

# Certification Practice Statement

# esFIRMA

## Overview

### Control Document

---

|                          |         |
|--------------------------|---------|
| Security classification: | Public  |
| Entity Target:           | ESFIRMA |
| Version:                 | 1.6     |

### formal state

---

| Prepared by:                        | Reviewed by:                             | Approved by:                         |
|-------------------------------------|--|--------------------------------------|
| Security Office<br>Date: 20/06/2018 | Responsible Security<br>Date: 20/06/2018 | Safety Committee<br>Date: 20/06/2018 |

## Control Version

| Version | changing  | Description of Change   | Author of change | Date of change  |
|---------|---|---|------------------|-----------------|
| 1.0     | Original  | Document Creation   | esFIRMA          | 04/29/2016      |
| 1.1     |   | rectifications  | andsFIRMA        | 02 /<br>06/2016 |
| 1.2     |   | ETSI  | andsFIRMA        | 05/19/2017      |
| 1.3     |   | review Review types of certificates                                       |                  |                 |
| 1.4     |   | ETSI<br>revision Review types of certificates<br>Acronyms and Definitions | esFIRMA          | 06/02/2017      |
| 1.5     | 1.3.1<br>1.3.2<br>1.3.3.1<br>1.3.3.2<br>1.4.1.8<br>3.1.1.8<br>4.3.1<br>6.1.5<br>9.2.1 9.4<br>9.6.2<br>9.6.4 | regulations,<br>referencessettings,<br>name change<br>changecertified     | esFIRMA          |                 |
|         | 6/11/201<br>7 1.6<br>6.1.1  | TSADuration   | esFIRMA          | 06/20/2018      |

# Index

|   |           |
|---|-----------|
| <b>ACRONYMS</b>   | <b>12</b> |
| <b>DEFINITIONS</b>  | <b>14</b> |
| <b>Introduction</b>   | <b>16</b> |
| Introduction  | 16        |
| document name and identification                                | 16        |
| certificates Identifiers  | 16        |
| Participantscertification services                              | 17        |
| certification service Provider                                  | 17        |
| EsFIRMA rootAC  | 18        |
| EsFIRMAAC AAPP  | 19        |
| Platform eGovernment  | 19        |
| Registrars  | 19        |
| Entityis final  | 20        |
| Certification service subscribers                               | 20        |
| Signatories   | 21        |
| parties   | 21        |
| UserUse of certificates   | 22        |
| Permitted uses for certificates                                 | 22        |
| Public Employee Certificate high level on Card                  | 22        |
| Public Employeeemedium level                                    | 24        |
| CertificateOrgan Seal Certificate medium level in software      | 25        |
| Organ Seal Certificate medium level in HSM                      | 27        |
| Public Employee Certificate with pseudonym high level in Card   | 28        |
| Public Employee Certificate with pseudonym medium level, in HSM | 30        |
| Web Authentication Certificate, medium level                    | 32        |
| Electronic Seal Certificate of TSA / TSU                        | 33        |
| Limits and prohibitions on the use of certificates              | 34        |
| Administration of the policy                                    | 35        |
| Organization that manages the document                          | 35        |
| Organization that approves the document                         | 35        |
| Contact details of the organization                             | 36        |
| Document management procedures                                  | 36        |
| <b>Publication of information and deposit of certificates</b>   | <b>38</b> |

|   |           |
|---|-----------|
| Deposit ( s) of certificates  | 38        |
| Publication of information Certification Services Provider                          | 38        |
| Publication Frequency   | 38        |
| Access Control  | 39        |
| <b>Identification and Authentication</b>  | <b>40</b> |
| Initial Registry  | 40        |
| Types of Names  | 40        |
| Public Employee Certificate, High Level, on Card                                    | 40        |
| Public Employee Certificate, Medium Level, on HSM                                   | 41        |
| Certificate of organ seal, medium level, in software                                | 42        |
| Certificate of organ seal, medium level, in HSM                                     | 43        |
| Certificate of public employee with pseudonym, high level, in card                  | 43        |
| Certificate of public employee with pseudonym, average level, in HSM                | 44        |
| Certificate EV web authentication, medium level                                     | 44        |
| TSA / TSU electronic seal certificate   | 45        |
| Meaning of names  | 45        |
| Use of anonymities and pseudonyms   | 45        |
| Interpretation of name formats  | 46        |
| Uniqueness of names   | 46        |
| Resolution of disputes concerning names   | 47        |
| Initial validation of the identity  | 47        |
| Proof of possession of a private key  | 48        |
| Authentication of the identity of the subscriber acting through a repre tative      | 48        |
| Authentication of the identity of an individual                                     | 50        |
| The certificates  | 51        |
| need for personal presence  | 51        |
| Certificate applications  | 51        |
| Renewal of certificates   | 51        |
| Linking individual  | 52        |
| Subscriber Information unverified   | 52        |
| Identification and authentication applications for renewal                          | 52        |
| Validation for the routine renewal of certificates                                  | 52        |
| Identification and authentication of the renewal application after prior revocation | 53        |
| Identification and authentication of the revocation request                         | 53        |
| Authentication of a suspension request  | 54        |
| <b>Requirements for the operation of the life cycle of the certificates</b>         | <b>55</b> |
| Application for the issuance of a certificate                                       | 55        |
| Standing to request issuance  | 55        |
| procedurehigh andresponsibilities   | 55        |

|   |    |
|---|----|
| processingcertification application                                   | 56 |
| executing the functions of identification and authentication          | 56 |
| Approval or rejection of the request                                  | 56 |
| period for the application  | 57 |
| issuing n certificate   | 57 |
| Actions of the CA during emission                                     | 57 |
| Notification broadcast tosubscriber                                   | 58 |
| delivery and acceptance of the certificate                            | 58 |
| Responsibilities CA   | 58 |
| Conduct an acceptance certificate                                     | 59 |
| Publication certificate   | 60 |
| Notification emission third   | 60 |
| Use of the key pair and certificate                                   | 60 |
| Use by the subscriber or signer                                       | 60 |
| Use by the subscriberSubscriber's                                     | 62 |
| obligations of the certificate  | 62 |
| Civil liability of the certificate subscriber                         | 62 |
| Use by the third party that relies on certificates                    | 63 |
| Obligations of the third party that relies on certificates            | 63 |
| Civil liability of the third party that relies on certificates        | 64 |
| Renewal of certificates   | 64 |
| Renewal of codes and certificates                                     | 64 |
| Reasons for the renewal of codes and certificates                     | 64 |
| Procedure with new identification                                     | 65 |
| Notification of the issuance of the renewed certificate               | 65 |
| Conduct that constitutes acceptance of the certificatethe certificate | 65 |
| Publication ofcertify do  | 65 |
| Notification of issuance to third parties                             | 65 |
| Modification of certificates  | 65 |
| Revocation and suspension of certificates                             | 66 |
| Reasons for revocation of certificates                                | 66 |
| Legitimation to request revocationRevocation                          | 67 |
| request procedures  | 68 |
| Term of application for revocationrevocation                          | 68 |
| Term for processing therequest  | 69 |
| Obligation to consult certificate revocation information              | 69 |
| Frequency of issuance of certificate revocation lists (LRCs)          | 69 |
| Maximum period of publication of LRCs                                 | 70 |
| Availability of online certificate verification servicescertificates  | 70 |
| Obligation to consult service ofcertificate status check              | 71 |

**esFIRMA: Prácticas de Certificación**

|  |           |
|--|-----------|
| Other forms of certificate revocation information                  | 71        |
| Special requirements in case of commitment of the private key      | 71        |
| Causes of suspension of certificates                               | 71        |
| Request for suspension   | 71        |
| Procedures for requesting suspension                               | 71        |
| Maximum period of suspension                                       | 72        |
| Finalización subscription  | 72        |
| Services Test Certificate Status                                   | 72        |
| operational characteristics of services                            | 72        |
| Availability of services   | 72        |
| Deposit and Key Recovery   | 72        |
| Policy and practices of deposit and key recovery                   | 73        |
| Policy and practices encapsulation and recovery key session        | 73        |
| <b>Physical, management and operational</b>                        | <b>74</b> |
| security controlsPhysical security controls                        | 74        |
| Location and construction of facilities                            | 75        |
| Physical access  | 75        |
| Electricity and air conditioning                                   | 76        |
| Water exposure   | 76        |
| Fire prevention and protection                                     | 76        |
| Storage of supports  | 76        |
| Waste treatment  | 77        |
| Off-site backup  | 77        |
| Procedures controls  | 77        |
| Reliable functions   | 77        |
| Number of people per task  | 78        |
| Identification and authentication for each function                | 78        |
| Roles requiring separation of tasks                                | 79        |
| PKI management system  | 79        |
| Personnel controls   | 79        |
| History requirements, qualifications, experience and authorization | 79        |
| History investigation procedures                                   | 80        |
| Training   | 81        |
| requirementsFormative update requirements and frequency            | 82        |
| Sequence and frequency of work rotation                            | 82        |
| Sanctions for unauthorized actions                                 | 82        |
| Requirements for hiring professionals                              | 82        |
| Providing documentation to staff                                   | 83        |
| Procedures security audit  | 83        |
| Types of events recorded   | 83        |

|  |            |
|--|------------|
| Frequency of processing audit records                                | 84         |
| Retention period of audit records                                    | 85         |
| Protection of audit records  | 85         |
| Backup procedures  | 86         |
| Locating the audit trail accumulation system                         | 86         |
| Notification of the event of audit to the cause of the event         | 86         |
| Vulnerability analysis   | 86         |
| Information files  | 87         |
| Types of archived records  | 87         |
| Retention period of records  | 88         |
| Protection of the file   | 88         |
| Back-up procedures   | 88         |
| Date stamping requirements and time                                  | 88         |
| Location of the file system  | 89         |
| Procedures for obtaining and verifying archival information          | 89         |
| Renewal of keys  | 89         |
| Commitment of keys and recovery of disaster                          | 89         |
| Procedures for management of incidents and commitments               | 90         |
| Corruption of resources, applications or data                        | 90         |
| Commitment of the entity's private key                               | 90         |
| Business continuity after a disaster                                 | 91         |
| Revocations management   | 91 Service |
| termination  | 91         |
| <b>Technical security controls</b>                                   | <b>93</b>  |
| Generating and installing the key pair                               | 93         |
| Generating the key pair  | 93         |
| Generating the signer's key pair                                     | 94         |
| Submission from the private key to the signer                        | 94         |
| Sending the public key to the issuer of the certificate              | 95         |
| Distribution of the public key of the certification service provider | 95         |
| Key sizes  | 95         |
| Generation of public key parameters                                  | 96         |
| Quality check of public key parameters                               | 96         |
| Generation of keys in computer applications or in bi Equipment       | 96         |
| purposesPurpose of using keys  | 96         |
| Protection of the private key  | 96         |
| Standards of cryptographic modules                                   | 96         |
| Control by more than one person (n of m) on the private key          | 97         |
| Deposit of the private key   | 97         |
| Backup of the private key  | 97         |
|  | 8          |

|  |            |
|--|------------|
| File of the private key                                      | 97         |
| Introduction of the private key in the cryptographic module  | 98         |
| Method of activation of the private key                      | 98         |
| Method of deactivation of the private key                    | 98         |
| Method of destruction of the private key                     | 98         |
| Classification of cryptographic modules                      | 99         |
| Other aspects of management of the key pair                  | 99         |
| Public key file  | 99         |
| Periods of use of public and private keys                    | 99         |
| Activation data  | 100        |
| Generation and installation of activation data               | 100        |
| Protection data protection                                   | 100        |
| Computer security controls                                   | 100        |
| Specific technical security requirements                     | 101        |
| Evaluation of the level of computer security                 | 102        |
| Technical controls of the cyclone or of life                 | 102 System |
| development  | 102        |
| controlsSecurity management controls                         | 102        |
| Classification and management of information and assets      | 102        |
| Management operationshandling                                | 103        |
| Mediaand security  | 103 System |
| planning   | 103        |
| Incident and response reports                                | 103        |
| Operational procedures and responsibilities                  | 103        |
| management system access                                     | 104        |
| AC General   | 104        |
| certificate Generation                                       | 104        |
| management revocation  | 104        |
| State revocation   | 104        |
| management lifecycle cryptographic hardware                  | 105        |
| security controls network                                    | 106        |
| engineering Controls cryptographic modules                   | 106        |
| Sources Time   | 106        |
| <b>Profiles and certificate revocation listscertificates</b> | <b>106</b> |
| certificate profile  | 106        |
| version Number   | 107        |
| certificate extensions                                       | 107        |
| object Identifiers (OID) algorithms                          | 107        |
| Format names   | 107        |
| Restricting names  | 107        |

## esFIRMA: Prácticas de Certificación

|   |            |
|---|------------|
| object identifier (OID) of the types of certificates                          | 108        |
| Profile of the list of re Certificate vocation                                | 108        |
| Version number  | 108        |
| OCSP profile  | 108        |
| <b>Compliance audit</b>   | <b>108</b> |
| Frequency of the compliance audit   | 108        |
| Identification and qualification of the auditor                               | 108        |
| Relationship of the auditor with the audited entity                           | 109        |
| List of elements subject to audit   | 109        |
| Actions to be undertaken as a result of a lack of conformity                  | 110        |
| Treatment of audit reports  | 110        |
| <b>commercial and legal requirements</b>                                      | <b>110</b> |
| Fees  | 110        |
| fee issue or renewal of certificates  | 110        |
| access fee certificates   | 110        |
| access fee status information certificate                                     | 111        |
| Fees for other services   | 111        |
| Policy reimbursement  | 111        |
| Financial capacity  | 111        |
| Insurance coverage  | 111        |
| Other assets  | 111        |
| Insurance coverage for subscribers and third parties who rely on certificates | 112        |
| ConfidentialityConfidential   | 112        |
| information   | 112        |
| Non-confidential information  | 112        |
| Disclosure of suspension and revocation information                           | 113        |
| Legal disclosure of information   | 113        |
| Disclosure of information by request of its owner                             | 114        |
| Other circumstances of disclosure of information                              | 114        |
| Protection of personal data   | 114        |
| Intellectual property rights  | 115        |
| Ownership of certificates and revocation information                          | 115        |
| Ownership of the Certification Practice Statement                             | 116        |
| Ownership of relative information to names                                    | 116        |
| Ownership of keys   | 116        |
| Obligations and civil liability   | 116        |
| Obligations of the Certification Body "esFIRMA"                               | 116        |
| Guarantees offered to subscribers and third parties that rely on certificates | 118        |
| Rejection of other guarantees   | 119        |

## esFIRMA: Prácticas de Certificación

|  |     |
|--|-----|
| Limitation of liability  | 119 |
| IndemnityIndemnity   | 119 |
| clausesclause subscriber   | 120 |
| indemnification of relying partycertificate                      | 120 |
| fortuitous and force majeure                                     | 121 |
| applicable law   | 121 |
| clausesseverability, survival, entire agreement and notification | 121 |
| of competent jurisdiction Clause                                 | 121 |
| conflict Resolution  | 122 |

| <b>a</b> CHRONYMS          |  |
|----------------------------|--|
| <b>AC (or also CA)</b>     | <i>Certificate Authority</i><br>Certification Authority  |
| <b>AR(or RA)</b>           | <i>Registration Authority</i><br>Registration Authority  |
| <b>CPD</b>                 | Data Processing Center   |
| <b>CPS(or also DPC)</b>    | <i>Certification Practice Statement.</i><br>Certification Practice Statement                                 |
| <b>CRL (or also LRC)</b>   | <i>Certificate Revocation List.</i><br>List of revoked certificates  |
| <b>DN</b>                  | <i>Distinguished Name.</i><br>Distinctive name within the digital certificate                                |
| <b>DNI</b>                 | National Identity Document   |
| <b>ETSI EN</b>             | <i>European Telecommunications Standards Institute - European Standard.</i>                                  |
| <b>EV (for SSL)</b>        | <i>Extended Validation</i> Extended validation, in SSL certificates.   |
| <b>FIPS</b>                | <i>Federal Information Processing Standard</i> Publication   |
| <b>HSM</b>                 | <i>Hardware Security Module</i><br>Hardware Security Module  |
| <b>IETF</b>                | <i>Internet Engineering Task Force</i>   |
| <b>NIF</b>                 | Tax Identification Number  |
| <b>NTP</b>                 | <i>Network Time Protocol</i><br>Network Time Protocol.   |
| <b>OCSP</b>                | <i>Online Certificate Status Protocol.</i> Access protocol to the status of thecertificates                  |
| <b>OID</b>                 | <i>Object Identifier.</i><br>Object Identifier   |
| <b>PDS</b>                 | <i>PKI Disclosure Statements</i> PKI Disclosure Text.  |
| <b>PIN</b>                 | <i>Personal Identification Number.</i><br>Personal identification number                                     |
| <b>PKI</b>                 | <i>Public Key Infrastructure.</i><br>Public key infrastructure   |
| <b>QSCD (or also DCCF)</b> | <i>Qualified Electronic Signature / Seal Creation Device.</i><br>Qualified signature / stamp creation device |
| <b>QCP</b>                 | <i>Qualified Certificate Policy</i> Qualified certificate policy   |
| <b>QCP-n</b>               | <i>Qualified Certificate Policy-natural person</i> Qualified certificate policy for natural persons.         |
| <b>QCP-l</b>               | <i>Qualified Certificate Policy-legal person</i> Qualified certificate                                       |

|                   |  |
|-------------------|--|
|                   | policy for legal entities.   |
| <b>QCP-n-qscd</b> | <i>Qualified Certificate Policy-natural person-qscd</i><br>Qualified certificate policy for individuals in qualified signature / seal device   |
| <b>QCP-l-qscd</b> | <i>Qualified Certificate Policy-legal person-qscd</i><br>Qualified certificate policy for legal entities with qualified device signature /seal   |
| <b>RFC</b>        | <i>Request for Comments</i><br>Document RFC  |
| <b>RSA</b>        | Rivest-Shamir-Adleman. Type of encryption algorithm  |
| <b>SHA</b>        | <i>Secure Hash Algorithm.</i><br>Hash Algorithm  |
| <b>SSL</b>        | <i>SecureSecure Sockets Layer.</i> Protocol designed by Netscape and converted into a network standard, allows the transmission of encrypted information between an Internet browser and a server. |
| <b>TCP / IP</b>   | <i>Transmission Control. Protocol / Internet Protocol.</i><br>System of protocols, defined in the framework of the IEFT.   |
| <b>TSA</b>        | <i>Time Stamping AuthorityTime Stamping Authority</i><br>Electronic  |
| <b>TSU</b>        | <i>Time Stamping Unit Time Stamping Unit</i><br>.  |
| <b>UTC</b>        | <i>Coordinated Universal Time Coordinated</i><br>universal time  |
| <b>VPN</b>        | <i>Virtual Private Network.</i><br>Virtual private network   |

| <b>DEFINITIONS</b>             |  |
|--------------------------------|--|
| <b>Certification Authority</b> | <i>It is the entity responsible for the issuance and management of digital certificates.</i>   |
| <b>Registration Authority</b>  | <i>Entity responsible for the management of applications, identification and registration of applicants for a certificate. You can be part of the Certification Authority or be an alien.</i>  |
| <b>Certificate</b>             | <i>File that associates the public key with some identification data of the Subject / Signatory and is signed by the AC.</i>   |
| <b>Public key</b>              | <i>A mathematical value publicly known and used for the verification of a digital signature or data encryption.</i>  |
| <b>Private key</b>             | <i>Mathematical value known only by the Subject / Signatory and used for the creation of a digital signature or data decryption. The private key of the CA will be used for signature of certificates and signature of CRLs. The private key of the TSA service will be used to sign the time stamps.</i>  |
| <b>CPS</b>                     | <i>Set of practices adopted by a Certification Authority for the issuance of certificates in accordance with a specific certification policy.</i>  |
| <b>CRL</b>                     | <i>File that contains a list of the certificates that have been revoked in a certain period of time and that are signed by the CA.</i>   |
| <b>Activation</b>              | <i>data Private data, such as PINs or passwords used for the activation of the private key</i>   |
| <b>DCCF</b>                    | <i>Qualified device for creating a signature. Software or hardware element, suitably certified, used by the Subject / Signatory for the generation of electronic signatures, so that the cryptographic operations are carried out within the device and its control is guaranteed only by the Subject / Signatory.</i>   |
| <b>Digital signature</b>       | <i>The result of the transformation of a message, or any type of data, by the application of the private key in conjunction with known algorithms, guaranteeing in this way:<br/>a) that the data has not been modified (integrity)<br/>b) that the person signing the data is who he / she claims to be (identification)<br/>c) that the person signing the data can not deny having done so (no repudiation at source)</i> |
| <b>OID</b>                     | <i>Unique numeric identifier registered under ISO standardization and referring to an object or class of determined object.</i>  |
| <b>Pair of keys</b>            | <i>Set consisting of the public and private key, both related mathematically.</i>  |
| <b>PKI</b>                     | <i>Set of hardware elements, software, human resources, procedures, etc., that make up a system based on the creation</i>  |

|                            |  |
|----------------------------|--|
|                            | <i>and management of public key certificates.</i>  |
| <b>Applicant</b>           | <i>In the context of this document, the applicant will be a natural person empowered with a special power to perform certain procedures on behalf of the entity.</i>                           |
| <b>Subscriber</b>          | <i>In the context of this document, the legal entity that owns the certificate (corporate level)</i>   |
| <b>Subject / Signatory</b> | <i>In the context of this document, the individual whose public key is certified by the CA and has, or has exclusive access to , a valid private key to generate digital signatures.</i>       |
| <b>User Part</b>           | <i>In the context of this document, a person who voluntarily relies on the digital certificate and uses it as a means of accrediting the authenticity and integrity of the signed document</i> |

# 1. Introduction

## 1.1. Presentation

---

This document declares esFIRMA's electronic signature certification practices.

The certificates that are issued are the following:

- **Public Employee Public**
  - Employee Medium level Public
  - Employee High level
- **Seal Organ Organ**
  - Seal Medium level
- **Public Employee Pseudonym**
  - Public Employee pseudonymous Average level
  - Public Employee pseudonymous level Alto
- **De electronic office**
  - electronic office administrative MEAN
- **electronic seal for TSA / tsu**
  - electronic seal for TSU HSM

## 1.2. document name and identification

---

This document is the "Certification Practice Statement of esFIRMA".

### 1.2.1. Identifiers of certificates

---

| Number OID                     | Policies of certificates                         |
|--------------------------------|--|
|                                | <b>of Public Employee</b>                        |
| <b>1.3.6.1.4.1.47281.1.1.1</b> | <i>Of Public Employee - High Level on card</i>   |
| <b>1.3.6.1.4.1.47281.1.1.4</b> | <i>Of Public Employee - Average Level in HSM</i> |
|                                | <b>of Body Seal</b>                              |

|                         |   |
|-------------------------|---|
| 1.3.6.1.4.1.47281.1.2.2 | <i>Organ Seal - Medium Level in software</i>      |
| 1.3.6.1.4.1.47281.1.2.4 | <i>Organ Seal - Medium Level in HSM</i>           |
|                         | <b>of Public Employee with a Pseudonym</b>        |
| 1.3.6.1.4.1.47281.1.3.1 | <i>EP with Pseudonym - High Level on Card</i>     |
| 1.3.6.1.4.1.47281.1.3.4 | <i>EP with a pseudonym - Average level in HSM</i> |
|                         | <b>of electronic headquarters</b>                 |
| 1.3.6.1.4.1.47281.1.4.2 | <i>Sede-e EV -Medium Level</i>                    |
|                         | <b>Electronic Seal for TSA / TSU</b>              |
| 1.3.6.1.4.1.47281.1.5.2 | <i>Seal-e for TSA / TSU in HSM</i>                |

In case of contradiction between this Declaration of Certification Practices and other documents of practices and procedures of esFIRMA, the provisions of this Declaration of Practice shall prevail.

EsFIRMA conforms to the current version of the CA / Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates published at <http://www.cabforum.org>. In case of incompatibility between this document and these Guidelines, these Guidelines prevail over this document (8.3 EVCG).

### 1.3. Participants in certification services of certification

---

#### 1.3.1. Provider services certification service

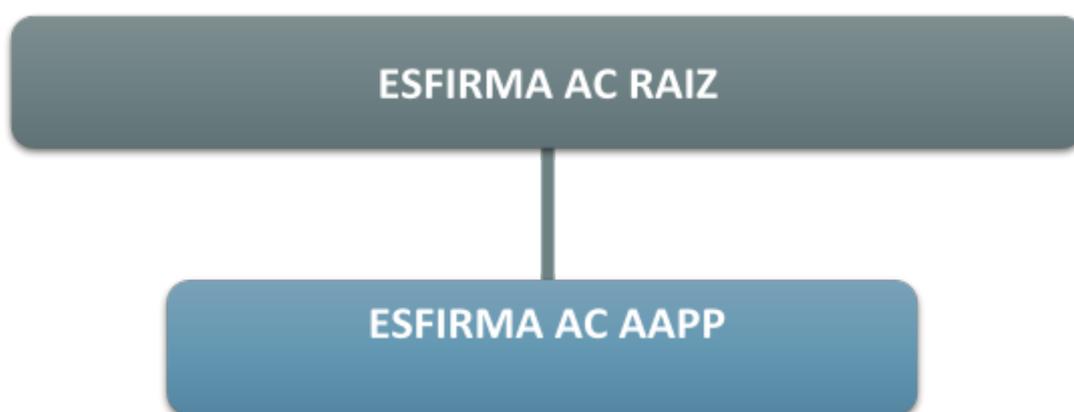
---

The provider is the person, physical or legal, that issues and manages certificates for final entities, employing a Certification Entity, or provides other services related to the electronic signature.

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (PREVIOUS AULOCE SA), hereinafter ESPUBLICO, with address at Calle Bari 39 (Edif. Binary Building), CP 50,197, of Zaragoza, CIF A-50.878.842, registered in the Mercantile Register of Zaragoza to volume 2,649, Folio 215, page Z-28722, and that operates under the trade name

EsFIRMA, trade name which will be used throughout this document to designate it, it is a certification service provider that acts in accordance with the provisions of the obligations and responsibilities regime of Regulation (EU) 910/2014, and the ETSI technical standards applicable to the issuance and management of qualified certificates, mainly ETSI EN 319 411-1 and ETSI EN 319 411-2, in order to facilitate compliance with legal requirements and international recognition of their services.

For the provision of the certification services, esFIRMA has established a hierarchy of certification entities:



#### 1.3.1.1. Root CA STRIKE

---

This is the root certification entity of the hierarchy that issues certificates to other certification entities, and whose public key certificate has been self-signed

Identification data:

|                        |  |
|------------------------|--|
| <b>CN:</b>             | ESFIRMA AC ROOT 2  |
| <b>Fingerprint</b>     | c6: 09: f9: 4f: 9c: ce: 20: cb: 2b: a0: 2e: 8b: 5b: 33: 55: 20: 06 |
| <b>SHA-256:</b>        | : c1: 5d: 17: 78: 32: 26: 11: 07: 0f: a1: 4f: ff: 9d: c9: 16       |
| <b>Valid since:</b>    | 2017-11-02T12: 52: 43Z   |
| <b>Valid until:</b>    | 2042-11-02T12 : 52: 43Z  |
| <b>RSA key length:</b> | 4,096 bits   |

### 1.3.1.2. ESFIRMA AC AAPP

---

This is the certification entity within the hierarchy that issues the certificates to the end entities, and whose public key certificate has been digitally signed by "esFIRMA AC RAIZ 2 "

Identification data:

|                                 |   |
|---------------------------------|---|
| <b>CN:</b>                      | ESFIRMA AC AAPP 2   |
| <b>Fingerprint<br/>SHA-256:</b> | 2c: 18: 23: 61: 9d: 80: 73: 11: 6c: 8f: 14: 8b: d3: 85: 79: de:<br>9c: 05: 39: 16: 02: db: ce: b9: 65: 73: e4: a1: 88: e1: 32: 6e |
| <b>Valid since:</b>             | 2017-11-02T13: 12: 47Z  |
| <b>Valid until:</b>             | 2030-11-02T13: 12: 47Z  |
| <b>RSA key length:</b>          | 4,096 bits  |

### 1.3.1.3. Electronic Administration Platform

---

This is the exclusive lifecycle management platform of the certificate, for its request, approval, issuance and revocation.

To complete the information on the functionalities of the Electronic Administration Platform in the certification services consult their documentation.

## 1.3.2. Registrars

---

In general, the certification service provider acts as registrar of the identity of the certificate subscribers.

The certificates subject to this Certification Practice Statement are also registrars, due to their status as corporate certificates, the units designated for this function by the certificate subscribers, such as the Secretary of the corporation or the personnel department of the Administration. , since they have authentic records about the link of the signatories with the subscriber.

Subscriber registration functions are carried out by delegation and in accordance with the instructions of the certification service provider, under the terms defined in Regulation (EU) 910/2014, and under the full responsibility of the certification service provider. To thirds.

### **1.3.3. Finalfinal**

---

entities The entities are the persons and organizations that receive the services of issuance, management and use of digital certificates, for the uses of identification and electronic signature.

The following entities will be the final entities of the esFIRMA certification services:

1. Subscribers of the certification service.
2. Signatories
3. User parties.

#### 1.3.3.1. Subscribers of the certification service

The subscribers of the certification service are the public administrations that acquire them to esFIRMA for use in their corporate or organizational scope, and they are identified in the certificates.

The subscriber of the certification service acquires a license to use the certificate, for its own use - electronic seal certificates -, or in order to facilitate the certification of the identity of a specific person duly authorized for various actions in the subscriber's organizational field - electronic signature certificates. In the latter case, this person is identified in the certificate, as provided in the following section.

The subscriber of the certification service is, therefore, the client of the certification service provider, in accordance with the commercial legislation, and has the rights and obligations that are defined by the provider of the certification service, which are additional and understood without prejudice to the rights and obligations of the signatories, as authorized and regulated in the European technical standards applicable to the issuance of electronic certificates qualified, especially in ETSI EN 319 411-2, sections 5.4.2 and 6.3.4.e )

#### 1.3.3.2. signers

---

the signers are individuals who own exclusively or have under their exclusive control, under the regime of obligations and responsibilities of Regulation (EU)910/2014,digital signature keys for identification and advanced orelectronic signature qualified; being typically the holders or members of the administrative bodies, in the certificates of electronic signature of the organ, or the persons at the service of the Public Administrations, in the certificates of public employee.

The signatories are duly authorized by the subscriber and duly identified in the certificate by his name and surnames, and valid tax identification number in the jurisdiction of issuance of the certificate, or with the corresponding pseudonym in the certificates of this type.

Given the existence of certificates for different uses of the electronic signature, such as identification, the more generic term of "natural person identified in the certificate" is also used, always with full respect for compliance with the electronic signature legislation in relation to the rights and obligations of the signer.

#### 1.3.3.3. Useruser

---

parties Theparties are the people and organizations that receive digital signatures and digital certificates.

As a previous step to trust the certificates, the user parties must verify them, as established in this certification practices statement and in the corresponding instructions available on the website of the Certification Entity.

## 1.4. Use of certificates

---

This section lists the applications for which each type of certificate can be used, establishes limitations for certain applications and prohibits certain applications of certificates.

#### 1.4.1. Permitted uses for certificates

---

The permitted uses indicated in the various fields of the certificate profiles must be taken into account, visible on the web <https://www.esfirma.com>

##### 1.4.1.1. Public Employee Certificate high level in Card

---

This certificate has the following following OIDs:

|                         |                                      |
|-------------------------|--------------------------------------|
| 1.3.6.1.4.1.47281.1.1.1 | In the hierarchy CEesFIRMA           |
| 0.4.0.194112.1.2        | In accordance with policy QCP-n-qscd |
| 2.16.724.1.3.5.7.1      | High-level Spanish public employee   |

Certificates of physical person public employee high level are certificates qualified in accordance with article 28 and with Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014 and comply with the provisions of the regulations technique identified with the reference ETSI EN 319 411-2.

These certificates are issued to public employees to identify them as persons at the service of the Administration, body or entity of public law, linking them with it, fulfilling the requirements established in article 43 of Law 40/2015, of October 1, Regime Legal of the Public Sector, for the electronic signature of the personnel at the service of the Public Administrations.

Certificates for individuals employed public high level, work with a secure signature creation device, in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and Council, of July 23, 2014.

Likewise, certificates of high level public employees are issued in accordance with the high levels of assurance of the certificate profiles established in point 10 of the document "Profiles of electronic Certificates" of the General Subdirectorate of

Information, Documentation and Publications of the Ministry of Finance and Public Administrations.

These certificates guarantee the identity of the subscriber and the signer, and allow the generation of the "qualified electronic signature"; that is to say, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, for which in accordance with the provisions of article 25.2 of Regulation (EU) 910/2014 of the European Parliament and the Council , of July 23, 2014, will have a legal effect equivalent to that of a signature handwritten.

.

They can also be used in applications that do not require an electronic signature equivalent to the written signature, such as the applications indicated below:

- a) Secure email signature.
- b) Other digital signature applications

**EsFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.**

La información de usos en el perfil de certificado indica lo siguiente:

- a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
  - a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
- b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
  - a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
  - b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
- c) El campo "User Notice" describe el uso de este certificado.

#### 1.4.1.2. Certificado de Empleado Público nivel medio

---

Este certificado dispone de los siguientes OIDs:

|                         |   |
|-------------------------|---|
| 1.3.6.1.4.1.47281.1.1.4 | En la jerarquía de la EC esFIRMA        |
| 0.4.0.194112.1.0        | De acuerdo con la política QCP-n        |
| 2.16.724.1.3.5.7.2      | Empleado público español de nivel medio |

Los certificados de persona física empleado público nivel medio son certificados cualificados de acuerdo con el artículo 28 y el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten a empleados públicos para identificarlos como personas al servicio de la Administración, organismo o entidad de derecho público, vinculándolos con ésta, cumpliendo los requisitos establecidos en el artículo 43 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para la firma electrónica del personal al servicio de las Administraciones Públicas.

Los certificados de persona física empleado público nivel medio son gestionados de forma centralizada.

Los certificados de persona física empleado público nivel medio se emiten de acuerdo con los niveles de aseguramiento medio de los perfiles de certificados establecidos en el punto 10 del documento “Perfiles de Certificados electrónicos” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas.

## esFIRMA: Prácticas de Certificación

Estos certificados garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la generación de la “firma electrónica avanzada basada en certificado electrónico cualificado”.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

- a) Firma de correo electrónico seguro.
- b) Otras aplicaciones de firma digital.

**EsFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.**

La información de usos en el perfil de certificado indica lo siguiente:

- a) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
  - a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
- b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
  - a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
- c) El campo “User Notice” describe el uso de este certificado.

### 1.4.1.3. Certificado de Sello de Órgano nivel medio en software

---

Este certificado dispone de los siguientes OIDs:

|                         |                                  |
|-------------------------|----------------------------------|
| 1.3.6.1.4.1.47281.1.2.2 | En la jerarquía de la EC esFIRMA |
|-------------------------|----------------------------------|

|                    |   |
|--------------------|---|
| 0.4.0.194112.1.1   | De acuerdo con la política QCP-I        |
| 2.16.724.1.3.5.6.2 | Empleado público español de nivel medio |

Los certificados de sello electrónico de órgano nivel medio son certificados cualificados de acuerdo con el artículo 38 y el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada de acuerdo con el artículo 42 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Los certificados de sello electrónico de órgano nivel medio se emiten de acuerdo con los niveles de aseguramiento medio de los perfiles de certificados establecidos en el punto 9 del documento “Perfiles de Certificados electrónicos” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones.

Estos certificados garantizan la identidad del suscriptor y del organismo público incluidos en el certificado.

**EsFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.**

La información de usos en el perfil de certificado indica lo siguiente:

- a) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
  - a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
  
- b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:

## esFIRMA: Prácticas de Certificación

- a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
- c) El campo “User Notice” describe el uso de este certificado.

### 1.4.1.4. Certificado de Sello de Órgano nivel medio en HSM

---

Este certificado dispone de los siguientes OIDs:

|                         |   |
|-------------------------|---|
| 1.3.6.1.4.1.47281.1.2.4 | En la jerarquía de la EC esFIRMA        |
| 0.4.0.194112.1.1        | De acuerdo con la política QCP-I        |
| 2.16.724.1.3.5.6.2      | Empleado público español de nivel medio |

Los certificados de sello electrónico de órgano nivel medio son certificados cualificados de acuerdo con el artículo 38 y el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada de acuerdo con el artículo 42 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Los certificados de sello electrónico de órgano nivel medio son gestionados de forma centralizada.

Los certificados de sello electrónico de órgano nivel medio se emiten de acuerdo con los niveles de aseguramiento medio de los perfiles de certificados establecidos en el punto 9 del documento “Perfiles de Certificados electrónicos” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones.

Estos certificados garantizan la identidad del suscriptor y del organismo público incluidos en el certificado.

**EsFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.**

La información de usos en el perfil de certificado indica lo siguiente:

- a) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
  - a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
- b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
  - a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
- c) El campo “User Notice” describe el uso de este certificado.

#### 1.4.1.5. Certificado de Empleado Público con Seudónimo nivel alto en Tarjeta

Este certificado dispone de los siguientes OIDs:

|                         |   |
|-------------------------|---|
| 1.3.6.1.4.1.47281.1.3.1 | En la jerarquía de la EC esFIRMA                  |
| 0.4.0.194112.1.2        | De acuerdo con la política QCP-n-qscd             |
| 2.16.724.1.3.5.4.1      | Empleado público español con seudónimo nivel alto |

Los certificados de persona física empleado público con seudónimo nivel alto son certificados cualificados de acuerdo con el artículo 28 y el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten a empleados públicos para identificarlos (por medio de un seudónimo) como personas al servicio de la Administración, organismo o entidad de derecho público, vinculándolos con ésta, cumpliendo los requisitos establecidos en el

## **esFIRMA:** Prácticas de Certificación

artículo 43 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para la firma electrónica del personal al servicio de las Administraciones Públicas.

Los certificados de persona física empleado público con seudónimo nivel alto, funcionan con dispositivo seguro de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Asimismo, los certificados de persona física empleado público con seudónimo nivel alto se emiten de acuerdo con los niveles de aseguramiento alto de los perfiles de certificados establecidos en el punto 11 del documento “Perfiles de Certificados electrónicos” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas.

Estos certificados permiten la generación de la “firma electrónica cualificada”; es decir, la firma electrónica avanzada que se basa en un certificado cualificada y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

- a) Firma de correo electrónico seguro.
- b) Otras aplicaciones de firma digital.

**EsFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.**

La información de usos en el perfil de certificado indica lo siguiente:

- a) El campo “key usage” tiene activadas, y por tanto permite realizar, las siguientes funciones:

**esFIRMA:** Prácticas de Certificación

- a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
- b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
  - a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
  - b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
- c) El campo “User Notice” describe el uso de este certificado.

1.4.1.6. Certificado de Empleado Público con seudónimo nivel medio, en HSM

Este certificado dispone de los siguientes OIDs:

|                         |  |
|-------------------------|--|
| 1.3.6.1.4.1.47281.1.3.4 | En la jerarquía de la EC esFIRMA                   |
| 0.4.0.194112.1.0        | De acuerdo con la política QCP-n                   |
| 2.16.724.1.3.5.4.2      | Empleado público español con seudónimo nivel medio |

Los certificados de persona física empleado público con seudónimo nivel medio son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten a empleados públicos para identificarlos (por medio de un seudónimo) como personas al servicio de la Administración, organismo o entidad de derecho público, vinculándolos con ésta, cumpliendo los requisitos establecidos en el artículo 43 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para la firma electrónica del personal al servicio de las Administraciones Públicas.

Los certificados de persona física empleado público con seudónimo nivel medio son gestionados de forma centralizada.

Los certificados de persona física empleado público con seudónimo nivel medio se emiten de acuerdo con los niveles de aseguramiento medio de los perfiles de certificados establecidos en el punto 11 del documento “Perfiles de Certificados electrónicos” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas.

Estos certificados permiten la generación de la “firma electrónica avanzada basada en certificado electrónico cualificado”.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

- c) Firma de correo electrónico seguro.
- d) Otras aplicaciones de firma digital.

**EsFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.**

La información de usos en el perfil de certificado indica lo siguiente:

- a) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
  - a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
- b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
  - a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
- c) El campo “User Notice” describe el uso de este certificado.

1.4.1.7. Certificado de Autenticación web, nivel medio

---

Este certificado dispone de los siguientes OIDs:

|                         |   |
|-------------------------|---|
| 1.3.6.1.4.1.47281.1.4.2 | En la jerarquía de la EC esFIRMA                        |
| 0.4.0.194112.1.4        | De acuerdo con la política QCP-web                      |
| 2.16.724.1.3.5.5.2      | Sede electrónica administrativa española de nivel medio |

Los certificados de autenticación web de nivel medio son certificados cualificados de acuerdo con el artículo 45 y con el Anexo IV del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten a direcciones web para identificarlos como sedes electrónicas administrativas de la Administración, organismo o entidad de derecho público, vinculándolas con ésta, cumpliendo los requisitos establecidos en el artículo 38 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para su identificación y garantizar una comunicación segura con los ciudadanos.

Los certificados de autenticación web de nivel medio se emiten de acuerdo con los niveles de aseguramiento medio de los perfiles de certificados establecidos en el punto 8 del documento “Perfiles de Certificados electrónicos” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas.

La información de usos en el perfil de certificado indica lo siguiente:

- a) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
  - a. Digital Signature (para la función de autenticación)
  - b. Key Encipherment (para la gestión y transporte de claves)
  
- b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:

## esFIRMA: Prácticas de Certificación

- a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
- c) El campo “User Notice” describe el uso de este certificado.

### 1.4.1.8. Certificado de Sello electrónico de TSA/TSU

---

Este certificado dispone de los siguientes OIDs:

|                         |                                  |
|-------------------------|----------------------------------|
| 1.3.6.1.4.1.47281.1.5.2 | En la jerarquía de la EC esFIRMA |
| 0.4.0.194112.1.1        | De acuerdo con la política QCP-I |

Los certificados de sello electrónico de TSA/TSU son certificados cualificados de acuerdo con el artículo 38 y el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 421 y ETSI EN 319 422.

Este certificado permite a Unidades de Sellado de Tiempo o TSU emitir los sellos de tiempo cuando reciben una solicitud bajo las especificaciones de la RFC3161.

Las claves se generan en soporte de un dispositivo HSM.

La información de usos en el perfil de certificado indica lo siguiente:

- a) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
  - a. Content Commitment
- b) El campo “extend key usage” tiene activada la función:
  - a. TimeStamping
- c) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
  - a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
- d) El campo “User Notice” describe el uso de este certificado.

#### **1.4.2. Límites y prohibiciones de uso de los certificados**

---

Los certificados se emplean para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados no pueden emplearse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC).

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, visibles en el web de esFIRMA <https://www.esfirma.com>

El uso de los certificados digitales de forma que se incumpla esta DPC y el resto de documentación aplicable, especialmente el contrato firmado con el suscriptor y los textos de divulgación o PDS tiene la consideración de uso indebido a los efectos legales oportunos, y exime a esFIRMA de cualquier responsabilidad por este uso indebido, ya sea del firmante o de tercero alguno.

EsFIRMA no tiene autorización de acceso ni obligación legal de supervisar los datos sobre los que se puede aplicar el uso de una clave certificada. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de esFIRMA emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en esta DPC, los documentos jurídicos vinculantes con cada certificado, o los contratos o convenios con las entidades de registro o con sus suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

Los certificados se usan de forma exclusiva y únicamente desde la Plataforma de Administración Electrónica o extensiones y complementos de la misma que la empresa ESPUBLICO pone a disposición del suscriptor.

## 1.5. Administración de la política

---

### 1.5.1. Organización que administra el documento

---

Oficina de Seguridad de ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)  
CALLE BARI 39 (Edif. Binary Building)  
50197 - ZARAGOZA  
(+34) 976300110

|                                |                                |
|--------------------------------|--------------------------------|
| <i>Identificación Registro</i> | Registro Mercantil de Zaragoza |
| <i>Tomo</i>                    | 2649                           |
| <i>Folio</i>                   | 215                            |
| <i>Hoja</i>                    | Z-28722                        |
| <i>CIF</i>                     | A-50.878.842                   |

### 1.5.2. Organización que aprueba el documento

---

**Comité de Seguridad** de ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)

El comité de seguridad de esFIRMA, formado por el Presidente del mismo, el Responsable de Información y servicio y el Responsable de Seguridad de esFirma, tiene la responsabilidad de la aprobación de esta Declaración de Prácticas.

Tanto las funciones como los miembros de dicho Comité se encuentran definidos en la Política de Seguridad de esFirma (esFIRMA\_PolíticaSeguridad\_v2r0.pdf).

### **1.5.3. Datos de contacto de la organización**

---

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)  
CALLE BARI 39 (Edif. Binary Building)  
50197 - ZARAGOZA  
(+34) 976300110

### **1.5.4. Procedimientos de gestión del documento**

---

El sistema documental y de organización de esFIRMA garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las especificaciones de servicio relacionados con el mismo.

EsFIRMA realiza revisiones como mínimo anuales de este documento.

Tal y como se define en la Política de Seguridad de esFIRMA (esFIRMA\_PolíticaSeguridad\_v2r0.pdf), la Oficina de Seguridad será la entidad responsable del mantenimiento de este documento.

La Oficina de Seguridad se responsabiliza de la redacción, mantenimiento y administración de la DPC, los textos de divulgación (PDS), hojas de entrega y aceptación, y el resto de documentación jurídica (convenios, contratos, etc.) de esFirma.

Siempre que existan cambios de importancia suficiente en la gestión de los certificados definidos en esta DPC, se creará una nueva revisión de este documento, que constarán en el cuadro inicial de "control de versiones" dentro del apartado de "información general".

La actuación de la Oficina de Seguridad se produce a instancia de su responsable en función de las necesidades que se produzcan.

EsFirma puede realizar cambios que no requieran notificación cuando éstos no afecten directamente a los derechos de los firmantes y suscriptores de los certificados o de los suscriptores de los sellos.

Cuando esFirma vaya a introducir cambios que modifiquen los derechos de los firmantes y suscriptores de los certificados y de los suscriptores de sellos deberá notificarlo públicamente con el objeto que presenten sus comentarios a la Oficina de Seguridad durante 15 días siguientes a la publicación de los futuros cambios.

Las revisiones anuales deberán disponer de fases para la actualización ordinaria consistentes en:

- Fase de recogida de propuestas de modificación
- Fase de análisis, comprobación y redacción de modificaciones
- Fase de comentarios y aprobación
- Fase de publicación

El departamento dispone de un libro de registro donde serán introducidas y registradas cada una de las propuestas, indicando la fecha de recepción de la propuesta, la descripción de la modificación propuesta, así como su justificación técnica y/o legal.

Para notificar públicamente los cambios producidos se publicará en el apartado de "documentación" en la página web <https://www.esfirma.com>

Las revisiones de esta DPC serán publicadas en la web de esFirma tras ser aprobadas por el Consejo de Administración de Esfirma.

## 2. Publicación de información y depósito de certificados

### 2.1. Depósito(s) de certificados

---

EsFIRMA dispone de un Depósito de certificados, en el que se publican las informaciones relativas a los servicios de certificación.

Dicho servicio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de esFIRMA, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 5.7.4 de esta Declaración de Prácticas de Certificación

### 2.2. Publicación de información del prestador de servicios de certificación

---

EsFIRMA publica las siguientes informaciones, en su Depósito:

- Los certificados emitidos, cuando se haya obtenido consentimiento de la persona física identificada en el certificado.
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- Las políticas de certificados aplicables.
- La Declaración de Prácticas de Certificación.
- Los textos de divulgación (PKI Disclosure Statements - PDS), como mínimo en lengua española y en lengua inglesa.

### 2.3. Frecuencia de publicación

---

La información del prestador de servicios de certificación, incluyendo las políticas y la Declaración de Prácticas de Certificación, se publica en cuanto se encuentra disponible.

Los cambios en la Declaración de Prácticas de Certificación se rigen por lo establecido en la sección 1.5 de este documento.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en las secciones 4.9.7 y 4.9.8 de esta Declaración de Prácticas de Certificación.

## **2.4. Control de acceso**

---

EsFIRMA no limita el acceso de lectura a las informaciones establecidas en la sección 2.2, pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Depósito, para proteger la integridad y autenticidad de la información, especialmente la información de estado de revocación.

EsFIRMA emplea sistemas fiables para el Depósito, de modo tal que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Los certificados sólo estén disponibles para consulta si la persona física identificada en el certificado ha prestado su consentimiento.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

## 3. Identificación y autenticación

### 3.1. Registro inicial

#### 3.1.1. Tipos de nombres

Todos los certificados contienen un nombre diferenciado X.501 en el campo *Subject*, incluyendo un componente *Common Name* (CN=), relativo a la identidad del suscriptor y de la persona física identificada en el certificado, así como diversas informaciones de identidad adicionales en el campo *SubjectAlternativeName*.

Los nombres contenidos en los certificados son los siguientes.

##### 3.1.1.1. Certificado de empleado público, nivel alto, en tarjeta

|   |   |
|---|---|
| Country (C)   | "ES"  |
| Organization (O)  | Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado |
| organizationalUnitName (OU)                                   | CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO   |
| organizationIdentifier  | Identificador de la organización según la norma técnica ETSI EN 319 412-1   |
| Surname   | Primer y segundo apellido, de acuerdo con documento de identidad (DNI/Pasaporte)  |
| Given Name  | Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)   |
| Serial Number   | DNI/NIE del empleado  |
| Common Name (CN)  | Nombre Apellido1 Apellido2 – NIF del empleado   |
| Tipo de certificado<br>OID: 2.16.724.1.3.5.7.1.1              | CERTIFICADO CUALIFICADO DE FIRMA DE EMPLEADO PUBLICO DE NIVEL ALTO  |
| Nombre de la entidad suscriptora<br>OID: 2.16.724.1.3.5.7.1.2 | Nombre de la entidad suscriptora  |

## esFIRMA: Prácticas de Certificación

|  |  |
|--|--|
| NIF entidad suscriptora<br>OID: 2.16.724.1.3.5.7.1.3 | NIF entidad subscription   |
| DNI/NIE del responsable<br>OID: 2.16.724.1.3.5.7.1.4 | DNI o NIE del responsable  |
| Nombre de pila<br>OID: 2.16.724.1.3.5.7.1.6          | Nombre de pila del responsable del certificado                   |
| Primer apellido<br>OID: 2.16.724.1.3.5.7.1.7         | Primer apellido del responsable del certificado                  |
| Segundo apellido<br>OID: 2.16.724.1.3.5.7.1.8        | Segundo apellido del responsable del certificado                 |
| Correo electrónico<br>OID: 2.16.724.1.3.5.7.1.9      | Correo electrónico del responsable del certificado.<br>Opcional. |

### 3.1.1.2. Certificado de empleado público, nivel medio, en HSM

|   |   |
|---|---|
| Country (C)   | "ES"  |
| Organization (O)  | Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado |
| organizationalUnitName (OU)                                   | CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO   |
| organizationIdentifier  | Identificador de la organización según la norma técnica ETSI EN 319 412-1   |
| Surname   | Primer y segundo apellido, de acuerdo con documento de identidad (DNI/Pasaporte)  |
| Given Name  | Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)   |
| Serial Number   | DNI/NIE del empleado  |
| Common Name (CN)  | Nombre Apellido1 Apellido2 – NIF del empleado   |
| Tipo de certificado<br>OID: 2.16.724.1.3.5.7.2.1              | CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO DE NIVEL MEDIO  |
| Nombre de la entidad suscriptora<br>OID: 2.16.724.1.3.5.7.2.2 | Nombre de la entidad suscriptora  |
| NIF entidad suscriptora<br>OID: 2.16.724.1.3.5.7.2.3          | NIF entidad suscriptora   |

## esFIRMA: Prácticas de Certificación

|  |   |
|--|---|
| <b>DNI/NIE del responsable</b><br>OID: 2.16.724.1.3.5.7.2.4          | DNI o NIE del responsable                                       |
| <b>Número de autenticación personal</b><br>OID: 2.16.724.1.3.5.7.2.5 | NRP o NIP del responsable del suscriptor del certificado        |
| <b>Nombre de pila</b><br>OID: 2.16.724.1.3.5.7.2.6                   | Nombre de pila del responsable del certificado                  |
| <b>Primer apellido</b><br>OID: 2.16.724.1.3.5.7.2.7                  | Primer apellido del responsable del certificado                 |
| <b>Segundo apellido</b><br>OID: 2.16.724.1.3.5.7.2.8                 | Segundo apellido del responsable del certificado                |
| <b>Correo electrónico</b><br>OID: 2.16.724.1.3.5.7.2.9               | Correo electrónico del responsable del certificad.<br>Opcional. |

### 3.1.1.3. Certificado de sello de órgano, nivel medio, en software

|  |   |
|--|---|
| <b>Country (C)</b>   | "ES"  |
| <b>Organization (O)</b>  | Denominación (nombre "oficial" de la organización) del suscriptor         |
| <b>organizationalUnitName (OU)</b>                                   | SELLO ELECTRONICO   |
| <b>organizationIdentifier</b>  | Identificador de la organización según la norma técnica ETSI EN 319 412-1 |
| <b>Serial Number</b>   | DNI/NIE de la organización suscriptora                                    |
| <b>Common Name (CN)</b>  | Denominación de sistema o aplicación de proceso automático.               |
| <b>Tipo de certificado</b><br>OID: 2.16.724.1.3.5.6.2.1              | SELLO ELECTRONICO DE NIVEL MEDIO  |
| <b>Nombre de la entidad suscriptora</b><br>OID: 2.16.724.1.3.5.6.2.2 | Nombre de la entidad suscriptora  |
| <b>NIF entidad suscriptora</b><br>OID: 2.16.724.1.3.5.6.2.3          | NIF entidad suscriptora   |
| <b>Denominación del sistema</b><br>OID: 2.16.724.1.3.5.6.2.5         | Segundo apellido del responsable del sello                                |
| <b>Correo electrónico</b><br>OID: 2.16.724.1.3.5.6.2.9               | Correo electrónico del responsable del sello                              |

3.1.1.4. Certificado de sello de órgano, nivel medio, en HSM

|   |   |
|---|---|
| Country (C)   | "ES"  |
| Organization (O)  | Denominación (nombre "oficial" de la organización) del suscriptor         |
| organizationalUnitName (OU)                                   | SELLO ELECTRONICO   |
| organizationIdentifier  | Identificador de la organización según la norma técnica ETSI EN 319 412-1 |
| Serial Number   | DNI/NIE de la organización suscriptora                                    |
| Common Name (CN)  | Denominación de sistema o aplicación de proceso automático.               |
| Tipo de certificado<br>OID: 2.16.724.1.3.5.6.2.1              | SELLO ELECTRONICO DE NIVEL MEDIO  |
| Nombre de la entidad suscriptora<br>OID: 2.16.724.1.3.5.6.2.2 | Nombre de la entidad suscriptora  |
| NIF entidad suscriptora<br>OID: 2.16.724.1.3.5.6.2.3          | NIF entidad suscriptora   |
| Denominación del sistema<br>OID: 2.16.724.1.3.5.6.2.5         | Segundo apellido del responsable del sello                                |

3.1.1.5. Certificado de empleado público con seudónimo, nivel alto, en tarjeta

|   |   |
|---|---|
| Country (C)   | "ES"  |
| Organization (O)  | Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado |
| organizationalUnitName (OU)                                   | CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO   |
| organizationIdentifier  | Identificador de la organización según la norma técnica ETSI EN 319 412-1   |
| Pseudonym   | Seudónimo obligatorio según ETSI EN 319 412-2 para este tipo de certificados  |
| Common Name (CN)  | Seudónimo y el Organismo  |
| Tipo de certificado<br>OID: 2.16.724.1.3.5.4.1.1              | CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO DE NIVEL ALTO   |
| Nombre de la entidad suscriptora<br>OID: 2.16.724.1.3.5.4.1.2 | Nombre de la entidad suscriptora  |

## esFIRMA: Prácticas de Certificación

|  |  |
|--|--|
| NIF entidad suscriptora<br>OID: 2.16.724.1.3.5.4.1.3 | NIF entidad suscriptora  |
| Seudónimo<br>OID: 2.16.724.1.3.5.4.1.12              | Seudónimo usado por el firmante y autorizado por el suscriptor |

### 3.1.1.6. Certificado de empleado público con seudónimo, nivel medio, en HSM

|   |   |
|---|---|
| Country (C)   | "ES"  |
| Organization (O)  | Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado |
| organizationalUnitName (OU)                                   | CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO   |
| organizationIdentifier  | Identificador de la organización según la norma técnica ETSI EN 319 412-1   |
| Pseudonym   | Seudónimo obligatorio según ETSI EN 319 412-2 para este tipo de certificados  |
| Common Name (CN)  | Seudónimo y el Organismo  |
| Tipo de certificado<br>OID: 2.16.724.1.3.5.4.2.1              | CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO DE NIVEL MEDIO  |
| Nombre de la entidad suscriptora<br>OID: 2.16.724.1.3.5.4.2.2 | Nombre de la entidad suscriptora  |
| NIF entidad suscriptora<br>OID: 2.16.724.1.3.5.4.2.3          | NIF entidad suscriptora   |
| Seudónimo<br>OID: 2.16.724.1.3.5.4.2.12                       | Seudónimo usado por el firmante y autorizado por el suscriptor  |

### 3.1.1.7. Certificado de autenticación web EV, nivel medio

|                        |   |
|------------------------|---|
| Country (C)            | "ES"  |
| Organization (O)       | Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado (custodio) |
| localityName           | Ciudad  |
| organizationalUnitName | Descripción del tipo de certificado: SEDE ELECTRONICA   |

|  |   |
|--|---|
| <b>organizationalUnitName</b>                  | El nombre descriptivo de la sede  |
| <b>serialNumber</b>                            | El NIF de la entidad responsable  |
| <b>businessCategory</b>                        | Categoría de la organización: Government Entity                           |
| <b>jurisdictionOfIncorporationCountry Name</b> | Jurisdicción  |
| <b>organizationIdentifier</b>                  | Identificador de la organización según la norma técnica ETSI EN 319 412-1 |
| <b>Common Name (CN)</b>                        | Nombre de dominio (DNS) donde residirá el certificado.                    |

#### 3.1.1.8. Certificado de sello electrónico de TSA/TSU

|                                    |   |
|------------------------------------|---|
| <b>Country (C)</b>                 | "ES"  |
| <b>Organization (O)</b>            | Denominación (nombre "oficial" de la organización) del suscriptor         |
| <b>organizationalUnitName (OU)</b> | AUTORIDAD DE CERTIFICACIÓN DE ESFIRMA                                     |
| <b>Serial Number</b>               | DNI/NIE de la organización suscriptora                                    |
| <b>organizationIdentifier</b>      | Identificador de la organización según la norma técnica ETSI EN 319 412-1 |
| <b>Common Name (CN)</b>            | Denominación de la TSU  |

#### 3.1.2. Significado de los nombres

Los nombres contenidos en los campos *SubjectName* y *SubjectAlternativeName* de los certificados son comprensibles en lenguaje natural, de acuerdo con lo establecido en la sección anterior.

#### 3.1.3. Empleo de anónimos y seudónimos

En ningún caso se pueden utilizar seudónimos para identificar una entidad/empresa/organización, y en ningún caso se emiten certificados anónimos, a excepción hecha de que, por razones de seguridad pública, los sistemas de firma electrónica puedan referirse sólo al número de identificación profesional del empleado público.

#### **3.1.4. Interpretación de formatos de nombres**

---

Los formatos de nombres se interpretarán de acuerdo con la ley del país de establecimiento del suscriptor, en sus propios términos.

El campo “país” será siempre España por ser los certificados emitidos exclusivamente a las Administraciones Públicas españolas.

El certificado muestra la relación entre una persona física y la Administración, organismo o entidad de derecho público con la que está vinculada, con independencia de la nacionalidad de la persona física. Ello deriva de la naturaleza corporativa del certificado, del cual es suscriptor la corporación, y la persona física vinculada la persona autorizada a su uso.

En los certificados emitidos a suscriptores españoles, el campo “número de serie” debe incluir el NIF del firmante, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

#### **3.1.5. Unicidad de los nombres**

---

Los nombres de los suscriptores de certificados serán únicos, para cada política de certificado de esFIRMA.

No se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente, situación que, en principio no se ha de dar, gracias a la presencia del Número de Identificación Fiscal, o equivalente, en el esquema de nombres.

Un suscriptor puede pedir más de un certificado siempre que la combinación de los siguientes valores existentes en la solicitud fuera diferente de un certificado válido:

- Número de Identificación Fiscal (NIF) u otro identificador legalmente válido de la persona física.
- Número de Identificación Fiscal (NIF) u otro identificador legalmente válido del suscriptor.
- Tipo de Certificado (Campo descripción del certificado).

### **3.1.6. Resolución de conflictos relativos a nombres**

---

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

EsFIRMA no estará obligada a determinar previamente que un solicitante de certificados tiene derechos de propiedad industrial sobre el nombre que aparece en una solicitud de certificado, sino que en principio procederá a certificarlo.

Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

Sin embargo, en caso de recibir una notificación relativa a un conflicto de nombres, conforme a la legislación del país del suscriptor, podrá emprender las acciones pertinentes orientadas a bloquear o retirar el certificado emitido.

En todo caso, el prestador de servicios de certificación se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

Toda controversia o conflicto que se derive del presente documento, se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, en el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte en el documento contractual que formaliza el servicio.

## **3.2. Validación inicial de la identidad**

---

La identidad de los suscriptores de certificados resulta fijada en el momento de la firma del contrato entre esFIRMA y el suscriptor, momento en el que se verifica la existencia del suscriptor, y de la documentación aportada justificativa de su identidad y del cargo y/o condición en el cual firma, de conformidad con lo indicado en la normativa de derecho administrativo que sea de aplicación.

La identidad de las personas físicas identificadas en los certificados se valida mediante los registros corporativos de la Administración, organismo o entidad de derecho público suscriptora de los certificados. El suscriptor, mediante certificación administrativa expedida por el Secretario del Ayuntamiento, producirá una certificación de los datos necesarios, y la remitirá a esFIRMA, por los medios que ésta habilite, para el registro de la identidad de los firmantes. Cuando el suscriptor no disponga de Secretaría, esta certificación será emitida por el Responsable del servicio de certificación designado.

Los ficheros de datos personales de cada Administración, organismo o entidad de derecho público deberán estar inscritos en la Agencia de Protección de Datos correspondiente, por cada una de ellas, siendo su responsabilidad, y no la de esFIRMA, que actúa como encargado del tratamiento, según se indica en la sección 9.4 de esta DPC.

Para evitar cualquier conflicto de intereses las Administraciones Públicas suscriptoras son entidades independientes del Prestador de servicios de confianza “esFIRMA” y de la empresa ESPUBLICO<sup>1</sup>.

### **3.2.1. Prueba de posesión de clave privada**

---

La posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del certificado por el firmante desde la Plataforma de Administración Electrónica, al firmar la hoja de aceptación, y su uso en dicha plataforma.

### **3.2.2. Autenticación de la identidad del suscriptor que actúa mediante un representante**

---

Las personas físicas con capacidad de actuar en nombre de una Administración, organismo o entidad de derecho público suscriptora de los certificados, podrán actuar como representantes de las mismas en relación a lo previsto en esta DPC, siempre y cuando exista una situación previa de representación legal o voluntaria entre la persona física y la Administración, organismo o entidad de derecho público suscriptora de los

---

<sup>1</sup> Ap 6.2.2.q) de ETSI EN 319 411-1

certificados, que exige su reconocimiento por esFIRMA, la cual se realizará mediante el siguiente procedimiento:

1. Un certificado de secretaría del acuerdo del pleno en el que se nombra al representante legal, con los siguientes datos:
  - a. como representante:
    - i. Nombre y apellidos
    - ii. Documento: NIF del representante
  - b. Los datos de identificación del suscriptor al que representa:
    - i. Nombre de la Administración, organismo o entidad de derecho público.
    - ii. Información sobre la extensión y vigencia de las facultades de representación del solicitante.
    - iii. Documento: NIF de Administración, organismo o entidad de derecho público.
    - iv. Documento: Documentos que sirvan para acreditar los extremos citados de manera fehaciente de conformidad con lo indicado en la normativa de derecho administrativo que sea de aplicación, y su inscripción en el correspondiente registro público si así resulta exigible.
  - c. Los datos relativos a la representación o la capacidad de actuación que ostenta:
    - i. La vigencia de la representación o la capacidad de actuación (fecha de inicio y fin).
    - ii. El ámbito y los límites, en su caso, de la representación o de la capacidad de actuación:
      1. TOTAL. Representación o capacidad total.
      2. PARCIAL. Representación o capacidad parcial.
2. Un contrato de prestación de servicios de certificación que firmará esFIRMA (ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA) y el representante legal de la Administración, que incluya:
3. Un Protocolo que firmará cada operador autorizado (incluyendo sus obligaciones)

Una vez firmados los documentos electrónicamente, se activarán las funciones de RA a los usuarios del Ayuntamiento que figuren en el contrato como operadores autorizados para desempeñar esta función.

### **3.2.3. Autenticación de la identidad de una persona física**

---

Esta sección describe los métodos de comprobación de la identidad de una persona física identificada en un certificado.

El procedimiento para solicitar y generar certificados se realiza a través de un procedimiento electrónico en la herramienta la Plataforma de Administración Electrónica disposición del suscriptor y de los firmantes.

El procedimiento electrónico para emitir un certificado a una persona física seguirá los siguientes pasos y se generarán los siguientes documentos:

1. Solicitud del Empleado del certificado a través de la Plataforma de Administración Electrónica (con su correspondiente registro de entrada y apertura de expediente)
2. Un certificado de secretaría, o del departamento de personal, en el que se certifica que esa persona está vinculada al Ayuntamiento.
3. Petición firmada por el operador autorizado por la entidad (o por el representante legal), que se registra de salida y se notifica a ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA(adjuntando copia del certificado y de la solicitud del empleado).

Para emitir un certificado de Sello electrónico se siguen los siguientes pasos, a través de un procedimiento electrónico en el que se generan los siguientes documentos:

1. Petición del representante legal de la entidad que se registra de salida y se notifica a ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA

Para emitir un certificado de Sede se siguen los siguientes pasos, a través de un procedimiento electrónico en el que se generan los siguientes documentos:

1. Petición del representante legal de la entidad que se registra de salida y se notifica a ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA.

#### 3.2.3.1. En los certificados

La información de identificación de las personas físicas identificadas en los certificados se valida comparando la información de la solicitud de la Administración, organismo o entidad de derecho público suscriptora de los certificados, con los registros de la Administración, organismo o entidad de derecho público a la que está vinculado, generados según lo indicado en el punto 3.2 de esta DPC, asegurando la corrección de la información a certificar.

#### 3.2.3.2. Necesidad de presencia personal

##### *Solicitud de certificados*

Para la solicitud de los certificados no se requiere la presencia física directa debido a la relación ya acreditada entre la persona física y la Administración, organismo o entidad de derecho público a la que está vinculada, ya que esta solicitud se realiza por un operador autorizado por el suscriptor en el contrato.

Tampoco es necesaria la presencia física directa del firmante para aceptar el certificado en aquellos casos en los que un sujeto ya previamente identificado en virtud de su relación con la Administración, organismo o entidad de derecho público de que se trate, firme la aceptación mediante su DNI electrónico.

Cuando no sea posible la firma mediante DNI electrónico, el firmante deberá imprimir el documento hoja de aceptación, para su firma ante el responsable del servicio de identificación, el cual deberá contrastar la identidad de la persona física identificada en el certificado mediante su presencia física. Durante este trámite se confirma fehacientemente la identidad de la persona física identificada en el certificado.

Por este motivo, sólo es necesario verificar presencialmente la identidad de la persona física firmante en el caso en que no sea posible firma la aceptación mediante su DNI electrónico.

##### *Renovación de certificados*

Si cualquiera de las informaciones de la persona física identificada en el certificado ha cambiado, será necesario registrar adecuadamente la nueva información y se producirá una autenticación completa, mediante identificación personal ante el operador autorizado por el suscriptor, el cual deberá contrastar la identidad de la persona física.

#### 3.2.3.3. Vinculación de la persona física

La justificación documental de la vinculación de una persona física identificada en un certificado con la Administración, organismo o entidad de derecho público a la que está vinculada viene dada por su constancia en los Registros de Personal de la Administración, organismo o entidad de derecho público a las que está vinculada la persona física.

#### **3.2.4. Información de suscriptor no verificada**

---

EsFIRMA no incluye ninguna información de suscriptor no verificada en los certificados.

### **3.3. Identificación y autenticación de solicitudes de renovación**

---

#### **3.3.1. Validación para la renovación rutinaria de certificados**

---

EsFIRMA, generalmente, no renueva certificados. Antes de su caducidad se firma la solicitud para la emisión de un nuevo certificado.

esFIRMA comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y de la persona física identificada en el certificado continúan siendo válidos.

Si cualquiera de las informaciones de la persona física identificada en el certificado ha cambiado, será necesario registrar adecuadamente la nueva información y se producirá una autenticación completa, de acuerdo con lo establecido en la sección 3.2.

### **3.3.2. Identificación y autenticación de la solicitud de renovación tras revocación previa**

---

Antes de generar un certificado a un suscriptor cuyo certificado fue revocado, esFIRMA comprobará que la información empleada en su día para verificar la identidad y los restantes datos del suscriptor y de la persona física identificada en el certificado continúa siendo válida, en cuyo caso se aplicará lo dispuesto en la sección anterior.

La renovación de certificados tras la revocación no será posible en los siguientes casos:

- El certificado fue revocado por emisión errónea a una persona diferente a la identificada en el certificado.
- El certificado fue revocado por emisión no autorizada por la persona física identificada en el certificado.
- El certificado revocado puede contener información errónea o falsa.

Si cualquier información del suscriptor o de la persona física identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una autenticación completa, de acuerdo con lo establecido en la sección 3.2.

## **3.4. Identificación y autenticación de la solicitud de revocación**

---

EsFIRMA autentica las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una persona autorizada.

Los métodos aceptables para dicha comprobación son los siguientes:

- El envío de una solicitud de revocación por parte del suscriptor o de la persona física identificada en el certificado, firmada electrónicamente.
- El uso de la "frase de comprobación de identidad", o de otros métodos de autenticación personal, que consiste en información que sólo conoce la persona física identificada en el certificado, y que le permite revocar de forma automática su certificado.
- La personación física en una oficina de la entidad suscriptora.
- Otros medios de comunicación, como el teléfono, cuando existan garantías razonables de la identidad del solicitante de la revocación, a juicio de esFIRMA.

### **3.5. Autenticación de una petición de suspensión**

---

Las peticiones de suspensión son tratadas como peticiones de revocación.

## 4. Requisitos de operación del ciclo de vida de los certificados

### 4.1. Solicitud de emisión de certificado

---

#### 4.1.1. Legitimación para solicitar la emisión

---

La Administración, organismo o entidad de derecho público debe firmar un contrato de prestación de servicios de certificación con esFIRMA.

Asimismo, con anterioridad a la emisión y entrega de un certificado, existe una solicitud de certificados en una hoja de solicitud de certificados por medio de la Plataforma de Administración Electrónica.

Existe una autorización del suscriptor para que el solicitante pueda realizar la solicitud, que se instrumenta jurídicamente mediante una hoja de solicitud de certificados suscrita por dicho solicitante en nombre de la Administración, organismo o entidad de derecho público.

#### 4.1.2. Procedimiento de alta y responsabilidades

---

EsFIRMA recibe solicitudes de certificados, realizadas por las Administraciones, organismos o entidades de derecho público públicas.

Las solicitudes se instrumentan mediante un documento en formato electrónico, cumplimentado por la Administración, organismo o entidad de derecho público, cuyo destinatario es esFIRMA, el cual incluirá los datos de las personas a las que se expedirán certificados. La solicitud será realizada por el operador autorizado por el suscriptor (responsable de certificación) y que ha sido identificado en el contrato entre este suscriptor y esFIRMA.

A la solicitud se deberá acompañar documentación justificativa de la identidad y otras circunstancias de la persona física identificada en el certificado, de acuerdo con lo establecido en la sección 3.2.3. También se deberá acompañar una dirección física, u otros datos, que permitan contactar a la persona física identificada en el certificado.

## **4.2. Procesamiento de la solicitud de certificación**

---

### **4.2.1. Ejecución de las funciones de identificación y autenticación**

---

Una vez recibida una petición de certificado, esFIRMA se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

En caso afirmativo, esFIRMA verifica la información proporcionada, comprobando que se han cumplido correctamente los requisitos descritos en la sección 3.2.

La documentación justificativa de la aprobación de la solicitud debe ser conservada y debidamente registrada y con garantías de seguridad e integridad durante el plazo de 15 años desde la expiración del certificado, incluso en caso de pérdida anticipada de vigencia por revocación, al ser los certificados, cualificados.

### **4.2.2. Aprobación o rechazo de la solicitud**

---

EsFIRMA aprueba la solicitud del certificado y procede a su emisión y entrega, tras la petición que se produce en la Plataforma de Administración Electrónica.

En caso de sospecha que la información no es correcta o que puede afectar a la reputación de la Entidad de Certificación o de los suscriptores, esFIRMA denegará la petición, o detendrá su aprobación hasta haber realizado las comprobaciones complementarias que considere oportunas.

En caso de que de las comprobaciones adicionales no se desprenda la corrección de las informaciones a verificar, esFIRMA denegará la solicitud definitivamente.

EsFIRMA notifica al solicitante la aprobación o denegación de la solicitud.

EsFIRMA podrá automatizar los procedimientos de verificación de la corrección de la información que será contenida en los certificados, y de aprobación de las solicitudes.

#### **4.2.3. Plazo para resolver la solicitud**

---

EsFIRMA atiende las solicitudes de certificados por orden de llegada, en un plazo razonable, pudiendo especificarse una garantía de plazo máximo en el contrato de emisión de certificados.

Las solicitudes se mantienen activas hasta su aprobación o rechazo.

### **4.3. Emisión del certificado**

---

#### **4.3.1. Acciones de la CA durante el proceso de emisión**

---

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se pone a disposición del firmante para su aceptación mediante el envío de un enlace al dispositivo móvil y/o dirección de correo electrónico que se haya designado por el suscriptor en la petición de certificados, según el procedimiento indicado en el apartado 4.4.2.

Durante el proceso, esFIRMA:

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.

## **esFIRMA:** Prácticas de Certificación

- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
- Incluye en el certificado las informaciones establecidas en el anexo 1 del Reglamento (UE) 910/2014, de acuerdo con lo establecido en las secciones 3.1.1 y 7.1.
- Indica la fecha y la hora en que se expidió un certificado.

### **4.3.2. Notificación de la emisión al suscriptor**

---

EsFIRMA notifica la emisión del certificado a la Administración, organismo o entidad de derecho público suscriptora del certificado, ya la persona física identificada en el certificado, a través de sus direcciones de correo electrónico, ya incluidas en la información de la Plataforma de Administración Electrónica.

## **4.4. Entrega y aceptación del certificado**

---

### **4.4.1. Responsabilidades de la CA**

---

Durante este proceso, esFIRMA debe realizar las siguientes actuaciones:

- Acreditar definitivamente la identidad de la persona física identificada en el certificado, con la colaboración de la Administración, organismo o entidad de derecho público de acuerdo con lo establecido en las secciones 3.2.2, 3.2.3, y 4.3.1.
- Entregar la hoja de entrega y aceptación del certificado a la persona física identificada en el certificado (con la colaboración de la Administración, organismo o entidad de derecho público en los casos en que el firmante no disponga de DNI electrónico), la cual dispone de los siguientes contenidos mínimos:

- o Información básica acerca del uso del certificado, incluyendo especialmente información acerca del prestador de servicios de certificación y de la Declaración de Prácticas de Certificación aplicable, como sus obligaciones, facultades y responsabilidades
  - o Información acerca del certificado.
  - o Reconocimiento, por parte del firmante, de recibir el certificado y la aceptación de los citados elementos.
  - o Régimen de obligaciones del firmante.
  - o Responsabilidad del firmante.
  - o Método de imputación exclusiva al firmante, de su clave privada y de sus datos de activación del certificado, de acuerdo con lo establecido en las secciones 6.2 y 6.4.
  - o La fecha del acto de entrega y aceptación.
- Obtener la firma, escrita o electrónica, de la persona identificada en el certificado.

Cuando sea necesario, la Administración, organismo o entidad de derecho público colabora en estos procesos, debiendo registrar documentalmente los anteriores actos y conservando los citados documentos originales (hojas de entrega y aceptación), remitiendo copia electrónica a esFIRMA, así como los originales cuando esFIRMA precise de acceso a los mismos.

#### **4.4.2. Conducta que constituye aceptación del certificado**

---

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se avisa al firmante para su aceptación mediante el envío de un enlace al dispositivo móvil y/o dirección de correo electrónico que se haya designado por el suscriptor en la petición de certificados o mediante el sistema de mensajería de la Plataforma de Administración Electrónica.

En los certificados emitidos en software, el certificado y las claves son gestionadas en un HSM, disponiendo el firmante de control exclusivo de su uso.

En los certificados emitidos en tarjeta, estas son enviadas al responsable de certificación del suscriptor, y los correspondientes PINes directamente a la dirección postal del firmante.

Además, la aceptación del certificado por la persona física identificada en el certificado se produce mediante la firma de la hoja de entrega y aceptación, por medio de la Plataforma de Administración Electrónica.

#### **4.4.3. Publicación del certificado**

---

EsFIRMA publica el certificado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes y siempre que esFIRMA disponga de la autorización de la persona física identificada en el certificado.

EsFIRMA publica el certificado de TSA/TSU en su página web.

#### **4.4.4. Notificación de la emisión a terceros**

---

EsFIRMA no realiza ninguna notificación de la emisión a terceras entidades.

### **4.5. Uso del par de claves y del certificado**

---

#### **4.5.1. Uso por el suscriptor o firmante**

---

EsFIRMA obliga a lo siguiente:

- Facilitar a esFIRMA información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de aceptación.
- Manifiestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4.
- Cuando el certificado funcione conjuntamente con un DCCF, reconocer su capacidad de producción de firmas electrónicas cualificadas; esto es,

## esFIRMA: Prácticas de Certificación

equivalentes a firmas manuscritas, así como otros tipos de firmas electrónicas y mecanismos de cifrado de información.

- Ser especialmente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6.1, 6.2 y 6.4.
- Comunicar a esFIRMA ya cualquier persona que se crea que pueda confiar en el certificado, sin retrasos injustificables:
  - La pérdida, el robo o el compromiso potencial de su clave privada.
  - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
  - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2.

EsFIRMA obliga al firmante a responsabilizarse de:

- Que todas las informaciones suministradas por el firmante que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el firmante es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

## 4.5.2. Uso por el suscriptor

---

### 4.5.2.1. Obligaciones del suscriptor del certificado

---

EsFIRMA obliga contractualmente al suscriptor a:

- Facilitar a la Entidad de Certificación información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de aceptación.
- Manifiestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4.
- Comunicar a esFIRMA ya cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
  - La pérdida, el robo o el compromiso potencial de su clave privada.
  - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
  - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
  - La pérdida, la alteración, el uso no autorizado, el robo o el compromiso, cuando exista, de la tarjeta.
- Trasladar a las personas físicas identificadas en el certificado el cumplimiento de las obligaciones específicas de los mismos, y establecer mecanismos para garantizar el efectivo cumplimiento de las mismas.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de esFIRMA, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación del prestador de servicios de certificación de esFIRMA, sin permiso previo por escrito.

### 4.5.2.2. Responsabilidad civil del suscriptor de certificado

---

EsFIRMA obliga contractualmente al suscriptor a responsabilizarse de:

- Que todas las manifestaciones realizadas en la solicitud son correctas.
- Que todas las informaciones suministradas por el suscriptor que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el suscriptor es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

### **4.5.3. Uso por el tercero que confía en certificados**

---

#### 4.5.3.1. Obligaciones del tercero que confía en certificados

EsFIRMA informa al tercero que confía en certificados de que el mismo debe asumir las siguientes obligaciones:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez, suspensión o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía
- Reconocer que las firmas electrónicas verificadas, producidas en un dispositivo cualificado de creación de firma (DCCF) tienen la consideración legal de firmas electrónicas cualificadas; esto es, equivalentes a firmas manuscritas, así como que el certificado permite la creación de otros tipos de firmas electrónicas y mecanismos de cifrado.
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.

## esFIRMA: Prácticas de Certificación

- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de esFIRMA, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación de la esFIRMA, sin permiso previo por escrito.

### 4.5.3.2. Responsabilidad civil del tercero que confía en certificados

---

EsFIRMA informa al tercero que confía en certificados de que el mismo debe asumir las siguientes responsabilidades:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

## 4.6. Renovación de certificados

---

EsFIRMA no realiza renovación de certificados. Caducado el certificado se emite un certificado nuevo, siguiendo el procedimiento de solicitud registrado en la Plataforma de Administración Electrónica.

## 4.7. Renovación de claves y certificados

---

### 4.7.1. Causas de renovación de claves y certificados

---

No aplica.

#### **4.7.2. Procedimiento con nueva identificación**

---

EsFIRMA advertirá al suscriptor de la necesidad de proceder a una nueva personación del firmante y firma de la hoja de aceptación, en aquellos casos en los que así sea necesario por transcurso del plazo legal de identificación de 5 años.

Dicha personación e identificación se realizará de conformidad con lo indicado en el apartado 3.2.

La firma de la hoja de aceptación se realizará de conformidad con lo indicado en el apartado 4.4.2.

#### **4.7.3. Notificación de la emisión del certificado renovado**

---

No aplica por no existir renovaciones.

#### **4.7.4. Conducta que constituye aceptación del certificado**

---

No aplica.

#### **4.7.5. Publicación del certificado**

---

No aplica.

#### **4.7.6. Notificación de la emisión a terceros**

---

EsFIRMA no realiza notificación alguna de la emisión a terceras entidades.

### **4.8. Modificación de certificados**

---

La modificación de certificados, excepto la modificación de la clave pública certificada, que se considera renovación, será tratada como una nueva emisión de certificado, aplicándose lo descrito en las secciones 4.1, 4.2, 4.3 y 4.4.

## 4.9. Revocación y suspensión de certificados

---

### 4.9.1. Causas de revocación de certificados

---

EsFIRMA revoca un certificado cuando concurre alguna de las siguientes causas:

- 1) Circunstancias que afectan a la información contenida en el certificado:
  - a) Modificación de alguno de los datos contenidos en el certificado, después de la correspondiente emisión del certificado que incluye las modificaciones.
  - b) Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
  - c) Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.
  
- 2) Circunstancias que afectan a la seguridad de la clave o del certificado:
  - a) Compromiso de la clave privada, de la infraestructura o de los sistemas del prestador de servicios de certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
  - b) Infracción, por esFIRMA, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta Declaración de Prácticas de Certificación.
  - c) Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado emitido.
  - d) Acceso o utilización no autorizados, por un tercero, de la clave privada correspondiente a la clave pública contenida en el certificado.
  - e) El uso irregular del certificado por la persona física identificada en el certificado, o la falta de diligencia en la custodia de la clave privada.
  
- 3) Circunstancias que afectan al suscriptor o a la persona física identificada en el certificado:
  - a) Finalización de la relación jurídica de prestación de servicios entre esFIRMA y el suscriptor.

- b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado a la persona física identificada en el certificado.
  - c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.
  - d) Infracción por el suscriptor o por la persona identificada en el certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente.
  - e) La incapacidad sobrevenida o el fallecimiento del poseedor de claves.
  - f) La extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor al poseedor de claves o la finalización de la relación entre suscriptor y persona identificada en el certificado.
  - g) Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 3.4.
- 4) Otras circunstancias:
- a) La terminación del servicio de certificación de esFIRMA, de acuerdo con lo establecido en la sección 5.8.
  - b) El uso del certificado que sea dañino y continuado para esFIRMA. En este caso, se considera que un uso es dañino en función de los siguientes criterios:
    - o La naturaleza y el número de quejas recibidas.
    - o La identidad de las entidades que presentan las quejas.
    - o La legislación relevante vigente en cada momento.
    - o La respuesta del suscriptor o de la persona identificada en el certificado a las quejas recibidas.

#### **4.9.2. Legitimación para solicitar la revocación**

---

Pueden solicitar la revocación de un certificado:

- La persona identificada en el certificado, mediante petición dirigida a esFIRMA o al suscriptor.
- El suscriptor del certificado, mediante petición dirigida a esFIRMA.

### **4.9.3. Procedimientos de solicitud de revocación**

---

La solicitud de revocación comprenderá la siguiente información:

- Fecha de solicitud de la revocación.
- Identidad del suscriptor o del firmante.
- Razón detallada para la petición de revocación.

La solicitud debe ser autenticada, por esFIRMA, de acuerdo con los requisitos establecidos en la sección 3.4 de esta política, antes de proceder a la revocación.

EsFIRMA podrá incluir cualquier otro requisito para la confirmación de las solicitudes de revocación<sup>2</sup>.

El servicio de revocación se encuentra en la Plataforma de Administración Electrónica, en la que el firmante y el suscriptor gestionan sus certificados.

En caso de que el destinatario de una solicitud de revocación por parte de una persona física identificada en el certificado fuera la entidad suscriptora una vez autenticada la solicitud ésta debe remitir una solicitud en este sentido a esFIRMA.

La solicitud de revocación será procesada a su recepción, y se informará al suscriptor y, a la persona física identificada en el certificado, acerca del cambio de estado del certificado revocado.

EsFIRMA no reactiva el certificado una vez ha sido revocado.

### **4.9.4. Plazo temporal de solicitud de revocación**

---

Las solicitudes de revocación se remitirán de forma inmediata en cuanto se tenga conocimiento de la causa de revocación, y no será superior a las 24 horas<sup>3</sup>.

---

<sup>2</sup> Ap 6.2.4.a) iii) de ETSI EN 319 411-1

<sup>3</sup> Ap 6.2.4.a) vi) de ETSI EN 319 411-1

#### **4.9.5. Plazo temporal de procesamiento de la solicitud**

---

La revocación se producirá inmediatamente cuando sea recibida, dentro del horario ordinario de operación de esFIRMA, y no será superior a los 60 minutos<sup>4</sup>.

#### **4.9.6. Obligación de consulta de información de revocación de certificados**

---

Los terceros deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se puede verificar el estado de los certificados es consultando la Lista de Revocación de Certificados más reciente emitida por la Entidad de Certificación de esFIRMA.

Las Listas de Revocación de Certificados se publican en el Depósito de la Entidad de Certificación, así como en las siguientes direcciones web, indicadas dentro de los certificados:

- *CA ROOT:*
  - <https://crls2.esfirma.com/acraiz/acraiz2.crl>
  
  - <https://crls1.esfirma.com/acraiz/acraiz2.crl>
  
- *CA INTERMEDIA:*
  - <https://crls1.esfirma.com/acaapp/acaapp2.crl>
  - <https://crls2.esfirma.com/acaapp/acaapp2.crl>

#### **4.9.7. Frecuencia de emisión de listas de revocación de certificados (LRCs)**

---

EsFIRMA emite una LRC al menos cada 24 horas y siempre que se produzca una revocación.

---

<sup>4</sup> Ap 6.2.4.a) vii) de ETSI EN 319 411-1

La LRC indica el momento programado de emisión de una nueva LRC, si bien se puede emitir una LRC antes del plazo indicado en la LRC anterior, para reflejar revocaciones.

La LRC mantiene obligatoriamente el certificado revocado o suspendido hasta que expira.

#### **4.9.8. Plazo máximo de publicación de LRCs**

---

Las LRCs se publican en el Depósito en un periodo inmediato razonable tras su generación, que en ningún caso no supera unos pocos minutos.

#### **4.9.9. Disponibilidad de servicios de comprobación en línea de estado de certificados**

---

EsFIRMA informa acerca del estado de revocación de los certificados, mediante el protocolo OCSP, que permite conocer el estado de vigencia de los certificados en línea desde las direcciones:

- <http://ocsp.esfirma.com/acaapp2/>
- <http://ocsp1.esfirma.com/acaapp2/>
- <http://ocsp2.esfirma.com/acaapp2/>

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de esFIRMA, ésta deberá realizar sus mejores esfuerzos por asegurar que este servicio se mantenga inactivo el mínimo tiempo posible, que no podrá superar un día.

EsFIRMA suministra información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

Los servicios de comprobación de estado de los certificados son de uso gratuito<sup>5</sup>.

---

<sup>5</sup> Ap 6.3.10 de ETSI EN 319 411-2

EsFIRMA mantiene disponible la información del estado de revocación pasado el período de validez del certificado<sup>6</sup>.

#### **4.9.10. Obligación de consulta de servicios de comprobación de estado de certificados**

Resulta obligatorio consultar el estado de los certificados antes de confiar en los mismos, de forma prioritaria, mediante acceso al servicio OCSP.

#### **4.9.11. Otras formas de información de revocación de certificados**

De forma alternativa, los terceros que confían en certificados podrán consultar el Depósito de certificados de esFIRMA, que se encuentra disponible las 24 horas de los 7 días de la semana en el web:

<https://www.esfirma.com>

#### **4.9.12. Requisitos especiales en caso de compromiso de la clave privada**

El compromiso de la clave privada de esFIRMA es notificado a todos los participantes en los servicios de certificación, en la medida de lo posible, mediante la publicación de este hecho en la página web de esFIRMA, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.

#### **4.9.13. Causas de suspensión de certificados**

- EsFIRMA no realiza suspensión de certificados.

#### **4.9.14. Solicitud de suspensión**

- EsFIRMA no realiza suspensión de certificados

#### **4.9.15. Procedimientos para la petición de suspensión**

EsFIRMA no realiza suspensión de certificados.

---

<sup>6</sup> Ap 6.3.10.b) de ETSI EN 319 411-2

#### **4.9.16. Período máximo de suspensión**

---

EsFIRMA no realiza suspensión de certificados.

### **4.10. Finalización de la suscripción**

---

Transcurrido el periodo de vigencia del certificado, finalizará la suscripción al servicio.

EsFIRMA puede emitir de oficio un nuevo certificado, mientras los suscriptores mantengan dicho estado.

### **4.11. Servicios de comprobación de estado de certificados**

---

#### **4.11.1. Características operativas de los servicios**

---

Los servicios de comprobación de estado de certificados se prestan mediante una interfaz de consulta web, en la web <https://www.esfirma.com>

También se pueden comprobar mediante acceso al servicio OCSP en las direcciones web indicadas en el apartado 4.9.6

#### **4.11.2. Disponibilidad de los servicios**

---

Los servicios de comprobación de estado de certificados se encuentran disponibles las 24 horas del día, los 7 días de la semana, durante todo el año, con excepción de las paradas programadas.

### **4.12. Depósito y recuperación de claves**

---

#### **4.12.1. Política y prácticas de depósito y recuperación de claves**

---

EsFIRMA no presta servicios de depósito y recuperación de claves.

#### **4.12.2. Política y prácticas de encapsulado y recuperación de claves de sesión**

---

Sin estipulación.

## 5. Controles de seguridad física, de gestión y de operaciones

### 5.1. Controles de seguridad física

---

EsFIRMA ha establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones de registro y aprobación de las solicitudes, generación técnica de los certificados y la gestión del hardware criptográfico.

En concreto, la política de seguridad física y ambiental aplicable a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación ha establecido prescripciones para las siguientes contingencias:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobo.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

Estas medidas resultan aplicables a las instalaciones donde se producen los certificados bajo la plena responsabilidad de esFIRMA, que la presta desde sus instalaciones de alta seguridad, tanto principales como, en su caso, de operación en contingencia, que son debidamente auditadas de forma periódica.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso.

#### **5.1.1. Localización y construcción de las instalaciones**

---

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

La sala donde se realizan las operaciones criptográficas en el Centro de Proceso de Datos:

- Cuenta con redundancia en sus infraestructuras.
- Cuenta con varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.
- Las operaciones de mantenimiento no requieren que el Centro esté offline en ningún momento.
- Fiabilidad del 99,995% mensual

EsFIRMA dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de los mismos

#### **5.1.2. Acceso físico**

---

El CPD donde se ubica la CA de EsFIRMA dispone de la calificación TIER IV.

El acceso físico a las dependencias de esFIRMA donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales. Así:

- Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

- El acceso a las salas se realiza con lectores de tarjeta de identificación.
- Para el acceso al rac donde se ubican los procesos criptográficos es necesario la autorización previa de esFIRMA a los administradores del servicio de hospedaje que disponen de la llave para abrir la jaula.

### **5.1.3. Electricidad y aire acondicionado**

---

Las instalaciones de esFIRMA disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado.

### **5.1.4. Exposición al agua**

---

Las instalaciones están ubicadas en una zona de bajo riesgo de inundación.

Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

### **5.1.5. Prevención y protección de incendios**

---

Las instalaciones y activos de esFIRMA cuentan con sistemas automáticos de detección y extinción de incendios.

### **5.1.6. Almacenamiento de soportes**

---

Únicamente personal autorizado tiene acceso a los medios de almacenamiento.

La información de más alto nivel de clasificación se guarda en una caja de seguridad fuera de las instalaciones del Centro de Proceso de Datos.

### 5.1.7. Tratamiento de residuos

---

La eliminación de soportes, tanto papel como magnéticos, se realizan mediante mecanismos que garanticen la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se procede al formateo, borrado permanente, o destrucción física del soporte, mediante software especializado que realice un mínimo de 3 pasadas de borrado y con patrones de borrado variable.

En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

### 5.1.8. Copia de respaldo fuera de las instalaciones

---

EsFIRMA utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del centro de operaciones.

Se requieren al menos dos personas autorizadas expresamente para el acceso, depósito o retirada de dispositivos.

## 5.2. Controles de procedimientos

---

EsFIRMA garantiza que sus sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal al servicio de esFIRMA ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

### 5.2.1. Funciones fiables

---

EsFIRMA ha identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- **Auditor Interno:** Responsable del cumplimiento de los procedimientos operativos. Se trata de una persona externa al departamento de Sistemas de

Información. Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.

- **Administrador de Sistemas:** Responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación
- **Administrador de CA:** Responsable de las acciones a ejecutar con el material criptográfico, o con la realización de alguna función que implique la activación de las claves privadas de las autoridades de certificación descritas en este documento, o de cualquiera de sus elementos.
- **Operador de CA:** Responsable necesario conjuntamente con el Administrador de CA de la custodia de material de activación de las claves criptográficas, también responsable de las operaciones de copia de respaldo y mantenimiento de la AC.
- **Administrador de Registro:** Persona responsable de aprobar las peticiones de certificación realizadas por el suscriptor.
- **Responsable de Seguridad:** Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de esFIRMA. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos.

### **5.2.2. Número de personas por tarea**

---

EsFIRMA garantiza al menos dos personas para realizar las tareas que se detallan en las Políticas de Certificación correspondientes. Especialmente en la manipulación del dispositivo de custodia de las claves de la Autoridad de Certificación raíz e intermedias.

### **5.2.3. Identificación y autenticación para cada función**

---

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurará que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante tarjetas criptográficas y códigos de activación.

#### **5.2.4. Roles que requieren separación de tareas**

---

Las siguientes tareas son realizadas, al menos, por dos personas:

- Emisión y revocación de certificados, y el acceso al depósito.
- Generación, emisión y destrucción de certificados de la Entidad de Certificación.
- Puesta en producción de la Entidad de Certificación.

#### **5.2.5. Sistema de gestión PKI**

---

El sistema de PKI se compone de los siguientes módulos:

- Componente/módulo de gestión de la Autoridad de Certificación Subordinada.
- Componente/módulo de gestión de la Autoridad de Registro.
- Componente/módulo de gestión de solicitudes.
- Componente/módulo de gestión de claves (HSM).
- Componente/módulo de bases de datos.
- Componente/módulo de gestión de CRL.
- Componente/módulo de gestión del servicio de OCSP.
- Componente/módulo de gestión de la Autoridad de Sellado de Tiempo (TSA)

### **5.3. Controles de personal**

---

#### **5.3.1. Requisitos de historial, calificaciones, experiencia y autorización**

---

Todo el personal que realiza tareas calificadas como confiables, lleva al menos un año trabajando en el centro de producción y tiene contratos laborales fijos.

Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

El personal en puestos de confianza no tiene intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

EsFIRMA se asegura de que el personal de registro es confiable para realizar las tareas de registro.

El Administrador de Registro ha realizado un curso de preparación para la realización de las tareas de validación de las peticiones.

En general, esFIRMA retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

EsFIRMA no asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por haber sido condenada por delito o falta que afecte su idoneidad para el puesto. Por este motivo, previamente se realiza una investigación, hasta donde permita la legislación aplicable, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales y comprobación que realmente se realizó el trabajo alegado.
- Morosidad.

### **5.3.2. Procedimientos de investigación de historial**

---

EsFIRMA, antes de contratar a una persona o de que ésta acceda al puesto de trabajo, realiza las siguientes comprobaciones:

- Referencias de los trabajos de los últimos años
- Referencias profesionales
- Estudios, incluyendo titulación alegada.

EsFIRMA obtiene el consentimiento inequívoco del afectado para dicha investigación previa, y procesa y protege todos sus datos personales de acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

La investigación se repetirá con una periodicidad suficiente.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

En la solicitud para el puesto de trabajo se informa acerca de la necesidad de someterse a una investigación previa, advirtiéndose de que la negativa a someterse a la investigación implicará el rechazo de la solicitud.

### **5.3.3. Requisitos de formación**

---

EsFIRMA forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación.

Los programas de formación son actualizados y mejorados de forma periódica.

La formación incluye, al menos, los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad de EsFIRMA. Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.

- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

#### **5.3.4. Requisitos y frecuencia de actualización formativa**

---

EsFIRMA actualiza la formación del personal de acuerdo con las necesidades, y con la frecuencia suficientes para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación

#### **5.3.5. Secuencia y frecuencia de rotación laboral**

---

No aplicable.

#### **5.3.6. Sanciones para acciones no autorizadas**

---

EsFIRMA dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable y, en especial, coordinado con el sistema sancionador del convenio colectivo que resulte de aplicación al personal.

Las acciones disciplinarias incluyen la suspensión y el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

#### **5.3.7. Requisitos de contratación de profesionales**

---

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por esFIRMA. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían, una vez evaluados, dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la DPC, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, no obstante, lo cual, la entidad de certificación será

responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto a esFIRMA.

### **5.3.8. Suministro de documentación al personal**

---

El prestador de servicios de certificación suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

## **5.4. Procedimientos de auditoría de seguridad**

---

### **5.4.1. Tipos de eventos registrados**

---

EsFIRMA produce y guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la AC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de éste.

- Las actividades de los cortafuegos y enrutadores<sup>7</sup>
- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor, en caso de certificados individuales, o de la persona física identificada en el certificado, en caso de certificados de organización.
- Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Certificación.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.

Las entradas del registro incluyen los siguientes elementos:

- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.
- Tipo de entrada.

Quedan registrados todos los sucesos relacionados con la preparación de los dispositivos cualificados de creación de firmas que son usados por los firmantes o custodios<sup>8</sup>.

#### **5.4.2. Frecuencia de tratamiento de registros de auditoría**

---

EsFIRMA revisa sus logs cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección

---

<sup>7</sup> Ap 6.4.5.a) de ETSI EN 319 411-1

<sup>8</sup> Ap 6.4.5.a) de ETSI EN 319 411-2

de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

EsFIRMA mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

#### **5.4.3. Período de conservación de registros de auditoría**

---

EsFIRMA almacena la información de los logs durante un periodo de entre 1 y 15 años, en función del tipo de información registrada.

#### **5.4.4. Protección de los registros de auditoría**

---

Los logs de los sistemas:

- Están protegidos de manipulación, borrado o eliminación<sup>9</sup> mediante la firma de los ficheros que los contienen.
- Son almacenados en dispositivos ignífugos.
- Se protege su disponibilidad mediante su almacenamiento en instalaciones externas al centro donde se ubica la AC.

El acceso a los ficheros de logs está reservado sólo a las personas autorizadas. Asimismo, los dispositivos son manejados en todo momento por personal autorizado.

Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

---

<sup>9</sup> Ap 7.10.f) de ETSI EN 319 401

#### **5.4.5. Procedimientos de copia de respaldo**

---

EsFIRMA dispone de un procedimiento adecuado de backup de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

EsFIRMA tiene implementado un procedimiento de backup seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo. Adicionalmente se mantiene copia en centro de custodia externo.

#### **5.4.6. Localización del sistema de acumulación de registros de auditoría**

---

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo, las comunicaciones de red y por el software de gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado. Todo ello compone el sistema de acumulación de registros de auditoría.

#### **5.4.7. Notificación del evento de auditoría al causante del evento**

---

Cuando el sistema de acumulación de registros de auditoría registre un evento, no es preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

#### **5.4.8. Análisis de vulnerabilidades**

---

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de EsFIRMA.

Los análisis de vulnerabilidad deben ser ejecutados, repasados y revisados por medio de un examen de estos acontecimientos monitorizados. Estos análisis deben ser ejecutados diariamente, mensualmente y anualmente.

Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

## 5.5. Archivos de informaciones

---

EsFIRMA, garantiza que toda la información relativa a los certificados se conserva durante un período de tiempo apropiado, según lo establecido en la sección 5.5.2 de esta política.

### 5.5.1. Tipos de registros archivados

---

Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por EsFIRMA (o por las entidades de registro):

- Todos los datos de auditoría de sistema (PKI, TSA y OCSP).
- Todos los datos relativos a los certificados, incluyendo los contratos con los firmantes y los datos relativos a su identificación y su ubicación
- Solicitudes de emisión y revocación de certificados, incluidos todos los informes relativos al proceso de revocación<sup>10</sup>.
- Todas aquellas elecciones específicas que el firmante o el suscriptor disponga durante el acuerdo de suscripción<sup>11</sup>.
- Tipo de documento presentado en la solicitud del certificado.
- Identidad de la Entidad de Registro que acepta la solicitud de certificado.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- El historial de claves generadas.
- Las comunicaciones entre los elementos de la PKI.
- Políticas y Prácticas de Certificación
- Todos los datos de auditoría identificados en la sección 5.4
- Información de solicitudes de certificación.
- Documentación aportada para justificar las solicitudes de certificación.
- Información del ciclo de vida del certificado.

EsFIRMA es responsable del correcto archivo de todo este material.

---

<sup>10</sup> Ap 6.4.5.h) de ETSI EN 319 411-1

<sup>11</sup> Ap 6.4.5.c) iv) de ETSI EN 319 411-1

### **5.5.2. Período de conservación de registros**

---

EsFIRMA archiva los registros especificados anteriormente durante al menos 15 años.

### **5.5.3. Protección del archivo**

---

EsFIRMA protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. El archivo es protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.

EsFIRMA asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas.

### **5.5.4. Procedimientos de copia de respaldo**

---

EsFIRMA dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido sólo a personal autorizado.

EsFIRMA como mínimo realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos y realizar copias de respaldo completas semanalmente para casos de recuperación de datos.

Además, esFIRMA (o las organizaciones que realizan la función de registro) guarda copia de los documentos en papel en un lugar seguro diferente de las instalaciones de la propia Entidad de certificación.

### **5.5.5. Requisitos de sellado de fecha y hora**

---

Los registros están fechados con una fuente fiable vía NTP.

EsFIRMA dispone de un procedimiento donde describe la configuración de tiempos de los equipos utilizados en la emisión de certificados.

La hora empleada para registrar los sucesos del registro de auditoría deberá ser sincronizada con la UTC, como mínimo, una vez al día<sup>12</sup>.

No es necesario que esta información se encuentre firmada digitalmente.

#### **5.5.6. Localización del sistema de archivo**

---

EsFIRMA dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

#### **5.5.7. Procedimientos de obtención y verificación de información de archivo**

---

EsFIRMA dispone de un procedimiento donde se describe el proceso para verificar que la información archivada es correcta y accesible.

### **5.6. Renovación de claves**

---

Con anterioridad a que el uso de la clave privada de la AC caduque, será realizado un cambio de claves. La antigua AC y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por dicha AC. Se generará una nueva AC con una clave privada nueva y un nuevo DN.

El cambio de claves del suscriptor es realizado mediante la realización de un nuevo proceso de emisión.

### **5.7. Compromiso de claves y recuperación de desastre**

---

---

<sup>12</sup> Ap 7.10.d) de la ETSI EN 319 401

### **5.7.1. Procedimientos de gestión de incidencias y compromisos**

---

Son almacenadas copias de seguridad de la siguiente información en instalaciones de almacenamiento externo a esFIRMA, que se ponen a disposición en caso de compromiso o desastre: datos técnicos de solicitud de certificados, datos de auditoría y registros de base de datos de todos los certificados emitidos.

Las copias de seguridad de las claves privadas de esFIRMA son generadas y mantenidas de acuerdo con lo establecido en la sección 6.2.4

### **5.7.2. Corrupción de recursos, aplicaciones o datos**

---

Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se comunicará la incidencia a seguridad, y se iniciarán los procedimientos de gestión oportunos, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres de esFIRMA.

### **5.7.3. Compromiso de la clave privada de la entidad**

---

En caso de sospecha o conocimiento del compromiso de esFIRMA, se activarán los procedimientos de compromiso de claves, dirigidos por un equipo de respuesta que evaluará la situación, desarrollará un plan de acción, que será ejecutado bajo la aprobación de la dirección de la Entidad de Certificación.

En caso de compromiso de la clave privada de esFIRMA puede darse el caso que los estados de los certificados y de los procesos de revocación usando esta clave, podrían no ser válidos<sup>13</sup>.

EsFIRMA ha desarrollado un Plan de contingencias para recuperar los sistemas críticos, si fuera necesario en un centro de datos alternativo.

El caso de compromiso de la clave raíz debe tomarse como un caso separado en el proceso de contingencia y continuidad de negocio. Esta incidencia afecta, en caso de

---

<sup>13</sup> Ap 6.4.8.g) ii) de ETSI EN 319 411-1

sustitución de las claves, a los reconocimientos por diferentes aplicativos y servicios privados y públicos. Una recuperación de la efectividad de las claves en términos de negocio dependerá principalmente de la duración de estos procesos. El documento de contingencia y continuidad de negocio tratará los términos puramente operativos para que las nuevas claves estén disponibles, no así su reconocimiento por terceros.

Cualquier fallo en la consecución de las metas marcadas por este Plan de contingencias, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la AC para implementar dichos procesos.

#### **5.7.4. Continuidad del negocio después de un desastre**

---

EsFIRMA restablecerá los servicios críticos (suspensión y revocación, y publicación de información de estado de certificados) de acuerdo con el plan de contingencias y continuidad de negocio existente restaurando la operación normal de los servicios anteriores en las 24 horas siguientes al desastre.

EsFIRMA dispone de un centro alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación descritos en el plan de continuidad de negocio.

#### **5.7.5. Gestión de revocaciones**

---

Tanto el servicio de gestión de las revocaciones como el servicio de consulta son considerados servicios críticos y así constan en el Plan de contingencias y el plan de continuidad de negocio de esFIRMA

### **5.8. Terminación del servicio**

---

EsFIRMA asegura que las posibles interrupciones a los suscriptores ya terceras partes son mínimas como consecuencia del cese de los servicios del prestador de servicios de certificación y, en particular, aseguran un mantenimiento continuo de los registros requeridos para proporcionar evidencia de certificación en caso de investigación civil o criminal, mediante su transferencia a un depósito notarial.

Antes de terminar sus servicios, esFIRMA desarrolla un plan de terminación, con las siguientes provisiones:

- Proveerá de los fondos necesarios (mediante seguro de responsabilidad civil) para continuar la finalización de las actividades de revocación.
- Comunicará al Ministerio de Industria, Energía y Turismo, con una antelación mínima de 2 meses, el cese de su actividad y el destino de los certificados especificando si se transfiere la gestión ya quién, o si se extinguirá su vigencia.
- Comunicará, también el Ministerio de Industria, Energía y Turismo, la apertura de cualquier proceso concursal que se siga contra esFIRMA así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.
- Informará a todos Firmantes/Suscriptores, Tercero que confían y otras AC's con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 6 meses.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.
- Transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios, al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio.
- Destruirá o deshabilitará para su uso las claves privadas de la AC.
- Se revocarán los certificados de las Unidades de Sellado de Tiempo (TSU)
- Mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos.
- Ejecutará las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los períodos de tiempo respectivos indicados al suscriptor ya los terceros que confían en certificados.

## 6. Controles de seguridad técnica

### 6.1. Generación e instalación del par de claves

#### 6.1.1. Generación del par de claves

El par de claves de la entidad de certificación intermedia “ESFIRMA AC AAPP” es creado por la entidad de certificación raíz “ESFIRMA AC ROOT” de acuerdo con los procedimientos de ceremonia de esFIRMA, dentro del perímetro de alta seguridad destinado a esta tarea.

Las actividades realizadas durante la ceremonia de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en la misma, con la presencia de un Auditor CISA. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por esFIRMA.

Para la generación de la clave de las entidades de certificación raíz e intermedia se utilizan dispositivos con las certificaciones Common Criteria EAL 4+ y FIPS 140-2 Nivel 3.

|                                 |            |         |
|---------------------------------|------------|---------|
| ROOT                            | 4.096 bits | 25 años |
| INTERMEDIA                      | 4.096 bits | 13 años |
| - Certificados de entidad final | 2.048 bits | 2 años  |
| - Certificado de TSA            | 4.096 bits | 5 años  |

Más información en las siguientes ubicaciones de las PDS:

| CERTIFICADO  | PDS   |
|--|---|
| <b>Empleado Público – ALTO</b><br>1.3.6.1.4.1.47281.1.1.1  | ESPAÑOL:<br><a href="https://www.esfirma.com/doc-pki/PDS2/EP2-ALTO-SMARTCARD-ES/">https://www.esfirma.com/doc-pki/PDS2/EP2-ALTO-SMARTCARD-ES/</a><br><br>INGLÉS:<br><a href="https://www.esfirma.com/doc-pki/PDS2/EP2-ALTO-SMARTCARD-EN/">https://www.esfirma.com/doc-pki/PDS2/EP2-ALTO-SMARTCARD-EN/</a> |
| <b>Empleado Público – MEDIO</b><br>1.3.6.1.4.1.47281.1.1.4 | ESPAÑOL: <a href="https://www.esfirma.com/doc-pki/PDS2/EP2-MEDIO-HSM-ES/">https://www.esfirma.com/doc-pki/PDS2/EP2-MEDIO-HSM-ES/</a><br>INGLÉS: <a href="https://www.esfirma.com/doc-pki/PDS2/EP2-MEDIO-HSM-EN/">https://www.esfirma.com/doc-pki/PDS2/EP2-MEDIO-HSM-EN/</a>                               |

|   |   |
|---|---|
| <b>Sello-e AAPP – MEDIO Soft</b><br>1.3.6.1.4.1.47281.1.2.2 | ESPAÑOL: <a href="https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-SOFT-ES/">https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-SOFT-ES/</a><br>INGLÉS: <a href="https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-SOFT-EN/">https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-SOFT-EN/</a>                       |
| <b>Sello-e AAPP – MEDIO HSM</b><br>1.3.6.1.4.1.47281.1.2.4  | ESPAÑOL: <a href="https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-HSM-ES/">https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-HSM-ES/</a><br>INGLÉS: <a href="https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-HSM-EN/">https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-HSM-EN/</a>                           |
| <b>EP Seudónimo – ALTO</b><br>1.3.6.1.4.1.47281.1.3.1       | ESPAÑOL:<br><a href="https://www.esfirma.com/doc-pki/PDS2/ES2-ALTO-SMARTCARD-ES/">https://www.esfirma.com/doc-pki/PDS2/ES2-ALTO-SMARTCARD-ES/</a><br>INGLÉS:<br><a href="https://www.esfirma.com/doc-pki/PDS2/ES2-ALTO-SMARTCARD-EN/">https://www.esfirma.com/doc-pki/PDS2/ES2-ALTO-SMARTCARD-EN/</a> |
| <b>EP Seudónimo – MEDIO</b><br>1.3.6.1.4.1.47281.1.3.4      | ESPAÑOL: <a href="https://www.esfirma.com/doc-pki/PDS2/ES2-MEDIO-HSM-ES/">https://www.esfirma.com/doc-pki/PDS2/ES2-MEDIO-HSM-ES/</a><br>INGLÉS: <a href="https://www.esfirma.com/doc-pki/PDS2/ES2-MEDIO-HSM-EN/">https://www.esfirma.com/doc-pki/PDS2/ES2-MEDIO-HSM-EN/</a>                           |
| <b>Sede electrónica EV MEDIO</b><br>1.3.6.1.4.1.47281.1.4.2 | ESPAÑOL: <a href="https://www.esfirma.com/doc-pki/PDS2/SE2-MEDIO-SOFT-ES/">https://www.esfirma.com/doc-pki/PDS2/SE2-MEDIO-SOFT-ES/</a><br>INGLÉS: <a href="https://www.esfirma.com/doc-pki/PDS2/SE2-MEDIO-SOFT-EN/">https://www.esfirma.com/doc-pki/PDS2/SE2-MEDIO-SOFT-EN/</a>                       |
| <b>TSA en HSM</b><br>1.3.6.1.4.1.47281.1.5.2                | ESPAÑOL: <a href="https://www.esfirma.com/doc-pki/PDS2/TS2-ES/">https://www.esfirma.com/doc-pki/PDS2/TS2-ES/</a><br>INGLÉS: <a href="https://www.esfirma.com/doc-pki/PDS2/TS2-EN/">https://www.esfirma.com/doc-pki/PDS2/TS2-EN/</a>   |

#### 6.1.1.1. Generación del par de claves del firmante

Las claves del firmante pueden ser creadas por él mismo mediante dispositivos hardware o software autorizados por esFIRMA.

EsFIRMA puede crear las claves únicamente por medio de un DCCF.

EsFIRMA nunca genera claves en software para ser enviadas al firmante.

Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

#### 6.1.2. Envío de la clave privada al firmante

En certificados en dispositivo seguro de creación de firma la clave privada se encuentra debidamente protegida en el interior de dicho dispositivo seguro.

En certificados en software la clave privada del firmante se crea en el sistema informático que utiliza este firmante cuando realiza la solicitud del certificado, por lo que la clave privada se encuentra debidamente protegida en el interior del sistema informático del firmante.

### **6.1.3. Envío de la clave pública al emisor del certificado**

---

El método de remisión de la clave pública al prestador de servicios de certificación es PKCS#10, otra prueba criptográfica equivalente o cualquier otro método aprobado por esFIRMA.

Cuando las claves se generan en un DCCF, esFIRMA se asegura que la clave pública que se remite al prestador de servicios de certificación proviene de un par de claves generadas por dicho DCCF<sup>14</sup>.

### **6.1.4. Distribución de la clave pública del prestador de servicios de certificación**

---

Las claves de esFIRMA son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en el Depósito.

Los usuarios pueden acceder al Depósito para obtener las claves públicas, y adicionalmente, en aplicaciones S/MIME, el mensaje de datos puede contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

El certificado de las CA root y subordinadas estarán a disposición de los usuarios en la página Web de esFIRMA.

### **6.1.5. Tamaños de claves**

---

La longitud de las claves de la Entidad de Certificación raíz es de 4096 bits.

La longitud de las claves de la Entidad de Certificación subordinada es de 4096 bits.

La longitud de las claves de la TSA es de 4096 bits.

---

<sup>14</sup> Ap 6.5.1.b) de ETSI EN 319 411-2

Las claves de los certificados de entidad final son de 2048 bits.

#### **6.1.6. Generación de parámetros de clave pública**

---

La clave pública de la CA Root, de la CA subordinadas y de los certificados de los suscriptores está codificada de acuerdo con RFC 5280.

#### **6.1.7. Comprobación de calidad de parámetros de clave pública**

---

- Longitud del Módulo = 4096
- Algoritmo de generación de claves: rsagen1
- Funciones criptográficas de Resumen: SHA256.

#### **6.1.8. Generación de claves en aplicaciones informáticas o en bienes de equipo**

---

Todas las claves se generan en bienes de equipo, de acuerdo con lo indicado en la sección 6.1.1.

#### **6.1.9. Propósitos de uso de claves**

---

Los usos de las claves para los certificados de las CA son exclusivamente para la firma de certificados y de CRLs.

Los usos de las claves para los certificados de entidad final son exclusivamente para la firma digital y el no repudio.

## **6.2. Protección de la clave privada**

---

### **6.2.1. Estándares de módulos criptográficos**

---

En relación a los módulos que gestionan claves de esFIRMA y de los suscriptores de certificados de firma electrónica, se asegura el nivel exigido por los estándares indicados en las secciones anteriores.

### **6.2.2. Control por más de una persona (n de m) sobre la clave privada**

---

Se requiere un control multi-persona para la activación de la clave privada de la AC. En el caso de esta DPC, en concreto existe una política de **3 de 5** personas para la activación de las claves.

Los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

### **6.2.3. Depósito de la clave privada**

---

EsFIRMA no almacena copias de las claves privadas de los firmantes.

### **6.2.4. Copia de respaldo de la clave privada**

---

EsFIRMA realiza copia de backup de las claves privadas de las CA que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de las mismas. Tanto la generación de la copia como la recuperación de ésta necesitan al menos de la participación de dos personas.

Estos ficheros de recuperación se almacenan en armarios ignífugos y en el centro de custodia externo.

Las claves del firmante en hardware no se pueden copiar ya que no pueden salir del dispositivo criptográfico.

### **6.2.5. Archivo de la clave privada**

---

Las claves privadas de las AC son archivadas por un periodo de **10 años** después de la emisión del último certificado. Se almacenarán en archivos ignífugos seguros y en el centro de custodia externo. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada de las AC en el dispositivo criptográfico inicial.

El suscriptor podrá almacenar las claves entregadas en software durante el periodo de duración del certificado. Posteriormente deberá destruirlas asegurándose antes de que no tiene ninguna información cifrada con la clave pública.

Solo en caso de certificados de cifrado, el suscriptor podrá almacenar la clave privada el tiempo que crea oportuno. En este caso esFIRMA también guardará copia de la clave privada asociada al certificado de cifrado.

#### **6.2.6. Introducción de la clave privada en el módulo criptográfico**

---

Las claves privadas se generan directamente en los módulos criptográficos de producción de esFIRMA.

#### **6.2.7. Método de activación de la clave privada**

---

Las claves privadas de la Entidad de Certificación se almacenan cifradas en los módulos criptográficos de producción de esFIRMA.

#### **6.2.8. Método de desactivación de la clave privada**

---

La clave privada de esFIRMA se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 6.2.2.

Las claves de la AC se activan por un proceso de  $m$  de  $n$ .

La activación de las claves privadas de la AC Intermedia es gestionada con el mismo proceso de  $m$  de  $n$  que las claves de la AC.

#### **6.2.9. Método de destrucción de la clave privada**

---

Para la desactivación de la clave privada de esFIRMA se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

Por su parte el firmante deberá introducir el PIN para la nueva activación.

### **6.2.10. Clasificación de módulos criptográficos**

---

Con anterioridad a la destrucción de las claves, se emitirá una revocación del certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de esFIRMA. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

Finalmente se destruirán de forma segura las copias de seguridad.

Las claves del firmante en software se podrán destruir mediante el borrado de las mismas, siguiendo las instrucciones de la aplicación que las alberga.

Las claves del firmante en hardware podrán ser destruidas mediante una aplicación informática especial en las dependencias de las RA o de esFIRMA.

## **6.3. Otros aspectos de gestión del par de claves**

---

### **6.3.1. Archivo de la clave pública**

---

EsFIRMA archiva sus claves públicas de forma rutinaria, de acuerdo con lo establecido en la sección 5.5 de este documento.

### **6.3.2. Períodos de utilización de las claves pública y privada**

---

Los periodos de utilización de las claves son los determinados por la duración del certificado, transcurrido el cual no pueden continuar utilizándose.

Como excepción, la clave privada de descifrado puede continuar empleándose incluso tras la expiración del certificado.

## 6.4. Datos de activación

---

### 6.4.1. Generación e instalación de datos de activación

---

Los datos de activación de los dispositivos que protegen las claves privadas de esFIRMA son generados de acuerdo con lo establecido en la sección 6.2.2 y los procedimientos de ceremonia de claves.

La creación y distribución de dichos dispositivos es registrada.

Asimismo, esFIRMA genera de forma segura los datos de activación.

### 6.4.2. Protección de datos de activación

---

Los datos de activación de los dispositivos que protegen las claves privadas de las Autoridades de certificación raíz y subordinadas, son protegidos por los poseedores de las tarjetas de administradores de los módulos criptográficos, según consta en el documento de ceremonia de claves.

El firmante del certificado es el responsable de la protección de su clave privada, con una contraseña lo más completa posible. El firmante debe recordar dicha contraseña.

## 6.5. Controles de seguridad informática

---

EsFIRMA emplea sistemas fiables para ofrecer sus servicios de certificación. EsFIRMA ha realizado controles y auditorías informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de EsFIRMA, en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.

- Configuración de Usuarios y permisos.
- Configuración de eventos de Log.
- Plan de backup y recuperación.
- Configuración antivirus.
- Requerimientos de tráfico de red.

### **6.5.1. Requisitos técnicos específicos de seguridad informática**

---

Cada servidor de EsFIRMA incluye las siguientes funcionalidades:

- Control de acceso a los servicios de la SubCA y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del suscriptor y la SubCA y datos de auditoría.
- Auditoría de eventos relativos a la seguridad.
- Auto-diagnóstico de seguridad relacionado con los servicios de la SubCA.
- Mecanismos de recuperación de claves y del sistema de la SubCA.

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

En el caso que esFIRMA distribuyese dispositivos cualificados de creación de firma, verificará en todo momento que dichos dispositivos continúan certificados como DCCF<sup>15</sup>.

La verificación de la certificación del DCCF se realiza durante todo el período de validez del certificado<sup>16</sup>. Si el DCCF perdiera su certificación como tal, esFIRMA avisará a los usuarios de este hecho y ejecutará un plan de renovación de estos dispositivos tal y como se detalla en el documento interno Procedimientos Generales de esFIRMA (esFIRMA\_ProcedimientosGenerales\_v1r0.pdf)

---

<sup>15</sup> Ap 6.5.1.a) de ETSI 319 411-2

<sup>16</sup> Ap 6.5.1.c) de ETSI EN 319 411-2

### **6.5.2. Evaluación del nivel de seguridad informática**

---

Las aplicaciones de autoridad de certificación y de registro empleadas por esFIRMA son fiables.

## **6.6. Controles técnicos del ciclo de vida**

---

### **6.6.1. Controles de desarrollo de sistemas**

---

Las aplicaciones son desarrolladas e implementadas por esFIRMA de acuerdo con estándares de desarrollo y control de cambios.

Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

### **6.6.2. Controles de gestión de seguridad**

---

EsFIRMA desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos, son actualizados después de su aprobación por un grupo para la gestión de la seguridad. En la realización de esta función dispone de un plan de formación anual.

EsFIRMA exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

#### **6.6.2.1. Clasificación y gestión de información y bienes**

---

EsFIRMA mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad de esFIRMA detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: SIN CLASIFICAR, USO INTERNO y CONFIDENCIAL.

#### 6.6.2.2. Operaciones de gestión

EsFIRMA dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos.

En el documento de seguridad de esFIRMA se desarrolla en detalle el proceso de gestión de incidencias.

EsFIRMA tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

#### 6.6.2.3. Tratamiento de los soportes y seguridad

Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

#### *Planificación del sistema*

El departamento de Sistemas de esFIRMA mantiene un registro de las capacidades de los equipos. Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

#### *Reportes de incidencias y respuesta*

EsFIRMA dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

#### *Procedimientos operacionales y responsabilidades*

## **esFIRMA:** Prácticas de Certificación

EsFIRMA define actividades, asignadas a personas con un rol de confianza, distintas de las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

### 6.6.2.4. Gestión del sistema de acceso

EsFIRMA realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.

En particular:

#### *AC General*

- Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
- EsFIRMA dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- EsFIRMA dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado un rol para realizar las operaciones de certificación.
- El personal de esFIRMA es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

#### *Generación del certificado*

La autenticación para el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de esFIRMA.

#### *Gestión de la revocación*

La revocación se realizará mediante autenticación fuerte a las aplicaciones de un administrador autorizado. Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador de esFIRMA.

### *Estado de la revocación*

La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación con certificados o con doble factor de identificación para evitar el intento de modificación de la información del estado de la revocación.

#### 6.6.2.5. Gestión del ciclo de vida del hardware criptográfico

EsFIRMA se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.

EsFIRMA registra toda la información pertinente del dispositivo para añadir al catálogo de activos.

El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

EsFIRMA realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable. La clave privada de firma de esFIRMA almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

La configuración del sistema de esFIRMA, así como sus modificaciones y actualizaciones son documentadas y controladas.

EsFIRMA posee un contrato de mantenimiento del dispositivo. Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

## 6.7. Controles de seguridad de red

---

EsFIRMA protege el acceso físico a los dispositivos de gestión de red, y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad, creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se transfiere por redes no seguras, se realiza de forma cifrada mediante uso de protocolos SSL o del sistema VPN con autenticación por doble factor.

## 6.8. Controles de ingeniería de módulos criptográficos

---

Los módulos criptográficos se someten a los controles de ingeniería previstos en las normas indicadas a lo largo de esta sección.

Los algoritmos de generación de claves empleados se aceptan comúnmente para el uso de la clave a que están destinados.

Todas las operaciones criptográficas de esFIRMA son realizadas en módulos con las certificaciones FIPS 140-2 nivel 3.

## 6.9. Fuentes de Tiempo

---

EsFIRMA tiene un procedimiento de sincronización de tiempo coordinado vía NTP.

# 7. Perfiles de certificados y listas de certificados revocados

## 7.1. Perfil de certificado

---

Todos los certificados cualificados emitidos bajo esta política cumplen el estándar X.509 versión 3, RFC 3739 y ETSI 101 862 “Qualified Certificate Profile”.

### 7.1.1. Número de versión

---

EsFIRMA emite certificados X.509 Versión 3

### 7.1.2. Extensiones del certificado

---

Las extensiones de los certificados se encuentran detalladas en los documentos de perfiles que son accesibles desde la página web de esFIRMA <https://www.esfirma.com>

De esta forma se permite mantener unas versiones más estables de la DPC y desligarlos de los frecuentes ajustes en los perfiles.

### 7.1.3. Identificadores de objeto (OID) de los algoritmos

---

El identificador de objeto del algoritmo de firma es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública es:

- 1.2.840.113549.1.1.1 rsaEncryption

### 7.1.4. Formato de Nombres

---

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política.

### **7.1.5. Restricción de los nombres**

---

Los nombres contenidos en los certificados están restringidos a “Distinguished Names” X.500, que son únicos y no ambiguos.

### **7.1.6. Identificador de objeto (OID) de los tipos de certificados**

---

Todos los certificados incluyen un identificador de política de certificados bajo la que han sido emitidos, de acuerdo con la estructura indicada en el punto 1.2.1

## **7.2. Perfil de la lista de revocación de certificados**

---

### **7.2.1. Número de versión**

---

Las CRL emitidas por esFIRMA son de la versión 2.

### **7.2.2. Perfil de OCSP**

---

Según el estándar IETF RFC 6960

## **8. Auditoría de conformidad**

EsFIRMA ha comunicado el inicio de su actividad como prestador de servicios de certificación por el Ministerio de Industria y se encuentra sometida a las revisiones de control que este organismo considere necesarias.

### **8.1. Frecuencia de la auditoría de conformidad**

---

EsFIRMA lleva a cabo una auditoría de conformidad anualmente, además de las auditorías internas que realiza bajo su propio criterio o en cualquier momento, debido a una sospecha de incumplimiento de alguna medida de seguridad.

## 8.2. Identificación y calificación del auditor

---

Las auditorías son realizadas por una firma de auditoría independiente externa que demuestra competencia técnica y experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública, y los elementos relacionados.

## 8.3. Relación del auditor con la entidad auditada

---

Las empresas de auditoría son de reconocido prestigio con departamentos especializados en la realización de auditorías informáticas, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con esFIRMA.

## 8.4. Listado de elementos objeto de auditoría

---

La auditoría verifica respecto a esFIRMA:

- a) Que la entidad tiene un sistema de gestión que garantiza la calidad del servicio prestado.
- b) Que la entidad cumple con los requerimientos de la DPC y otra documentación vinculada con la emisión de los distintos certificados digitales.
- c) Que la DPC y demás documentación jurídica vinculada, se ajusta a lo acordado por esFIRMA y con lo establecido en la normativa vigente.
- d) Que la entidad gestiona de forma adecuada sus sistemas de información

En particular, los elementos objeto de auditoría serán los siguientes:

- a) Procesos de la AC, ARs y elementos relacionados.
- b) Sistemas de información.
- c) Protección del centro de proceso de datos.
- d) Documents

## 8.5. Acciones a emprender como resultado de una falta de conformidad

---

Una vez recibido por la dirección el informe de la auditoría de cumplimiento realizada, se analizan, con la firma que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta un plan correctivo que solventa dichas deficiencias.

Si la esFIRMA es incapaz de desarrollar y/o ejecutar dicho plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicarlo inmediatamente a la alta dirección de esFIRMA que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Revocar la clave de la AC y regenerar la infraestructura.
- Terminar el servicio de la AC.
- Otras acciones complementarias que resulten necesarias.

## 8.6. Tratamiento de los informes de auditoría

---

Los informes de resultados de auditoría se entregan a la alta dirección de esFIRMA en un plazo máximo de 15 días tras la ejecución de la auditoría.

# 9. Requisitos comerciales y legales

## 9.1. Tarifas

---

### 9.1.1. Tarifa de emisión o renovación de certificados

---

EsFIRMA puede establecer una tarifa por la emisión o por la renovación de los certificados, de la que, en su caso, se informará oportunamente a los suscriptores.

### **9.1.2. Tarifa de acceso a certificados**

---

EsFIRMA no ha establecido ninguna tarifa por el acceso a los certificados.

### **9.1.3. Tarifa de acceso a información de estado de certificado**

---

EsFIRMA no ha establecido ninguna tarifa por el acceso a la información de estado de certificados.

### **9.1.4. Tarifas de otros servicios**

---

Sin estipulación.

### **9.1.5. Política de reintegro**

---

Sin estipulación.

## **9.2. Capacidad financiera**

---

EsFIRMA dispone de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios, según lo establecido en la ETSI EN 319 401-1 7.12 c), en relación a la gestión de la finalización de los servicios y plan de cese.

### **9.2.1. Cobertura de seguro**

---

EsFIRMA dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional que cumple con lo indicado en el régimen de obligaciones y responsabilidades del Reglamento (UE) 910/2014, con un mínimo asegurado de 3.000.000 de euros.

### **9.2.2. Otros activos**

---

Sin estipulación.

### **9.2.3. Cobertura de seguro para suscriptores y terceros que confían en certificados**

---

EsFIRMA dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional que cumple con lo indicado en el régimen de obligaciones y responsabilidades del Reglamento (UE) 910/2014, con un mínimo asegurado de 3.000.000 de euros.

## **9.3. Confidencialidad**

---

### **9.3.1. Informaciones confidenciales**

---

Las siguientes informaciones son mantenidas confidenciales por esFIRMA:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.
- Claves privadas generadas y/o almacenadas por el prestador de servicios de certificación.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por la Entidad de Certificación y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Política y planes de seguridad.
- Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.
- Toda otra información identificada como “Confidencial”.

### **9.3.2. Informaciones no confidenciales**

---

La siguiente información se considera no confidencial:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por la Entidad de Certificación.

- El nombre y los apellidos de la persona física identificada en el certificado, así como cualquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- La dirección de correo electrónico de la persona física identificada en el certificado, o la dirección de correo electrónico asignada por el suscriptor, en el supuesto de que sea significativa en función de la finalidad del certificado.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (LRCs), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Cualquier otra información que no esté indicada en la sección anterior.

### **9.3.3. Divulgación de información de suspensión y revocación**

---

Véase la sección anterior.

### **9.3.4. Divulgación legal de información**

---

EsFIRMA divulga la información confidencial únicamente en los casos legalmente previstos.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado, así como los registros relacionados con la fiabilidad de los datos y los relacionados con la operativa<sup>17</sup>, serán divulgados en caso de ser requerido para ofrecer evidencia de la certificación en un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

---

<sup>17</sup> Apartado 7.10.c) de la ETSI EN 319 401

EsFIRMA indicará estas circunstancias en la política de privacidad prevista en la sección 9.4.

#### **9.3.5. Divulgación de información por petición de su titular**

---

EsFIRMA incluye, en la política de privacidad prevista en la sección 9.4, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, de la persona física identificada en el certificado, directamente a los mismos oa terceros.

#### **9.3.6. Otras circunstancias de divulgación de información**

---

Sin estipulación.

### **9.4. Protección de datos personales**

---

EsFIRMA se obliga a cumplir la normativa sobre protección de datos de carácter personal, con las medidas de seguridad correspondientes según se relaciona en la Ley Orgánica 15/1999 de Protección de Datos Personales, y en el Real Decreto 1720/2007 de desarrollo de la citada Ley.

EsFIRMA obtiene los datos personales que figuran en los ficheros por captación de los datos por parte del SUSCRIPTOR, que debe haberlos obtenido legalmente de quien pertoque, en las condiciones previstas en la normativa sobre firma electrónica y sobre protección de datos de carácter personal.

EsFIRMA tiene la condición de encargado del tratamiento en tanto que no decide sobre la finalidad, contenido y uso del tratamiento de dichos datos de carácter personal, mientras que el SUSCRIPTOR es el responsable del fichero.

EsFIRMA utilizará los datos contenidos en sus ficheros, única y exclusivamente para los fines que figuran en esta Declaración de Prácticas de Certificación.

Asimismo, esFIRMA ha desarrollado una política de privacidad, de acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y

ha documentado en esta Declaración de Prácticas de Certificación los aspectos y procedimientos de seguridad correspondientes al documento de seguridad en cumplimiento del régimen de obligaciones y responsabilidades del Reglamento (UE) 910/2014, y los artículos 82 y 88 del Real Decreto Real Decreto 1720/2007, de 21 de diciembre, por el cual se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de trece de diciembre de 1999, de protección de datos de carácter personal. Esta Declaración de Prácticas de Certificación tiene, por tanto, la consideración de documento de seguridad.

EsFIRMA no divulga ni cede datos personales, excepto en los casos previstos en las secciones 9.3.2 a 9.3.6, y en la sección 5.8, en caso de terminación del servicio de certificación.

La información confidencial de acuerdo con la normativa en protección de datos personales se protege de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de conformidad con las prescripciones establecidas en este documento, que cumplen las obligaciones previstas en el Real Decreto 1720/2007, de 21 de diciembre, por el cual se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de trece de diciembre de 1999, de protección de datos de carácter personal.

## **9.5. Derechos de propiedad intelectual**

---

### **9.5.1. Propiedad de los certificados e información de revocación**

---

Únicamente esFIRMA goza de derechos de propiedad intelectual sobre los certificados que emita, sin perjuicio de los derechos de los suscriptores, poseedores de claves y terceros, a los que conceda licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de uso del certificado, y de acuerdo con la documentación que los vincula.

Adicionalmente, los certificados emitidos por esFIRMA contienen un aviso legal relativo a la propiedad de los mismos.

Las mismas reglas resultan de aplicación al uso de la información de revocación de los certificados.

### **9.5.2. Propiedad de la Declaración de Prácticas de Certificación**

---

Únicamente esFIRMA goza de derechos de propiedad intelectual sobre esta Declaración de Prácticas de Certificación.

### **9.5.3. Propiedad de la información relativa a nombres**

---

El suscriptor y, en su caso, la persona física identificada en el certificado, conserva la totalidad de derechos, de existir los mismos, sobre la marca, producto o nombre comercial contenido en el certificado.

El suscriptor es el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 3.1.1

### **9.5.4. Propiedad de claves**

---

Los pares de claves son propiedad de los firmantes de los certificados.

Cuando una clave se encuentra fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

## **9.6. Obligaciones y responsabilidad civil**

---

### **9.6.1. Obligaciones de la Entidad de Certificación “esFIRMA”**

---

EsFIRMA garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la DPC, siendo el único responsable del cumplimiento de los

procedimientos descritos, incluso si una parte o la totalidad de las operaciones se subcontratan externamente.

EsFIRMA presta los servicios de certificación conforme con esta Declaración de Prácticas de Certificación.

Con anterioridad de la emisión y entrega del certificado al suscriptor, esFIRMA informa al suscriptor de los términos y condiciones relativos al uso del certificado, de su precio y de sus limitaciones de uso, mediante un contrato de suscriptor que incorpora por referencia los textos de divulgación (PDS) de cada uno de los certificados adquiridos.

El documento de texto de divulgación, también denominado PDS<sup>18</sup>, cumple el contenido del anexo A de la ETSI EN 319 411-1 v1.1.1 (2016-02), documento el cual puede ser transmitido por medios electrónicos, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

EsFIRMA comunica de forma permanente los cambios<sup>19</sup> que se produzcan en sus obligaciones publicando nuevas versiones de su documentación jurídica en su web <https://www.esfirma.com>

EsFIRMA vincula a suscriptores, poseedores de claves y terceros que confían en certificados mediante dicho texto de divulgación o PDS, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en las secciones Error: no se encontró el origen de la referencia, 4.5.3, 9.2, 9.6.7, 9.6.8, 9.6.9 y 9.6.10.
- Indicación de la política aplicable, con indicación de que los certificados no se expiden al público.
- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para la publicación del certificado en el depósito y acceso por terceros al mismo.

---

<sup>18</sup> “PKI Disclosure Statement”, o declaración de divulgación de PKI aplicable.

<sup>19</sup> Ap 6.2.3.b) de ETSI EN 319 411-1

- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la Entidad de Certificación sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo las establecidas en la sección 1.4.2
- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.
- Forma en que se garantiza la responsabilidad patrimonial de la Entidad de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Entidad de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.
- Si la Entidad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

#### **9.6.2. Garantías ofrecidas a suscriptores y terceros que confían en certificados**

EsFIRMA, en la documentación que la vincula con suscriptores y terceros que confían en certificados, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

EsFIRMA, como mínimo, garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Entidad de Certificación.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación del mismo.
- Que los certificados cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

## **esFIRMA:** Prácticas de Certificación

- Que los servicios de revocación y el empleo del Depósito cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

EsFIRMA, como mínimo, garantizará al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- En caso de certificados publicados en el Depósito, que el certificado ha sido emitido al suscriptor identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con la sección 4.4
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y Depósito.

Adicionalmente, esFIRMA garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado cualificado, de acuerdo con el anexo 1 del Reglamento (UE) 910/2014.
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, persona física identificada en el certificado, se mantiene su confidencialidad durante el proceso.
- La responsabilidad de la Entidad de Certificación, con los límites que se establezcan.

### **9.6.3. Rechazo de otras garantías**

---

EsFIRMA rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 9.6.2.

### **9.6.4. Limitación de responsabilidades**

---

EsFIRMA limita su responsabilidad de acuerdo con lo que dispone el régimen de obligaciones y responsabilidades del Reglamento (UE) 910/2014.

### 9.6.5. Cláusulas de indemnidad

---

#### 9.6.5.1. Cláusula de indemnidad de suscriptor

---

EsFIRMA incluye en el contrato con el suscriptor, una cláusula por la cual el suscriptor se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Falsedad o manifestación errónea realizada por el usuario del certificado.
- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión medió dolo o negligencia con respecto a la Entidad de Certificación o a cualquier persona que confía en el certificado.
- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de dominio), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

#### 9.6.5.2. Cláusula de indemnidad de tercero que confía en el certificado

---

EsFIRMA incluye en el texto de divulgación o PDS, una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.

- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.

#### **9.6.6. Caso fortuito y fuerza mayor**

---

EsFIRMA incluye en el texto de divulgación o PDS, cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

#### **9.6.7. Ley aplicable**

---

EsFIRMA establece, en el contrato de suscriptor y en el texto de divulgación o PDS, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la Ley española.

#### **9.6.8. Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación**

---

EsFIRMA establece, en el contrato de suscriptor, y en el texto de divulgación o PDS, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, la Entidad de Certificación vela porque, al menos los requisitos contenidos en las secciones 9.6.1 (Obligaciones y responsabilidad), 8 (Auditoría de conformidad) y 9.3 (Confidencialidad), continúen vigentes tras la terminación del servicio y de las condiciones generales de emisión/uso.
- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

### **9.6.9. Cláusula de jurisdicción competente**

---

EsFIRMA establece, en el contrato de suscriptor y en el texto de divulgación o PDS, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles.

La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

### **9.6.10. Resolución de conflictos**

---

EsFIRMA establece, en el contrato de suscriptor, y en el texto de divulgación o PDS, los procedimientos de mediación y resolución de conflictos aplicables.