Security Policy

General Information

Document control

Classification	Public
Version	3
Date of creation	29/04/2016
Date last updated	28/04/2026
File	Security Policy

Formal status

Prepared by:	Reviewed by:	Approved by:
Security Office	Security Officer	Safety Committee

Version Control

Version	Description of the change	Author of the change	Date of change
1.0	Document creation	Security Office	29/04/2016
1.1	Review	Security Office	10/03/2017
2.0	Review of roles and their appointments	Security Office	02/06/2017
2.1	Review of roles and separation of appointments to the Annex document.	Security Office	08/06/2017
2.2	The role of the Revocation Officer is added. The reference to AULOCE is replaced by ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.	Security Office	02/10/2020
2.3	Registration Operator role is included	Security Office	14/04/2023
2.4	The details of the functions of the Security Officer are revised (ETSI EN 319 401 (v3.1.1))	Security Office	11/03/2025

2.5	The wording of the functions of the Auditor role is reviewed and clarified	Security Office	28/03/2025
3	Adaptation to the new version of ETSI EN 319 401, format update and inclusion of the role of Development Manager	Security Office	28/04/2026

Table of Contents

1. Introduction

ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. with CIF A-50.878.842 and domiciled at Calle Bari 39, C.P. 50.197 (Zaragoza), registered in the Mercantile Registry of Zaragoza in volume 2.649, Folio 215, page Z-28722, operates under the trade name "**esFirma**" as a provider of certification services.

esFIRMA acts in accordance with the national and European regulations that apply to it, in order to facilitate compliance with legal requirements and the international recognition of its services. Among others:

- Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation).
- ETSI technical standards applicable to the issuance and management of qualified certificates, mainly ETSI EN 319 411-1 and ETSI EN 319 411-2.
- National regulations on electronic signatures.

esFIRMA has promoted the development of a security policy that serves as a guide for the protection of the information systems and networks that support the provision of its certification services. This policy is appropriate and complementary to esFirma's strategy and business objectives, integrating security as a fundamental element for the continuity and development of the service.

The management of esFirma is committed to providing the necessary resources for the effective implementation of this policy, ensuring the availability of specialized human capital, sufficient financial endowment, as well as the processes, technological solutions and infrastructure required.

2. Scope

This security policy covers all the certification services provided by esFIRMA and is mandatory for all esFIRMA personnel, as well as for third parties that provide or use services and transfer or handle information for which esFirma is responsible (hereinafter, jointly referred to as the "**personnel**").

3. Principles

This policy will be developed, in general, in accordance with the following principles:

- **Principle of confidentiality.** ICT assets must be accessible only by those authorised persons or processes.

- **Principle of integrity and quality.** The integrity of the information must be maintained, as well as the processes for processing it.

- **Principle of availability and continuity.** A high level of availability of ICT assets will be guaranteed and the necessary plans and measures will be provided to ensure the continuity of services.

- **Principle of traceability.** Measures will be implemented to ensure that at all times it can be determined who and when an action was triggered in order to have analysis capabilities on security incidents that are detected.

- **Principle of authenticity.** Measures must be articulated to guarantee the source of information from which the data come and that the entities where the data originate are reliable.

- **Risk management principle.** The risks will be analysed and the necessary security measures will be established to minimise them.

- **Principle of proportionality in cost.** The security measures adopted to mitigate the risks will be implemented under a perspective of proportionality in the costs involved.

- **Principle of awareness and training.** All the people in charge of the management of the information systems will be trained so that they can know their obligations regarding the secure treatment of the information they handle.
- **Principle of prevention.** Initiatives will be carried out for the prevention of cybersecurity incidents.

- **Principle of continuous improvement.** esFirma will maintain an explicit commitment to the continuous improvement of the security of its networks and information systems, periodically reviewing its controls and adapting them to new threats.

- **ICT security principle in the life cycle of information systems**: In all phases of the life cycle of assets, the corresponding security specifications and control procedures will be applied.

- **Principle of security by design and by default**: esFIRMA will establish and apply rules for the secure development of networks and information systems that cover all phases: specification, design, development, implementation and testing.

- **Principle of differentiated function.** Responsibility for the security of information systems shall be separate from responsibility for service.

4. Security objectives

esFirma establishes the following strategic objectives in terms of network and information systems security:

- **Safeguarding assets.** Protect the confidentiality of user information and ensure the absolute integrity of certificate issuance, management, and revocation processes.

- **Operational resilience.** Implement proactive detection and response mechanisms, ensuring business continuity through recovery plans that guarantee the resilience of trust services to contingencies.

- **Regulatory compliance.** To ensure full and continuous compliance with the legal framework applicable to esFIRMA.

- **Generation of trust:** Strengthen the reputation of esFIRMA with its stakeholders through transparent security management and the maintenance of high levels of service availability.

5. Security organization

The organization of esFirma is articulated according to the roles described below. Assigned roles, responsibilities and roles will be reviewed annually and when significant incidents or changes in operations or risks occur.

5.1. Safety Committee

The Security Committee will be made up of three members: its Chairman, the Information and Service Officer and the Security Officer. The Security Committee is responsible for:

a) Approval of the level of risk appetite and the risk tolerance threshold.
b) Approval of the risk analysis and, where appropriate, the risk treatment plan.
c) Approval of new documents or relevant modifications to the security regulatory framework and relevant documentation of the certificate authority (cessation plan, continuity plan, statement of certification practices, security policy...).

5.2. Security Office

The Security Office corresponds to the Regulatory Compliance Department and is made up of the Security Manager and the personnel considered necessary at all times for the performance of their functions.

Its functions include:

a) Carrying out the annual risk assessment and, where appropriate, the risk treatment plan, which must be approved by the Safety Committee.
b) Preparation of proposals relating to the revision of the regulatory framework for safety and relevant documentation of the certification authority (cessation plan, continuity plan, statement of certification practices, security policy, etc.), which must be approved by the Security Committee.
c) Minor modifications to regulations, procedures, instructions and other elements within the regulatory structure of safety.
d) Training of personnel in information security.

e) Report information to the Security Committee, through the Security Officer, on matters related to the security of networks and information systems.

To carry out its functions, the Security Office relies on the Security Operations Centre (SOC) as the unit responsible for the active surveillance and maintenance of esFirma's security environment (continuous monitoring, early detection and analysis of threats, incident response, etc.).

5.3. Trusted roles

The people who perform each of the roles are defined in the ANNEX document. ESFIRMA – DEFINITION OF TRUST ROLES.

5.3.1. Roles and Functions in the CA Scope

- **Systems Administrator**. Responsible for the correct operation of the hardware and software support of the certification platform.

- **CA Administrator**. Responsible for the actions to be carried out with the cryptographic material, or with the performance of any function that involves the activation of the private keys of the certification authorities described in this document, or any of their elements.

- **Auditor**. Authorized to view log files and audits for the purpose of auditing system operations against established security policies. The tasks of the Auditor are incompatible with the operation and administration of the systems.

- **AC operator**. Responsible for the custody of cryptographic key activation material jointly with the CA Administrator, also responsible for backup operations and maintenance of the CA.

- **Security Manager**. In charge of coordinating, controlling and enforcing the security measures defined by the security policies of esFIRMA. Responsible for aspects related to information security: logical, physical, networks, organizational, etc., as well as reporting to senior management through the Security Committee.

- **Information and service manager**. Defines the requirements for information and services in terms of security. This role has the ultimate responsibility for the use made of the information and services and therefore for their level of protection.

- **Validation specialist**. Responsible for the validation of certificate requests.

- **Revocation Officer**. Responsible for the operation of changing the status of the certificates.

- **Registry operator**. Responsible for the approval of certification requests by the subscriber.

- **Development Manager.** Assumes the functions of implementation and control of the development lifecycle of PKI software and firmware systems.

5.3.2. Roles and functions in the scope of the remote signing system (PIN signing)

- **Security Manager**. Global responsibility for managing and implementing security practices and policies.

- **L1 System Administrator**. Authorized with a minimum quorum (3/5) to initialize and update SSCDs. SSCDs are immutable once initialized. They are the holders of a share of the system's activation key

- **L2 System Administrator**. Authorized to configure and maintain the PIN signing system with controlled access to security information. They can adjust the time source. They can create login credentials for the SSA. Back up those credentials.

- **System operator**. Responsible for the daily operation of the system. They cannot in any case administer or configure the system.

- **Auditor**. Authorized to view log files and audits for the purpose of auditing system operations against established security policies. The tasks of the Auditor are incompatible with the operation and administration of the systems.

- **Development Manager.** Assumes the functions of implementation and control of the development lifecycle of the remote signature system.

6. Safety regulatory structure

The security policy generates a security regulatory structure composed of the policy itself, security regulations and procedures, with hierarchically related levels, as described below:

6.1.1. First level: Information security policy.

The safety policy is approved by the Safety Committee. The security policy is communicated and made available to esFirma staff and interested third parties through a permanent link on the esFIRMA website.

6.1.2. Second level: Information security standards

Security standards arise as a development of policy in a given area of information security. Among others, it is worth noting:

- ✓ Regulations on the use of resources and access to information systems
- ✓ Off-site work regulations
- ✓ Information classification regulations
- ✓ Regulations for the use of Cloud Services
- ✓ Regulations for the use of e-mail
- ✓ Media management regulations
- ✓ Cyber incident management regulations
- ✓ Secure data erasure regulations
- ✓ Password Configuration Policy

The security regulations are communicated to esFirma staff and are available for consultation on a permanent basis on the company's Intranet.

6.1.3. Third level: Information security procedures.

The procedures indicate the flow of activities related to the information services or assets carried out by esFirma.

6.1.4. Fourth level: Technical Instructions

Technical instructions are commands that specify how to do what is stipulated in the procedures.

7. Secure Network and System Development

Before any deployment of software, network or information system, esFIRMA will apply the following security guidelines:

- Requirements analysis: a security analysis will be carried out in the initial phases of specification and design of any project or acquisition of ICT products.

- Secure engineering: Secure systems engineering and secure coding principles will be applied, promoting "zero trust" architectures.

- Controlled environments: Specific requirements will be established to ensure the security of development, pre-production, and test environments.

- Test cycle: Security testing processes will be implemented throughout the development lifecycle.

- Test data management: data used in development and test environments will be appropriately selected and protected; through data purification and anonymization.

- Outsourced development: in the case of subcontracting, suppliers will be contractually required to comply with these same requirements.

esFIRMA has processes for change management, acquisition of information system assets, design and secure development that complement and develop the provisions of this Policy.

8. Compliance

8.1. Staff compliance

All esFirma personnel are responsible for knowing, understanding and strictly complying with this security policy, as well as the derived rules and procedures that affect their specific functions; each person being responsible for the correct use of the information and communications technology assets made available to them.

Likewise, the staff has the obligation to immediately and without undue delay report any security incident, through the mechanisms made available to them by esFIRMA.

To ensure the effectiveness of this commitment, esFirma implements the following actions:

- **Internal communication:** the policy is communicated and formally recognized by all employees. It is permanently available for consultation on the esFIRMA website.

- **Awareness and training:** regular information security training programmes are implemented to ensure that staff identify risks and act in accordance with established protocols.

The corresponding disciplinary sanctions will be applied to personnel who violate this policy or the safety regulations that develop it, in accordance with the provisions of the applicable labor legislation.

8.2. Third-Party Compliance

Third parties that provide services to esFIRMA or handle information under the responsibility of esFIRMA must comply with the provisions of this Policy, and may develop their own operating procedures to satisfy it.
Specific procedures for reporting and resolving incidents will be established. In particular, third parties must inform esFIRMA of any incident of which they are aware and which may affect an information system and/or the information in question or the services provided.

Third-party personnel will be encouraged to be adequately aware of security and privacy, at least at the same level as that established in this Policy.

9. Documentation management and conservation

esFirma maintains an inventory of the documentation of the information security management system (policies, regulations, technical instructions, etc.).

All documentation, records and data of the trust services will be kept in accordance with the legal deadlines established in the eIDAS Regulation and Law 6/2020, guaranteeing their availability for a minimum period of 15 years (or as determined by the regulations in force at any given time).

10. Monitoring and indicators

To supervise the effective implementation of this policy and determine the level of maturity of esFirma in terms of network and information systems security, a continuous measurement framework is established, supported by the activity of the SOC (Security Operations Center).

This framework uses the following key indicators:

- **Incident Management Indicators:** monitoring of the response capacity and treatment of security events detected through the SOC, ensuring effective management of anomalies and mitigation of possible operational risks.

- **Efficiency of controls:** Measurement of the level of technical maturity through periodic vulnerability scans and penetration tests.

- **Safety culture:** Assessment of the level of staff training through indicators of participation and success in training programmes and awareness campaigns.

- **Availability and continuity:** monitoring the availability levels of trust services and analyzing the results obtained in periodic testing of continuity and disaster recovery plans.

11. Review

This policy, as well as the security regulations, are subject to periodic review to ensure that they are appropriate to the risks and the operating environment of esFirma.

This review will be carried out at least annually and whenever there are significant security incidents or substantial changes in operations, the technologies used or the risk analysis.

The Security Office will assess the validity of the document and propose the necessary updates where appropriate. The Safety Committee is responsible for the formal approval of this policy.

The outcome of each review, regardless of whether it generates a document update or not, must be duly documented to ensure the traceability of the security governance process.