improvement opportunities for risk treatment, bringing risk to an acceptable level while taking into account the Context of the Organization.

Security controls shall be implemented, maintained, and continuously improved, and shall be available as documented information subject to review and approval by the Information Security Committee.

In compliance with Article 12 of Royal Decree 311/2022 (ENS), this Security Policy shall be developed by applying the following minimum requirements, which shall be included in the system documentation:

- Organization and implementation of the security process;
- Risk analysis and management;
- Personnel management;
- Professionalism;
- Authorization and access control;
- Protection of facilities;
- Acquisition of security products and contracting of security services;
- Principle of least privilege;
- Integrity and system updating;
- Protection of information at rest and in transit;
- Protection against risks arising from interconnected information systems;
- Activity logging and detection of malicious code;
- Security incident management;
- Business continuity;
- Continuous improvement of the security process.

In addition to applying the requirements of UNE-ISO/IEC 27001 and Royal Decree 311/2022, the CCN-STIC Security Guides shall be used. These include standards, instructions, guidelines, and recommendations developed by the National Cryptologic Centre (CCN) to improve the security level of organizations, particularly the CCN-STIC-800 series, which defines policies and procedures for implementing ENS security measures, as well as the Code of Practice for Information Security Controls (UNE-ISO/IEC 27002) within the ISMS.

Documented information regarding security controls shall be communicated to all personnel working within the organization (internal and external), who shall be obliged to apply it in the performance of their duties, thereby committing to compliance with ISMS/ENS requirements.

Documented information shall be classified as public, internal, or confidential, and used appropriately in accordance with such classification and the criteria established in the Information Classification, Labelling, and Protection Procedure.

Audits shall be conducted to review and verify compliance of the ISMS/ENS with the requirements of UNE-ISO/IEC 27001 for the ISMS and Royal Decree 311/2022 of 3 May regulating the National Security Framework

(ENS). Personnel within the scope of such audits shall cooperate fully to ensure their effectiveness, including the implementation of corrective actions derived from audits for continuous improvement.

12. Personnel Awareness

Information security is based on the ability to preserve its integrity, confidentiality, availability, and accessibility, through the elements involved in its processing: equipment, software, procedures, and the human resources that use these components.

In this regard, it is essential to educate and inform personnel from the moment they join the organization and on an ongoing basis, regardless of their employment relationship with the entity, about the security measures applicable to the performance of their duties and the expectations placed upon them in terms of security and confidentiality matters. Likewise, it is necessary to define the sanctions to be applied in case of non-compliance.

The implementation of the ISMS aims to minimize the likelihood of incidents. Therefore, it is necessary to implement mechanisms that allow weaknesses and incidents to be reported as soon as possible, so that they can be corrected and potential recurrence avoided. It is therefore important to analyze the root causes of incidents and learn from them in order to correct existing practices that failed to prevent them and avoid their recurrence.

12.1. Objective

To reduce the risk of human error, unlawful acts, improper use of facilities and resources, and unauthorized handling of information.

To clearly define information security responsibilities during the onboarding phase, include them in the agreements to be signed, and verify compliance throughout the individual's employment.

To ensure that users are aware of threats and responsibilities related to information security and are trained to comply with ISMS requirements during the performance of their regular duties.

To establish confidentiality commitments with all personnel and external users related to the handling of organizational information.

To establish the necessary tools and mechanisms to promote the reporting of security weaknesses and incidents, in order to minimize their impact and prevent recurrence.

12.2. Scope

This applies to all ANF AC personnel and personnel provided by third parties, regardless of their employment status, as well as to external personnel performing tasks for the organization.

12.3. Responsibility

The Legal and Human Resources Officer shall include information security responsibilities in job descriptions; inform all new personnel of their obligations regarding compliance with the Information Security Policy; manage confidentiality commitments with personnel; coordinate user training activities related to the Policy.

The Security Officer shall be responsible for monitoring, documenting, and analyzing reported security incidents; communicating such incidents to the Information Security Committee and to the relevant information processing stakeholders.

The Information Security Committee shall establish the necessary mechanisms and channels to enable the Security Officer to manage incident and anomaly reports; be informed of incidents, monitor investigations, oversee their evolution, and promote their resolution.

The Legal and Human Resources Officer shall also participate in drafting confidentiality commitments to be signed by employees, contractors, and third parties; provide guidance on sanctions for non-compliance with ISMS requirements; participate in the handling of security incidents requiring their involvement.

All ANF AC personnel shall be responsible for reporting any identified security weaknesses and incidents in a timely manner.

13. Capacity Planning

Capacity sizing / management

For each project, as well as for the organization's core infrastructure, the following shall be considered:

- Processing requirements;
- Information storage requirements, both during processing and for the required retention period;
- Communication requirements;
- Personnel requirements: number and professional qualifications;
- Facility requirements and supporting resources;
- Continuous improvement of capacity management.

For new projects, a study shall be conducted prior to go-live to determine the requirements for each of the parameters listed above.

Capacity forecasting shall be carried out and kept up to date throughout the entire lifecycle of the system.

13.1 Responsibility

The Development and Technology Manager shall: monitor the development environment, including projected consumption of RAM, storage, and processing capacity; assess the capacity requirements of systems in operation and forecast future demands, in order to ensure adequate processing and storage capacity.

The Systems Manager shall: determine the capacity requirements of systems in operation and forecast future demands to ensure adequate processing and storage; take into account new system requirements, as well as current and projected trends in the organization's information processing over the defined lifecycle of each component;

Report identified capacity requirements that may prevent potential bottlenecks which could pose a threat to security or processing continuity, and plan appropriate corrective actions.

The Development and Security Managers shall define approval criteria for new information systems, updates, and new versions, requiring the necessary testing prior to final approval. The following aspects shall be considered:

- Verifying the impact on performance and capacity requirements of computer systems;
- Ensuring error recovery mechanisms;
- Preparing and testing routine operational procedures in accordance with defined standards;
- Ensuring the implementation of security controls;
- Designing continuity plans for organizational activities;
- Ensuring that the deployment of new systems does not negatively affect existing systems, particularly during peak processing periods;
- Considering the impact of new systems on the overall security of ANF AC's technological infrastructure;
- Developing training plans for the operation and/or use of new systems.

13.2 Cryptographic Responsibility

Areas making use of cryptography shall be subject to supervision by the Compliance Officer.

14. Personal Data

ANF AC shall apply the principles established in the General Data Protection Regulation (GDPR) when processing personal data.

ANF AC has a Privacy Policy, and its reading is strongly recommended: https://anf.es/politica-de-privacidad/

A summary of the main relevant elements is provided below:

- Principle of "lawfulness, fairness and transparency": Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- Principle of "purpose limitation": Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Principle of "data minimization": Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- Principle of "accuracy": Personal data shall be accurate and, where necessary, kept up to date. ANF AC shall take all reasonable steps to ensure that inaccurate data are rectified or erased without delay.
- Principle of "storage limitation": Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed. Once such purposes have been fulfilled, the data shall be deleted or, at least, anonymized.
- Principle of "integrity and confidentiality": Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
- Principle of "accountability": ANF AC shall implement appropriate technical and organizational measures and be able to demonstrate that processing is performed in accordance with the GDPR.

ANF AC shall implement security measures to guarantee the fundamental right to data protection by ensuring the confidentiality, integrity, and availability of personal data. Such measures shall be appropriate to the level of risk, taking into account the likelihood and severity of risks to the rights and freedoms of individuals, in accordance with Article 32 of the GDPR.

With regard to security measures in the public sector, ANF AC shall comply with the First Additional Provision of Organic Law 3/2018 (LOPDGDD), which requires entities listed in Article 77.1—including public sector foundations such as ANF AC—to apply the security measures set out in the National Security Framework (ENS) to personal data processing, and to promote an equivalent level of implementation among affiliated private entities.

Where applicable, ANF AC shall carry out a Data Protection Impact Assessment (DPIA) in accordance with Article 35 of the GDPR.

Appropriate technical and organizational measures shall be implemented in accordance with Articles 24 and 32 of the GDPR, including, among others: pseudonymization and encryption; access control mechanisms; activity logging; periodic evaluation of the effectiveness of security measures.

ANF AC maintains a Record of Processing Activities for personal data, containing the elements required under Article 30 of the GDPR.

15. Security Organization

15.1. Published Policies and Documents

The detailed list of all documents published and approved by the organization, including a summary explanation of their purpose and regulatory references, is described in the document "Scope and Document Structure of the Information Security Management System" (OID 1.3.6.1.4.1.18332.101.79.1), of which this document forms part.

This Information Security Policy shall be developed through the creation of additional policies or security regulations addressing specific aspects. Based on these policies and regulations, procedures may be developed describing how they shall be implemented.

The Information Security Policy is mandatory and is structured in the following hierarchical levels:

- First level: Information Security Policy
- Second level: Information Security Standards
- Third level: Information Security Procedures and Technical Instructions
- Fourth level: Reports, records, and electronic evidence

Additional documentation

Where appropriate, procedures, standards, and STIC technical instructions, as well as CCN-STIC guidelines, may be followed at all times.

Review and Approval

This document and all documents prepared and approved by ANF AC shall be reviewed at least every two years, or whenever circumstances warrant a revision.

This Information Security Policy has been approved by Top Management, within the framework of CCN-STIC series 400, 500, 600, and 800.

15.2. Internal Audits and Continuous Improvement

The organization shall ensure the execution of periodic internal audits of the Information Security Management System (ISMS), in accordance with applicable regulations, with the aim of verifying the effectiveness, adequacy, and continuous improvement of the system.

Requirements:

1. Frequency of internal audits
   - Comprehensive internal audits of compliance with applicable regulations shall be carried out, covering all requirements derived from the system's category, as well as any justified exclusions, in years where external certification audits are not performed (biennial in the case of the ENS).
   - Additionally, partial internal audits shall be conducted annually, covering at least half of the applicable requirements, ensuring continuous and systematic review.
2. Monitoring of corrective and improvement actions

- Findings identified during internal audits shall lead to the initiation of corrective and improvement actions, which shall be documented, prioritized, and monitored until closure.
- The Security Officer, in coordination with the System Owner and the Service Owner, shall oversee the monitoring of these actions, ensuring the continuous improvement of the ISMS.

3. Integration with risk management and regulatory compliance
   - Audit results shall be integrated into the risk management process and reviewed by the Security Committee, ensuring consistency with risk assessment and treatment.
   - Compliance with applicable regulatory obligations (ISO/IEC 27001, ENS, NIS2, etc.) shall be ensured, including requirements for traceability, documented evidence, and reporting to competent authorities when applicable.
4. Continuous improvement actions
   - In addition to audits, additional reviews, self-assessments, cross-checks between departments, or any other measures that promote continuous improvement of the ISMS and the security of information systems may be carried out.