Supply Chain Security Policy

General Information

Document control

Classification	Public
Version	1
Date of creation	28/04/2026
Date last updated	28/04/2026
File	Supply Chain Security Policy

Formal status

Prepared by:	Reviewed by:	Approved by:
Security Office	Regulatory Compliance	Safety Committee

Version Control

Version	Description of the change	Author of the change	Date of change
1.0	Document creation	Security Office	28/04/2026

Table of Contents

1. Introduction

This policy establishes the control framework for managing the security risks associated with the supply chain of ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. (hereinafter, "**esFIRMA"),** as a trust service provider.

esFIRMA recognizes that the security of its services depends on the integrity and resilience of its suppliers and service providers. Therefore, in its relationship with the supply chain, esFIRMA assumes responsibility for:

1. Identify the necessary security requirements for each service.
2. Clearly communicate these requirements to your direct suppliers.
3. Monitor ongoing compliance with agreed service levels.

Therefore, the objective of this policy is to define the controls to mitigate the risks identified for the security of networks and information systems, ensuring that third-party ICT assets and services meet the same levels of demand as their own.

2. Scope

This policy is mandatory (i) for all esFIRMA personnel involved in the acquisition of ICT products or services and (ii) for all suppliers and service providers who have access to esFIRMA's information or infrastructures.

3. Selection and hiring criteria

In line with the provisions of procedure PS-06 Selection of suppliers and PS-07-b Purchase of information system assets, the selection of a given ICT supplier, product or service will be based on the following:

- esFIRMA will specify the minimum security requirements and evaluate the cybersecurity criteria that the provider must meet, according to the criticality of the asset:

Criteria	Description
Cybersecurity Practices	Evaluation of your secure development and vulnerability management procedures.
Technical Capability	Ability to meet specifications, manage risks, and maintain safety rating levels.
ICT Product Resilience	Quality and risk management measures integrated into the ICT products supplied.
Diversification	Strategy to limit dependence on a single supplier and ensure continuity of service.
Certifications	Certifications in ISO 27001 standards, ENS, or specific product certifications will be valued.

- The supplier must ensure: (i) the availability of security updates throughout the expected useful life of the asset and (ii) the commitment of technical support or, failing that, a replacement/transition plan before the end of the maintenance period.

- For complex assets, the vendor will be asked for descriptive information of the hardware and software components, statement of implemented cybersecurity functions, and configuration guidance for safe operation.

4. Supplier Risk Management

esFIRMA will define processes to manage the risks associated with the use of third-party products or services:

- **Initial assessment:** before contracting, esFIRMA will verify compliance with the product/service in terms of risks, security, data protection and contractual conditions and environmental requirements (when applicable). In particular, the product will be assessed on the basis of the conclusions of the risk analysis, as well as the technical, training and financing needs.

  For the initial evaluation, criteria such as: quality of the product or service supplied, experience of the supplier, historical relationship with it, price, reputation, product or company certifications will be taken into account. In particular, the supplier's risk from the point of view of information security shall be analysed and, depending on this risk, the appropriate safeguards shall be required.

  In addition, if the product or service supplied by the supplier is likely to have a significant environmental impact, this initial assessment will take into account any environmental certifications or safeguards that the supplier has.

- **Periodic evaluation:** suppliers are subject to periodic evaluation (annually) and when there is any significant modification in the products or services supplied.

5. Mandatory contractual requirements

Supplier contracts and service level agreements (SLAs) should specify:

- Specific technical requirements for the acquisition of services or products.
- Obligation of safety education and training for the supplier's personnel.
- Eligibility requirements for vendor employees accessing critical systems.
- Obligation to inform esFIRMA, without undue delay, of any incident affecting the security of the network or the information of esFIRMA.
- Faculty of esFIRMA to carry out audits or receive audit reports from third parties.
- Commitment to manage vulnerabilities that represent a risk to esFIRMA.
- Standards for subcontracting, requiring compliance with the same safety requirements.
- Protocols for the recovery and safe disposal of information at the end of the relationship.

6. Supervision and control

To ensure the effectiveness of this policy, it is SIGNATURE:

- Will periodically review service level agreement (SLA) compliance reports.
- It will analyze incidents related to ICT products provided by third parties.
- Assess the need for additional reviews based on the level of risk detected.
- It will maintain a constant monitoring of the performance of accepted suppliers, through their continuous evaluation.

7. Review and update

This policy will be reviewed at least annually and whenever there are changes in the cybersecurity practices of suppliers and service providers, or significant changes in supply operations or relevant security incidents affecting the supply chain.