

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	1



CERTIFICATION PRACTICES  
STATEMENT

marzo 4

2026

 <b>SECURITY DATA</b> TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	2

## VERSION HISTORY

VERSION	DESCRIPTION	DATE	PREPARED BY	REVIEWED BY	APPROVED BY
V1	Initial Edition	12/2/2025	Legal Coordinator	Technical Manager	General Manager
V2	-	03/31/2011	Legal Coordinator	Technical Manager	General Manager
V3	-	06/24/2011	Legal Coordinator	Technical Manager	General Manager
V4	-	09/01/2011	Legal Coordinator	Technical Manager	General Manager
V5	-	09/26/2011	Legal Coordinator	Technical Manager	General Manager
V6	-	12/13/2011	Legal Coordinator	Technical Manager	General Manager
V7	-	07/04/2011	Legal Coordinator	Technical Manager	General Manager
V8	-	09/13/2013	Legal Coordinator	Technical Manager	General Manager
V9	-	09/13/2019	Legal Coordinator	Technical Manager	General Manager
V10	-	04/18/2022	Legal Coordinator	Technical Manager	General Manager
V11	<ul style="list-style-type: none"> <li>* Format update.</li> <li>* Updated root certificate links.</li> </ul>	11/29/2024	Quality and Management Coordinator	Technical Manager / Legal Coordinator	General Manager
V12	<ul style="list-style-type: none"> <li>* General update of the CPS in accordance with the Technical Regulations.</li> <li>* Modification of the Representations and Warranties section of the CA regarding the custody of information.</li> <li>* Updated links for CRL and certificate PCs.</li> <li>* Updating of references to procedures in accordance with those formalized internally.</li> </ul>	02/25/2026	Management System Coordinator	Chief Technology Officer (CTO) Supervisor Legal	General Manager

 <b>SECURITY DATA</b> <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	3

## Contents

1.	Legal Framework .....	12
1.1.	LEGAL BASE. ....	12
1.2.	VALIDITY. ....	12
1.3.	LEGAL SUPPORT. ....	12
2.	Introduction. ....	13
2.1.	PRESENTATION.....	13
2.2.	NAME AND IDENTIFICATION OF THE DOCUMENT.....	13
2.2.1.	Identification. ....	13
2.3.	Participating entities. ....	14
2.3.1.	Accredited Entity (EA). ....	14
2.3.2.	Certificate Authority (AC). ....	14
2.3.3.	Root Certification Authority. ....	15
2.3.4.	Registration Authorities (RAs). ....	15
2.3.5.	Related Third Party.....	15
2.3.6.	Applicant. ....	16
2.3.7.	Subscriber.....	16
2.3.8.	Signatory.....	16
2.3.9.	Custodian of the keys.....	16
2.3.10.	Third, who trusts the certificates. ....	16
2.4.	PARTICULAR USE OF CERTIFICATES.....	17
2.4.1.	Appropriate uses of certificates. ....	17
2.4.2.	Unauthorized uses of certificates.....	17
2.5.	POLICY MANAGEMENT. ....	18
2.5.1.	Organization that administers the document.....	18
2.5.2.	Contact Person. ....	18
2.5.3.	Person who determines the appropriateness of the Policy.....	18
2.5.4.	Frequency of Review. ....	18
2.5.5.	Approval Procedure. ....	18
2.6.	DEFINITIONS AND ACRONYMS.....	19
2.6.1.	Definitions. ....	19
2.6.2.	Acronyms.....	20
3.	Publishing and Repository Responsibilities.....	21
3.1.	REPOSITORIES.....	21

<b>CODE</b>	SD-ID-PE-09
<b>VERSION</b>	V12
<b>APPROVAL DATE</b>	03/4/2026
<b>PAGES</b>	4

3.2.	PUBLICATION OF INFORMATION. ....	21
3.2.1.	Certification Policies and Practices. ....	21
3.2.2.	Terms and Conditions. ....	21
3.2.3.	Dissemination of Certificates. ....	22
3.3.	FREQUENCY OF PUBLICATION. ....	22
3.4.	CONTROL OF ACCESS TO REPOSITORIES. ....	22
4.	Identification and Authentication. ....	22
4.1.	NAME REGISTRY. ....	23
4.1.1.	Types of Names. ....	23
4.1.2.	Need for names to be meaningful. ....	23
4.1.3.	Anonymity or pseudonym of Subscribers. ....	23
4.1.4.	Rules for interpreting various name formats. ....	23
4.1.5.	Uniqueness of names. ....	24
4.1.6.	Recognition, authentication and function of trademarks. ....	24
4.1.7.	Resolution of conflicts related to names. ....	24
4.1.8.	Verification of the powers of representation. ....	24
4.2.	INITIAL IDENTITY VALIDATION. ....	24
4.2.1.	Method of Proof of Possession of the Private Key. ....	25
4.2.2.	Authentication of the Identity of a Legal Entity. ....	25
4.2.3.	Authentication of the identity of a Natural Person. ....	25
4.2.4.	Authentication of the Identity of the Linked Third Party and Operators of the Linked Third. ....	26
4.2.5.	Unverified subscriber information. ....	26
4.2.6.	Authority Validation. ....	27
4.2.7.	Interoperability criteria. ....	27
4.3.	IDENTIFICATION AND AUTHENTICATION IN THE RENEWAL OF CERTIFICATES. ....	27
4.3.1.	Identification and authentication for routine key renewal. ....	27
4.3.2.	Identification and authentication for key renewal after revocation. ....	27
4.4.	IDENTIFICATION AND AUTHENTICATION IN THE REVOCATION OF CERTIFICATES. ....	28
5.	Operational Requirements for the Life Cycle of Certificates. ....	28
5.1.	CERTIFICATE REQUEST. ....	28
5.1.1.	Who can apply for a Certificate. ....	28
5.1.2.	Enrollment Process and Responsibilities. ....	28
5.2.	VALIDITY OF THE ELECTRONIC SIGNATURE CERTIFICATE. ....	29
5.3.	PROCESSING OF CERTIFICATE REQUESTS. ....	29

<b>CODE</b>	SD-ID-PE-09
<b>VERSION</b>	V12
<b>APPROVAL DATE</b>	03/4/2026
<b>PAGES</b>	5

5.3.1.	Performing the functions of Identification and Authentication. ....	29
5.3.2.	Approval or denial of certificate requests.....	30
5.3.3.	Processing time for certificate applications. ....	30
5.4.	ISSUANCE OF CERTIFICATES. ....	31
5.4.1.	Actions of the AC during the Issuance of the Certificates.....	31
5.4.2.	Notification to the subscriber by the AC of the Issuance of the Certificate. ....	31
5.5.	ACCEPTANCE OF THE CERTIFICATE. ....	32
5.5.1.	Form in which the Certificate is Accepted. ....	32
5.5.2.	Publication of the Certificate. ....	32
5.5.3.	Notification of the issuance of certificates by the AC to other entities. ....	32
5.6.	USES OF KEYS AND CERTIFICATE. ....	32
5.6.1.	Use of Private Key and Certificate by Subscriber. ....	32
5.6.2.	Use of the Public Key and Certificate of the trusting party.....	33
5.7.	RENEWAL OF CERTIFICATES. ....	33
5.8.	Certificate key change. ....	33
5.8.1.	Circumstances for the renewal of the certificate key. ....	33
5.8.2.	Who can apply.....	34
5.8.3.	Processing of Certificate Key Renewal requests. ....	34
5.8.4.	Notification of the issuance of a new certificate to the Subscriber.....	34
5.8.5.	Conduct that constitutes acceptance of a certificate with a new key. ....	34
5.8.6.	Publication of the certificate with a new key by the AC. ....	35
5.8.7.	Notification of the issuance of the certificate by the AC to other entities. ....	35
5.9.	MODIFICATION OF CERTIFICATES. ....	35
5.9.1.	Circumstances for the Modification of the Certificate.....	35
5.9.2.	Who can request the modification of the certificate.....	35
5.9.3.	Processing of certificate modification requests.....	35
5.9.4.	Notification of the issuance of a new certificate to the subscriber. ....	35
5.9.5.	Conduct that constitutes acceptance of the modified certificate. ....	36
5.9.6.	Publication of the certificate modified by the CA. ....	36
5.9.7.	Notification of the issuance of the certificate by the CA to other entities. ....	36
5.10.	REVOCAION AND SUSPENSION OF CERTIFICATES.....	36
5.10.1.	Grounds for Revocation. ....	36
5.10.2.	Who Can Request Revocation.....	37
5.10.3.	Revocation Request Procedures. ....	38

<b>CODE</b>	SD-ID-PE-09
<b>VERSION</b>	V12
<b>APPROVAL DATE</b>	03/4/2026
<b>PAGES</b>	6

5.10.4.	Grace period for Revocation Requests.....	41
5.10.5.	Period within which the AC must process the request for Revocation. ....	41
5.10.6.	Revocation Verification Requirement for Relying Parties.....	41
5.10.7.	CRL Emission Frequency.....	41
5.10.8.	Maximum latency for CRL. ....	41
5.10.9.	Availability of the Online Certificate Status Verification System. ....	41
5.10.10.	Online Revocation Check Requirements. ....	42
5.10.11.	Other forms of revocation notices available.....	42
5.10.12.	Special Key Compromise Requirements. ....	42
5.10.13.	Circumstances for Suspension. ....	42
5.10.14.	Who Can Request the Suspension. ....	42
5.10.15.	Procedure for requesting suspension. ....	43
5.10.16.	Suspension Period Limits.....	43
5.11.	CERTIFICATE STATUS SERVICES. ....	43
5.11.1.	Operational Characteristics.....	43
5.11.2.	Availability of Service. ....	43
5.11.3.	Optional Features.....	44
5.12.	END OF SUBSCRIPTION.....	44
5.13.	KEY ESCROW AND KEY RECOVERY. ....	44
5.13.1.	Key escrow and key Recovery Policy and Practices. ....	44
5.13.2.	Session key encapsulation and retrieval policy and practices. ....	44
6.	Controls of Facilities, Management and Operation. ....	45
6.1.	PHYSICAL CONTROLS.....	45
6.1.1.	Physical location and construction.....	45
6.1.2.	Physical Access. ....	45
6.1.3.	Electric Power and Air Conditioning.....	46
6.1.4.	Water Exposure.....	46
6.1.5.	Fire Protection and Prevention. ....	46
6.1.6.	Storage System.....	46
6.1.7.	Elimination of Information Carriers. ....	46
6.1.8.	External Backup.....	46
6.2.	PROCEDURAL CONTROLS. ....	46
6.2.1.	Roles of Trust.....	46
6.2.2.	Number of people needed per task. ....	47

<b>CODE</b>	SD-ID-PE-09
<b>VERSION</b>	V12
<b>APPROVAL DATE</b>	03/4/2026
<b>PAGES</b>	7

6.2.3.	Identification and authentication for each role. ....	47
6.2.4.	Roles that require separation of duties. ....	48
6.3.	PERSONNEL CONTROLS.....	48
6.3.1.	Requirements on Qualification, Experience and Professional Knowledge. ....	48
6.3.2.	Background Check Procedure. ....	48
6.3.3.	Training Requirements.....	48
6.3.4.	Requirements and Frequency of Training Updates. ....	49
6.3.5.	Frequency and Sequence of Task Rotation. ....	49
6.3.6.	Penalties for Unauthorized Actions. ....	49
6.3.7.	Personnel Hiring Requirements. ....	49
6.3.8.	Documentation Provided to Staff. ....	50
6.4.	AUDIT TRAIL PROCEDURES.....	50
6.4.1.	Types of Events Recorded. ....	50
6.4.2.	Frequency of Audit Log Processing. ....	51
6.4.3.	Audit Log Retention Period. ....	51
6.4.4.	Protection of Records.....	51
6.4.5.	Procedures for Supporting Audit Trails.....	51
6.4.6.	Audit Information Collection System. ....	51
6.4.7.	Event Notification.....	51
6.4.8.	Vulnerability Analysis. ....	51
6.5.	LOG FILE.....	52
6.5.1.	Type of Archived Events.....	52
6.5.2.	Record Retention Period. ....	52
6.5.3.	Protection of the Archive. ....	52
6.5.4.	File Backup Procedures. ....	52
6.5.5.	Requirements for the Time Stamping of Records.....	53
6.5.6.	Audit Information Filing System.....	53
6.5.7.	Procedures for obtaining and verifying information on file. ....	53
6.6.	CHANGE OF KEY OF THE CA.....	53
6.6.1.	AC Raíz.....	53
6.6.2.	Subordinate AC.....	53
6.7.	DISASTER Management AND RECOVERY. ....	53
6.7.1.	Incident and Vulnerability Management Procedures. ....	54
6.7.2.	Alteration of Hardware, Software and/or Data Resources. ....	54

 <b>SECURITY DATA</b> <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	8

6.7.3.	Procedure for Action in the Event of a Certification Authority Private Key Compromise .....	54
6.7.4.	Business Continuity after a disaster. ....	54
6.8.	TERMINATION OF CA OR RA. ....	55
6.8.1.	Certification Authority.....	55
6.8.2.	Registration Authority.....	55
7.	Technical Security Controls. ....	55
7.1.	KEY PAIR GENERATION AND INSTALLATION. ....	55
7.1.1.	Key Pair Generation.....	55
7.1.2.	Delivery of the Private Key to the Subscriber. ....	56
7.1.3.	Delivery of the Public Key to the Certificate Issuer.....	56
7.1.4.	Delivery of the Public Key of the CA to the Third Parties Trust the Certificates. ....	56
7.1.5.	Key sizes. ....	57
7.1.6.	Generation of public key parameters and quality control.....	57
7.1.7.	Supported Key Applications (X.509v3 KeyUsage field). ....	57
7.2.	PROTECTION OF PRIVATE KEYS AND ENGINEERING OF CRYPTOGRAPHIC MODULES.....	57
7.2.1.	Standards for Cryptographic Modules. ....	57
7.2.2.	Multi-person control (k of n) of the Private Key. ....	57
7.2.3.	Custody of the Private Key. ....	58
7.2.4.	Backup of the Private Key of the CA.....	58
7.2.5.	Subscriber's Private Key File.....	58
7.2.6.	Transfer of the Private Key or from the Cryptographic Module. ....	58
7.2.7.	Private key storage in the cryptographic module. ....	59
7.2.8.	Private Key Activation Method. ....	59
7.2.9.	Private Key Deactivation Method. ....	59
7.2.10.	Private Key Destruction Method.....	59
7.2.11.	Classification of the cryptographic module.....	60
7.3.	OTHER ASPECTS OF KEY PAIR MANAGEMENT. ....	60
7.3.1.	Public Key File.....	60
7.3.2.	Certificate Operating Periods and Key Pair Usage Period.....	60
7.4.	ACTIVATION DATA.....	60
7.4.1.	Generation and Installation of Activation Data. ....	60
7.4.2.	Activation Data Protection. ....	60
7.4.3.	Other aspects of activation data. ....	61
7.5.	COMPUTER SECURITY CONTROLS. ....	61

<b>CODE</b>	SD-ID-PE-09
<b>VERSION</b>	V12
<b>APPROVAL DATE</b>	03/4/2026
<b>PAGES</b>	9

7.5.1.	Specific Technical Safety Requirements.....	61
7.5.2.	Computer Security Classification. ....	61
7.6.	TECHNICAL CONTROLS OF THE LIFE CYCLE. ....	62
7.6.1.	Systems Development Controls. ....	62
7.6.2.	Security Management Controls.....	62
7.6.3.	Lifecycle Security Controls. ....	63
7.7.	NETWORK SECURITY CONTROLS. ....	63
7.8.	TIME STAMPING.....	64
8.	Profile of the Certificates. ....	64
8.1.	CERTIFICATE PROFILE. ....	64
8.1.1.	Types of Certificates.....	64
8.1.2.	Types of Support. ....	66
a)	Secure Signature Creation Device (DSCF). ....	66
8.1.3.	Certificate Profile.....	67
8.1.4.	Version Number. ....	71
8.1.5.	Extension of Certificates (OID-Object Identifier). ....	71
8.1.6.	Algorithm object identifiers. ....	71
	For the issuance and validation of the certificate, the CA uses the following Object Identifiers (OIDs) associated with the cryptographic algorithms used:.....	71
8.1.7.	Name formats.....	72
8.1.8.	Name restrictions. ....	72
8.1.9.	Certificate Policy object identifier.....	72
8.1.10.	Using the Policy Restrictions extension. ....	73
	It is not stipulated. ....	73
8.1.11.	Syntax and semantics of policy qualifiers. ....	73
8.1.12.	Processing semantics for the extension of critical certificate policies.....	73
	It is not stipulated. ....	73
8.2.	CRL Profile. ....	73
8.2.1.	Version Number. ....	73
8.2.2.	CRL and CRL Input Extensions. ....	73
	AC Root CRL.....	74
8.3.	OCSP Profile.....	74
8.3.1.	Version number(s).....	74
8.3.2.	OCSP extensions.....	74
9.	Compliance Audits and Other Controls.....	76

<b>CODE</b>	SD-ID-PE-09
<b>VERSION</b>	V12
<b>APPROVAL DATE</b>	03/4/2026
<b>PAGES</b>	10

9.1.	FREQUENCY OF AUDITS.....	76
9.2.	QUALIFICATION OF THE AUDITOR. ....	77
9.3.	RELATIONSHIP BETWEEN THE AUDITOR AND THE AUDITED AUTHORITY.....	77
9.4.	ASPECTS COVERED BY THE CONTROLS. ....	77
9.4.1.	Audit at the Registration Authorities. ....	77
9.5.	ACTIONS TO BE TAKEN AS A RESULT OF THE DETECTION OF INCIDENTS.....	78
9.6.	COMMUNICATION OF RESULTS. ....	78
10.	Other Legal and Activity Issues. ....	78
10.1.	RATES.....	78
10.1.1.	Certificate Issuance or Renewal Fees.....	78
10.1.2.	Certificate Access Fees.....	78
10.1.3.	Status Information Access or Revocation Fees. ....	79
10.1.4.	Fees for Other Services. ....	79
10.1.5.	Refunds.....	79
10.2.	FINANCIAL RESPONSIBILITY.....	79
10.2.1.	Insurance Coverage.....	79
10.2.2.	Other Assets. ....	79
10.2.3.	Insurance or Guarantee of Coverage for Final Entities. ....	80
10.3.	CONFIDENTIALITY OF INFORMATION. ....	80
10.3.1.	Scope of Confidential Information. ....	80
10.3.2.	Non-Confidential Information.....	80
10.3.3.	Responsibility for the Protection of Confidential Information. ....	81
10.4.	PRIVACY OF PERSONAL INFORMATION. ....	81
10.4.1.	Privacy Policy.....	81
10.4.2.	Information treated as Private.....	81
10.4.3.	Information Not Classified as Private.....	81
10.4.4.	Responsibility for the Protection of Personal Data.....	81
10.4.5.	Notice and Consent to Use Personal Data. ....	81
10.4.6.	Disclosure in the framework of an administrative or judicial process.....	82
10.4.7.	Other circumstances of disclosure of information.....	82
10.5.	INTELLECTUAL PROPERTY RIGHTS.....	82
10.6.	REPRESENTATIONS AND WARRANTIES.....	82
10.6.1.	CA Representations and Warranties.....	82
10.6.2.	RA Representations and Warranties.....	84

 <b>SECURITY DATA</b> <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	11

10.6.3.	Applicants' Representations and Warranties.....	85
10.6.4.	Subscriber Representations and Warranties. ....	85
10.6.5.	Representations and Warranties of the Relying Party.....	86
10.6.6.	User Representations and Warranties.....	86
	Responsibilities.....	87
10.7.	DISCLAIMERS OF WARRANTIES.....	89
10.8.	LIMITATIONS OF LIABILITY. ....	89
10.9.	COMPENSATION.....	89
10.10.	TERM AND TERMINATION.....	89
10.10.1.	Term. ....	89
10.10.2.	Termination.....	89
10.11.	INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS.....	90
10.12.	AMENDMENTS. ....	90
10.13.	DISPUTE RESOLUTION PROVISIONS. ....	90
10.14.	GOVERNING LAW. ....	90
10.15.	COMPLIANCE WITH APPLICABLE LAW. ....	91
10.16.	MISCELLANEOUS PROVISIONS. ....	91
10.16.1.	Entire Agreement. ....	91
10.16.2.	Assignment.....	91
10.16.3.	Severability.....	91
10.16.4.	Execution.....	91
10.16.5.	Force Majeure. ....	91
10.17.	OTHER PROVISIONS.....	91
11.	Control of Approvals. ....	92

 <b>SECURITY DATA</b> <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	12

## 1. Legal Framework.

### 1.1. LEGAL BASE.

Law on Electronic Commerce, Electronic Signatures and Data Messages, its Regulations; Organic Law on Consumer Protection, Organic Law on the Protection of Personal Data, Organic Law on Transparency of Information and Accreditation of ARCOTEL, Technical Standard for the Provision of Certification Services and Related Services, issued by the Agency for the Regulation and Control of Telecommunications (ARCOTEL).

### 1.2. VALIDITY.

This document will enter into force as of the date of its approval.

### 1.3. LEGAL SUPPORT.

1. Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos, published in Official Gazette No. 577 of April 17, 2002.
2. In accordance with the provisions of Article 37 of the Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos, the National Telecommunications Council is the Agency for the authorization, registration and regulation of Accredited Information Certification Entities and Related Services.
3. General Regulations to the Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos, issued by Executive Decree No. 3496 published in the Official Gazette 735 of December 31, 2002, and constant reforms in Executive Decree 1356 of September 29, 2008, published in the Official Gazette No. 440 of October 6, 2008.
4. Ley Orgánica de Protección de Datos Personales, Official Register Supplement 459, May 26, 2021, which governs the treatment, storage and protection of the information of certificate holders.
5. That, the second article listed added by article 4 of Executive Decree No. 1356 after article 17 of the General Regulations to the Law of Electronic Commerce, Electronic Signatures and Data Messages, provides that the accreditation as an entity of certification of information and related services, will consist of an administrative act issued by CONATEL through a resolution that will be registered in the National Public Registry of Accredited Information and Related Services Certification Entities and Related Third Parties.
6. Resolution 477-20-CONATEL-2008 of October 8, 2008, approved the resolution model for Accreditation as an Information and Related Services Certification Entity.
7. Resolution No. TEL-640-21-CONATEL-2010 of October 22, 2010, approved the request for Accreditation of the Company SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL SA as Information and Services Certification Entity Related, for which SENATEL signed the respective administrative act, according to the model approved by the CONATEL.

 <p><b>SECURITY DATA</b> TU IDENTIDAD DIGITAL, EN UNA FIRMA.</p>	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	13

## 2. Introduction.

### 2.1. PRESENTATION.

Security Data Seguridad en Datos y Firma Digital S.A. (here in after Security Data), is a certifying entity that was born in order to meet the needs of the Ecuadorian market of electronic signatures and digital certificates.

Security Data is a company constituted according to Ecuadorian legislation, registered in the commercial register under number 2246 on July 13, 2010, with legal existence until July 13, 2060.

The Information Certification Services and Related Electronic Services offered by Security Data Seguridad en Datos y Firma Digital S.A are aimed at individuals, Public and Private Corporations (such as companies, public entities) and their objective is to accredit the digital identity of corporations and natural persons acting through the network.

This Certification Practices Statement specifies the conditions, policies and procedures applicable to the application, issuance, use, suspension and revocation of electronic signature certificates, as well as for the provision of related services and contains:

1. Identification data of the Certification Entity of Information and Related Services of the AC.
2. Conditions for handling the information provided by users.
3. Liability limits in the provision of information certification services and services related to the electronic signature
4. Obligations of the Accredited Information and Related Services Certification Entity in the provision of information certification services and services related to the signature
5. Obligations of users and precautions that must be observed in the handling, use and custody of certificates and keys.
6. Policies for handling electronic signature certificates.
7. Policies and conditions management of services related to electronic signature
8. Guarantees in compliance with the obligations arising from its activities
9. Costs and Rates of information certification services and services related to the electronic signatura

The structure of this document is based on the standard specification "RFC3647 - Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework", created by the IETF PKIX working group. In addition to the General Conditions established in this CPS, each type of certificate issued by Security Data Seguridad en Datos y Firma Digital S.A is It is governed by specific issuance conditions contained in a document called "Certification Policy" (in English CP or Certificate Policy). There is a certification policy for each type of certificate issued.

### 2.2. NAME AND IDENTIFICATION OF THE DOCUMENT.

#### 2.2.1. Identification.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	14

Name: CERTIFICATION PRACTICES STATEMENT (CPS)  
 Version: 12  
 Description: Statement of Security Data Certification Practices Data Security and Digital Signature SA  
 Date of issue: February 25, 2026  
 Website: www.securitydata.net.ec  
 Company Name: Security Data Seguridad en Datos y Firma Digital S.A  
 Postal Code: 170528  
 Email: info@securitydata.net.ec  
 Address: Alonso de Torres y Av. Del Parque C8  
 Phone Number: 023922169  
 Website: www.securitydata.net.ec  
 OID: 1.3.6.1.4.1.37746.1

### 2.2.2. Publication.

This document may be freely available at the following e-mail address:

[https://www.securitydata.net.ec/wp-content/downloads/Normativas/p\\_certificacion/certificacion.pdf](https://www.securitydata.net.ec/wp-content/downloads/Normativas/p_certificacion/certificacion.pdf)

## 2.3. PARTICIPATING ENTITIES.

### 2.3.1. Accredited Entity (EA).

Security Data Seguridad en Datos y Firma Digital S.A, is an Accredited Entity (EA) that issues certificates recognized under the Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Security Data Seguridad en Datos y Firma Digital is the entity that issues the certificates and is responsible for the operations of the certificate lifecycle. The functions of authorization, registration, issuance and revocation with respect to the personal certificates of the end entity may be performed by other entities by delegation contractually supported by Security Data Seguridad en Datos y Firma Digital, which will act as intermediaries. Security Data Seguridad en Datos y Firma Digital also offers electronic signature validation, electronic seal and time stamping services, governed by its particular policies, not included in this document, may be issued at the request of the interested party or ex officio, an informative document on the status of the certificate. This document will certify the validity, revocation or suspension of the electronic signature at a specific date and time, granting legal certainty about the status of the certificate's life cycle before third parties.

### 2.3.2. Certificate Authority (AC).

The certification system of Security Data Seguridad en Datos y Firma Digital is composed of various Certificate Authorities (CA or Certificate Authority) organized under a Certification Hierarchy.

 <b>SECURITY DATA</b> TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	15

### 2.3.3. Root Certification Authority.

A Root Certificate Authority is the entity within the hierarchy that issues certificates to other Certificate Authorities, and whose public key certificate has been self-signed. Its function is to sign the certificate of the other CAs belonging to the Certification Hierarchy.

### 2.3.4. Registration Authorities (RAs).

Security Data Seguridad en Datos y Firma Digital as the registration authority, is responsible for verifying the identity of applicants for digital certificates, as well as validating, approving or rejecting requests for issuance, renewal, revocation or suspension of such certificates, for this, it will use advanced biometrics systems and liveness check detection. In those cases where the biometric system does not reach the required confidence threshold, or there are inconsistencies in the data, the RA will mandatorily apply a Reinforced Validation protocol, which consists of:

- Face-to-face: The applicant must physically appear at the authorized offices or service centers.
- Validation video: Failing that, an identity validation video will be requested mentioning the required information.

### 2.3.5. Related Third Party.

A Linked Third Party of Security Data Seguridad en Datos y Firma Digital, is the entity responsible for:

- To process requests for certificates.
- Identify the applicant and verify that they meet the necessary requirements for the application for the certificates.
- Validate the personal circumstances of the person who will appear as the signatory of the certificate.
- Manage key generation and certificate issuance.
- Deliver the instructions for the issuance of the certificate to the subscriber and, if applicable, deliver the cryptographic device.

The following may act as a Linked Third Party of Security Data Seguridad en Datos y Firma Digital:

- Any trusted entity that enters into an agreement with Security Data Seguridad en Datos y Firma Digital to act as a third party on behalf of Security Data Seguridad en Datos y Firma Digital. These will act as an extension of the Registration Authority and are subject to the same audits and security levels as the parent office.
- Security Data itself Data Security and Digital Signature directly.

Security Data Seguridad en Datos y Firma Digital will contractually formalize the relations between it and each of the entities that act as Security Data Related Third Party; Subsequently, the link will be formalized through the respective registration of the control entity.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	16

The entity acting as a Linked Third Party of Security Data may authorize one or more persons as the Operator of the Linked Third Party to operate with the Computer System for the issuance of Security Data certificates on behalf of the Linked Third.

Where the geographic location of subscribers poses a logistical challenge to subscriber identification and certificate request and delivery, the Tied Third Party or Security Data may delegate these functions to another trusted entity or person called a mobile agent or authorized reseller. Said entity or person must have a special relationship with the Linked Third Party or with Security Data and a close relationship with the subscribers of the certificates that justifies the delegation. The trusted entity or person must sign a collaboration agreement with the Related Third Party or with Security Data in which the delegation of these functions is accepted. Security Data Seguridad en Datos y Firma Digital must be aware of and expressly authorize the agreement.

### **2.3.6. Applicant.**

Applicant is the natural person who, on his or her own behalf or on behalf of a third party, requests the issuance of a certificate to Security Data Seguridad en Datos y Firma Digital. The requirements that an applicant must meet will depend on the type of certificate requested and will be included in the "Certification Policy" of each specific type of certificate.

### **2.3.7. Subscriber.**

The Subscriber is the natural or legal person who has contracted the Security Data Seguridad en Datos y Firma Digital certification services. Therefore, you will be the owner of the certificate.

### **2.3.8. Signatory.**

The Signer is the person who owns a signature creation device or access to the signing certificate in software and who acts on his or her own behalf or on behalf of a legal entity that he or she represents.

The Signatory will be responsible for safeguarding the signature creation data, i.e. the private key associated with the certificate.

### **2.3.9. Custodian of the keys.**

The custody of the signature creation data associated with each electronic certificate of a legal person will be the responsibility of the requesting natural person, whose identification will be included in the electronic certificate.

### **2.3.10. Third, who trusts the certificates.**

A third party that trusts in certificates (relaying party) is understood to be any person or organization that voluntarily trusts a certificate issued by Security Data Seguridad en Datos y Firma Digital.

 <b>SECURITY DATA</b> TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	17

The recognized certificates issued by Security Data are universal and are accepted by the public bodies of the Ecuadorian state, such as Ministries, Secretariats, etc.

Security Data obligations and responsibilities to third parties who voluntarily rely on the certificates shall be limited to those set out in this CPS.

Third parties who rely on these certificates should be aware of the limitations on their use.

## **2.4. PARTICULAR USE OF CERTIFICATES.**

### **2.4.1. Appropriate uses of certificates.**

- The certificates do not have a technical, administrative, financial, etc. limitation for their use.
- The subscriber may make use of the Electronic Signature certificate as established in this CPS, in the service provision contract signed with Security Data Seguridad en Datos y Firma Digital, and the PC.
- The authorized uses of the Certificates issued by SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL may be specified in each type of certificate.
- If the subscriber's certificate in the period of validity is compromised, that is, his private key, he must initiate the revocation procedure as mentioned in this CPS and in the PCs.
- The electronic signature certificate issued by SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL to the subscriber must be used as supplied. Any alteration of the certificate by the user is prohibited.
- Electronic signature certificates may not be used for illegal actions, in accordance with the provisions of Ecuadorian legislation.
- Electronic signature certificates have the following guarantees:
  - Authenticity: The information in the document and its electronic signature undoubtedly correspond to the person who has signed.
  - Integrity: The information contained in the electronic document has not been modified or altered after its signature.
  - Non-repudiation: The person who has signed electronically cannot deny his or her authorship.
  - Confidentiality: The information contained has been encrypted and by the will of the sender, only the receiver is allowed to decrypt it.
- The purpose of using AC keys is set forth in the x509 v3 standard.
- The root digital certificate can only be used for identification by the root certificate authority itself and for the secure distribution of its public key.

### **2.4.2. Unauthorized uses of certificates.**

Use that is contrary to Ecuadorian and Community regulations, international conventions ratified by the Ecuadorian State, customs, morals and public order is not permitted. Nor is use other than that established in this Statement of Certification Practices and its corresponding Certification Policy permitted.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	18

The certificates have not been designed, cannot be used for and are not authorized for use or resale as hazardous situation control equipment or for uses that require fail-safe actions, such as the operation of nuclear facilities, air navigation or communications systems, or weapons control systems, where a failure could directly lead to death, personal injury or severe environmental damage.

A Certificate will be considered to be misused when it is used to perform unauthorized operations according to the Certificate Policies applicable to each of the Certificates, and the contracts with their subscribers, as a result of this, Security Data may revoke the certificate and terminate the contract.

End-user certificates cannot be used to sign public key certificates of any kind, or to sign certificate revocation lists.

## **2.5. POLICY MANAGEMENT.**

### **2.5.1. Organization that administers the document.**

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. is the entity that manages and is the author of this CPS, Certification Policies and other regulatory documents.

### **2.5.2. Contact Person.**

Contact person: Lenin Alberto Vásquez González  
 Email: [cto@securitydata.net.ec](mailto:cto@securitydata.net.ec)  
 Address: Alonso de Torres and Av. Del Parque Administrative Offices C8.  
 Phone Number: 023922169  
 Website: [www.securitydata.net.ec](http://www.securitydata.net.ec)

### **2.5.3. Person who determines the appropriateness of the Policy.**

This document is digitally signed by the Head of the Security Data CA before being published, and is in charge of evaluating and approving that its content is adequate, sufficient and consistent with the services provided, the requirements established in RFC 3647, as well as with the applicable legal and regulatory regulations.

### **2.5.4. Frequency of Review.**

The CPD and the various CPs will be reviewed and, if necessary, updated annually or when any changes are presented.

### **2.5.5. Approval Procedure.**

The publication of the revisions of this CPS and the Certificate Policies of each type of certificate must be approved by the Directorate General of Security Data Seguridad en Datos y Firma Digital, after verifying compliance with the requirements expressed therein.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	19

Updated and approved versions of the PCs as well as other regulatory documents will be forwarded to the Supervisory Authority and subsequently published on the Security Data website.

Each document will maintain a version history, in which the changes made will be recorded, in order to prevent unauthorized alterations or impersonations.

## 2.6. DEFINITIONS AND ACRONYMS.

### 2.6.1. Definitions.

**Electronic Certificate:** It is a document electronically signed by a certification service provider, which links signature verification data to a signatory and confirms their identity.

**Recognised Certificate:** Certificate issued by an Accredited Entity that meets the requirements established in the Law in terms of verifying the identity and other circumstances of the applicants, and the reliability and guarantees of the certification services they provide.

**Public Key and Private Key:** The asymmetric cryptography on which PKI is based uses a pair of keys (it could be two pairs of keys), what is encrypted with one of them can only be decrypted with the other and vice versa. One of these keys is called public and is included in the electronic certificate, while the other is called private and is only known to the holder of the certificate.

**Signature Creation Data (Private Key):** This is unique data, such as codes or private cryptographic keys, that the subscriber uses to create the electronic signature.

**Signature Verification Data (Public Key):** This is the data, such as codes or public cryptographic keys, that is used to verify the electronic signature.

**Secure Signature Creation Device (DSCF):** Instrument used to apply signature creation data.

**Electronic Signature:** It is the set of data in electronic form, consigned together with others or associated with them, which can be used as a means of personal identification.

**Advanced Electronic Signature:** It is the electronic signature that allows the personal identity of the subscriber to be established with respect to the signed data and to verify its integrity, as it is exclusively linked to both the subscriber and the data to which it refers, and because it has been created by means that it maintains under its exclusive control.

**Electronic seal:** It is a data message that identifies the public or private legal entity that is the owner of the signature and its relationship with the signatory, who is responsible for its protection and custody.

**Hash Function:** It is an operation that is performed on a set of data of any size, so that the result obtained is another set of data of fixed size, regardless of the original size, and which has the property of being uniquely associated with the initial data.

**Lists of Revoked Certificates (CRLs):** List of lists of revoked or suspended certificates.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	20

**Hardware Cryptographic Module (HSM):** Hardware module used to perform cryptographic functions and store keys in secure mode.

**Time stamping:** An electronic annotation signed electronically and added to a data message stating at least the date, time and identity of the person making the annotation.

**Time-Stamping Authority (TSA):** A trusted entity that issues time-stamps.

**Validation Authority (VA):** A trusted entity that provides information on the validity of digital certificates and electronic signatures.

**Linked Third Party:** A trusted entity that provides and/or manages certification services.

**Enhanced Validation:** Exceptional procedure of identity verification through physical presence or video validation where information is mentioned that allows validating the identity of the subscriber, when the automatic means are not conclusive.

**Proof of Life Detection:** Technology intended to determine if the biometric sample comes from a person alive and present at the time of capture, and not from a reproduction.

## 2.6.2. Acronyms.

<b>AC:</b>	Certificate Authority
<b>AC Sub:</b>	Subordinate Certificate Authority
<b>AR:</b>	Registration Authority
<b>PC:</b>	Certification Policy
<b>CPS:</b>	Certification Practices Statement
<b>CRL:</b>	Certificate Revocation List
<b>HSM:</b>	Hardware Security Module
<b>LDAP:</b>	Lightweight Directory Access Protocol
<b>OCSP:</b>	Online Certificate Status Protocol.
<b>PKI:</b>	Public Key Infrastructure
<b>PSC:</b>	Certification Service Provider
<b>TSA:</b>	Time Stamp Authority
<b>VA:</b>	Validation Authority
<b>ECI:</b>	Information Certification Entity
<b>OID:</b>	Unique Object Identifier
<b>DN:</b>	Distinguished Name
<b>C:</b>	Country
<b>CN:</b>	Common Name
<b>Or:</b>	Organization
<b>OU:</b>	Organizational Unity
<b>SN:</b>	SurName
<b>ISO:</b>	International Organization for Standardization
<b>PKCS:</b>	Public Key Cryptography Standards, PKI Standards
<b>UTF8:</b>	Unicode Transformation Format – 8 bits.

 <b>SECURITY DATA</b> TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	21

### 3. Publishing and Repository Responsibilities.

#### 3.1. REPOSITORIES.

The repositories of Security Data Seguridad en Datos y Firma Digital are referenced in the <https://consultacertificados.securitydata.net.ec/app-consulta-certificados/#/consultarCert>. Any changes to URLs will be notified to all entities that may be affected. The IP addresses corresponding to each URL may be multiple and dynamic, and may be modified without prior notice.

Certification Practice Statement:

[https://www.securitydata.net.ec/wp-content/downloads/Normativas/p\\_certificacion/certification.pdf](https://www.securitydata.net.ec/wp-content/downloads/Normativas/p_certificacion/certification.pdf)

PC Natural Person: [https://www.securitydata.net.ec/wp-content/downloads/Normativas/P\\_de\\_Certificados/pc\\_pn\\_en.pdf](https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/pc_pn_en.pdf)

PC Legal Representative: [https://www.securitydata.net.ec/wp-content/downloads/Normativas/P\\_de\\_Certificados/pc\\_rl\\_en.pdf](https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/pc_rl_en.pdf)

PC Company Member: [https://www.securitydata.net.ec/wp-content/downloads/Normativas/P\\_de\\_Certificados/pc\\_me\\_en.pdf](https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/pc_me_en.pdf)

CA Root Certificate:

[https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema\\_Windows/SECDATA-CA-2.cer](https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema_Windows/SECDATA-CA-2.cer)

Subordinate CA Certificate:

<http://subca2.securitydata.net.ec/subca2sd/subca2.crt>

CRL:

<http://crl1.securitydata.net.ec/subca2crl1/crlfile.crl>

<http://crl2.securitydata.net.ec/subca2crl2/crlfile.crl>

#### 3.2. PUBLICATION OF INFORMATION.

##### 3.2.1. Certification Policies and Practices.

Both the current CPS, as well as the Certification Policies of each type of certificate, will be available in electronic format on the Security Data website.

Previous versions will be removed from your online consultation, but may be requested by interested parties at the Contact Address of Security Data Seguridad en Datos y Firma Digital.

##### 3.2.2. Terms and Conditions.

 <b>SECURITY DATA</b> TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	22

The contractual relationship between Security Data and the Subscribers is based on the signing of a Certification Services Provision Agreement and the acceptance of the General Terms and Conditions of Contract for Security Data Seguridad en Datos y Firma Digital published on its website.

### **3.2.3. Dissemination of Certificates.**

The Certificate Subscriber is responsible for sending their certificate to any third party who wishes to authenticate a user or verify the validity of a signature. This will generally be sent automatically, attaching the certificate to any electronically signed document.

Security Data Seguridad en Datos y Firma Digital publishes on its website, permanently and uninterruptedly, the issued, revoked and suspended certificates, through a free online consultation by serial number of the certificate, where data such as: status, date of issue, expiration date, time of validity, date of revocation, reason for revocation, date of suspension; the latter three when applicable.

### **3.3. FREQUENCY OF PUBLICATION.**

The CA shall publish the list of certificates issued immediately after they are issued.

The Root CA will issue a List of Revoked CAs (ARLs) at least every six months, or extraordinarily, when a certificate of authority is revoked. Each Subordinate CA shall issue a List of Revoked Certificates (CRLs) on a daily basis, and extraordinarily, each time a certificate is suspended or revoked.

The CRLs of the Subordinate CA will be updated and published every 24 hours, and extraordinarily when a certificate is revoked or suspended.

Security Data Seguridad en Datos y Firma Digital S.A will review and, if appropriate, update the CPS and PC annually, or when any changes are made, and will promptly post any changes to certification policies and practices.

### **3.4. CONTROL OF ACCESS TO REPOSITORIES.**

The CPS, Certification Policies, General Terms and Conditions of Contract, CA certificates and lists of revoked certificates (CRLs) will be published in publicly accessible repositories on the website, without access control.

Issued certificates may be published in public or restricted access repositories as needed. Validation services by the OCSP protocol are free and time-stamping services by the TSP protocol will be restricted and paid.

## **4. Identification and Authentication.**

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	23

#### **4.1. NAME REGISTRY.**

##### **4.1.1. Types of Names.**

All certificates require a distinguished name (DN) in accordance with the X.500 standard. In addition, all the names of the recognized certificates are consistent with the provisions of the standards:

- ETSI TS 101 862 known as "European profile for Qualified Certificates"
- RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
- RFC 3739 "Qualified Certificates Profile".

##### **4.1.2. Need for names to be meaningful.**

Security Data shall ensure that the names assigned to digital certificates, both for the holder (Subject) and the issuer, are meaningful, clear, precise, and unambiguous, in accordance with the Technical Standard.

The fields of the DN referring to Names and Surnames will correspond to the legally registered data of the subscriber, expressed exactly in the format that appears in the Identity Card, residence card, passport or other means recognized by law.

The names used must explicitly identify the legal person or entity that owns it and ensure that the use of the electronic seal can be objectively attributed to the corresponding entity.

In the event that the data entered in the DN are fictitious or their invalidity is expressly indicated (e.g. "PROOF" or "INVALID"), the certificate will be considered without legal validity, only valid for technical interoperability tests.

##### **4.1.3. Anonymity or pseudonym of Subscribers.**

The use of aliases, pseudonyms or informal denominations, abbreviations that do not appear in official documents, unregistered trade names, expressions that may lead to error, confusion or identity theft will not be allowed.

##### **4.1.4. Rules for interpreting various name formats.**

Security Data Seguridad en Datos y Firma Digital complies in any case with the X.500 reference standard in ISO/IEC 9594.

The name of the certificate holder must correspond exactly to the legal or institutional name that appears in the official documents presented during the validation process.

The names included in the identification fields of the certificate must allow the unequivocal identification of the holder of the electronic signature certificate, without ambiguities or elements that may mislead as to their identity, legal nature or scope of action.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	24

#### 4.1.5. Uniqueness of names.

The distinguished name (DN) of the certificates issued will be unique to each subscriber or signatory. However, for the same person who has several certificates and types of certificates, there is a unique serial for each one.

#### 4.1.6. Recognition, authentication and function of trademarks.

The CA is not required to collect or request evidence in relation to the possession or ownership of trademarks or other distinctive signs prior to the issuance of the certificates. Security Data does not assume any obligation in the issuance of certificates regarding the use of trademarks or other distinctive signs.

#### 4.1.7. Resolution of conflicts related to names.

Security Data does not act as an arbitrator or mediator, nor does it resolve any disputes regarding the ownership of names of persons or organizations, domain names, trademarks or trade names, etc. Security Data also reserves the right to reject a certificate request due to name conflict.

#### 4.1.8. Verification of the powers of representation.

The verification of the applicant's representation before Security Data will be carried out by verifying the documentation according to the type of certificate established in Ecuadorian regulations through its regulatory entity ARCOTEL.

### 4.2. INITIAL IDENTITY VALIDATION.

For identity validation, Security Data will apply the following Tiered Security Protocol:

1. Automated Biometric Validation: A live face capture will be made comparing it against the Civil Registry database. The system will apply *Liveness Detection* algorithms to rule out the use of photos, videos or masks.
2. Enhanced Validation (Biometric Failure): If the biometric system is unable to verify identity with the required confidence level or higher, the applicant must mandatorily choose to:
  - Video validation: the applicant must make an express statement that confirms their identity and willingness to obtain or renew the certificate, in accordance with the internal procedures established by Security Data.
  - Face-to-face: Physically go to an office with your original document.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	25

#### **4.2.1. Method of Proof of Possession of the Private Key.**

When a certificate is issued on a hardware device, the private key is created instantly prior to the generation of the certificate, through a procedure that guarantees its confidentiality and its link to the identity of the applicant.

Each Linked Third Party is responsible for ensuring the delivery of the device to the requestor in a secure manner.

In other cases, the keys are delivered to the controller through files protected using the PKCS#12 standard. The security of the process is guaranteed because the access code to the PKCS#12 file that allows the installation of it in the applications, is defined by the subscriber and only he has full knowledge of it.

#### **4.2.2. Authentication of the Identity of a Legal Entity.**

The Registration Authority shall request the documentation or information necessary to ensure that a name or trademark belongs to the applicant or representative of a digital certificate.

The Registration Authority shall verify the following data in order to authenticate the identity of the organization:

- The data relating to the name or corporate name of the organisation.
- The data relating to the constitution and legal personality of the subscriber.
- The data relating to the extent and validity of the applicant's powers of representation.
- The data relating to the tax identification code of the RUC organisation.

In addition, the legal representative or company member of the legal entity must present the identity card, passport or other means recognized by law that identifies him/her, and the identity will be validated in accordance with the provisions of this section.

Security Data Seguridad en Datos y Firma Digital reserves the right not to issue the certificate if it considers that the documentation provided is not sufficient or adequate for the verification of the aforementioned data.

#### **4.2.3. Authentication of the identity of a Natural Person.**

The linked Third Party will reliably verify the identity of the natural person identified in the certificate. For this, the natural person must appear in person and present the Identity Card, passport or other legally recognized means that identifies him or her, or a biometric validation process or other legally recognized means that identifies him or her will be carried out.

In the event that the subscriber claims the modification of the personal identification data to be registered with respect to those of the identification document presented, he must present the corresponding Civil Registry Certificate stating the variation.

 <b>SECURITY DATA</b> <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	26

The linked Third Party will verify, either by showing sufficient original documentation, or with its own sources of information, photograph and the rest of the data and attributes to be included in the certificate (distinguished name of the certificate), and must keep the documentation accrediting the validity of those data that cannot be verified through its own data sources.

Security Data Seguridad en Datos y Firma Digital S.A reserves the right not to issue the certificate if it considers that the documentation provided is not sufficient or adequate for the verification of the aforementioned data.

#### **4.2.4. Authentication of the Identity of the Linked Third Party and Operators of the Linked Third.**

In the constitution of a new Third Party, the following actions will be carried out:

- Security Data Seguridad en Datos y Firma Digital S.A will verify the existence of the entity through its own sources of information.
- An authorized representative of the organization must sign a contract with Security Data Seguridad en Datos y Firma Digital S.A, specifying the specific aspects of the delegation and the responsibilities of each agent.

In addition, the Linked Third Party will be required to comply with the following with respect to the operators of the Linked Third Party:

- Verify and validate the identity of the new operators of the Linked Third Party. The linked Third Party must send Security Data Seguridad en Datos y Firma Digital S.A the corresponding documentation to the new operator, as well as its authorization to act as an operator of the linked Third Party.
- Ensure that registration operators have received sufficient training for the performance of their duties, by attending at least one operator training session.
- Ensure that communication between the Linked Third Party Security Data Seguridad en Datos y Firma Digital S.A is carried out securely through the use of digital operator certificates.
- All operators of Security Data or linked Third Parties must sign a Statement of Responsibility and Confidentiality. In this document, the operator assumes civil and criminal liability for the correct validation of identity and the handling of personal data in accordance with the LOPDP. Failure to comply will be cause for immediate revocation of your access credentials.

#### **4.2.5. Unverified subscriber information.**

Under no circumstances will Security Data omit the verification tasks that lead to the identification of the Subscriber and that results in the request for the disclosure of the aforementioned documents for legal and natural persons.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	27

#### **4.2.6. Authority Validation.**

The CA verifies that the applicant for the certificate has the authority, faculty or legal representation necessary to act on behalf of the natural person, legal person, position or function to which the requested certificate will be associated.

In the case of certificates issued to legal entities, the CA validates that the applicant has a valid appointment, power of attorney or authorization, granted in accordance with the applicable legal regulations, which empowers him or her to request and use the electronic signature certificate on behalf of the entity, in accordance with the provisions of the section *Authentication of the Identity of a Legal Entity*.

For certificates associated with institutional positions, the CA verifies that the applicant is duly authorized by the corresponding organization, through formal documentation that supports such attribution, such as designations, internal resolutions or letters of authorization issued by the competent authority.

The validation of the authority is carried out prior to the issuance of the certificate, based on official documents and reliable sources, in accordance with the procedures established in this Statement of Certification Practices.

The CA does not assume responsibility for the subsequent validity of the representation or authorization, once the certificate has been issued, except in the cases provided for by current regulations.

#### **4.2.7. Interoperability criteria.**

Security Data issues electronic signature certificates in accordance with internationally recognized technical standards, guaranteeing their interoperability and the possibility of validation by trusted systems, applications and third parties.

Security Data reserves the right to provide interoperation services and interoperate with other CAs; the terms and criteria of which they must be contractually established.

### **4.3. IDENTIFICATION AND AUTHENTICATION IN THE RENEWAL OF CERTIFICATES.**

#### **4.3.1. Identification and authentication for routine key renewal.**

Security Data does not offer the renew service without rekeying. The subscriber may process the renewal of the electronic signature certificates, after the expiration of the same or when the subscriber so requires, as a new process of acquisition of electronic signature, and the validation will be carried out as a new one.

#### **4.3.2. Identification and authentication for key renewal after revocation.**

 <b>SECURITY DATA</b> <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	28

The subscriber may process the renewal of the electronic signature certificates after the revocation of the same, as a new process of acquisition of electronic signature. Identity validation will be carried out in accordance with what is defined in the *Initial Identity Validation section*, as a new process.

#### **4.4 IDENTIFICATION AND AUTHENTICATION IN THE REVOCATION OF CERTIFICATES.**

The identification of subscribers in the certificate revocation process may be carried out by:

- a) The subscriber himself, identifying himself and authenticating himself on the Security Data website Security Data Seguridad en Datos y Firma Digital S.A in the Account Administration.
- b) Any Third Party Linked to Security Data Seguridad en Datos y Firma Digital S.A must identify the subscriber in the event of a revocation request according to the means it deems necessary.

## **5. Operational Requirements for the Life Cycle of Certificates.**

### **5.1. CERTIFICATE REQUEST.**

#### **5.1.1. Who can apply for a Certificate.**

The requirements that an applicant must meet will depend on the type of certificate requested and will be included in the "Certification Policy" of each specific type of certificate.

Security Data only accepts a request for the issuance of a certificate processed by a natural person, under a relationship of dependency (in the case of legal persons), of legal age and with full legal capacity to act.

#### **5.1.2. Enrollment Process and Responsibilities.**

The registration process for the issuance of electronic certificates is initiated at the request of the interested party, through the channels enabled by the CA, either directly or through one of the authorized Related Third Parties.

The applicant must contact Security Data Seguridad en Datos y Firma Digital S.A to manage the request for the certificate, either through the CA's website, in person or through one of the associated Related Third Parties. The Linked Third Party will provide the applicant with the following information:

- Documentation required to submit for the processing of your application and to verify the subscriber's identity.
- Availability to carry out the registration process.
- Information about the issuance and revocation process, the custody of the private key, as well as the responsibilities and conditions of use of the certificate and the device.
- How to access and consult this document and the Certification Policies.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	29

The Certification Authority shall register the application and proceed to verify the identity of the applicant, as well as the completeness and sufficiency of the information and documentation provided, in accordance with the requirements established in the “Certification Policy” corresponding to each specific type of certificate.

For this purpose, the documentation provided shall be validated through real-time consultation of the official databases of the Civil Registry and the Internal Revenue Service (SRI), as applicable. Once the validation process has been completed, the Certification Authority shall notify the applicant of the approval or rejection of the application, in accordance with the criteria defined in this CERTIFICATION PRACTICES STATEMENT (CPS).

The applicant or subscriber is responsible for providing truthful and up-to-date information, as well as for properly safeguarding their credentials and using the certificate in accordance with the provisions of this CPS. The Certification Authority is responsible for managing the registration process in a secure and reliable manner and in compliance with applicable technical and regulatory standards.

## **5.2. VALIDITY OF THE ELECTRONIC SIGNATURE CERTIFICATE.**

According to the Regulations of the Law on Electronic Commerce, Electronic Signatures and Data Messages (Decree No.3469):

“The duration of the electronic signature certificate will be contractually established between the owner of the electronic signature and the information certifying entity or whoever acts on its behalf. In the event that the parties do not agree on anything in this regard, the electronic signature certificate will be issued with a validity of two years from its issuance. In the case of electronic signature certificates issued in relation to the exercise of public or private positions, the duration of the electronic signature certificate may be more than two years but may not exceed the duration of said public or private position unless there is one of the extensions of functions established in the laws.”

## **5.3. PROCESSING OF CERTIFICATE REQUESTS.**

### **5.3.1. Performing the functions of Identification and Authentication.**

It is the responsibility of the CA and the linked Third Party to reliably identify and authenticate the subscriber. This process must be carried out prior to the issuance of the certificate.

The validation of identity and documentation will be carried out both in person and online, before an operator of the CA or the linked Third Party, applying the same procedures and criteria in both cases. The verification will be carried out through the review of the identification documents presented and biometric validation; if the latter is not possible, an alternative video verification mechanism will be used, which will be reviewed by the operator to confirm the identity of the applicant.

The validation of the documentation will be done in person or online, the operator of the CA or the linked Third Party will carry out the review and validation of the information provided. Once

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	30

the identity and documents have been validated, the electronic signature certificate will be issued.

### 5.3.2. Approval or denial of certificate requests.

Once the certificate request has been made, the Registry operator or Linked Third Party must verify the information provided by the applicant, including the validation of the subscriber's identity.

In addition, the Applicant must also accept the conditions of use and privacy policy. Subsequently, the documentation provided will be validated by consulting in real time the official databases of the Civil Registry and the Internal Revenue Service (SRI), as appropriate. If the information is incorrect, the Linked Third Party will deny the request, contacting the requester to inform them of the reason. If it is correct, the invoice will be issued, payment and confirmation of the transaction and the signing of the binding legal instrument between the subscriber and/or the applicant and Security Data Seguridad en Datos y Firma Digital S.A.. The certificate will then be issued.

Security Data will deny the request in the following security cases:

- Detection of documents with expired validity or with indications of physical/digital manipulation.
- Inconsistency between the data of the SRI/Civil Registry, or another control entity, and the information provided.
- Repeated failure in the life tests (biometrics) without the user accepting the validation by video or in person.

### 5.3.3. Processing time for certificate applications.

The processing of applications for electronic signature certificates online will be carried out within a maximum period of twenty-four (24) hours, provided that the applicant has fully complied with the established requirements, including, but not limited to, the complete and valid submission of the required documentation, confirmation of the corresponding payment in favor of Security Data and the correct validation of identity.

In the event of detecting inconsistencies, errors in the files provided or incomplete information, the management time may be extended up to a maximum period of 48 hours, counted from the receipt of the request, while the holder corrects the observations communicated.

Throughout the process, the user will be informed in a timely and permanent manner by email about the status of their request, the causes of any delay and the necessary steps to give continuity to the procedure until its correct completion.

The processing time for face-to-face applications will be 15 minutes, if you meet all the requirements and conditions indicated in this section.

 <b>SECURITY DATA</b> <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	31

## 5.4. ISSUANCE OF CERTIFICATES.

### 5.4.1. Actions of the AC during the Issuance of the Certificates.

Security Data generates electronic certificates, both new and renewed, within systems with secure environments, which is configured to ensure a correct issuance, controlled and in accordance with internal policies, practices and procedures, ensuring that each certificate is issued uniformly and in accordance with the type of electronic certificate requested.

Additionally, Security Data issues signing certificates in compliance with the laws, rules and regulations that govern Ecuadorian territory.

Once the application has been approved, the certificate will be issued, which must be delivered securely to the subscriber.

For the issuance of certificates, the following actions will be carried out:

#### For certificates on hardware support:

- The Registration Operator or the Linked Third Party shall deliver the DSCF to the applicant empty, that is, without the certificate being imported into the device. In the event that the applicant provides their own device, it must be a DSCF previously delivered by Security Data Seguridad en Datos y Firma Digital. A list of assigned devices will be available to Linked Third Parties.
- Device activation: In the event that the applicant does not have a DSCF, the device activation data will be generated.
- The AC will issue the certificate on the DSCF device if the customer wishes, otherwise it will send a video tutorial to the subscriber so that the subscriber can import their certificate into the DSCF.
- If the DSCF device is removed by a third party duly authorized by the owner, the signature will not be issued, if applicable, it will be done by the subscriber later.
- Key pair generation: The client is responsible for generating the key associated with the certificate. Once the validation process has been completed and the key has been generated, it will be imported into the DSCF device.
- The AC will provide the procedure for changing the DSCF password or pin.

#### For Software certificates:

- The AC will notify the subscriber via email that the certificate is in the customer portal ready for download.
- After the subscriber accepts the terms and conditions and fills out the download form, the AC will send the security PIN to their email for the signature download.
- The AC will send the email the backup of the signature key that the subscriber placed at the time of download.

### 5.4.2. Notification to the subscriber by the AC of the Issuance of the Certificate.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	32

**a) In Hardware**

- The AC or the linked Third Party will deliver the empty DSCF, i.e. without issuing the certificate within the device, to the subscriber or to the person authorized by the requestor.
- The AC will issue the certificate on the DSCF device if the holder wishes, otherwise it will send a video tutorial to their email so that the subscriber can import their certificate into the DSCF.

**b) In Software**

- The CA will notify the subscriber via email that the certificate is in the customer portal ready for download.

The CA after approving the application, will notify the subscriber by email that the electronic signature certificate is in the customer portal ready for download.

**5.5. ACCEPTANCE OF THE CERTIFICATE.**

**5.5.1. Form in which the Certificate is Accepted.**

The certificate will be accepted at the time the legal instrument binding between the subscriber and Security Data Seguridad en Datos y Firma Digital has been signed.

As evidence of acceptance, there must be an acceptance document signed by the applicant. The certificate will be considered valid from the date on which the acceptance document was signed.

The acceptance document must be signed electronically once the subscriber has the corresponding electronic signature.

**5.5.2. Publication of the Certificate.**

Once the certificate has been generated and accepted by the subscriber or signatory, the certificate will be immediately published in the certificate repositories deemed necessary.

**5.5.3. Notification of the issuance of certificates by the AC to other entities.**

It is not stipulated.

**5.6. USES OF KEYS AND CERTIFICATE.**

**5.6.1. Use of Private Key and Certificate by Subscriber.**

Certificates may be used as stipulated in this CPS and the corresponding Certification Policy.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	33

In case the certificate has been compromised, i.e. its private key, the subscriber must initiate a revocation procedure. The electronic signature certificate issued by Security Data to the subscriber must be used as supplied.

Electronic signature certificates have the following guarantees:

- **Authenticity:** The information of the document and its digital signature undoubtedly correspond to the subscriber who must be in possession of the certificate at all times.
- **Integrity:** The information contained in the electronic document has not been modified or altered after its signature.
- **Non-repudiation:** The person who has signed electronically cannot deny his or her authorship.
- **Confidentiality:** The information contained has been encrypted and by the will of the sender, only the receiver is allowed to decrypt it.

#### **5.6.2. Use of the Public Key and Certificate of the trusting party.**

Certificates may be used by third parties relying on the certificates for the purposes of this CPS and the applicable Certificate Policies.

It is the responsibility of third parties to verify the status of the certificate through the services offered by Security Data Seguridad en Datos y Firma Digital S.A, specifically for this purpose and specified in this document.

#### **5.7. RENEWAL OF CERTIFICATES.**

Security Data does not renew certificates without changing keys, because the renewal process is done in the same way as issuing a new certificate.

#### **5.8. CERTIFICATE KEY CHANGE.**

Security Data does not renew certificates without changing keys, because the renewal process is done in the same way as issuing a new certificate.

##### **5.8.1. Circumstances for the renewal of the certificate key.**

The renewal process will be carried out in the same way as the issuance of a new certificate, since the subscriber has in its possession the public and private key, for this reason the certification entity does not store this information and a new certificate is issued and therefore cannot extend the validity of the certificate without a new issuance of it. Under no circumstances does Security Data Seguridad en Datos y Firma Digital S.A offer certificate rekey services.

The electronic signature certificate may be renewed under the following circumstances:

- The certificate has expired.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	34

- The certificate has been violated.
- Compromise or suspicion of compromise of the keys.
- Loss or theft of the keys.
- The certificate has been revoked.

### 5.8.2. Who can apply.

The renewal of the electronic signature certificate may be requested by the holder or a duly authorised third party and the requirements that must be met will depend on the type of certificate requested and will be included in the "Certification Policy" of each specific type of certificate.

### 5.8.3. Processing of Certificate Key Renewal requests.

The application for renewal of the electronic signature certificate can be made in person or online.

The validation of the identity can be verified by the biometric of the applicant's face in face-to-face or online service, in case it is not possible to validate by this means, the applicant can record a video that will be reviewed by an operator of the AC or the linked Third Party, which will validate the identity of the applicant through the identification documents. The validation of the documentation will be done in person or online before an operator of the AC or the linked Third Party. Once the identity and documents have been validated, the electronic signature certificate will be issued.

The validation of the identity will be carried out based on the *Initial Validation of the Identity* section of this document.

### 5.8.4. Notification of the issuance of a new certificate to the Subscriber.

Security Data will notify the subscriber of the certificate expiration by email 30 days prior to the certificate expiration date.

It is the subscriber's power to renew or not the signature certificate.

### 5.8.5. Conduct that constitutes acceptance of a certificate with a new key.

The certificate will be accepted at the time the legal instrument binding between the subscriber and Security Data Seguridad en Datos y Firma Digital S.A has been signed.

As evidence of acceptance, there must be an acceptance document signed by the applicant. The certificate will be considered valid from the date on which the acceptance document was signed.

The acceptance document must be signed electronically once the subscriber has the corresponding electronic signature.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	35

#### **5.8.6. Publication of the certificate with a new key by the AC.**

Once the certificate has been generated and accepted by the subscriber or signatory, the certificate may be published in the certificate repositories published on the Security Data website.

#### **5.8.7. Notification of the issuance of the certificate by the AC to other entities.**

Security Data does not notify other entities of certificate issuance.

### **5.9. MODIFICATION OF CERTIFICATES.**

The modification of an electronic signature certificate implies the revocation of the same and the issuance of a new signature.

Acceptance of terms and conditions for updating data by the client.

- Generation of a revocation form, which will be electronically signed with the client's current certificate.
- Notification of the creation of the updated certificate and the revocation of the previous certificate via email to the customer.

#### **5.9.1. Circumstances for the Modification of the Certificate.**

An electronic signature certificate can be modified in the following circumstances:

- Correction of typographical errors in the data with which the signature was issued.
- The certifying entity, in accordance with changes in legislation or business lines, requires an update of data in the customer's electronic signature certificate.

#### **5.9.2. Who can request the modification of the certificate.**

Certificate modification may be requested by the subscriber or a duly authorized third party.

#### **5.9.3. Processing of certificate modification requests.**

If the subscriber detects any error in the data of their electronic signature, they must approach the offices of the AR or contact Security Data through the customer service channels, with the respective evidence for correction.

The subscriber must revoke the erroneous electronic signature certificate, signing the application with it. The AC operator will then correct the error(s) and the new certificate will be issued at no cost to the customer.

#### **5.9.4. Notification of the issuance of a new certificate to the subscriber.**

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	36

The CA will notify the subscriber via email that their new certificate is ready for download from their user profile.

#### **5.9.5. Conduct that constitutes acceptance of the modified certificate.**

The certificate will be accepted at the time the legal instrument binding between the subscriber and Security Data Seguridad en Datos y Firma Digital S.A has been signed.

As evidence of acceptance, there must be an acceptance document, signed by the applicant. The certificate will be considered valid from the date on which the acceptance document was signed.

The acceptance document must be signed electronically once the subscriber has the corresponding electronic signature.

#### **5.9.6. Publication of the certificate modified by the CA.**

Once the certificate has been generated and accepted by the subscriber or signatory, the certificate will be immediately published in the certificate repositories deemed necessary.

#### **5.9.7. Notification of the issuance of the certificate by the CA to other entities.**

Security Data does not notify other entities of certificate issuance.

### **5.10. REVOCATION AND SUSPENSION OF CERTIFICATES.**

The revocation of a certificate means the loss of validity of the certificate, and is irreversible. The suspension involves the temporary loss of validity of a certificate and is reversible.

Revocations and suspensions take effect from the moment they are published in the CRL, which are detailed in the *CRL Emission Frequency* section of this document.

#### **5.10.1. Grounds for Revocation.**

A certificate may be revoked due to the following causes:

##### **a) Circumstances affecting the information contained in the certificate:**

- Modification of any of the data contained in the certificate.
- Discovery that some of the data contained in the certificate request is incorrect.
- Loss or change of the signatory's relationship with the Organization.

##### **b) Circumstances affecting the security of the private key or certificate:**

- Compromise of the private key or the infrastructure or systems of the AC, whenever it affects the reliability of the certificates issued from that incident.

 <b>SECURITY DATA</b> TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	37

- Infringement by the AC or the Third Party of the requirements set out in the certificate management procedures, established in the CPS.
- Compromise or suspected compromise of the security of the subscriber's key or certificate.
- Unauthorized access or use by a third party of the subscriber's private key.
- Irregular use of the certificate by the subscriber or signatory.
- Failure by the subscriber or signatory to comply with the rules for the use of the certificate set out in this CPS or in the legal instrument binding between Security Data Seguridad en Datos y Firma Digital S.A and the subscriber.

**c) Circumstances affecting the security of the cryptographic device:**

- Compromise or suspected compromise of the security of the cryptographic device.
- Loss or disabling due to damage of the cryptographic device.
- Unauthorized access by a third party to subscriber activation data.
- Failure by the subscriber or signatory to comply with the rules for the use of the certificate set out in this CPS or in the legal instrument binding between Security Data Seguridad en Datos y Firma Digital S.A and the subscriber.

**d) Circumstances affecting the subscriber:**

- Termination of the legal relationship between Security Data Seguridad en Datos y Firma Digital S.A and the Subscriber.
- Modification or termination of the underlying legal relationship or cause that allowed the issuance of the certificate to the signatory.
- Infringement by the applicant of the certificate of the pre-established requirements for the application of the same.
- Infringement by the subscriber of its obligations, liability and guarantees, established in the corresponding legal instrument or in the CPS.
- Supervening disability, total or partial.
- Due to the death of the subscriber or signatory: The revocation due to death will take effect from the upload of the death certificate on the portal or its physical notification, invalidating any signature made after the death as recorded in the Civil Registry, regardless of the date of notification to the AC.

**e) Other circumstances:**

- The suspension of the digital certificate for a period longer than that established in the CPS.
- By judicial or administrative resolution that orders it.
- Due to the concurrence of any other cause specified in the CPS.

### 5.10.2. Who Can Request Revocation.

The following can request the revocation of a certificate:

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	38

- The subscriber himself, who must request the revocation of the certificate if he becomes aware of any of the circumstances indicated above.
- The legal representative may request the revocation of the certificate of any member of the company of his or her represented.
  - The EC that issued the certificate.
  - The ER through which the certificate was issued.
  - A judge who, according to the law, decides to revoke the certificate.
- Succession: Legitimate heirs in the event of death (attaching documentation).
- Judicial Mandate: Express order of competent authority.
- Any person may request the revocation of a certificate if they become aware of any of the circumstances indicated above.

The following may process the revocation of the certificate:

- The authorized operators of the RA or the Linked Third Party to which the subscriber of the certificate belongs.
- Authorized operators of the AC.

### 5.10.3. Revocation Request Procedures.

There are different alternatives for the subscriber when requesting the revocation of the certificate.

In any case, at the time of suspension or revocation of the certificate, a communication will be sent to the subscriber.

#### Online revocation of electronic signatures.

The revocation of the electronic signature is carried out from the Security Data customer portal, where you will find the option to revoke the user's certificate.

The electronic signature may be revoked in the following ways:

- I. **Natural Person Holder:** The holder, in his or her capacity as a natural person, may request the revocation of his or her certificate through the portal, making the corresponding electronic signature. The revocation will be carried out immediately, and the entry of the password associated with your electronic signature certificate constitutes a valid authentication and expression of will mechanism:
  - The holder accesses its portal.
  - Generates the request.
  - Enter the requested data.

In addition, you are requested:

- Copy of Identity Document.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	39

- In case of requesting revocation for deceased persons, the death certificate must also be uploaded.

In the event that the system detects that the holder does not have an active electronic signature certificate to authenticate online, the revocation request will be generated and will allow you to download it filled with the information entered, to sign it manually. This document must be uploaded to the same account and wait for the response in the course of the day regarding the requested revocation. The physical form must be delivered to the offices of the AC for the definitive revocation, otherwise the certificate will be suspended, or at the end of a period of 90 days the certificate will be revoked. Within these 90 days, the applicant or signatory may cancel the suspension and the revocation procedure.

II. **Legal Entity Holder:** The holder, in his or her capacity as legal representative or member of the company, may request the revocation of his or her certificate through the portal, making the corresponding electronic signature. The system will request to enter the password of the signature and it will be reviewed by the department in charge, who in the course of the day will give the response regarding the revocation, the entry of the password associated with your electronic signature certificate, constitutes a valid mechanism of authentication and expression of will:

- The holder accesses its portal.
- Generates the request.
- Enter the requested data.

In addition, you are requested:

- Copy of the applicant's ID.
- Current appointment or equivalent document.
- In the case of deceased people, the death certificate must be uploaded.

In the event that the system detects that the holder does not have an active electronic signature certificate to authenticate online, the revocation request will be generated and will allow you to download it filled with the information entered, to sign it manually. This document must be uploaded to the same account and wait for the response in the course of the day regarding the requested revocation. The physical form must be delivered to the offices of the AC for definitive revocation, otherwise the certificate will be suspended, or at the end of a period of 90 days the certificate will be revoked. Within these 90 days, the applicant or signatory may cancel the suspension and the revocation procedure.

III. **Revocation by a third party:** A third party may request the revocation of a third-party certificate, only when it proves legal competence or legitimate interest. The applicant must:

- Enter your personal portal, duly authenticated.
- Generate the request, entering the data of the person who owns the signature to be revoked and the data of the applicant.

In addition, you are requested:

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	40

- a. Natural Persons
  - Copy of the applicant's ID.
  - In the case of deceased people, the death certificate must be uploaded.
  
- b. Legal Entities
  - Copy of the applicant's ID.
  - Current appointment or equivalent document.
  - In the case of deceased people, the death certificate must be uploaded.

In the event that the system detects that the applicant does not have an active electronic signature certificate to authenticate online, the revocation request will be generated and will allow them to download it filled with the information entered to sign it manually. This document must be uploaded to the same account and wait for the response in the course of the day regarding the requested revocation. Any third-party application will remain pending, and the certificate will be placed on precautionary hold until the Security Data validation department confirms the validity of the documents.

The definitive revocation will occur only after the physical delivery of the form or after the 90-day suspension period has expired, without the holder having requested the reactivation.

#### **Face-to-face revocation in offices.**

If the subscriber or signatory attends in person, he or she will be authenticated by means of his or her identity card or passport and the certificate may be immediately revoked, after filling out the revocation request and delivered to the operator of the registration authority, in case of suspension, the subscriber may request prior validation of data from the AC.

If you call 02-3922169/04-3922169, the subscriber will receive information to carry out the certificate revocation process and the process will not begin until the request is sent by WhatsApp or email.

If it is done via email to or WhatsApp 0986442122, the subscriber must send the copy of the identity document and the revocation form, in case the revocation request is electronically signed, the definitive revocation is carried out, otherwise the certificate will be suspended and the physical form must be delivered to the offices of the CA for the definitive revocation, or at the end of a period of 90 days the certificate will be revoked. Within these 90 days, the applicant or signatory may cancel the suspension and the revocation procedure.

Security Data will strictly verify the legal competence of the third-party applicant prior to any revocation action:

1. The revocation requested by a third party will not proceed if he or she does not reliably prove his or her legal capacity (v.gr. Appointment of a Legal Representative, Special Power of Attorney, or pertinent Judicial Document) that expressly empowers him or her to act on the holder's certificate. The absence of proven legal competence will be grounds for immediate rejection of the application.

 <p><b>SECURITY DATA</b> TU IDENTIDAD DIGITAL, EN UNA FIRMA.</p>	<p><b>CERTIFICATION PRACTICES STATEMENT</b></p>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	41

2. A third party who, through the use of false, outdated documentation or acting maliciously, misleads the AC to revoke a certificate and cause damage to the holder or the organization, shall assume exclusive civil and criminal liability arising from such act.
3. Security Data acts as a bona fide executor after the administrative validation of the documentation submitted. Once the apparent legal competence has been verified, in accordance with the official records (Mercantile Registry, portal of the Superintendence of Companies, etc.), the AC will proceed with the revocation, being exempt from liability for internal conflicts or administrative disputes between the third party and the holder of the certificate.

#### **5.10.4. Grace period for Revocation Requests.**

There is no grace period for revocation requests. The revocation process will begin immediately upon receipt of such request.

Revocations and suspensions take effect from the moment they are published in the CRLs.

#### **5.10.5. Period within which the AC must process the request for Revocation.**

Once the subscriber's identity has been authenticated as set out above, and the revocation duly processed, the revocation will be effective immediately.

#### **5.10.6. Revocation Verification Requirement for Relying Parties.**

Verification of the status of certificates is mandatory for each use of certificates, either by querying the Revocation List (CRL) or the OCSP service.

#### **5.10.7. CRL Emission Frequency.**

The CRL of end-entity certificates is issued daily or when a revocation or suspension occurs, and for quick reference the AC issues a delta CRL every 24 hours.

The CRL for certificates of authority (ARLs) is issued every 6 months or when a revocation occurs.

#### **5.10.8. Maximum latency for CRL.**

Since the publication of the CRLs is made at the time of their generation, the elapsed time is considered zero or null.

#### **5.10.9. Availability of the Online Certificate Status Verification System.**

Information regarding the status of the certificates will be available online 24 hours a day, 7 days a week.

In the event of a system failure, or any other factor not within the control of the AC, the AC shall make every effort to ensure that this information service is not unavailable for longer than the maximum period of 24 hours.

 <b>SECURITY DATA</b> <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	42

#### **5.10.10. Online Revocation Check Requirements.**

For the use of the CRLs service, which is freely accessible, the following must be considered:

- In any case, the last CRL issued must be checked, which can be downloaded from the URL address contained in the certificate itself in the "CRL Distribution Point" extension.
- The user shall additionally check the relevant CRL(s) of the hierarchy certification chain.
- The user must ensure that the revocation list is signed by the authority that has issued the certificate they want to validate.
- Expired revoked certificates will be removed from the CRL.

#### **5.10.11. Other forms of revocation notices available.**

Not applicable.

#### **5.10.12. Special Key Compromise Requirements.**

Not applicable.

#### **5.10.13. Circumstances for Suspension.**

Security Data Seguridad en Datos y Firma Digital may suspend a certificate in the following cases:

- If a key compromise is suspected, until this fact is confirmed or denied.
- If the subscriber has defaulted on payment of their certificate.
- If they do not have all the information necessary to determine the revocation of a certificate.
- It is ordered by ARCOTEL, in accordance with the provisions of the Law on Electronic Commerce, Electronic Signatures and Data Messages.
- The information certification authority verifies that the data provided by the certificate holder is false.
- There is a breach of the contract entered into between the information certification authority and the holder of the electronic signature.

#### **5.10.14. Who Can Request the Suspension.**

The following may only suspend the certificate:

- The authorized operators of the Linked Third Party to which the subscriber of the certificate belongs.
- Authorized operators of the AC.
- The same users.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	43

#### 5.10.15. Procedure for requesting suspension.

For the procedure for suspension of the certificate, the provisions of the Procedure *for the Request for Revocation* section of this section will be followed.

#### 5.10.16. Suspension Period Limits.

Under no circumstances does Security Data Seguridad en Datos y Firma Digital make copies of the certificates in case of expiration, revocation or suspension. The customer will be the only entity authorized to lift the suspension, in accordance with the subscriber's criteria, and it may not be delegated to a third party.

Once the suspension has been made, the unique serial number of the certificate goes to the list of CRLs in suspended status, with the subscriber being the only one who can lift the suspension, and Security Data will execute the necessary processes to remove the serial number of the subscriber's certificate from the CRL's, and in case the certificate has expired or is no longer valid, a new one will be issued.

An electronic certificate may be kept for 90 days in a state of suspension. If this period has elapsed without the subscriber having requested or obtained the lifting of the suspension, the Certification authority will proceed to the definitive revocation of the certificate.

### 5.11. CERTIFICATE STATUS SERVICES.

#### 5.11.1. Operational Characteristics.

Security Data Seguridad en Datos y Firma Digital S.A offers a free Web publication service of Revoked Certificate Lists (CRLs) without access restrictions which contain the list of revocations since their creation and are signed by the Root AC, the query is carried out by LDAP protocol.

CRLs can be downloaded from the official website <https://www.securitydata.net.ec/firma-electronica-en-ecuador/> in the Electronic Signature, Support and Queries tab "Signature Expiration and CRL" option URL: <https://consultacertificados.securitydata.net.ec/app-consulta-certificados/#/consultarCert>

The download links of the CRLs can be found at the following addresses:

<http://crl1.securitydata.net.ec/subca2crl1/crlfile.crl>  
<http://crl2.securitydata.net.ec/subca2crl2/crlfile.crl>

#### CRL emission parameters.

The lists of revocation certificates (CRLs) are signed by the Root AC with a sha256RSA signing algorithm, which is valid for one day after they are updated.

#### 5.11.2. Availability of Service.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	44

Security Data has implemented the following measures to ensure the availability of the service:

- Redundant configuration of computer systems, in order to avoid single points of failure,
- Redundant high-speed connections to avoid loss of service,
- Use of uninterruptible power supplies.

Although these measures guarantee the availability of the Security Data service, 100% annual availability cannot be guaranteed. Security Data aims to provide 99.6% annual service availability.

### **5.11.3. Optional Features.**

Not applicable.

### **5.12. END SUBSCRIPTION.**

All certificates issued must incorporate the date of issue and the date of expiration, which are explicitly included in the structure of the digital certificate. These dates allow the certificate to automatically change its status to "Expired" once the defined validity period has been reached, thus ensuring the proper closure of its life cycle without manual intervention.

In addition, the expiration of the certificate is verifiable directly in the certificate itself through validation with tools.

The subscription will end at the time of expiration or revocation of the certificate.

### **5.13. KEY ESCROW AND KEY RECOVERY.**

#### **5.13.1. Key escrow and key Recovery Policy and Practices.**

Security Data does not store, nor does it have the possibility to store the private key of subscribers.

#### **5.13.2. Session key encapsulation and retrieval policy and practices.**

The AC limits its function to issuing and managing certificates and their status (validity, revocation), without intervening in the generation/management of session keys.

Any request for session key retrieval will be rejected, informing the requestor that the service is not part of the certification scheme.

 <b>SECURITY DATA</b> <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	45

## 6. Controls of Facilities, Management and Operation.

### 6.1. PHYSICAL CONTROLS.

The AC has established physical and environmental security controls to protect the resources of the facilities where the systems and equipment used for operations are located.

The physical and environmental security policy applicable to certificate generation services protects against:

- Unauthorized physical access
- Natural disasters
- Fires
- Failure of support systems (e-power, telecommunications, etc.)
- Collapse of the structure
- Flooding
- Theft
- Unauthorised departure of equipment, information, supports and applications related to components used for the Accredited Entity's services.

The facilities have preventive and corrective maintenance systems with assistance 24 hours a day, 365 days a year, with assistance within 24 hours of the notification. The location of the facilities guarantees the presence of security forces within a period of no more than 30 minutes.

#### 6.1.1. Physical location and construction.

The CA facilities are built with materials that guarantee protection against brute force attacks, and are located in an area of low disaster risk and allows quick access.

Specifically, the room where cryptographic operations are carried out is a cage with protection from external radiation, double flooring, fire detection and extinguishing, anti-humidity systems, double cooling system and double electricity supply system.

#### 6.1.2. Physical Access.

Physical access to the premises of the Accredited Entity where certification processes are carried out is limited and protected by a combination of physical and procedural measures.

It is limited to expressly authorized personnel, with identification at the time of access and registration, including CCTV filming and archiving. The facilities have presence detectors at all vulnerable points, as well as alarm systems for intrusion detection with warning through alternative channels.

Access to the rooms is made with ID card and fingerprint readers, managed by a computer system that maintains an automatic log of entrances and exits.

 <p>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</p>	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	46

### 6.1.3. Electric Power and Air Conditioning.

The AC installations have current stabilizing equipment and an electrical supply system for duplicated equipment by means of a redundant generator set with fuel tanks that can be refilled from the outside.

The rooms that house computer equipment have temperature control systems with duplicate air conditioning equipment.

### 6.1.4. Water Exposure.

The rooms where computer equipment is housed have a humidity detection system.

### 6.1.5. Fire Protection and Prevention.

The rooms where computer equipment is housed have automatic fire detection and extinguishing systems.

### 6.1.6. Storage System.

Each detachable storage medium (tapes, cartridges, floppy disks, etc.) containing classified information is labeled with the highest level of classification of the information it contains and remains within the reach of authorized personnel only.

Information classified as Confidential, regardless of the storage device, is kept in fireproof cabinets or locked up permanently, requiring express authorization for its removal.

### 6.1.7. Elimination of Information Carriers.

When it is no longer useful, sensitive information is destroyed in the most appropriate way for the medium that contains it:

- Printed matter and paper: by shredders or in bins provided for this purpose to be subsequently destroyed, under control.
- Storage media: before being discarded or reused, they must be processed for deletion physically destroyed or make the information contained illegible.

### 6.1.8. External Backup.

Daily backups of the information are established.

## 6.2. PROCEDURAL CONTROLS.

### 6.2.1. Roles of Trust.

The trusted roles are those described in the respective Certification Policies and the personnel that are part of the Information Security Committee, so that a segregation of duties is

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	47

guaranteed that disseminates control and limits internal fraud, not allowing a single person to control from start to finish all certification functions. The minimum roles established are:

- PKI system administrator: who will be in charge of ensuring compliance with the technological actions implemented for operational continuity, managing resources, policies, standards and procedures.
- PKI System Operator: will advise the security officer on matters related to the security of information assets, will also be responsible for the day-to-day management of the system (monitoring, backup, recovery, etc.).
- Technical Secretary (in charge of Infrastructure): will advise on a permanent and close basis to the different areas of the Company on issues related to the segregation of duties. Coordinate the response to incidents that affect the segregation of duties.
- Legal Area: will ensure that the Certification Practices Statement (CPS) and other regulatory documents applicable to the AC are in accordance with current national legislation and regulatory bodies and that the PC Certification Policies are constantly updated by the company's function.
- Internal Auditor: Will review the periodic planning of audits to the certification system and will ensure compliance with the audits and that the findings found are mitigated. In addition, he will be authorized to access the system logs and verify the procedures that are carried out on it.
- AC Operator - Certification Operator: Responsible for activating the AC keys in the Online environment, or for the certificate and CRL signing processes in the Root Offline environment.
- Linked Third Party Operator: Responsible for approving, issuing, suspending, and revoking End Entity certificates.

### **6.2.2. Number of people needed per task.**

The AC guarantees at least two people to perform the tasks that require multi-person control and are detailed below:

- The generation of the key to the AC's.
- The recovery and backup of the private key of the CA's.
- The issuance of AC certificates.
- Activation of the private key of the CA's.
- Any activity performed on the hardware and software resources that support root CA.

### **6.2.3. Identification and authentication for each role.**

The people assigned to each role are identified by the internal auditor, who will ensure that each person performs the operations for which he or she is assigned.

Each person only controls the assets necessary for their role, thus ensuring that no one person has access to unallocated resources.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	48

Access to resources is done depending on the asset through login/password, digital certificates, physical access cards and keys.

**6.2.4.Roles that require separation of duties.**

The Auditor tasks are incompatible in time with the Certification tasks and incompatible with Systems. These functions will be subordinate to the head of operations, reporting both to it and to the technical management.

Persons involved in Systems Administration may not carry out any activity in the tasks of Auditing or Certification.

**6.3. PERSONNEL CONTROLS.**

**6.3.1.Requirements on Qualification, Experience and Professional Knowledge.**

All AC personnel have the academic background, professional experience, and specific training necessary to competently perform the functions assigned to them in accordance with their role.

In addition, all staff have signed an employment contract that includes confidentiality clauses, as well as an additional non-disclosure agreement (NDA), in order to ensure the protection of sensitive information and prevent its exposure or misuse.

Personnel in positions of trust declare that they are free of conflicts of interest that may affect the proper execution of their functions and compromise the impartiality, integrity or security of the AC's operations.

Security Data Seguridad en Datos y Firma Digita will remove an employee from their functions of trust when it becomes aware of the existence of the commission of a criminal act that could affect the performance of these functions.

**6.3.2.Background Check Procedure.**

Security Data maintains documented procedures for the verification of personal, employment and background data of personnel who aspire to be hired, regardless of whether or not they perform a role of trust.

In general, verification methods include identity validation, review of work and academic history, verification of professional references, and consultation of judicial records, using official sources and reliable mechanisms.

**6.3.3.Training Requirements.**

Security Data defines in the profiles and job descriptions the training requirements and competencies necessary for each of the positions established within the AC.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	49

Likewise, all AC personnel receive continuous training in information security, with the aim of ensuring compliance with internal policies, current regulations and best practices in the sector, as well as taking the necessary courses to ensure the correct performance of certification tasks, especially when substantial modifications are made to them and based on the personal knowledge of each operator.

#### **6.3.4. Requirements and Frequency of Training Updates.**

Security Data provides the necessary training to its employees, at least once a year and when significant modifications are implemented in the process of issuing digital certificates, ensuring that personnel keep their knowledge and skills updated.

#### **6.3.5. Frequency and Sequence of Task Rotation.**

It is not stipulated.

#### **6.3.6. Penalties for Unauthorized Actions.**

Security Data has a Sanctions Enforcement policy that establishes the disciplinary measures applicable to the CA's employees in the event of carrying out unauthorized, improper actions or actions contrary to the established policies and procedures.

Upon detection of an unauthorized action, Security Data Seguridad en Datos y Firma Digital will initiate an investigation process to determine the veracity and impact of the action and the collaborators involved. After this, disciplinary measures will be taken according to the seriousness and intention of the action.

Regardless of employment sanctions, Security Data reserves the right to take legal action for recourse against any employee or related third party who, through intent or gross negligence, causes economic or reputational damage to the CA by failing to comply with the protocols described in this CPS.

#### **6.3.7. Personnel Hiring Requirements.**

Third parties hired by Security Data must sign a non-disclosure agreement (NDA), as well as a contract for the provision of services that expressly includes a confidentiality clause, guaranteeing the protection of the information to which they have access during the contractual relationship.

Personnel hired for specific purposes within the operations of the AC will be evaluated with respect to their criminal record, knowledge, academic training and experience necessary for the position.

In addition, new personnel must undergo a medical evaluation to verify that they are fit to perform their duties.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	50

### 6.3.8. Documentation Provided to Staff.

All personnel incorporated within Security Data Seguridad en Datos y Firma Digital are provided with all the documentation required for the performance of their functions, these are policies, procedures and formats of all CA processes, taking into account the following documentation:

- Internal Regulations on Occupational Health and Safety.
- Internal Regulations.
- Information Security User Manual.
- Information Security Organization.

## 6.4. AUDIT TRAIL PROCEDURES.

### 6.4.1. Types of Events Recorded.

SECURITY DATA records and saves the logs of all events related to the CA security system. These include the following events:

- Switching the system on and off.
- Attempts to create, delete, set passwords, or change privileges.
- Login and logout attempts.
- Attempts to gain unauthorized access to the SECURITY DATA system through the network.
- Attempts to gain unauthorized access to SECURITY DATA's internal network.
- Unauthorized access attempts to the file system.
- System configuration and maintenance changes.
- Logs of SECURITY DATA applications.
- Turning the SECURITY DATA application on and off.
- Changes to SECURITY DATA details and/or your passwords.
- Changes to certificate profiling.
- Generation of own keys.
- Certificate lifecycle events.
- Events associated with the use of the SECURITY DATA cryptographic module.
- Records of the destruction of the media containing the keys, activation data.

In addition, Security Data retains, either manually or electronically, the following information:

- System maintenance and configuration changes.
- Changes in the personnel who perform trust tasks in the CA.
- Reports of commitments and discrepancies.
- Records of the destruction of material containing key information, activation data, or subscriber personal information, if that information is managed.
- Possession of activation data, for operations with the private key of the CAs.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	51

#### **6.4.2. Frequency of Audit Log Processing.**

The audit logs will be reviewed every week and in any case when there is an alert from the system due to the existence of an incident, in search of suspicious or unusual activity.

#### **6.4.3. Audit Log Retention Period.**

The information in the audit logs will be stored for as long as it is considered necessary to guarantee the security of the system depending on the importance of each specific log.

#### **6.4.4. Protection of Records.**

The logs of the systems are protected from manipulation by signing the files that contain them.

They are stored in fireproof devices. Its availability is protected by storing it in facilities outside the centre where the Certification Authority is located.

The devices are operated at all times by authorized personnel.

#### **6.4.5. Procedures for Supporting Audit Trails.**

SECURITY DATA has an appropriate backup procedure, so that in the event of loss or destruction of relevant files, the corresponding backup copies of the logs are available within a short period of time.

The CA has implemented a secure backup procedure for audit logs, making a weekly copy of all logs. Daily, incremental, and full weekly copies are made.

#### **6.4.6. Audit Information Collection System.**

Security Data event audit information is collected internally and in an automated manner by the operating system and certification software.

#### **6.4.7. Event Notification.**

The CA has a procedure for the monitoring of incidents and their resolution where the responses are recorded and an economic evaluation that involves the resolution of the incident.

Security Data states that consideration is given to allowing notification to a holder in cases where it is established that the event is accidental and likely to occur again.

#### **6.4.8. Vulnerability Analysis.**

Security Data performs a constant analysis of vulnerabilities which are treated and corrected immediately. In addition, an annual review of discrepancies in the information in the logs and suspicious activities is carried out.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	52

## 6.5. LOG FILE.

### 6.5.1.Type of Archived Events.

Events that take place during the life cycle of the certificate, including the renewal of the certificate, will be retained. The following shall be stored by the CA or by its delegation to the linked Third Party:

- All audit data.
- All data relating to certificates, including contracts with subscribers and data relating to their identification.
- Requests for the issuance and revocation of certificates.
- All certificates issued or published.
- CRL's issued or records of the status of the certificates generated.
- The documentation required by the auditors.
- Communications between PKI elements.

The CA is responsible for the correct filing of all this material and documentation.

### 6.5.2.Record Retention Period.

All system data relating to the life cycle of certificates shall be retained for the period established by applicable legislation. Certificates will be kept published in the repository for at least one year after their expiration.

Contracts with subscribers and any information relating to subscriber identification and authentication will be kept for at least 10 years or the period established by current legislation.

### 6.5.3.Protection of the Archive.

The CA ensures the correct protection of the files by assigning qualified personnel for their treatment and storing them in fireproof safe deposit boxes and external facilities where required.

The CA has technical and configuration documents detailing all the actions taken to ensure the protection of the files.

### 6.5.4.File Backup Procedures.

The CA has a storage centre to ensure the availability of copies of the electronic file archive. Physical documents are stored in secure locations with access restricted only to authorized personnel.

 <b>SECURITY DATA</b> <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	53

### **6.5.5. Requirements for the Time Stamping of Records.**

The records are dated with a reliable source. Within the technical and configuration documentation of the CA, a section is established on the configuration of times of the equipment used in the issuance of certificates.

### **6.5.6. Audit Information Filing System.**

Not stipulated.

### **6.5.7. Procedures for obtaining and verifying information on file.**

Recorded events are protected from unauthorized tampering or tampering. Access to the files containing such records is strictly restricted to duly authorized personnel, who are responsible for carrying out the corresponding integrity checks to ensure their reliability and traceability.

During the audit required by this CPS, the auditor shall verify the integrity of the information on file. The CA shall provide the information and means to the auditor to verify the information on file.

## **6.6. CHANGE OF KEY OF THE CA.**

### **6.6.1. AC Raíz.**

Before the Root CA certificate expires, a key change (rekeying) will be carried out and, where appropriate, changes will be made to the content of the certificate that better conform to current legislation and the reality of Security Data, Data Security and Digital Signature and the market. The old CA and its private key will only be used for CRL signing as long as they exist active certificates issued by the old CA. A new CA will be generated with a new private key.

The CA technical and security documentation details the process of changing CA keys. The keys of certificates issued by Root AC will become invalid at the same time as your self-signed certificate. Once the Root CA expires, it will generate a new pair of keys that it self-signs to generate the new root certificate. The change of passwords is not a recurring operation of a Certification authority and must be planned in accordance with the technical and regulatory conditions in force.

### **6.6.2. Subordinate AC.**

In the case of subordinate CAs, you can choose to renew the certificate with or without changing the keys. Only when the change is made will the provisions of the AC Root section of this section apply.

## **6.7. DISASTER MANAGEMENT AND RECOVERY.**

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	54

### **6.7.1. Incident and Vulnerability Management Procedures.**

The CA, based on its infrastructure, can recover all systems in less than 48 hours, although it ensures the revocation and publication of information on the status of the certificates in less than 24 hours.

### **6.7.2. Alteration of Hardware, Software and/or Data Resources.**

In the event of an incident that alters or corrupts both hardware, software and data resources, Security Data Seguridad en Datos y Firma Digital will proceed as stipulated in the Information Security Event and Incident Management procedure.

### **6.7.3. Procedure for Action in the Event of a Certification Authority Private Key Compromise**

The compromise or suspicion of your private key is considered an incident and will be dealt with as a major incident of the provision of digital certification services, so the internal procedures established for incident management will be followed.

In the event of compromise of the private key of the CA, Security Data Seguridad en Datos y Firma Digital:

- It will inform all subscribers, users and other CAs with whom it has agreements or other types of relationship of the commitment, at least by publishing a notice on the CA's website.
- It will indicate that the certificates and information regarding the status of the revocation, signed using this key are invalid.

After having informed through the pertinent means, Security Data will carry out the process of issuing new keys of the CA, as stipulated in the internal procedures.

### **6.7.4. Business Continuity after a disaster.**

For business continuity, Security Data has defined that:

- The CA will restore critical services (Revocation and Publication of Revoked Certificates) in accordance with this CPS within 24 hours of a disaster or unforeseen emergency.
- The CA has an alternative centre, if necessary, for the implementation of the certification systems.
- The restoration is done logically.
- Backups run on a daily basis at a logical level with a 7-day hold.

 <b>SECURITY DATA</b> TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	55

## 6.8. TERMINATION OF CA OR RA.

### 6.8.1. Certification Authority.

Before the cessation of its activity, the CA will carry out the following actions:

- It will provide the necessary funds to continue the completion of the revocation activities until the definitive cessation of the activity, if applicable.
- It will inform all subscribers, applicants, users, other ACs or entities with which it has agreements or any other type of relationship of the termination with a minimum of 2 months' notice, or the period established by current legislation.
- It will revoke any authorization for subcontracted entities to act on behalf of the CA.
- It will inform the competent administration, with the indicated advance, of the cessation of its activity and the destination to be given to the certificates, specifying, where appropriate, whether the management is to be transferred and to whom.
- The CA records will be archived and transferred to a specific custodian.
- In the event that the CA is terminated, all certificates issued under the CA will be revoked and the CA will stop issuing certificates.

### 6.8.2. Registration Authority.

In the event of the cessation of a registration authority for a specific group, Security Data Seguridad en Datos y Firma Digital S.A:

- It will stop issuing and renewing certificates of that AR.
- It will revoke the operator certificates of that AR.
- It will revoke the subscriber certificates issued by that AR, unless expressly decided otherwise.

## 7. Technical Security Controls.

### 7.1. KEY PAIR GENERATION AND INSTALLATION.

#### 7.1.1. Key Pair Generation.

Two cases will be distinguished in the generation of keys for recognized certificates:

##### **In hardware (physical support).**

The generation of the key of the CAs is carried out, in accordance with the documented process of key ceremony, within the security room of the Accredited Entity, on hardware cryptographic devices (HSM), by appropriate personnel according to the roles of trust and, at least with a dual control and witnesses of Security Data Seguridad en Datos y Firma Digital, of the organization that owns the CA and the external auditor.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	56

For end-entity certificates, the key pair will be created on the same device using the system provided by the AR. This process is securely linked to the certificate generation process, ensuring the confidentiality of the private key during the generation process and the complementarity between the creation and signature verification data.

**In software.**

The subscriber will receive an email to connect to the Security Data Seguridad en Datos y Firma Digita certificate generation service. The subscriber will generate the key pair on their system and send the public key to the CA in PKCS10 format or equivalent.

In other cases, the generation of subscriber keys will be carried out on devices that reasonably ensure that the private key will be protected by the subscriber against use by others, either by physical means, or by establishing the subscriber the appropriate controls and security measures.

**7.1.2.Delivery of the Private Key to the Subscriber.**

**In hardware (physical support).**

The private key will be delivered together with the certificate in the signature creation device, when the subscriber wishes it to be imported into the DSCF device; However, even if the import has not been carried out, both the private key and the device will remain under the responsibility and custody of the subscriber. The Linked Third Party will be responsible for guaranteeing the delivery of the device to the subscriber and indicating the change of key of the physical device, thus ensuring that the latter is in possession of the signature creation data corresponding to the verification data that appears in the certificate.

The cryptographic device uses an activation key for access to private keys.

**In software.**

The subscriber will generate the key pair directly in. p12 format.

**7.1.3.Delivery of the Public Key to the Certificate Issuer.**

The sending of the public key to the CA for the generation of the certificate is done using a standard format, preferably in self-signed PKCS#10 or X.509 format, the root and subordinate are published on the Security Data and client website according to the previous section since it is a set of public and private keys.

**7.1.4.Delivery of the Public Key of the CA to the Third Parties Trust the Certificates.**

The certificate of the CAs of the certification chain is available to users on the Security Data Seguridad en Datos y Firma Digital S.A website.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	57

### **7.1.5.Key sizes.**

The size of the public and private key used by the Root and Subordinate AC is 4096 bits. The size of the end-user keys is 2048 bits.

### **7.1.6.Generation of public key parameters and quality control.**

The CA establishes formal procedures for the issuance of electronic certificates, guaranteeing the use of algorithms and key lengths in accordance with recognized cryptographic standards and current regulations.

The generation of cryptographic parameters and key pairs is carried out in secure and controlled environments, using certified cryptographic modules, such as Hardware Security Modules (HSM), under strict physical and logical access controls, and applying the principle of segregation of duties.

The cryptographic quality of the key material and the public key received will be verified by automatic controls by the PKI Software and hardware, in the same way the logs of creation and issuance of certificates will be stored.

### **7.1.7.Supported Key Applications (X.509v3 KeyUsage field).**

All certificates include the Key Usage and Extended Key Usage extension, indicating the enabled uses of the keys.

The permitted uses of the key for each certificate are defined in the corresponding Certification Policy.

## **7.2. PROTECTION OF PRIVATE KEYS AND ENGINEERING OF CRYPTOGRAPHIC MODULES.**

### **7.2.1.Standards for Cryptographic Modules.**

The cryptographic modules used to generate and store the keys of the Certificate Authorities are certified to the FIPS-140-2 level 3 standard.

The keys of the subscribers of certificates recognized with DSCF and of operators and administrators are generated by the interested party in a secure way using a cryptographic device CC EAL4+, FIPS 140-1 level 3, ITSEC E4 High or another of equivalent level.

The cryptographic devices for the custody of the private key of the subscriber of recognized certificates with DSCF and of the operator or administrator provide a level of security.

### **7.2.2.Multi-person control (k of n) of the Private Key.**

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	58

Access to the private keys of the CA requires the simultaneous concurrence of three different cryptographic devices out of five possible, protected by an access key.

### **7.2.3.Custody of the Private Key.**

The root CA's private key is escrowed by a FIPS 140-2 Level 3 certified hardware cryptographic device, ensuring that the private key is never clear outside of the cryptographic device. Activation and use of the private key requires the multi-person control detailed above. After the operation is carried out, the session is closed, and the private key is deactivated.

The private keys of the Subordinate CAs are kept in secure cryptographic devices certified with the FIPS 140-2 level 3 standard.

### **7.2.4.Backup of the Private Key of the CA.**

There are some devices that allow the CA's private key to be restored, which are stored securely and only accessible by authorized personnel according to trust roles, using at least dual control on a secure physical medium.

Root CA keys can be restored in accordance with the procedure to ensure compliance with CA Operations.

For the procedure of backup of private keys of the CA, the HSM security software will be loaded into the cryptographic device and the necessary configurations are made for the availability of the private keys and the services are started on a server without internet access.

### **7.2.5.Subscriber's Private Key File.**

The CA will not archive or store the certificate signing private key after the expiration of the certificate signing private key.

The private keys of the internal certificates used by the various components of the CA system to communicate with each other, sign and encrypt the information will be archived for a period of at least 10 years, after the issuance of the last certificate.

Subscribers' private keys can be archived by themselves, by preserving the certificate in PKCS#12 format, because they may be necessary to decrypt historical information encrypted with the public key, as long as the escrow device allows the operation. The CA will not store the subscriber's certificates, they will be deleted once they have been sent through the secure mechanism.

### **7.2.6.Transfer of the Private Key or from the Cryptographic Module.**

There is a CA key ceremony document that describes the private key generation processes and the use of cryptographic hardware.

 <b>SECURITY DATA</b> TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	59

In other cases, a file in PKCS12 format can be used to transfer the private key to the cryptographic module. In any case, the file will be protected by an activation code.

### **7.2.7. Private key storage in the cryptographic module.**

The private keys associated with the CA are generated and stored exclusively within secure cryptographic modules (HSMs), certified with the FIPS 140-2 level 3 standard.

The private key is stored in such a way that the key is not exportable or accessible in clear text, guaranteeing its confidentiality, integrity and availability throughout its life cycle. In no case will the private key be revealed, transferred or made available to unauthorized persons.

Access to the cryptographic module is strictly controlled by means of strong authentication mechanisms, segregation of duties and double custody controls, being limited exclusively to authorised and duly authorised personnel in accordance with the provisions of the CPS and this SPS.

The Certificate Authority implements audit controls and permanent monitoring on the use of the cryptographic module, maintaining traceable records of all operations related to the management of private keys.

### **7.2.8. Private Key Activation Method.**

The keys of the Root EC are activated by a process that requires the simultaneous use of 3 ACs (cards). Subordinate CE keys are activated by a process that requires the use of 1 of 2 cryptographic devices (cards).

Access to the subscriber's private key is made by means of a PIN or password or, if applicable, by means of a fingerprint. The pin device has a protection system against access attempts that block it when an erroneous passcode is entered more than six times.

### **7.2.9. Private Key Deactivation Method.**

The private key of the DSCF certificate subscriber will be deactivated once the cryptographic signature device is removed from the reading device. For keys in software, deactivation occurs when you log out of the signing application. The CA will not be liable for any use made if the subscriber leaves the device connected or logged in on their computer equipment.

To deactivate the private key of the Root CA and Subordinate CA, the steps described in the administrator's manual of the corresponding cryptographic equipment will be followed.

### **7.2.10. Private Key Destruction Method.**

The method of destruction must be governed in accordance with the Procedure for Deletion of Information and Destruction of Keys.

**Criteria for destruction:**

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	60

- In case of unauthorized tampering with the cryptographic device.
- When the device is replaced, the device's CA keys are removed.
- Due to an incorrect operation of the software and hardware of the cryptographic device.
- Backup and recovery of cryptographic device information.
- At the end of the life cycle of the CA key pair, for the deletion of copies and their fragments.
- In case the keys contained in the device do not serve a valid business purpose.
- Raising a new cryptographic device for use.

Security Data will use individuals in trusted roles to delete private keys when it meets the criteria described above.

#### **7.2.11. Classification of the cryptographic module.**

The qualification of the Cryptographic Module shall comply with the requirements set forth in the *Standards for Cryptographic Modules section* of this document.

### **7.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT.**

#### **7.3.1. Public Key File.**

The CA shall retain all public keys for the period required by applicable law, when applicable, or while the certification service is active and for at least an additional six months, otherwise.

#### **7.3.2. Certificate Operating Periods and Key Pair Usage Period.**

The period of use of a certificate will be determined by its temporary validity.

A certificate must not be used after its validity period, although the relying party may use it to verify historical data, considering that there will be no valid online verification service for that certificate.

### **7.4. ACTIVATION DATA.**


#### **7.4.1. Generation and Installation of Activation Data.**

The activation data is generated at the time of the certificate generation in PKCS#12 format.

If the initialization occurs in an external entity, the activation data will be delivered to the subscriber through a process that ensures their confidentiality before third parties.

#### **7.4.2. Activation Data Protection.**

Only authorized personnel have knowledge of the activation data of the private keys of the root CA and subordinate CAs.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	61

For end-entity certificates, once the device and activation data have been delivered, it is the subscriber's responsibility to maintain the confidentiality of this data.

#### **7.4.3. Other aspects of activation data.**

Not stipulated.

### **7.5. COMPUTER SECURITY CONTROLS.**

The CA uses reliable systems and commercial products to offer its certification services. The equipment used is initially configured with the appropriate security profiles by the personnel of Security Data Seguridad en Datos y Firma Digital S.A systems in the following aspects:

- Operating system security settings.
- Application security settings.
- Correct sizing of the system.
- User and Permissions Settings.
- Log Event Configuration.
- Backup and recovery plan.
- Antivirus settings.
- Network traffic requirements.

The technical and configuration documentation of Security Data Seguridad en Datos y Firma Digital S.A details the architecture of the equipment that offers the certification service, both in its physical and logical security.

#### **7.5.1. Specific Technical Safety Requirements.**

Each CA server includes the following functionality:

- Access control to CA services and privilege management.
- Identification and authentication of roles associated with identities.
- Archiving subscriber and CA history and audit data.
- Audit of security-related events.
- Self-diagnosis of safety related to CA services.
- Key and CA system recovery mechanisms.

The exposed functionalities are provided through a combination of Operating System, PKI software, physical protection and procedures.

#### **7.5.2. Computer Security Classification.**

The security of the equipment is reflected by an initial risk analysis in such a way that the security measures implemented are a response to the probability and impact produced when a group of defined threats can take advantage of security breaches.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	62

The physical protection of the environment is supported by the facilities mentioned above, while the management of personnel is efficient thanks to the small group of workers that operates in the Security Data Seguridad en Datos y Firma Digital data center.

## 7.6. TECHNICAL CONTROLS OF THE LIFE CYCLE.

### 7.6.1. Systems Development Controls.

The CA carries out the systematic survey and analysis of the security requirements applicable to any project for the development or evolution of systems, in order to prevent vulnerabilities and ensure the confidentiality, integrity, availability of information and services.

The CA maintains a formal change control procedure for versions and applications that introduce security enhancements or fix detected vulnerabilities. Any change requires registration, risk analysis, test planning, pre-approval, and, where applicable, a rollback plan.

### 7.6.2. Security Management Controls.

The EC develops the necessary activities for the training and awareness of employees in terms of safety. The materials used for training and the descriptive documents of the processes are updated after their approval by a forum for safety management.

The CA maintains an inventory of assets and documentation, set out in its internal procedures, to ensure their use. The documents are catalogued in three levels: PUBLIC, INTERNAL and CONFIDENTIAL.

For the management of access to the systems, the AC makes all reasonable efforts to confirm that access to the system is limited to authorized persons. In particular:

a) General management of CA:

- Controls based on high availability firewalls are available.
- Sensitive data is protected using cryptographic techniques or access controls with strong authentication.
- The CA has a documented procedure for managing user registrations and cancellations and access policy.
- Each person has their identifier associated with them to perform certification operations according to their role.
- CA staff will be held accountable for their actions, for example, by retaining event logs.

b) Certificate Generation:

- The CA facilities are equipped with continuous monitoring systems and alarms to detect, record and be able to act immediately in the event of an attempt to access their resources without authorization and/or irregularity.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	63

- The authentication to carry out the issuance process is carried out by a system of n operators for the activation of the private key of the CA.

c) Revocation management:

- Revocation refers to the loss of effectiveness of a digital certificate permanently, the revocation will be carried out through strong authentication. The log systems will generate the evidence that guarantees the non-repudiation of the action carried out by the AC operator.

d) Revocation Status:

- The revocation status application has access control based on certificate authentication to prevent attempts to modify the revocation status information.

In addition, Security Data follows the security approach according to ISO 27001.

### 7.6.3.Lifecycle Security Controls.

Security Data manages lifecycle security by:

- CA ensures that cryptographic hardware used for certificate signing is not tampered with during transport.
- Cryptographic hardware is built on supports prepared to prevent any manipulation.
- The CA registers all the relevant information of the device to be added to the asset catalog of Security Data Seguridad en Datos y Firma Digital, S.A.
- The use of cryptographic certificate signing hardware requires the use of at least two trusted employees.
- Security Data Seguridad en Datos y Firma Digital S.A performs periodic tests to ensure the correct operation of the device.
- The cryptographic device is only tampered with by trusted personnel.
- The CA private signing key stored on the cryptographic hardware will be deleted once the device has been removed.
- The CA has a maintenance contract for the device for its correct maintenance. Changes or updates are authorised by the security manager and are reflected in the corresponding work reports. These configurations will be made by at least two trusted people.

### 7.7. NETWORK SECURITY CONTROLS.

CA protects physical access to network management devices and has an architecture that orders the traffic generated, based on its security features by creating clearly defined network sections. This division is done through the use of firewall.

Sensitive information that is transferred over unsecured networks is done in encrypted form.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	64

## 7.8. TIME STAMPING.

The CA also offers the time-stamping service in order to provide reliable evidence of the date and time on which an electronic document was signed, securely linking such temporary information to a specific set of data, guaranteeing its integrity and verifiability.

Time stamping does not imply any validation of the content, origin or legality of the sealed data, and the use made of the service is the sole responsibility of the applicant. The specific conditions of the time-stamping service are detailed in the corresponding Time-Stamping Practice Statement.

## 8. Profile of the Certificates.

### 8.1. CERTIFICATE PROFILE.

The profile of the certificates is found in the Certificate Policies (PC) corresponding to each type of certificate and are consistent with the provisions of the following standards:

- ETSI TS 101 862 known as "European profile for Qualified Certificates"
- RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
- RFC 3739 "Qualified Certificates Profile"
- Resolution ARCOTEL-2024-0176 "TECHNICAL STANDARD FOR THE PROVISION OF INFORMATION SERVICES AND RELATED SERVICES OF ACCREDITED CERTIFICATION BODIES AND RELATED THIRD PARTIES".

#### 8.1.1. Types of Certificates.

The types of certificates issued by Security data are:

- Natural Person.
- Legal Representative.
- Member of the Company or Employee with a Relationship of Dependency.
- Electronic seal.

The Certificate Policy can be found at the following URLs:

Natural	Person:	<a href="https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/pc_pn_en.pdf">https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/pc_pn_en.pdf</a>
Legal	Representative:	<a href="https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/pc_rl_en.pdf">https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/pc_rl_en.pdf</a>
Company	Member:	<a href="https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/pc_me_en.pdf">https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/pc_me_en.pdf</a>
Electronic	Seal:	<a href="https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/pc_se.pdf">https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/pc_se.pdf</a>

 <b>SECURITY DATA</b> <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	65

Time Stamp: [https://www.securitydata.net.ec/normativas/pc\\_ts.pdf](https://www.securitydata.net.ec/normativas/pc_ts.pdf)

The validity of the key pair will be as requested by the subscriber based on the following parameters:

- For Natural Persons: from 1 day and 1 month, exclusively without RUC, and from 1 to 5 years.
- For Legal Entities: the maximum allowed by the appointment of the legal representative which can vary between 1 to 5 years.

#### **Real Estate Certificates.**

- CA Root Certificate  
[https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema\\_Windows/cacert.cer](https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema_Windows/cacert.cer)
- SUBCA-1 Subordinate Root Certificate  
[https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema\\_Windows/SUBCA-1.cer](https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema_Windows/SUBCA-1.cer)
- CA-2 Root Certificate  
[https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema\\_Windows/SECDATA-CA-2.cer](https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema_Windows/SECDATA-CA-2.cer)
- SUBCA-2 Subordinate Root Certificate  
[https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema\\_Windows/SECDATA-SUBCA2.cer](https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema_Windows/SECDATA-SUBCA2.cer)

#### **Legal Entity Certificates.**

Corporate Certificates are recognized electronic signature certificates whose subscriber is a Corporation (either a company, an organization, or a Public Administration):

- Corporate Certificates of Legal Representative: These are recognized certificates of natural persons that identify the subscriber as a corporation and the signatory as the legal representative of said corporation.
- Corporate Certificates of Company Member: These are recognized certificates of natural persons that identify the subscriber as a Corporation and the signatory as linked to that corporation as an employee.

#### **Natural Person Certificates.**

Natural Person Certificates: These are recognized certificates of natural persons that identify the subscriber as a natural person, and this certificate can be used for tax, legal and personal matters.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	66

### 8.1.2. Types of Support.

Natural or Legal Person Certificates can be generated in two types of hardware, software:

#### a) **Secure Signature Creation Device (DSCF).**

The private keys of certificates issued on hardware media are generated and stored in a "Secure Signature Creation Device (DSCF)", such as a Smart Card or a cryptographic DSCF. The DSCFs provided by Security Data Seguridad en Datos y Firma Digital S.A are FIPS certified.

Therefore, the use of Company Member Certificates with DSCF allows electronic signatures to be carried out with high security.

Certificate keys generated in DSCF cannot be copied in any way, so if the device is lost or damaged, a new certificate issuance process will be necessary.

To activate the DSCF it will be necessary to enter the activation code (PIN) provided by the manufacturer. For security reasons, the owner of the device is recommended, both in person and by email, to immediately change said password, establishing a personal and confidential credential.

From the modification of the initial PIN, the user will be solely responsible for the administration, custody and use of their new password, and must adopt the necessary measures for its adequate protection and to prevent unauthorized access to the device.

If the password or PIN is entered five times in a row incorrectly, the device will be locked, and therefore unusable. To proceed with the unlocking, you must approach the Linked Third Party where you acquired the certificate with the locked device or send it to it, where the unlocking will be carried out, or you can process it remotely. The PIN is secret and personal to the user, an initial PIN will be given which must be modified later by the user using the corresponding applications.

#### **DSCF distribution.**

The DSCFs distributed by Security Data, after validation of the subscriber's identity, are delivered in three ways:

- Directly to the subscriber.
- To a third person duly authorized by the subscriber.
- Home delivery.

#### b) **Software Support.**

This service allows the user, after having made the request and being approved by the Certifying Entity and after having received the certificate generation email, to access the Security Data portal and be able to generate the digital certificate with their public and private keys, being

 <b>SECURITY DATA</b> TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	67

stored in the Windows CAPI of the client's PC or as a file with a .p12/.pfx extension in it. being the use of these certificates to sign and encrypt documents and for encrypted mail.

### 8.1.3. Certificate Profile.

The basic profile to all subscriber certificates is as follows:

**Table 1:** Basic profile of all subscriber certificates.

CERTIFICATE FIELD	NAME	DESCRIPTION
Version	Version number	V3 (Standard x.509 Version)
Serial Number	Serial Number	Unique code with respect to the distinguished name of the issuer
Signature Algorithm	Signature algorithm	sha256RSA signature algorithm
Signature hash algorithm	Signature hashing algorithm	Sha256
Issuer	Transmitter	DN of the CA issuing the certificate
Validity	Validity	Start and end date of validity, UTC time
Subject	Subject	Distinguished name of the subscriber.
Subject Public key info	Public Key	public key of the subscriber

Certificate profiles, specific to each type of certificate granted by Security Data, are set within the PC.

#### a) Root CA and subordinate CA.

The chain of trust issued for the public key infrastructure for both the root and subordinate CAs were issued with sha256RSA encryption algorithms and with a key size of 4096 bits.

**Table 2:** Root Certified Profile – AC

ROOT CERTIFICATE – AC(ROOT) - ANNEX 6				
Field	Contents	Required	Crit.	OID Observations 1.3.6.1.4.1.37746.1
<b>1. Basic structure</b>				
1.1 Version	3	Yes		Paragraph "2" corresponds to version 3.
1.2 Serial Number	Hexadecimal Positive Number 0x41BBD251	Yes		It cannot be a negative number or 0.
1.3 Signature Algorithm		Yes		
1.3.1 Identifier	SHA-256 with RSA	Yes		1.2.840.113549.1.1.11
1.3.2 Description	OBJECT IDENTIFIER	Yes		
1.4 Issuer		Yes		
1.4.1 Common Name (CN)	ROOT CA-2 SECURITY DATA CERTIFICATE AUTHORITY	Yes		OID 2.5.4.3
1.4.2 Country (C)	EC	Yes		OID 2.5.4.6
1.4.3 Organization Name (O)	SECURITY DATA S.A. 2	Yes		OID 2.5.4.10

1.4.5 Organizational Unit (OU)	INFORMATION CERTIFICATION ENTITY	No		OID 2.5.4.11
<b>1.5 Validity</b>		Yes		
1.5.1 Not Before	2019-10-15 16:20:12 ECT	Yes		YYMMDDHHMMSSZ
1.5.2 Not After	2039-10-06 16:20:12 ECT	Yes		YYMMDDHHMMSSZ
<b>1.6 Subject</b>		Yes		
1.6.1 Common Name (CN)	ROOT CA-2 SECURITY DATA CERTIFICATE AUTHORITY	Yes		OID 2.5.4.3
1.6.2 Country (C)	EC	Yes		OID 2.5.4.6
1.6.3 Organization Name(O)	SECURITY DATA S.A. 2	Yes		OID 2.5.4.10
1.6.5 Organizational Unit (OU)	INFORMATION CERTIFICATION ENTITY	No		OID 2.5.4.11
<b>1.7 Subject Public Key Info</b>		Yes		
1.7.1 AlgorithmIdentifier				
1.7.1.1 Algorithm	RsaEncryption	Yes		OID 1.2.840.113549.1.1.1
1.7.1.2 Parameters		No		
1.7.2 SubjectPublicKey		Yes		
<b>2.1 Authority Key Identifier</b>		No	No	OID 2.5.29.35 (Marked as NOT critical according to EN 319412-2) It is not required as long as the public key of the CA is distributed in the form of a "SELF-SIGNED" certificate
2.1.1 Key Identifier		No		Derived from the public key
<b>2.2 Subject Key Identifier</b>		Yes	No	OID 2.5.29.14 (Marked as NOT critical according to EN 319412-2)
2.2.1 KeyIdentifier		Yes		
<b>2.3 Key Usage</b>		Yes		OID 2.5.29.15
2.3.1 Digital Signature	True -> Digital Signature			
2.3.2 Content commitment				
2.3.3 Key Encipherment				
2.3.4 Data Encipherment				
2.3.5 Key Agreement				
2.3.6 Key Certificate Signature	True -> Certificate Signing	Yes		
2.3.7 CRL Signature	True -> CRL Signing	Yes		
<b>2.4 Certificate Policies</b>		Yes	No	OID 2.5.29.32 (Marked as NOT critical according to EN 319412-2)
2.4.1 Policy Information		Yes		
2.4.1.1 Policy Identifier	<b>1.3.6.1.4.1.37746.1</b>	Yes		Policy ID
2.4.1.2 Policy Qualifier ID		Yes		
2.4.1.2.1 CPS Pointer		Yes		
2.4.1.2.2 User Notice		Yes		

 <b>SECURITY DATA</b> TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	69

<b>2.5 Subject Alternative Names</b>			No	
<b>2.6 Basic Constraints</b>		Yes	Yes	OID 2.5.29.19
2.6.1 Subject type	Subject is a CA	Yes		
2.6.2 Path Length Constraints	None	Yes		

**Table 3:** Subordinate Certificate Profile – AC SUB

SUBORDINATE CERTIFICATE - AC SUB - ANNEX 7				
Field	Contents	Required	Crit.	OID Observations 1.3.6.1.4.1.OID_Ac.n
<b>1. Basic structure</b>				
<b>1.1 Version</b>	3	Yes		The item "2" corresponds to version 3. X.509 v3
<b>1.2 Serial Number</b>	Hexadecimal Positive Number 0x589AE890	Yes		It cannot be a negative number or 0.
<b>1.3 Signature Algorithm</b>		Yes		
1.3.1 Identifier	SHA-256 with RSA	Yes		1.2.840.113549.1.1.11
1.3.2 Description	OBJECT IDENTIFIER	Yes		
<b>1.4 Issuer</b>		Yes		
1.4.1 Common Name (CN)	ROOT CA-2 SECURITY DATA CERTIFICATE AUTHORITY	Yes		OID 2.5.4.3
1.4.2 Country Name (C)	EC	Yes		OID 2.5.4.6
1.4.3 Organization Name (O)	SECURITY DATA S.A. 2	Yes		OID 2.5.4.10
1.4.5 Organizational Unit (OU)	INFORMATION CERTIFICATION ENTITY	No		OID 2.5.4.11
<b>1.5 Validity</b>		Yes		
1.5.1 Not Before	2019-10-15 17:15:57 ECT	Yes		YYMMDDHHMMSSZ
1.5.2 Not After	2039-04-07 17:15:57 ECT	Yes		YYMMDDHHMMSSZ
<b>1.6 Subject</b>		Yes		
1.6.1 Common Name (CN)	SUBCA-2 SECURITY DATA CERTIFICATION AUTHORITY	Yes		OID 2.5.4.3
1.6.2 Country Name(C)	EC	Yes		OID 2.5.4.6
1.6.3 Organization Name (O)	SECURITY DATA S.A. 2	Yes		OID 2.5.4.10
1.6.5 Organizational Unit (OU)	INFORMATION CERTIFICATION	No		OID 2.5.4.11
<b>1.7 Subject Public Key Info</b>		Yes		
1.7.1 AlgorithmIdentifier				OID 1.2.840.113549.1.1.1
1.7.1.1 Algorithm	RsaEncryption	Yes		
1.7.1.2 Parameters		No		
1.7.2 SubjectPublicKey		Yes		
<b>2.1 Authority Key Identifier</b>		No	No	OID 2.5.29.35 (Marked as NOT critical according to EN 319412-2) It is not required as long as the public key of the CA is

				distributed in the form of a "SELF-SIGNED" certificate
2.1.1 Key Identifier		No		
<b>2.2 Subject Key Identifier</b>		Yes	No	OID 2.5.29.14 (Marked as NOT critical according to EN 319412-2)
2.2.1 KeyIdentifier		Yes		
<b>2.3 Key Usage</b>		Yes		OID 2.5.29.15
2.3.1 Digital Signature	True -> Digital Signature			
2.3.2 Content commitment				
2.3.3 Key Encipherment				
2.3.4 Data Encipherment				
2.3.5 Key Agreement				
2.3.6 Key Certificate Signature	True -> Certificate Signing	Yes		
2.3.7 CRL Signature	True -> CRL Signing	Yes		
<b>2.4 Certificate Policies</b>		Yes	No	OID 2.5.29.32 (Marked as NOT critical according to EN 319412-2)
2.4.1 Policy Information		Yes		
2.4.1.1 Policy Identifier	1.3.6.1.4.1.37746.1.9	Yes		Policy ID
2.4.1.2 Policy Qualifier ID	(1.3.6.1.5.5.7.2.1)	Yes		
2.4.1.2.1 CPS Pointer	<a href="https://www.securitydata.net.ec/wp-content/downloads/Normativas/p_certificacion/declaracion.pdf">https://www.securitydata.net.ec/wp-content/downloads/Normativas/p_certificacion/declaracion.pdf</a>	Yes		1.3.6.1.5.5.7.2.1
<b>2.5 Subject Alternative Names</b>		No	No	OID 2.5.29.17 (Marked as NOT critical according to EN 319412-2)
<b>2.6 cRLDistributionPoint</b>		Yes		OID 2.5.29.31 (Marked as NOT critical according to EN 319412-2)
2.6.1 distributionPoint	ldap://ldapsdca2.securitydata.net.ec/CN=AUTORIDAD OF CERTIFICATION ROOT CA-2 SECURITY DATA,OU=INFORMATION CERTIFICATION AUTHORITY,O=SECURITY DATA S.A.2,C=EC?authorityRevocationList?base	Yes		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.6.2 distributionPoint		No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
<b>2.7 Authority Information Access</b>		No	No	OID 1.3.6.1.5.5.7.1.1 (Marked as NOT critical according to EN 319412-2)
2.7.1 Access Method		No		OID 1.3.6.1.5.5.7.48.1
2.7.2 Access Location		No		OCSP Access URL (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.7.3 Access Location		No		OCSP Access URL

 <b>SECURITY DATA</b> TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	71

				( <a href="http://">http://</a> ) IETF RFC 7230-7235 [3] or <a href="https://">https</a> ( <a href="https://">https://</a> ) IETF RFC 2818 [5]
<b>2.8 Basic Constraints</b>		Yes	Yes	OID 2.5.29.19
2.8.1 Subject type	Subject is a CA	Yes		
2.8.2 Path Length Constraints	None	Yes		

#### 8.1.4. Version Number.

The certificates follow the X.509 version 3 standard for subscribers and version 2 for CRLs.

#### 8.1.5. Extension of Certificates (OID-Object Identifier).

The extensions presented here correspond to all those that may be contained in the certificates issued. In the Certification Policy of each type of certificate, the required extensions are specified in detail.

**Table 2.** Certificate Extension (OID)

EXTENSION	FILM REVIEW	DESCRIPTION
Authority Key Identifier	No	Issuer key identifier
Subject Key Identifier	No	Subscriber key identifier
Key Usage	Yes	Permitted Uses of the Certificate
Certificate Policies	No	Certification policy for the certificate.
Subject Alternative Names	No	Alternative name the subscriber
Extended Key Usage	No	Define the specific purpose of the certificate
cRLDistributionPoint	No	Official URL where CRLs are published
Authority Information Access	No	Issuer CA and OCSP (Certificate Status Online Validation)
Basic Constraints	Yes	Differentiates user and authority certificates.

#### 8.1.6. Algorithm object identifiers.

For the issuance and validation of the certificate, the CA uses the following Object Identifiers (OIDs) associated with the cryptographic algorithms used:

Category	Name / Description	OID	Observation
Public Key Algorithm	RSA (PKCS #1) / rsaEncryption	1.2.840.113549.1.1.1	Public Key <b>RSA 2048-bit</b>
Certificate Signing Algorithm	sha256WithRSAEncryption	1.2.840.113549.1.1.11	Signing the certificate with <b>SHA-256 + RSA</b>
Hash algorithm	SHA-256 / id-sha256	2.16.840.1.101.3.4.2.1	Associated hash function

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	72

Category	Name / Description	OID	Observation
EKU (Extended Use)	Client Authentication / id-kp-clientAuth	1.3.6.1.5.5.7.3.2	Present on the certificate
EKU (Extended Use)	Mail Protection (S/MIME) / id-kp-emailProtection	1.3.6.1.5.5.7.3.4	Present on the certificate

#### Key Usage of the certificate (not OID, they are "bits")

Extension	Value on the certificate
digitalSignature	TRUE
contentCommitment (non-repudiation)	TRUE
keyEncipherment	TRUE
dataEncipherment	FALSE
keyAgreement	FALSE
keyCertSign	FALSE
cRLSign	FALSE

#### 8.1.7. Name formats.

Certificates issued under Security Data contain the "full name", in X.500 format, for the issuer and subscriber, located in the "Issuer Name" and "Subject Name" fields, respectively, and are formed as defined in *Table 3*.

**Table 3.** Name formats

DN FIELD	NAME	DESCRIPTION
CN, Common Name	Subscriber's Name	Subscriber's Name and Surname
CN, Common Name	CA Name	Names and Surnames of the CA
OU, Organizational Unit	Organizational Unit	Information Certification Authority
O, Organization	Organization	Name of the AC
C, Country	Country	Two-digit country code according to ISO 3166-1. Default "ES".

#### 8.1.8. Name restrictions.

The X.509 "Name Constraints" extension is not used in the certificates in this policy, i.e. no technical restrictions are included using OID 2.5.29.30. As a result, there are no "permittedSubtrees/excludedSubtrees" expressed in the certificate.

#### 8.1.9. Certificate Policy object identifier.

The object identifier of the Certificate Policy corresponding to each type of certificate, as established in the Certification Policy of Security Data certificates, any change will be communicated to the Competent Authority, the general format is 1.3.6.1.4.1.37746.2.x.x where

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	73

the last values correspond to the type of certificate. . Y For Time Stamping and Electronic Stamping the general format is 1.3.6.1.4.1.37746.102.2.x.x

#### 8.1.10. Using the Policy Restrictions extension.

It is not stipulated.

#### 8.1.11. Syntax and semantics of policy qualifiers.

The policy qualifier is defined in the "Certificate Policies" extension and contains a reference to the URL where the CPS of the certification service provider is published.

**Table 4:** Semantics of Policy Qualifiers

Field		Required	Critical	Observations
2.4. Certificate Policies	-	YES	NO	OID 2.5.29.32(Marked as NOT critical according to EN 319412-2)
2.4.1. Policy Information	Policy Information	YES	-	-
2.4.1.1. Policy Identifier	1.3.6.1.4.1.37746.2.1 .1 – Policy Identifier	YES	-	CA Policy Identifier
2.4.1.2. Policy Qualifiers		YES	-	-
2.4.1.1.1 CPS URI	( <a href="https://www.repoexchange.com/cps/">https://www.repoexchange.com/cps/</a> ) – CPS URI or PC	YES	-	OID 1.3.6.1.5.5.7.2.1 Certificate Policy URL of the Certification Authority
2.4.1.1.2. User Notice/Explicit text	Type of Certificate	YES	-	OID 1.3.6.1.5.5.7.2.2 Indicative text

#### 8.1.12. Processing semantics for the extension of critical certificate policies.

It is not stipulated.

### 8.2. CRL PROFILE.

The profile of the CRLs corresponds to the one proposed in the corresponding certification policies and to the X.509 standard version 3 of the 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". CRLs are signed by the certificate authority that issued the certificates.

#### 8.2.1. Version Number.

The CRLs issued by the CA are version 2.

#### 8.2.2. CRL and CRL Input Extensions.

 <b>SECURITY DATA</b> TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	74

## AC Root CRL.

**Table 5:** Root Authority CRL

FIELDS	VALUES
Version	2
CRL Number	Incremental number
Signature algorithm	sha256RSA
Issuer	Distinguished Name (DN) of the issuer
Effective Date of Issue	(CRL issue date, UTC time)
Next update date	Effective date of issue + 6 months
Authority Key Identifier	Hash of the sender key
Contains only User Certificates	NO
Contains only CA Certificates	YES
Indirect Certificate Revocation List (CRL)	NO
CRL Tickets	Certificate Serial Number Date of Revocation Reason Code

## Subordinate AC CRLs

**Table 6:** CRLs of subordinate certificate authorities.

FIELDS	VALUES
Version	2
CRL Number	Incremental number
Signature algorithm	sha256RSA
Issuer	Distinguished Name (DN) of the issuer
Effective Date of Issue	(CRL issue date, UTC time)
Next update date	Effective date of issue + 1 days
Authority Key Identifier	Hash of the sender key
Contains only User Certificates	NO
Contains only CA Certificates	NO
Indirect Certificate Revocation List (CRL)	NO
CRL Tickets	Certificate Serial Number Date of Revocation Reason Code

### 8.3. OCSP PROFILE.

#### 8.3.1. Version number(s).

The OCSP profile corresponds to the one proposed in the corresponding Certification Policies and to the X.509 version 3 standard.

#### 8.3.2. OCSP extensions.

The OCSP profile is specified in the following table:

<b>CODE</b>	SD-ID-PE-09
<b>VERSION</b>	V12
<b>APPROVAL DATE</b>	03/4/2026
<b>PAGES</b>	75

FIELD	CONTENTS
<b>1. Basic structure</b>	
<b>1.1. Version</b>	"2"
<b>1.2. Serial Number</b>	Automatically set by the AC Unique Identification Number of the certificate.
<b>1.3. Signature Algorithm</b>	
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	Not applicable
<b>1.4. Issuer</b>	
1.4.1. Country Name ( C )	Country Code "EC" (ISO 3166)
1.4.3. Organizational Unit Name (OU)	Name of the Organizational Unit of the Subordinate CA ej ELECTRONIC SIGNATURE UNIT
1.4.4. Organization Name(O)	Name of the Subordinate CA "Organization"
1.4.5. Common Name (CN)	Name of the Subordinate CA
<b>1.5. Validity</b>	Recommended (maximum 5 years)
1.5.1. Not Before	Validity Start Date
1.5.2. Not After	Expiration Date
<b>1.6. Subject</b>	
1.6.1. Country Name (C)	Country Code "EC" (ISO 3166)
1.6.2. Locality Name (L)	Locality of the Subordinate CA (City) ej.. QUITO
1.6.3. Organization Unit Name (OU)	Name of the Organizational Unit of the Subordinate CA ej. ELECTRONIC SIGNATURE UNIT
1.6.4. Organization Name (O)	Name of the Subordinate CA "Organization"
1.6.5. Common Name (CN)	Name of the Subordinate CA
1.6.6. Organization Identifier	"VAT(CÓDIGO_PAIS)-RUC Ex. VATEC-1716151413001
<b>1.7. Subject Public Key Info</b>	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	Not aplicable
1.7.2. SubjectPublicKey	Public key encoded according to the 2048-bit cryptographic algorithm
<b>2. Extensions</b>	
<b>2.1. Authority Key Identifier</b>	Issuer Key Identifier
2.1.1. KeyIdentifier	
<b>2.2. Subject Key Identifier</b>	Subject key identifier
2.2.1. KeyIdentifier	
<b>2.3. Key Usage</b>	
2.3.1. Digital Signature	Selected "1"
2.3.2. Content commintment	Selected "1"
2.3.3. Key Encipherment	Not selected. "0"

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	76

2.3.4. Data Encipherment	Not selected. "0"
2.3.5. Key Agreement	Not selected. "0"
2.3.6. Key Certificate Signature	Not selected. "0"
2.3.7. CRL Signature	Not selected. "0"
2.3.8. Encipher Only	Not selected. "0"
2.3.9. Decipher Only	Not selected. "0"
<b>2.4. Certificate Policies</b>	
2.4.1. Policy Information	
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.6.1
2.4.1.2. Policy Qualifiers	
2.4.1.1.1 CPS URI	(https://www.repo_example.com/cps/)
2.4.1.1.2. User Notice/Explicit text	"OCSP VALIDATION CERTIFICATE"
<b>2.5. Subject Alternative Names</b>	
2.5.1. rfc822Name	Email from the Accredited Entity "info@example.com.ec"
<b>2.6. Extended Key Usage</b>	
2.6.1. ocspSigning	Present (1.3.6.1.5.5.7.3.9)
2.6.2. ocspNoCheck	Present (1.3.6.1.5.5.7.48.1.5)
<b>2.7. cRLDistributionPoint</b>	
2.7.1. distributionPoint	(http://crl1.example.com/example1subordinada.crl)
2.7.2. distributionPoint	(http://crl2.example.com/example2subordinada.crl)
<b>2.8. Authority Information Access</b>	
2.8.1. Access Description	
2.8.1.1. Access Method	id-ad-caIssuers
2.8.1.1.1 Access Location	(http://ocsp1.example.com/subordinate1.crt)
<b>2.9. Basic Constraints</b>	
2.9.1. cA	FALSE

## 9. Compliance Audits and Other Controls.

The Security Data Certificate issuance system is audited to keep the Webtrust Seal active.

### 9.1. FREQUENCY OF AUDITS.

Internal audit plans will be carried out with reporting, in order to have control over the life cycle of the certification authority and external audits will be carried out whenever requested by the regulatory authority.

Webtrust seal maintenance audits are conducted annually.

 <b>SECURITY DATA</b> <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	77

## 9.2. QUALIFICATION OF THE AUDITOR.

Audits can be internal or external. In this second case, they are carried out by companies of recognized prestige in the field of audits.

## 9.3. RELATIONSHIP BETWEEN THE AUDITOR AND THE AUDITED AUTHORITY.

The companies that carry out external audits never represent any conflict of interest that could distort their performance in their relationship with Security Data, Data Security and Digital Signature.

However, Security Data Seguridad en Datos y Firma Digital will carry out planned internal audits with monthly reports to the CA of the hierarchy, to guarantee at all times its adequacy to the requirements set by the Certification Policies of the hierarchy.

## 9.4. ASPECTS COVERED BY THE CONTROLS.

The audit verifies the following principles:

- a) **Publication of Information:** The CA makes public its Business and Certificate Management Practices (this CPS), as well as its information privacy and personal data protection policy, and provides its services in accordance with these statements.
- b) **Service Integrity:** That the CA maintains effective controls to reasonably ensure that:
  - Subscriber information is properly authenticated (for registration activities performed by the CA), and
- c) **General Controls:** the CA maintains effective controls to reasonably ensure that:
  - Subscriber and user information is restricted to authorized personnel and protected from uses not specified in the CA's published business practices.
  - Continuity of operations related to key and certificate lifecycle management is maintained.
  - The tasks of operation, development and maintenance of the CA systems are properly authorised and carried out to maintain their integrity.

### 9.4.1. Audit at the Registration Authorities.

The Registration Authorities that have access to the software/system provided by Security Data Seguridad en Datos y Firma Digital for the management of certificates, are audited by a third party prior to its effective implementation. In addition, audits are carried out to verify compliance with the requirements demanded by the Certification Policies for the development of the registration tasks set out in the signed service contract. The frequency of the audits will be determined by the agreement between Security Data Seguridad en Datos y Firma Digital and the Registration Authority, always taking into account the planned activity to be carried out by

 <b>SECURITY DATA</b> TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	78

the Registration Authority in terms of the number of certificates or specific security requirements.

However, and exceptionally, Security Data Seguridad en Datos y Firma Digital may exempt a Registration Authority from the obligation to undergo an initial audit and maintenance audits.

#### **9.5. ACTIONS TO BE TAKEN AS A RESULT OF THE DETECTION OF INCIDENTS.**

The deficiencies detected during the audit process must be corrected through a Corrective Action Plan that contains the actions, procedures or implementation of the controls required to minimize risks.

In the event that incidents or non-conformities are detected, the appropriate measures will be taken to resolve them in the shortest possible time, according to the procedures established by Security Data.

#### **9.6. COMMUNICATION OF RESULTS.**

The auditor will communicate the results to Senior Management, and if necessary, to the owners of each process, in the event that the analysis and resolution of any deviation from compliance is required, Security Data will be in charge of drawing up a subsequent corrective action plan.

Security Data will publish the current reports and Webtrust seal on its website <https://www.securitydata.net.ec/nosotros-security-data-ecuador/>

### **10. Other Legal and Activity Issues.**

#### **10.1. RATES.**

##### **10.1.1. Certificate Issuance or Renewal Fees.**

The prices of the certification services or any other service will be provided to customers or potential customers by the Commercial Department of Security Data Seguridad en Datos y Firma Digital or through the website: [www.securitydata.net.ec](http://www.securitydata.net.ec).

##### **10.1.2. Certificate Access Fees.**

Access to the public key of the certificates issued is free, however, the CA reserves the right to impose a fee for cases of mass download of certificates or any other circumstance that in the opinion of the CA should be taxed.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	79

### 10.1.3. Status Information Access or Revocation Fees.

Security Data Seguridad en Datos y Firma Digital provides free access to information regarding the status of certificates or revoked certificates, through the publication of the corresponding CRLs.

Security Data Seguridad en Datos y Firma Digital offers other services for the validation of commercial certificates (such as OCSP).

### 10.1.4. Fees for Other Services.

The rates applicable to other services will be negotiated between Security Data Seguridad en Datos y Firma Digital and the customers of the services offered.

### 10.1.5. Refunds.

Certificate subscribers may request reimbursement under the following guidelines:

- When an excess deposit has been made.
- When the service has not been provided and the client does not wish to continue with the procedure.

In these cases, the customer must demonstrate the evidence of the payment made, once the circumstances have been analyzed to make the refund, the financial department will proceed with the respective refund.

In the event of malfunctions due to technical causes or errors in the data contained in the certificate, the subscriber or the person responsible for the certificate may send an email to [info@securitydata.net.ec](mailto:info@securitydata.net.ec) Security Data, informing them of the reason for the return. Security Data will verify the causes of return, revoke the issued certificate and proceed to issue a new certificate within a maximum period of 72 hours.

## 10.2. FINANCIAL RESPONSIBILITY.

### 10.2.1. Insurance Coverage.

The insurance covers all contractual and non-contractual damages of the holders, clients of Security Data, who trust exempt from fault derived from errors and omissions, or acts of bad faith of the administrators, legal representatives or employees of the Security Data Certification Authority in the development of the activities for which it is authorized.

### 10.2.2. Other Assets.

No stipulation.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	80

### 10.2.3. Insurance or Guarantee of Coverage for Final Entities.

Security Data has acquired insurance issued by an insurance company authorized to operate in Ecuador, which covers all contractual and non-contractual damages of the owners and third parties who trust Security Data, free of fault, derived from errors and omissions, or acts of bad faith of the administrators, legal representatives or employees of Security Data in the development of the activities for which it is authorized.

## 10.3. CONFIDENTIALITY OF INFORMATION.

Security Data personnel must sign contracts that include confidentiality clauses regarding the protection of privacy and confidentiality of all information submitted by customers, as well as a confidentiality agreement. Any action that compromises the safety of the accepted critical processes may lead to the termination of the employment contract.

### 10.3.1. Scope of Confidential Information.

Security Data Seguridad en Datos y Firma Digital will consider confidential all information that is not expressly classified as public. Information declared confidential shall not be disseminated without the express written consent of the entity or organization that granted it confidentiality, unless there is a legal imposition.

- Subscribers' private signing keys are confidential and are not provided to the CA or related third parties.
- Information specific to the operation and control of the CA, such as safety parameters and audit trails, is kept confidential by the CA and is not disclosed outside the CA organization unless required by law.
- Information about subscribers held by the CA or related third parties, excluding information published in certificates, CRLs, Certificate Policies, or this CPS, is considered confidential and will not be disclosed outside of the CA unless required by the Certification Policy or law.
- Other circumstances of disclosure of information.
- Publication of information concerning the revocation.
- Any other information relating to the subscriber or SECURITY DATA, which may be confidential in nature.

### 10.3.2. Non-Confidential Information.

The following information will be considered non-confidential:

- That contained in this CPS.
- That contained in the different Certification Policies (PC).
- The information contained in the certificates, since the subscriber previously gives his consent for their issuance, including the different statuses or situations of the certificate.
- Certificate revocation lists (CRLs), as well as other revocation status information.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	81

- The information contained in the certificate deposits.
- All information expressly classified as "PUBLIC".
- Any information whose publicity is required by law.

### **10.3.3. Responsibility for the Protection of Confidential Information.**

It is the responsibility of Security Data Seguridad en Datos y Firma Digital to establish adequate measures for the protection of confidential information.

Security Data's employees, agents, and contractors are contractually obligated to protect confidential information.

Certificate subscribers are responsible for protecting their own private key and all activation information (i.e., passwords or PINs) required to access or use the private key.

## **10.4. PRIVACY OF PERSONAL INFORMATION.**

### **10.4.1. Privacy Policy.**

Security Data's privacy policy is the provisions of the right to habeas data: "Private information will be that which, because it deals with personal information or not, and because it is in a private sphere, can only be obtained or offered by order of a judicial authority in the fulfillment of its functions."

Security Data processes personal data in accordance with the Organic Law on the Protection of Personal Data (LOPDP). The processing is based on the explicit consent of the owner and compliance with the legal obligations arising from the provision of certification services.

### **10.4.2. Information treated as Private.**

Personal information about an individual that is not publicly available in the contents of a certificate or CRL is considered private.

### **10.4.3. Information Not Classified as Private.**

The contents of the certificate and the status information of the certificate are not considered private.

### **10.4.4. Responsibility for the Protection of Personal Data.**

SECURITY DATA is responsible for and has the appropriate security and control mechanisms to ensure the protection, confidentiality and proper use of the information provided by the owner.

### **10.4.5. Notice and Consent to Use Personal Data.**

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	82

Personal data may not be communicated to third parties without the due notification and consent of its owner.

#### **10.4.6. Disclosure in the framework of an administrative or judicial process.**

SECURITY DATA may disclose private information without notice to requestors or subscribers when such disclosure is required by law or regulation.

The disclosure of personal data to judicial or administrative authorities shall be carried out after verification of the competence of the requesting authority and in compliance with the principle of proportionality.

#### **10.4.7. Other circumstances of disclosure of information.**

Not stipulated

### **10.5. INTELLECTUAL PROPERTY RIGHTS.**

SECURITY DATA, has intellectual property rights over all its regulatory documents, plans, processes, patents, trademarks, commercial material and certificates that it issues unless explicitly agreed otherwise, and may not be modified or attributed to another entity in an unauthorized manner.

### **10.6. REPRESENTATIONS AND WARRANTIES.**

#### **10.6.1. CA Representations and Warranties.**

It is guaranteed, under its full responsibility, that it complies with all the requirements established in the Certification Policy, Statement of Certification Practices, being responsible for compliance with the procedures described, in accordance with the indications contained in this document.

Security Data provides Digital Certification services in accordance with this Certification Practices Statement, PC and applicable standards. In addition to:

- Issue Certificates in accordance with this CPS and the provisions of the PC and the applicable standards.
- Issue Certificates whose minimum content is defined in the CPS and CP in force.
- Issue Certificates according to the information in their possession and free of data entry errors.
- To keep your own private keys under your sole control by using reliable systems and products to store them in a way that ensures their confidentiality and makes them inaccessible to unauthorized persons, preventing their loss or disclosure.
- Issue the requested Certificates in accordance with the provisions of the CPS, in the PC and, where appropriate, in the corresponding certification service provision contracts.

 <p><b>SECURITY DATA</b> TU IDENTIDAD DIGITAL, EN UNA FIRMA.</p>	<p><b>CERTIFICATION PRACTICES STATEMENT</b></p>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	83

- Facilitate access to the current versions of the CPS and the PCs of each type of Certificates.
- To offer and maintain the necessary infrastructure for the certification services, as well as the physical, procedural and personal security controls necessary for the practice of the certification activity.
- Likewise, it issues the electronic certificates according to the information in its possession and free of data entry errors, delivering the services with the reliability and accuracy established in the respective contracts and in this document.
- Use reliable systems and products that are protected against alteration and that guarantee the technical security, and where appropriate, cryptography of the certification processes to which they support.
- Publish the certificates issued in accordance with the provisions of the Ecuadorian Technical Standard and the Law on Electronic Commerce, Electronic Signatures and Data Messages.
- Protect personal data as established in the Law on Electronic Commerce, Electronic Signatures and Data Messages, and the Organic Law on the Protection of Personal Data.
- Use reliable systems to store recognised certificates to verify their authenticity and prevent unauthorised persons from altering data.
- Provide the minimum information necessary for the use of the certificates to the applicant, whose information must be transmitted free of charge, in writing or electronically.
- Take measures against certificate forgery and ensure the confidentiality of signature creation data during the generation process, as well as its delivery by a secure procedure to the subscriber.
- Do not copy or store subscriber signature creation data.
- Inform Subscribers and related Third Parties about the modifications to the Certificate Policies and the Certification Practices Statement.
- Comply with the obligations of this CPS.
- All those obligations imposed by this CPS and, where applicable, in the Law on Electronic Commerce, Electronic Signatures and Data Messages and Ecuadorian Technical Standard.
- To approve or deny requests for the issuance of digital certificates of electronic signature, in accordance with the provisions of this CPS and in the PCs.
- Make the list of revoked certificates (CRLs) available to users.
- Safeguard, by any secure means, all the information and documentation relating to a recognised certificate and the declarations of certification practices in force at any given time, at least for the entire duration of the accreditation, so that the signatures made with it can be verified. For these purposes, SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL stores in digital or paper format all published versions of the CPS and a copy of the service provision contract between the Information Certification authority and the subscriber.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	84

- Immediately communicate to the holders of the certificates issued by the ECI, the compromise of their private key, loss, disclosure, modification, unauthorized use, in order to revoke them.
- Carry out the identification and authentication of users as steps prior to the revocation of electronic signature certificates.
- Protect the personal data of applicants and users of digital or electronic certificates.
- Carry out each of the steps described in the procedure for issuing electronic signature certificates.
- Implement and maintain the security requirements imposed on the private key of the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, according to this CPS and PCs.
- To offer and maintain the technological infrastructure necessary for the establishment of a structure, both in hardware and software, to operate in accordance with international standards.
- Keep all the information and documentation related to each Certificate, in the proper security conditions, throughout the validity of the accreditation counted from the moment of the issuance of the root certificate, so that the signatures made with it can be verified.
- Submit the updated list of related third parties that are part of the Security Data certification entity approved by ARCOTEL, which can be consulted at the following link: [https://www.securitydata.net.ec/wp-content/downloads/terceros\\_vinculados.pdf](https://www.securitydata.net.ec/wp-content/downloads/terceros_vinculados.pdf)

### 10.6.2. RA Representations and Warranties.

The responsibilities of the registry entity are as follows:

- Verify the identity of certificate applicants, as well as the veracity of the information and documents provided.
- Respect the provisions of the CPS and PC.
- Provide the minimum information necessary for the use of the certificates to the applicant, whose information must be transmitted free of charge, in writing or electronically.
- Take measures against certificate forgery and ensure the confidentiality of signature creation data during the generation process, as well as its delivery by a secure procedure to the subscriber.
- Do not copy or store subscriber signature creation data.
- Protect the personal data of applicants and users of digital or electronic certificates.

The Linked Third Party may assume the following obligations for which it will be responsible:

- Correctly identify and authenticate the Subscriber and/or Applicant and/or the organization they represent, in accordance with the procedures established in this CPS and in the specific Certification Practices for each type of Certificate, using any of the means admitted by law.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	85

- Formalise the contracts for the issuance of the certificates with the Subscriber under the terms and conditions established by the CA.
- Store securely and for a period of no less than 15 years the documentation provided in the process of issuing the Certificate and in the process of suspending/revoking it, under the terms and conditions established in this CPS, in the PC of each type of certificate and, where applicable, in the agreement for the Related Third Party.
- Carry out any other function that corresponds to them, through the personnel that is necessary in each case, as established in this CPS and in the PC of each type of certificate and, where applicable, the Agreement for the Related Third Party.
- In any case, the Linked Third Party will allow SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL access to the files and the file retention procedures assumed by the Linked Third Party and will give it the right to investigate any suspected violation of the CPS and/or the PCs by the Linked Party or any holder of a Certificate. The Linked Third Party and the holders of any Certificate shall inform the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL immediately of any suspected infringement.

#### **10.6.3. Applicants' Representations and Warranties.**

- Pay the corresponding registration fees by virtue of the services requested.
- Provide the Related Third Party or the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL with the information necessary to carry out a correct identification.
- Confirm the accuracy and veracity of the information provided.
- Notify any change in the data provided for the creation of the certificate during its validity period.
- Request the certificate as stipulated in the terms and conditions established on the PC of each type of Certificates and, where applicable, in the Contract for the provision of certificate services signed with the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL.

#### **10.6.4. Subscriber Representations and Warranties.**

The Subscriber shall be obliged to comply with the provisions of the regulations in force and also to:

- Comply at all times with the rules and regulations issued by Security Data in its CPS and the corresponding Certificate Policy.
- Notify Security Data of any modification or variation of the data provided to obtain the Electronic Signature Certificate.
- Verify, through the List of Revoked Certificates, the status of the Electronic Signature Certificates.
- Protect and preserve the Secure Signature Creation Device.\or in turn access to the certificate in software.
- Request the revocation of the certificate and the issuance of a new one to Security Data, in case of forgetting the protection key of the Electronic Signature Certificate.
- To be responsible for the use of the Electronic Signature Certificate and the consequences arising from its use.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	86

- Comply with the provisions of Article 17 of the Law on Electronic Commerce, Electronic Signatures and Data Messages.
- Respect the provisions of the legal instruments binding on the CA.
- The Subscriber shall be liable for any damages caused by the breach of its respective obligations listed in this CPS.

#### **10.6.5. Representations and Warranties of the Relying Party.**

The responsibilities of trusted third parties are as follows:

- The trusting third party is responsible for verifying the status and validity of digital certificates at the time of making any transaction.
- The relying third party must be aware of and comply with the obligations set out in the CPD and CP of the Certification Authority.
- The relying third party undertakes to use the certificates within the terms established within the framework of the laws and regulations in force.
- The relying third party should review the Lists of Revoked Certificates.

#### **10.6.6. User Representations and Warranties.**

- Users who intend to trust and use the Certificates issued by the CA must verify the validity of the signatures issued by the Subscribers.
- In the event that Users do not proceed to verify the signatures through the CRL (List of Revoked Certificates), the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL is not responsible for the use and trust that Users make of these Certificates.
- Any person shall have the right to rely on an electronic signature issued through a certificate from the Certification Authority ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, to the extent that it is reasonable to do so.
- To determine whether reliance is reasonable; The following must be taken into account, where appropriate:
  - The nature of the corresponding transaction that the firm intends to guarantee. It shall not be considered reasonable to rely on a signature issued by an ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL certificate if such operation may be considered improper use.
  - If the relying party has taken the appropriate measures to determine the reliability of the signature, and in particular, if it has verified that the certificate has not expired, been suspended, or revoked. The expiration date shall appear in the certificate itself. Any possible suspension or revocation of the certificate must be checked in the Certificate Revocation List (CRL).
  - If the relying party knew or should have known that the signature was compromised or that the certificate had been revoked or suspended.
- The policies and procedures that govern the activity of the SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL in relation to the different Electronic Signatures made with the types of certificates issued by the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA

 <b>SECURITY DATA</b> TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	87

DIGITAL, policies and procedures that are specified in this CPS and in the PCs for each different type of certificate.

## **Responsibilities.**

### **a) CA Liability**

- Ensure compliance with the responsibilities and obligations described in this CPS; and the provisions of the Law on Electronic Commerce, Electronic Signatures and Data Messages, and its Regulations.
- The ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, solely and exclusively, will be liable for damages caused to any person, when they fail to comply with their legal obligations derived from the legislation in force in the Republic of Ecuador or when they act negligently in the provision of certification services.
- The ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL shall not be liable for damages arising from or related to the non-execution or defective execution of the obligations of the Applicant, Subscriber and/or User.
- The ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL shall not be liable for the negligent or fraudulent use of certificates and keys.
- The ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL will not be liable for damages arising from negligent or willful actions by third parties in relation to the certificates issued by it in favor of a specific subscriber.
- The ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL will not be responsible for any inaccuracies in the Certificate resulting from the information provided by the Subscriber, provided that it has always acted with the maximum negligence required.
- The ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL will not be responsible for any damages arising from those operations in which the limitations of use indicated on the PCs corresponding to each type of certificate have been breached.
- The ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL shall not assume any liability for the non-performance or delay in the performance of any of the obligations under this CPS if such failure to perform or delay results from or is the result of a force majeure event, fortuitous event or, in general, any circumstances over which the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL cannot have reasonable control.
- The ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL will not be responsible for the content of those digitally signed electronic documents. Neither the SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL nor its registration authorities shall be liable in any case for any damage caused by the use of its public certification services in these environments.
- The ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL has the appropriate guarantee policy, which is renewed every year and is delivered to the regulatory entity in accordance with the regulations and requirements of ARCOTEL.
- The Conditions General of the SE Policy You can consult the following link <http://www.securitydata.net.ec/ayuda-security-data-ecuador/> in the Regulations section, item 17. "Guarantee" where the updated information of the policy will be found.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	88

**b) Liability of the Related Third Party.**

- The Related Third Party will be responsible for the functions that correspond to it in accordance with this CPS and, in particular, will assume full responsibility for the correct identification and validation of the Applicant/Subscriber, with the same limitations as established in the previous section in relation to the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL.
- The Related Third Party will be liable to the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL for any damages that may arise from the execution of these functions arranged negligently or in a manner different from that contemplated in this CPS and the PCs issued for each type of certificate.
- However, the Related Third Party is not responsible, in any case, for the identity or identification of the applicant and/or subscriber in the event of falsification of the documentation or other data provided, by it or by the third party that impersonates it.

**c) Subscriber's Responsibility.**

- The Subscriber shall be liable for any damages caused by the breach of its respective obligations listed in this CPS.
- The Subscriber will be responsible for complying with all those obligations imposed by this CPS, the PCs of each type of Certificate, and by the regulations in force regarding the provision of certification services.
- The Subscriber undertakes to indemnify the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL for any damages that may be caused by any culpable or intentional act or omission on its part, also assuming the procedural costs that the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL may incur for this reason, including the professional fees of Lawyers and Solicitors.
- The Subscriber shall indemnify and hold harmless the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL for any damage that it may suffer due to the total, partial or defective fulfilment of the obligations assumed and on the basis of any claim directed against it by any third party with which the subscriber has contracted.

**d) User's Responsibility.**

- The User shall be liable for damages caused by the breach of their respective obligations listed in this CPS.
- The User will be responsible for complying with all those obligations imposed by this CPS, the PCs of each type of Certificate, and by the regulations in force regarding the provision of certification services.
- In any case, the User will assume all the responsibility and risks arising from the acceptance of a Certificate without having complied with the obligations set out in the CPS and, where appropriate, in the specific PCs of each certificate, guaranteeing the full indemnity of the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL for this concept.

 <b>SECURITY DATA</b> <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	89

### **10.7. DISCLAIMERS OF WARRANTIES.**

SECURITY DATA hereby disclaims all warranties, including the warranty of merchantability and/or fitness for a particular purpose other than to the extent prohibited by law or expressly stipulated in this CPS and its corresponding PC.

### **10.8. LIMITATIONS OF LIABILITY.**

To the extent that the SECURITY DATA AC has issued and managed the electronic signature certificate in accordance with the CPS and its corresponding PC, it shall have no liability to the Subscriber, the relying third party or any Third Party for any loss or damage suffered as a result of the use of or reliance on such certificate.

SECURITY DATA shall be liable to certificate holders or relying third parties for direct losses arising from any breach of this CPS and its corresponding PC, or for any other liability they may incur in contract, tort or otherwise, including liability for negligence by subscriber or trusted third party or third party by certificate, provided that the subscriber, trusted third party or third party is in full compliance with this CPS and its PC.

SECURITY DATA's liability to any person for damages arising under, out of, or in connection with this CPS and your PC, Subscriber Agreement, applicable contract, or any other related agreement, whether in contract, warranty, tort, or otherwise, shall be limited to the actual damages suffered by that person. SECURITY DATA shall not be liable for any indirect, consequential, incidental, special, exemplary, or punitive damages with respect to any person, regardless of how such damages or liability may arise, whether in tort, negligence, equity, contract, statute, common law, or otherwise.

### **10.9. COMPENSATION.**

The cases of compensation are defined in the contracts of the holders.

### **10.10. TERM AND TERMINATION.**

#### **10.10.1. Term.**

This Statement of Certification Practices document and any amendments to it will become effective upon publication on the SECURITY DATA website and will remain in force until it is replaced by a newer version.

#### **10.10.2. Termination.**

This Certification Practices Statement document, and any amendments, will remain in effect until modified or replaced by a newer version.

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	90

### **10.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS.**

In general, the SECURITY DATA website will be used to make any type of notification and communication. In the event of security problems or loss of integrity that may affect a natural or legal person, SECURITY DATA will notify them of this incident. It may also notify the affected owners and the Data Protection Authority directly and expeditiously, in accordance with the established legal deadlines.

### **10.12. AMENDMENTS.**

Amendments and changes will be communicated to ARCOTEL, and after their approval they will be published on the website and notified to the holders and subscribers, in accordance with the means specified in their contracts.

### **10.13. DISPUTE RESOLUTION PROVISIONS.**

The dispute resolution procedure will be defined in the contracts of the holders. Any differences that may arise between the parties during the execution of this Service or due to its interpretation will be resolved in the first instance directly between the User and SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A.

If there is no such agreement, they may submit the dispute to the mediation process as a constitutionally recognized alternative dispute resolution system, for which the parties stipulate to go to the Mediation Center of the Attorney General's Office.

The mediation process will be subject to the Arbitration and Mediation Law and the Operating Regulations of the Mediation Center of the Attorney General's Office.

If a full agreement is signed, it will have the effect of an enforceable judgment and res judicata and its execution will be in the same way as the judgments of last instance following the enforcement procedure, as provided for in Article 47 of the Arbitration and Mediation Law.

In the event that there is no agreement between the parties, they shall sign the respective act of impossibility of agreement, and the dispute shall be settled before the competent District Court of Administrative Litigation.

In the event that partial agreement minutes are signed, they will have the effect of res judicata on the agreed matters; and in the case of aspects on which no agreement is reached, these shall be resolved before the competent District Court of Administrative Litigation.

### **10.14. GOVERNING LAW.**

Law on Electronic Commerce, Electronic Signatures and Data Messages, its Regulations; Organic Law on the Protection of Personal Data (LOPD) and its Regulations; Organic Code of the Social Economy of Knowledge in relation to intellectual property. Organic Law on Consumer Protection, Organic Law on Transparency of Information and Accreditation of ARCOTEL,

	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	91

Technical Standard for the Provision of Certification Services and Related Services, issued by the Agency for the Regulation and Control of Telecommunications (ARCOTEL).

#### **10.15. COMPLIANCE WITH APPLICABLE LAW.**

Certificates issued under SECURITY DATA will be used by subscribers and relying third parties only in accordance with the laws and regulations of the jurisdiction in which they are used or based.

#### **10.16. MISCELLANEOUS PROVISIONS.**

##### **10.16.1. Entire Agreement.**

No stipulation.

##### **10.16.2. Assignment.**

Issuing CAs, subscribers, relying third parties, Registration Entities, or any other entity operating under this Statement of Certification Practices, have no right to assign any of their rights or obligations hereunder without the prior written consent of SECURITY DATA.

##### **10.16.3. Severability.**

If any of the provisions of this Certification Practices Statement and on your PC, are held to be invalid by a competent authority in the applicable jurisdiction, the remainder of the Statement of Practices and Certification Policy shall remain valid and enforceable.

##### **10.16.4. Execution.**

No stipulation.

##### **10.16.5. Force Majeure.**

Security Data accepts no liability for any delay or failure to perform an obligation under its Statement of Practices and Certification Policy, to the extent that such delay or failure is caused by events beyond its reasonable control.

#### **10.17. OTHER PROVISIONS.**

No stipulation.

 <b>SECURITY DATA</b> <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	<b>CERTIFICATION PRACTICES STATEMENT</b>	<b>CODE</b>	SD-ID-PE-09
		<b>VERSION</b>	V12
		<b>APPROVAL DATE</b>	03/4/2026
		<b>PAGES</b>	92

### 11. Control of Approvals.

<b>PREPARED BY</b>	COORDINATOR OF THE MANAGEMENT SYSTEM	
<b>REVIEWED BY</b>	CHIEF TECHNOLOGY OFFICER (CTO)	
	LEGAL SUPERVISOR	
<b>APPROVED BY</b>	GENERAL MANAGER	