Translated from Spanish to English - www.onlinedoctranslator.com

Quality and ISMS Manual

or 171,443. CIF G-63287510.

© ANF Certification Authority

Corporate headquarters: Paseo de la Castellana, 79 - 28046 - Madrid

Administration and Legal Services: GV Corts Catalanes, 996 -08018 - Barcelona Telephone: 902 902 172 (Calls from Spain) - International (+34) 933 935 946

Fax: (+34) 933 031 611 · Web: www.anf.es

Security level

PUBLIC

Important announcement

This document is the property of ANF Certification Authority

Its reproduction and dissemination is prohibited without the express authorization of ANF Certification Authority

Copyright © ANF Certification Authority 2013 - 2018

Document control

Version	1.3
Author	Moses Amador
Creation date	04/15/13

Modification Control

Date	Modified by	Reason
06/26/2013	Moses Amador	Expansion and upgrade
07/10/2013	Moses Amador	Update list of documents and organization chart
09/03/2018	MariCarmen Mateo	Upgrade

Approval Control

Date	Responsable	Comments
06/26/2013	Florencio Diaz	Approved
07/10/2013	Florencio Diaz	Approved
09/03/2018	Florencio Diaz	Approved

Index

1 Presentation of ANF AC

ANF Certification Authority (ANF AC - 1997), born within the National Association of Manufacturers of Spain (ANF - 1980). Initially as an R + D + i Division specialized in cryptography and computer security, it developed the entire technological platform that allows ANF AC to develop its activity as a certification entity.

In 2000, ANF AC acquired its own legal entity. That same year, the Ministry of Science and Technology was notified of the start of activity as an issuer of electronic signature certificates, requesting its registration in the official registry of certification authorities in accordance with the legislation in force at that time.

ANF AC was the **first entity in Spain** in issuing recognized electronic certificates. Currently ANF AC is officially accredited as a Qualified Trust Service Provider, and approved by the entire state, regional and municipal public administration.

Our success is due to a single cause: continued investment in **R + D + i** to equip users with innovative technology. Equally important is our commitment to customers when meeting their needs, creating**scalable and interoperable products and services** for any sector.

ANF AC, in all its lines of products and services, assumes the commitment to use the most advanced technology and develop all the necessary elements for its putting into operation. ANF AC does not use third-party software, it guarantees full control and support from the source.

ANF AC was a pioneer in offering as standard in all its approved devices, signatures with **time stamp** and **validation at source.**

ANF AC has its own subsidiaries in Malta, Ecuador, Peru, Cuba, the USA and Hong Kong.

ANF AC has been assigned the private company code (SMI Network Management Private Enterprise Code) 18332 by the international organization IANA, (Internet Assigned Numbers Authority), under the iso.org.dod.internet.private.enterprise branch (1.3.6.1. 4.1 -IANA –Registered Private Enterprise-).

ANF AC is committed to the United Nations Global Compact, it has been part of the Spanish organization since 2013. The Governing Board of ANF AC is committed to the principles ten principles that encompass a corporate social commitment on Human Rights , Labor, Environment, Anti-Corruption. For its monitoring and compliance, it follows the guidelines of ISO 26000.

ANF AC, we declare in all our actions as corporate values:

- Honesty, integrity, transparency, independence, impartiality, confidentiality, and professionalism.

- Trust in the services of ANF AC, through certification mechanisms carried out by independent auditors against internationally recognized norms and standards.

ANF AC follows and respects the Triple Balance business philosophy, in which profitability is one of the objectives that business activity has to pursue, along with sustainability and social commitment. ANF AC only intervenes in areas that may have a relationship with certification services, which presuppose a competitive improvement for the organization through the incorporation of clearly differential elements. In addition, it must bring improvements to society and presuppose a novelty in the market.

1.1 Legal entity

ANF Certification Authority, (hereinafter ANF AC), is a legal entity, established under Organic Law 1/2002 of March 22 and registered in the Ministry of the Interior with national number 171.443 and CIF G-63287510.

1.2 Financing

ANF AC is financed with its own resources generated by the activities it develops.

ANF AC, responds with all its assets to face possible legal responsibilities as indicated by the regulations, has CR Policies that guarantee its responsibility in accordance with current legislation:

- Insurer: CFC Underwriting Limited (Lloyd's of London). Branch:
- Professional Civil Liability.
- Insured coverage: Five million euros (€ 5,000,000). Policy number: BA
- 059760 A.

ANF AC, is an organization with a business experience of more than fifteen years. During this entire period of time, ANF AC has had no incidence whatsoever. ANF AC guarantees financial stability, has sufficient financial resources to meet its long-term commitments. Their budgets are consistent and all their business development is based on their own resources.

ANF AC has different subsidiaries, all of them are independent legal entities in which ANF AC does not assume relevant financial commitments.

The Governing Board of ANF AC is the body responsible for guaranteeing the financial stability of the entity.

1.3 Subcontracting

ANF AC does not have contractors in the terms defined by the ISO 17024 standard.

1.4 Accreditations

ANF Certification Authority is officially recognized by the Ministry of Industry, Commerce and Tourism as a Qualified Provider of Trust Services in the areas in which it provides its services:

- Qualified Electronic Signature Certificates Qualified
- Electronic Seal Certificates Qualified Electronic
- Time Stamps SSL Secure Web Certificates
-
- Qualified Electronic Signature Devices (*Resolution Ministry and certifications of conformity ISO 15408 Common Criteria EAL 4+ and 5+)*
- Electronic Signature Validation Service (*pending, how much with conformity audit)*
- Electronic Stamp Validation Service (*pending, how much with conformity audit)*

ISO 27001 Compliance Audit

Applied to the Provision of Electronic Signature Certification Services.

Auditor: GUARDIAN

ISO 9001 Compliance Audit

Auditor: Quality Management System (QMS)

ETSI Standards Audit

Service	Usually	In scope	Profile / semantics
Signature creation, verification and validation electronic	EN 319 401	EN 319 411-1 EN 319 411-2	EN 319 412-1 EN 319 412-2 EN 319 412-3 EN 319 412-4 EN 319 412-5
The creation, verification and validation of electronic stamps.	EN 319 401	EN 319 411-1 EN 319 411-2	EN 319 412-3
The creation, verification and validation of electronic time stamps.	EN 319 401	EN 319 421	EN 319 422

Auditor: CSQA Italia

ISO 17024 - AEPD-DPD Certification Scheme

In process. Provisional authorization from the Spanish Data Protection Agency

1.5 Organizational structure

The Governing Board of ANF AC is the entity's administrative body in the sense established by the ISO 17024 standard. There is a President of the Governing Board who is the commercial factor of the organization, who in turn assumes the functions of Director General, at the head of the Executive Directorate, with the maximum responsibility in making certification decisions.

Also part of the Executive Directorate, the Legal Director with advisory functions in the adoption of decisions by the Director General.

An advisory body called **"Committee of Experts",** also known as the Impartiality Committee, where the participation of all parties involved in the process of certifying people is guaranteed. Its function is to protect the independence and impartiality of the governing body of ANF AC, in its decisions in relation to certification in all areas of action. It also performs appeal resolution functions, in the event that the candidate appeals the examination review carried out by the Evaluator, or other decisions on certification.

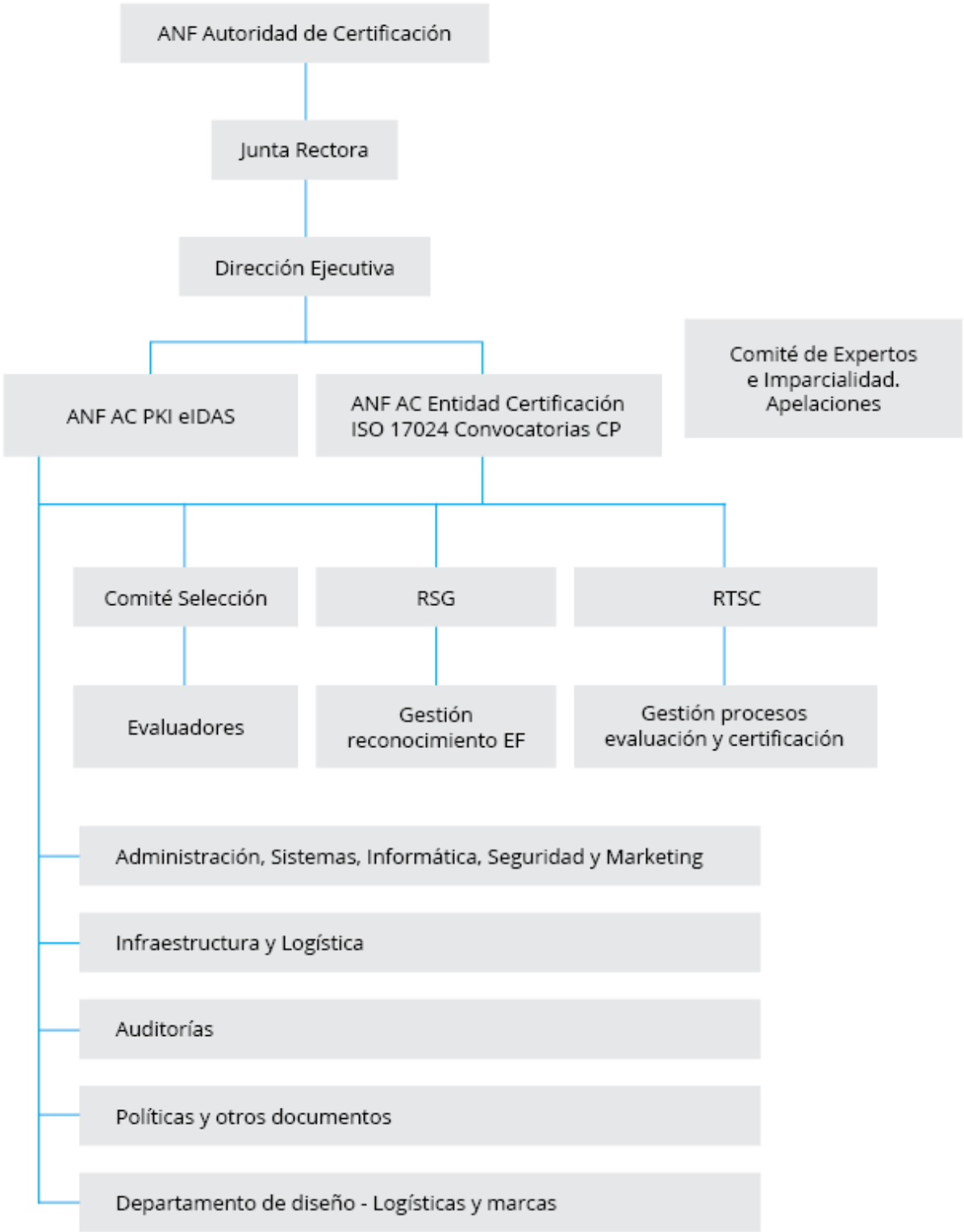
In cases where there may be a conflict of interest, after hearing the Committee of Experts, it will decide whether to challenge.

The requirements of the jobs, functions and responsibilities are defined in an internal document, which is complemented by those described in the procedures and instructions of the certification system.

There are no Related Bodies in the terms defined in the ISO 17024 standard that could compromise their independence and impartiality.

The Legal Directorate of ANF AC is responsible for the function of Data Protection Delegate and, in coordination with the General Directorate, that of *Compliance Officer.*

The following is the organization chart of the organizational structure of ANF AC.


ANF Autoridad de Certificación
Junta Rectora
Dirección Ejecutiva
ANF AC PKI eIDAS
ANF AC Entidad Certificación ISO 17024 Convocatorias CP
Comité de Expertos e Imparcialidad. Apelaciones
Comité Selección
RSG
RTSC
Evaluadores
Gestión reconocimiento EF
Gestión procesos evaluación y certificación
Administración, Sistemas, Informática, Seguridad y Marketing
Infraestructura y Logística
Auditorías
Políticas y otros documentos
Departamento de diseño - Logísticas y marcas

2 objective

ANF has established an Information Security and Quality Management System (hereinafter, SGCSI) based on the ISO 9001 standard and on the ISO / IEC 27001 standard with the aim of establishing a process of continuous improvement of quality and security of the information.

This document establishes the general security measures, aimed at ensuring the integrity, availability, access control of authorized persons and conservation of the information. In addition, it establishes the Quality Policy of ANF AC.

Fundamental states of information: transmission, reception, storage and publication. The information must be adequately protected whatever the form it takes or the means used in said states.

Likewise, the information has the following security-related characteristics:

- Confidentiality: characteristic that prevents against the making available, communication and disclosure of information to unauthorized individuals, entities or processes.
- Integrity: characteristic that ensures that the information has not been transformed or modified in an unauthorized way during its processing, transport or storage, easily detecting possible modifications that may have occurred.
- Availability: characteristic that ensures that authorized users have access to the information when required and prevents against attempts to deny the authorized use of it.
- Authenticity: characteristic by which the identity of the user who originates an information is guaranteed. It allows to know with certainty who sends or generates specific information.
- Information preservation: in a broad sense, it is the set of processes and operations that work together to stabilize and protect documents from deterioration. When talking about the management of digital resources, whatever their form or function, all the stages that make up the life cycle of documents must be taken into account in order to apply preservation measures as soon as possible. Therefore, more than an intrinsic characteristic of the information, reference is made to the management of the information life cycle.
- Traceability: characteristic of the information that ensures knowledge of key aspects of the creation, modification and consultation operations, such as: who carried out the operation? When was the operation carried out? What results did the operation have?

Information security requires a preventive approach adapted to the dynamics of use of the information generated. Only in this way will it be possible to preserve the information, safeguarding the guarantees described, and complying with the laws that affect data processing.

2.6 Scope and exclusions

The scope of this document reaches:

- The products and services marketed by ANF AC, in all its areas of activity.

- The applications, infrastructure and technological components (network elements, services, user equipment, peripherals), necessary for the development of the activity.
- The information processed, that is, all the information that ANF AC staff collects, guards or creates, in any type of medium or state.
- Organizational processes regarding the use of applications.

2.7 Normative references

This document has been prepared taking into account compliance with the following legal and technical standards applicable to the activity carried out by the organization:

LAWS

- **Regulation (EU) 910/2014 of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market.**
- **Law 59/2003, of December 19, on electronic signature.**
- **Regulation (EU) 679/2016 of April 27, 2016 regarding the protection of natural persons with regard to the processing of personal data and the free circulation of these data.**
- **Organic Law 15/1999, of December 13, on the Protection of Personal Data.**
- **Royal Decree 1720/2007, of December 21, approving the Regulations for the development of Organic Law 15/1999, of December 13, on the protection of personal data.**
- **Law 34/2002 on Services of the Information Society and Electronic Commerce (LSSI).**

TECHNICAL RULES

- **ISO / IEC 27001**
- **Iso 9001**
- **ISO 17024**
- **ETSI Standards - Trust Services**

3 Administrative processes

Administrative processes of ANF AC, general requirements:

I. Application process and processing of the service or product

1. Service requests can only be made in:
    to. Points officially accredited by ANF AC. These points have an accrediting panel in a visible place and are published on the corporate website of anf.es
    b. Online service on the corporate website of anf.es, with SSL OR TLS communication protocol.

2. Applicants must identify themselves by means of a valid legal document. In general:
    to. In person by means of: DNI, passport or residence card. Always with a photograph that allows the holder to be recognized.
    b. Electronically: through the use of a recognized electronic certificate.

3. Applicants have to determine the service or product, ANF AC assumes responsibility:
    to. Check the adequacy of the service or product with respect to the applicant.
    b. Clearly and accurately report the scope and limitations of the service or product.
    c. Establish the price of the service.
    d. Document the characteristics of the service or product.
    and. Provide standardized document to formalize the request. Normalizing a document at a minimum requires:
        i. Be personalized with the ANF AC letterhead.
        ii. Have an OID code that uniquely identifies it in the list of documents published by ANF AC.
        iii. When the type of document requires it, you must also:
            1. Have a version control.
            2. Establish a safety range.
            3. Author and approval date.

4. Applicants have to formally agree to requests for service or product. This procedure can be done by:
    to. In person: handwritten signature or sufficient power of attorney.
    b. In electronic form: electronic signature recognized in accordance with current legislation is required:
        i. The signature must have been prepared with a qualified electronic signature certificate.
        ii. The signature must have been generated with a qualified electronic signature creation device.
        iii. The issuer of the certificate must have and provide trusted third parties with a validation device for qualified electronic signatures that complies with the provisions of article 32 of Regulation (EU) 910/2014.

iv. The electronic signature must allow its long-term conservation, for this, AdES LTV signatures are required in accordance with the ETSI reference standard according to the XAdES, CAdES or PAdES format.

5. Applicants have the right and ANF AC the obligation, to provide prior to the formal acceptance of documents:

to. Read the content of the documents to which your adherence is required.

b. Receive advice on any queries or doubts they may have, whether of a technical, legal or merely functional nature.

c. Receive a copy of the documents they have signed.

d. Receive information on the warranty associated with the service or product.

and. Have channels and procedures that allow you to submit complaints, claims or reports.

6. ANF AC must comply with the obligations established in the legal regulations, especially regarding data protection.

7. ANF AC uniquely identifies each request, granting an identifier that enables each request process to be located and audited.

8. When the request requires encrypted material or with access control through secret passwords, especially seeds of electronic certificates, ANF AC will communicate them privately and securely, for this it may use different means between the trusted mailboxes that have been communicated by the applicant or even a combination of them, eg email, SMS, push notifications, letter, etc.

9. ANF AC does not store passwords of its clients, using SHA56 digestion algorithm.

10. Users of ANF AC's online systems have the ability to manage their access passwords, and configure their security requirements in credentials based on electronic certificates.

11. ANF AC, does not intervene in the generation of RSA asymmetric keys, it provides the necessary technology for each user to generate their public and private key pair.

II. Service renewal process

1. The user, before the expiration date of the service, is notified in writing by ANF AC.

2. ANF AC, provides information and advice to renew the service.

3. ANF AC, informs in a clear and precise way the price of renewal of the service.

III. Process of revocation or cancellation of a service

1. The user has different communication channels and procedures for the early cancellation of a service.

2. ANF AC, provides information and support that allows all users to cancel services without undue delay.

3. ANF AC, will register without undue delay the cancellations of service that occur, and will provide all users who request it, proof of revocation or cancellation.

IV. User incident treatment process

1. Reception of the incident:

   to. If the incident is attended by telephone, the incident is recorded in an mp3 file that will be attached to the incident ticket. Requirements:
      i. Every user will be informed that a recording will be made for reasons of security and quality of service.
      ii. Each incident is registered with a unique identifier associated with an incident ticket.

   b. If the incident is dealt with by any other means, the incident ticket is generated directly, which must have a unique identifier.

   c. Each identifier must allow the location of the associated ticket.

2. The incident ticket is assigned:
   A typology, level of severity / urgency, contact details, mp3 file (if any), any other file referring to the incident, explanation of the incident, and an agent who will attend to the incident.

3. The incident is dealt with by the assigned person.

4.- Once the incident is resolved, the incident is closed with information on the resolution applied.

5.- Whenever possible, users will have online access to incident processing files.

.

V. Process of validation of a service

1. Each service request is verified by an operator specialized in the required service.

2. Each request must receive formal confirmation from a responsible operator.

3. ANF AC, has a formal procedure to accept, deny, or request documentary extension from users. The decisions that are adopted are communicated in writing to the interested parties.

4. The interested parties have communication channels and procedures to appeal those decisions that they consider contrary to the regulations.

5. All procedures have established time limits, clearly setting the beginning and end.

SAW. Service or product supply process

1. Each service clearly and precisely identifies the moment in which the supply and materialization of the service provision takes place. Establishing a term that allows the user to determine the adequacy of the service received with the service that he contracted.

2. Each product supplied is delivered safely and establishing the moment in which it is produced. From that moment on, the warranty period begins.

3. In those cases in which the user must activate the service or collect the product, the delivery date is set at 24 hours. in which the user receives the communication of his
made available.

4 ISMS flows

The following ISMS procedures are identified. Each of them is documented with its slack diagram, and has its corresponding operator.

- ➢ Operators: Hiring, Training and Control.
- ➢ Preparation, approval and administration of documentation.
- ➢ Internal audits.
- ➢ New data processing.
- ➢ Registration process Calls.
- ➢ Calls execution process.
- ➢ Evaluation process.
- ➢ Reviews and Appeals
- ➢ Complaints and claims
- ➢ DPD Certification Process
- ➢ AR and EF audit
- ➢ Preparation, approval and administration of documentation
- ➢ Continuous improvement SGCSI

5 Responsibility of the senior management of ANF AC

5.1 Commitment

The senior management of ANF AC has acquired the commitment with the establishment, implementation, operation, monitoring, review, maintenance and improvement of the SGCSI. To do this, it has taken the following initiatives:

- Establish a quality and information security policy.
- Ensure that ISMS objectives and plans are established.
- Establish roles and responsibilities for quality and information security, as well as a policy of disciplinary sanctions in case of non-compliance.
- Communicate to the organization both the importance of achieving the information quality and security objectives and of complying with the quality and security policy, as well as its legal responsibilities and the need for continuous improvement.
- Allocate sufficient resources to the ISMS in all its phases.
- Decide on the risk acceptance criteria and their corresponding levels.
- Ensure that internal audits are performed.
- Hire and ensure that audits are performed by independent, highly prestigious auditors against internationally accepted standards.

5.2 Resource allocation

For the correct development of all activities related to the ISMS, the allocation of resources is essential. ANF's senior management ensures that sufficient resources are allocated to:

- Establish, implement, operate, monitor, review, maintain and improve the ISMS.
- Ensure that information quality and security procedures support business requirements.
- Identify and address all legal and regulatory requirements, as well as contractual security obligations.
- Correctly apply all the implemented controls, thus maintaining quality and adequate safety.
- Conduct reviews when necessary and act appropriately based on the results of the themselves.
- Improve the effectiveness of the ISMS where necessary.

5.3 Training

ANF AC ensures that all personnel with responsibilities in the SGCSI are competent to perform the required tasks.

Staff are provided with the necessary training and the effectiveness of the actions taken is evaluated.

Records of the education, training, skills, experience and qualifications of ANF AC personnel involved in the ISMS are kept.

It ensures that anyone who has access to the assets knows and accepts their responsibilities regarding the security of the information systems and resources with which they work. The main guarantee to cover is confidentiality.

In addition, it also ensures that all relevant personnel are aware of the importance of their information security activities (including security requirements and legal responsibilities) and of how they contribute to the achievement of the objectives of the ISMS.

5.4 Statement of impartiality

Senior management, all area managers and operators involved in certification actions, have signed Declarations of Impartiality.

5.5 Confidentiality commitments

Senior management, all those responsible for the area and operators involved in actions of certification, they have signed confidentiality commitment documents.

6 Definition, implementation and operation

6.1 Documentation requirements

ANF AC has established all the records and documented procedures required by the reference technical standards, as well as all those it has considered necessary to demonstrate compliance with the quality and information security requirements.

Through its document control and records control procedure, it defines the actions necessary for the management of documents and records. For its management, it administers the document called "Structure of OID's of ANF AC" with OID 1.3.6.1.4.1.18332.45.4.1, which contains the complete list of documents published by the organization.

ANF AC, has secure repositories of documentation.

6.2 Quality policy of ANF AC

Published on the ANF AC corporate website, and identified with the OID 1.3.6.1.4.1.18332.101.40.1

At ANF AC we are aware that the needs of our clients are the exact measure for the quality of our customer service. Satisfaction is the key to the success of our company and we try to get the customer to return to us and not to the product we supply.

Therefore, it is our primary goal to meet the demands of our customers in terms of product quality, diligent service, friendly treatment, honest advice and faithful compliance with the commitment to supply error free. It is of the utmost importance for us to improve in everything on a daily basis and introduce innovations as the best means of maintaining the loyalty of our customers.

Recognized AR collaborators and recognized Training Entities are the most important capital of our company to achieve success. We assume the responsibility of giving them adequate training, providing them with all the necessary tools and means of work in addition to creating optimal professional relationships with them. We take care of these resources by giving them the important strategic value they have.

Both as an individual person or as a member of a team we are responsible for our actions and the results that come from them. Full knowledge of the responsibilities that the position implies and the responsibilities assumed by the organization as a Qualified Provider of Certification Services, or as a Personnel Certification Entity is essential. Each process in which we intervene is regulated by legal regulations and technical standards that must be known and respected.

The work environment is a primary factor in fostering positive communication and employee dedication. It is one of our objectives to monitor the health and well-being of each of them. Respect for the feeling of personal fulfillment through a professional activity is a priority objective for
the organization.

The sum of intelligences gives rise to greater intelligence and to achieve this, the involvement of all the people who are part of the Organization is necessary.

This is only possible through the correct evaluation of the effort, providing opportunities in an equitable way, providing sufficient autonomy so that each one can perceive the fruit of their work, while the Organization prioritizes honest and transparent support among colleagues, and a global vision of all the processes that make up the service our clients receive.

Our goal is excellence, to achieve this it is necessary to respond to all the needs of our customers, and analyze and respond to their dissatisfactions. For this, it is necessary to increase the efficiency and quality of our services and products through continuous improvement.

6.3 Code of conduct

Published on the ANF AC corporate website, and identified with the OID 1.3.6.1.4.1.18332.105.12

6.4 Privacy Policy

Published on the ANF AC corporate website, and identified with the OID 1.3.6.1.4.1.18332.101.20.1

6.5 Guarantee of products and services

Statement published on ANF AC's corporate website,

STATEMENT

ANF AC, as well as the manufacturers that integrate ANF AC devices or components into their products and other suppliers that distribute it, guarantee that:

The software works substantially in accordance with the provisions of the accompanying written materials, for a period of ninety (90) days from the date of receipt.

In general, the hardware associated with ANF AC solutions is free from defects in material and manufacturing, with normal use and service, for a period of one (1) year from the date of receipt.

The equipment delivered on assignment of use has an unlimited warranty. In those equipments that include a warranty extension, the coverage will attend to what is specified therein.

Some countries do not allow limits to be established on the duration of a tacit guarantee, so it is possible that the aforementioned limitation is not applicable, and must be adapted at most to the current legislation in each applicable case.

In case of application of the guarantee, the total responsibility of ANF AC, that of the software manufacturer, that of the distributor or that of the integrators that install it, and that, where appropriate, has supplied the devices.
from ANF AC, it will be optional:

The refund of the price paid.

The repair or replacement of software or hardware that does not comply with this Limited Warranty that is returned to the Software Manufacturer or distributor or integrator with a copy of the purchase receipt.

This Limited Warranty is void if the software or hardware fails as a result of accident, abuse, unauthorized manipulation or misapplication.

Accreditation in the signature document of the secure signature device used to generate it.

Equipment replaced

Replaced software and hardware will be guaranteed for the remainder of the original warranty period or for thirty (30) days, whichever is longer of both periods. The return of the product is excluded from this limited warranty due to its unsuitability for the user's needs.

No liability for consequential damages

To the maximum extent permitted by applicable legislation, neither ANF AC Certification Authority, nor the Software Manufacturer, nor its suppliers, nor integrators will be liable for damages (including, among others, direct or indirect damages due to injuries to people, profit business interruption, loss of business information or any other pecuniary loss) arising from the use or inability to use this product, even if the Software Manufacturer, supplier or integrators have been informed of the possibility of such damages .

In any case, all the responsibility of the Manufacturer, its suppliers or integrators, by virtue of any stipulation of this contract, will be limited to the amount actually paid per user for the software and / or hardware of ANF AC.

Some countries do not allow the exclusion or limit of liability with respect to consequential or contingent damages, so it may happen that the aforementioned limitation does not apply to them.

6.6 ANF AC security policy

The security policy is the high-level statement of objectives, guidelines and commitments of ANF AC, to undertake the management of information security in the electronic, computer and telematic means used in the provision of the service. This security framework will be supported by a set of security measures, procedures and tools for the protection of information assets.

ANF AC, has different specific documents related to information security.

6.7 Organization of information security

ANF AC manages information security through the approval of the quality and information security policy, assigning security roles and coordinating and reviewing the implementation of quality and security throughout the organization.

It also ensures the maintenance of the security of information resources and assets that are accessible by outsiders through the control of any access to ANF information and the information processing carried out by outsiders.

ANF AC provides organizational means that allow initiating, achieving and maintaining the implementation of information quality and security objectives.

Independent reviews of existing vulnerabilities, associated risks and established controls will be carried out.

In addition, in the case of the provision of services by third parties, ANF analyzes the existing risks and ensures that there is effective management of them.

6.8 Asset management

ANF AC ensures adequate protection of assets (including maintenance, inventory and classification), identifying the owners of these assets, whose responsibility is to maintain adequate controls over them. All the media and supports that transmit, store and process information are taken into account and a classification will be made to ensure that the information receives an adequate level of protection.

This classification will allow to indicate the need, priorities and degree of protection expected for the information handled. Asset management has a special impact on the guarantee of confidentiality and it is important to state the duty of those responsible to comply with the security guarantees defined in the introduction: confidentiality, integrity, availability, authenticity and preservation of the information.

ANF will prepare an inventory of the information assets of the computer applications it has, ensuring that there is a person responsible for each of the assets.

6.9 Human resource security

Any person from ANF AC who has access to the inventoried assets within the indicated scope (own and subcontracted personnel) knows and accepts their responsibilities regarding the security of the information systems and resources with which they work (before hiring, during their working life and once your employment relationship has ended).

Therefore, it is intended to cover confidentiality through the use of clauses referring to the obligations and responsibilities of employees. Another objective is to cover the risk of theft, fraud and misuse of the facilities.

All personnel will be informed so that they are aware of the importance of safety and that they know what is expected of them, what their responsibilities are and that they accept them.

ANF AC establishes a communication plan that includes safety training sessions for all employees.

6.10 Physical and Environmental Security

ANF AC secures the tangible assets described through access controls. The guarantees that are covered are the availability, integrity and confidentiality of the information.

The infrastructure that supports the development of the company's activities, as well as the storage media that are used, which reside in its building and in that of the suppliers of

service or third parties are protected against physical damage or theft using physical access control mechanisms that ensure that only authorized personnel have access to them.

Therefore, said infrastructure will be located in areas with restricted access, with different levels of security, which can only be accessed by duly authorized personnel. The accesses to each of the levels are registered by access control mechanisms, being available for subsequent audits.

6.11 Communications and Operations

ANF AC ensures the correct and safe operation of the information processing means.

Responsibilities and procedures are established for the management and operation of all information processing means; as well as for the management and control of third-party services. Procedures have also been defined for the management of customer relationships, the purchasing process and equipment control.

Segregation of duties is implemented, where appropriate, to reduce the risk of deliberate or negligent misuse.

Appropriate controls and measures will be introduced to prevent and detect the introduction of harmful software, and to avoid the infection of information systems.

Procedures are established for making backup copies and their recovery.

Adequate procedures are established to protect documents and supports, when necessary; as well as the storage, handling, transport, destruction and disposal accessible and recoverable only by authorized personnel.

The exchanges of information and software between organizations are controlled, which will comply with all current legislation and with previously established formal agreements.

6.12 Access Control

ANF AC has developed the necessary procedures for access control that ensures authorized user access and prevents unauthorized access to network services, operational services, information maintained in application systems and information systems by unauthorized personnel.

It is taken into account:

- Registration and de-registration to grant access to information systems and services.
- Restriction and control of assignments and use of privileges.
- Good security practices in the selection and use of keys.
- Adequate protection for unattended equipment.
- Authentication methods for remote user access control, when applicable.

- Secure registration procedures for access to operational services.
- Controls for teleworking, when applicable.

6.13 Acquisition, development and maintenance of information systems

ANF AC is aware that security is an integral part of its information systems.

To do this, it performs the necessary tasks for input data validation, internal processing controls, message integrity and output data validation.

Cryptographic controls will be used to protect the confidentiality, authenticity and integrity of the information.

To guarantee the security of the system files, procedures will be established for the control of operational software, the test data of the system will be controlled, and access control to the source code of the program will be created.

To maintain the security of the software and information of the application system, change control procedures will be established, the technical review of the applications will be carried out after changes in the operating system, the modifications to the software packages will be limited to the necessary changes and these changes will be strictly controlled.

To reduce the risks resulting from the exploitation of technical vulnerabilities, the organization's exposure to those vulnerabilities will be evaluated and the appropriate measures will be taken to address the associated risk.

6.14 Incident management

ANF AC ensures that information on events and information security weaknesses are communicated in a way that allows taking the appropriate corrective actions.

A procedure has been documented to control the reporting of events and security weaknesses, which defines responsibilities and systems to ensure a quick, effective and orderly response to security incidents.

6.15 Business continuity

ANF AC ensures the availability of the service in the event of a catastrophe and establishes an action plan to minimize its effects. This action covers the integrity, availability and preservation of the information.

An activity continuity management process has been established to guarantee the recovery of critical processes in the event of a disaster, reducing the time of non-availability to acceptable levels, through the appropriate combination of organizational, technological and procedural controls,
both preventive and recovery.

6.16 Compliance

ANF AC, through the security policies and standards defined in the SGCSI, tries to avoid breaches of any law and any security requirement. It also tries to maximize the effectiveness of the information systems audit process.

ANF AC acquires the responsibility of complying with current legislation regarding information security. ANF AC identifies the relevant statutes, regulations, laws and contractual requirements related to information security that affect the security of its information assets.

It is the responsibility of all the departments involved to know and comply with the current legislation that is applicable to them.

All ANF AC personnel undertake not to disclose any type of information.

Computer applications will be periodically audited, in charge of verifying compliance with security regulations and ISMS procedures.

6.17 Risk analysis

ANF AC has made a description of the methodology for risk assessment, a report on said assessment and a risk treatment plan, according to regulatory requirements.

A risk criterion has been defined to determine the significance of the risks. Risk assessments identify, quantify and prioritize risks against the criteria for risk acceptance and the relevant objectives for ANF and its clients.

The results guide and determine the appropriate management action and priorities to manage information security risks and to implement selected security measures to protect against these risks.

6.18 Statement of applicability

The applicability statement includes:

1) The control objectives and controls selected [to address risks, based on risk acceptance criteria, in addition to legal, regulatory and contractual requirements] and the justifications for their selection;

2) the control objectives and controls currently in place; and

3) the exclusion of any control and control objective of Annex A and the justification for this exclusion.

Note: The applicability statement provides a summary of the decisions regarding the treatment of risks. The justification for the exclusions facilitates a cross-checking that no
inadvertently omitted any controls.

7 Control and review

ANF AC establishes different procedures for monitoring and reviewing the ISMS.

7.1 Customer satisfaction

ANF AC has defined a system to measure customer satisfaction by periodically conducting random surveys.

7.2 Internal Audits

ANF AC carries out internal audits of the SGCSI at planned intervals, as detailed in its Internal Audits procedure.

7.3 Monitoring and measurement of processes and product.

ANF AC has defined indicators for its processes, assigning persons responsible for their monitoring and objectives to be achieved.

They are regularly reviewed in a meeting that also includes the review of the results of security audits, incidents, review of risk assessments, review of the residual risk level and the identified acceptable risk, suggestions and feedback from all interested parties.

7.4 Incident control

ANF AC defines in a procedure the system for managing the incidents detected, including a method of recording and evaluation in order to correct them and prevent their occurrence.

7.5 Review by ANF senior management

Top management reviews the reports issued by the internal and external audits carried out by the ISMS at regular intervals to ensure their continued suitability, convenience and effectiveness. The review includes assessment for continuous improvement and the need for changes to the ISMS, including quality and safety policies and objectives. The results of the reviews must be clearly documented.

To do this, a series of information is received, which helps to make decisions, among which you can enumerate:

- Results of audits and reviews of the ISMS.
- Comments from all interested parties.
- Techniques, products or procedures that could be useful to improve the performance and effectiveness of the ISMS.
- Information on the status of preventive and corrective actions.
- Vulnerabilities or threats that were not adequately addressed in previous risk assessments.
- Results of efficacy measurements.
- Status of actions initiated as a result of previous Management reviews.
- Any change that may affect the ISMS.
- Recommendations for improvement.

Based on all this information, Management must review the ISMS and take decisions and actions related to:

- Improving the effectiveness of the ISMS.
- Updating of the risk assessment and risk treatment plan.
- Modification of procedures and controls that affect information security, in response to internal or external changes in business requirements, security requirements, business processes, legal framework, contractual obligations, risk levels and
  risk acceptance criteria.
- Resource needs.
- Improvement of the way of measuring the effectiveness of controls.

8 Maintenance and improvement of the ISMS

ANF AC, as indicated in its corrective and preventive actions procedure, defines the corrective actions necessary to eliminate or minimize the causes of the incidents detected (internal or external) or potential to avoid recurrence.

018