



COMPANY MEMBER
CERTIFICATION
POLICIES

marzo 4
2026



 www.securitydata.net.ec

 info@securitydata.net.ec

 392 2169 /  098 644 2122

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	2

VERSION HISTORY

VERSION	DESCRIPTION	DATE	PREPARED BY	REVIEWED BY	APPROVED BY
V1	Initial Edition	24/01/2011	Legal Coordinator	Technical Manager	General Manager
V2	-	31/03/2011	Legal Coordinator	Technical Manager	General Manager
V3	-	27/06/2011	Legal Coordinator	Technical Manager	General Manager
V4	-	01/09/2011	Legal Coordinator	Technical Manager	General Manager
V5	-	26/09/2011	Legal Coordinator	Technical Manager	General Manager
V6	-	15/12/2011	Legal Coordinator	Technical Manager	General Manager
V7	-	25/02/2015	Legal Coordinator	Technical Manager	General Manager
V8	-	25/06/2019	Legal Coordinator	Technical Manager	General Manager
V9	-	23/08/2022	Legal Coordinator	Technical Manager	General Manager
V10	* General update of the CPS in accordance with the Technical Regulations. * Adaptation of the document to the RFC 3647 standard.	25/02/2026	Management System Coordinator	Chief Technology Officer (CTO) Supervisor Legal	General Manager

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	3

Contents

1.	Introduction.	12
1.1.	GENERAL DESCRIPTION.	12
1.2.	NAME AND IDENTIFICATION OF THE DOCUMENT.	12
1.3.	PKI PARTICIPANTS.	12
1.3.1.	Accredited Entity (EA).	12
1.3.2.	Certificate Authority (CA).	13
1.3.3.	Root Certification Authority.	13
1.3.4.	Registration Authority (AR).	13
1.3.5.	Related Third Party.	13
1.3.6.	Applicant.	14
1.3.7.	Subscriber.	14
1.3.8.	Signatory.	14
1.3.9.	Custodian of the keys.	15
1.3.10.	Third, who trusts the certificates.	15
1.4.	USE OF THE CERTIFICATE.	15
1.4.1.	Appropriate Uses of the Certificate.	15
1.4.2.	Prohibited Uses of the Certificate.	16
1.5.	POLICY MANAGEMENT.	16
1.5.1.	Organization that administers the document.	16
1.5.2.	Contact person.	16
1.5.3.	Person who determines the adequacy of the Certification Policies.	17
1.5.4.	Procedures for approving Certification Policies.	17
1.6.	DEFINITIONS AND ACRONYMS.	17
1.6.1.	Definitions.	17
1.6.2.	Acronyms.	18
2.	Publishing and Repository Responsibilities.	19
2.1.	REPOSITORIES.	19
2.2.	PUBLICATION OF CERTIFICATION INFORMATION.	20
2.3.	TIME OR FREQUENCY OF PUBLICATION.	20
2.4.	ACCESS CONTROLS TO REPOSITORIES.	20
3.	Identification and Authentication.	21
3.1.	NAME.	21
3.1.1.	Types of names.	21

CODE	SD-ID-PE-1 7
VERSION	V10
APPROVAL DATE	03/04/2026
PAGES	4

3.1.2.	Need for names to have meaning.	21
3.1.3.	Anonymity or pseudonym of subscribers.....	21
3.1.4.	Rules for the interpretation of the different forms of names.	21
3.1.5.	Uniqueness of names.	22
3.1.6.	Recognition, authentication and function of trademarks.	22
3.2.	INITIAL IDENTITY VALIDATION.....	22
3.2.1.	Method to prove possession of the private key.....	22
3.2.2.	Authentication of the organization's identity.....	23
3.2.3.	Authentication of individual identity.....	23
3.2.4.	Unverified subscriber information.	23
3.2.5.	Authority validation.	23
3.2.6.	Interoperability criteria.	24
3.3.	IDENTIFICATION AND AUTHENTICATION FOR KEY RENEWAL REQUESTS.....	24
3.3.1.	Identification and authentication for routine key renewal.	24
3.3.2.	Identification and authentication for key renewal after revocation.	24
3.4.	IDENTIFICATION AND AUTHENTICATION FOR THE REVOCATION REQUEST.....	24
4.	Operational requirements of the certificate life cycle.....	25
4.1.	APPLICATION FOR THE CERTIFICATE.	25
4.1.1.	Who can submit a certificate application.....	25
4.1.2.	Enrollment Process and Responsibilities.....	25
4.2.	PROCESSING OF THE CERTIFICATE APPLICATION.....	26
4.2.1.	Performing identification and authentication functions.....	26
4.2.2.	Approval or rejection of certificate requests.	26
4.2.3.	Processing time for certificate applications.	27
4.3.	ISSUANCE OF THE CERTIFICATE.....	28
4.3.1.	Actions of the CA during the issuance of the certificate.	28
4.3.2.	Notification to the subscriber by the CA of the issuance of the certificate.....	28
4.4.	ACCEPTANCE OF THE CERTIFICATE.....	29
4.4.1.	Conduct that constitutes acceptance of the certificate.	29
4.4.2.	Publication of the certificate by the CA.....	29
4.4.3.	Notification of the issuance of certificates by the CA to other entities.....	29
4.5.	USE OF KEY PAIRS AND CERTIFICATES.....	29
4.5.1.	Use of the subscriber's private key and certificate.....	29
4.5.2.	Use of the trusting party's public key and certificate.	30

CODE	SD-ID-PE-1 7
VERSION	V10
APPROVAL DATE	03/04/2026
PAGES	5

4.6.	RENEWAL OF THE CERTIFICATE.	30
4.6.1.	Circumstance for the renewal of the certificate.	30
4.6.2.	Who can apply for renewal.	31
4.6.3.	Processing of applications for renewal of certificates.	31
4.6.4.	Notification of the issuance of a new certificate to the subscriber.	31
4.6.5.	Conduct that constitutes acceptance of a renewal certificate.	31
4.6.6.	Publication of the renewal certificate by the CA.	32
4.6.7.	Notification of the issuance of certificates by the CA to other entities.	32
4.7.	CHANGE OF CERTIFICATE KEY.	32
4.7.1.	Circumstances for the renewal of the certificate key.	32
4.7.2.	Who can request certification of a new public key.	32
4.7.3.	Processing certificate key renewal requests.	32
4.7.4.	Notification of the issuance of a new certificate to the subscriber.	33
4.7.5.	Conduct that constitutes acceptance of a certificate with a new key.	33
4.7.6.	Publication of the certificate with a new key by the CA.	33
4.7.7.	Notification of the issuance of certificates by the CA to other entities.	33
4.8.	MODIFICATION OF THE CERTIFICATE.	33
4.8.1.	Circumstances for the modification of the certificate.	34
4.8.2.	Who can request the modification of the certificate.	34
4.8.3.	Processing of certificate modification requests.	34
4.8.4.	Notification of the issuance of a new certificate to the subscriber.	34
4.8.5.	Conduct that constitutes acceptance of the modified certificate.	34
4.8.6.	Publication of the certificate modified by the CA.	34
4.8.7.	Notification of the issuance of certificates by the CA to other entities.	35
4.9.	REVOCATION AND SUSPENSION OF THE CERTIFICATE.	35
4.9.1.	Circumstances of Revocation.	35
4.9.2.	Who can request the revocation.	36
4.9.3.	Procedure for the request for revocation.	36
4.9.4.	Grace period for the request for revocation.	38
4.9.5.	Period within which the CA must process the request for revocation.	38
4.9.6.	Revocation check requirement for relying parties.	39
4.9.7.	CRL emission frequency.	39
4.9.8.	Maximum latency for CRL.	39
4.9.9.	Online health check/revocation availability.	39

CODE	SD-ID-PE-1 7
VERSION	V10
APPROVAL DATE	03/04/2026
PAGES	6

4.9.10.	Online revocation check requirements.	39
4.9.11.	Other forms of revocation notices available.	39
4.9.12.	Special key compromise requirements.	39
4.9.13.	Circumstances of suspension.	40
4.9.14.	Who can request the suspension.	40
4.9.15.	Procedure for requesting suspension.	40
4.9.16.	Limits on the suspension period.	40
4.10.	CERTIFICATE STATUS SERVICES.	41
4.10.1.	Operational characteristics.	41
4.10.2.	Service Availability.	41
4.10.3.	Optional features.	41
4.11.	END OF SUBSCRIPTION.....	41
4.12.	CUSTODY AND RECOVERY OF PASSWORDS.	42
4.12.1.	Key Deposit and Recovery Policy and Practices.	42
4.12.2.	Session key encapsulation and retrieval policy and practices.	42
5.	Facilities, Management and Operation Controls.....	42
5.1.	PHYSICAL CONTROLS.....	42
5.1.1.	Site location and construction.....	42
5.1.2.	Physical Access.....	42
5.1.3.	Energy and Air Conditioning.....	42
5.1.4.	Water Exposure.....	42
5.1.5.	Fire Protection and Prevention.	42
5.1.6.	Storage System.....	43
5.1.7.	Elimination of Information Carriers.....	43
5.1.8.	External Backup.....	43
5.2.	PROCEDURAL CONTROLS.	43
5.2.1.	Roles of Trust.	43
5.2.2.	Number of people needed per task.	43
5.2.3.	Identification and authentication for each role.....	43
5.2.4.	Roles that require separation of duties.....	43
5.3.	PERSONNEL CONTROLS.....	43
5.3.1.	Requirements on Qualification, Experience and Professional Knowledge.	43
5.3.2.	Background Check Procedure.	43
5.3.3.	Training Requirements.....	43

CODE	SD-ID-PE-1 7
VERSION	V10
APPROVAL DATE	03/04/2026
PAGES	7

5.3.4.	Requirements and Frequency of Training Updates.	44
5.3.5.	Frequency and Sequence of Task Rotation.	44
5.3.6.	Penalties for Unauthorized Actions.	44
5.3.7.	Personnel Hiring Requirements.	44
5.3.8.	Documentation Provided to Staff.	44
5.4.	AUDIT TRAIL PROCEDURES.	44
5.4.1.	Types of Events Recorded.	44
5.4.2.	Frequency of Audit Log Processing.	44
5.4.3.	Audit Log Retention Period.	44
5.4.4.	Protection of Records.	44
5.4.5.	Procedures for Supporting Audit Trails.	45
5.4.6.	Audit Information Collection System.	45
5.4.7.	Event Notification.	45
5.4.8.	Vulnerability Analysis.	45
5.5.	LOG FILE.	45
5.5.1.	Type of Archived Events.	45
5.5.2.	Record Retention Period.	45
5.5.3.	Protection of the Archive.	45
5.5.4.	File Backup Procedures.	45
5.5.5.	Requirements for the Time Stamping of Records.	45
5.5.6.	Audit Information Filing System.	45
5.5.7.	Procedures for obtaining and verifying information on file.	45
5.6.	CHANGE OF KEY OF THE CA.	46
5.7.	DISASTER ENGAGEMENT AND RECOVERY.	46
5.7.1.	Incident and Vulnerability Management Procedures.	46
5.7.2.	Alteration of Hardware, Software and/or Data Resources.	46
5.7.3.	Procedure for Action in the Face of the Vulnerability of the Private Key of the CA.	46
5.7.4.	Business Continuity after a disaster.	46
5.8.	TERMINATION OF CA OR RA.	46
6.	Technical Security Controls.	46
6.1.	KEY PAIR GENERATION AND INSTALLATION.	46
6.1.1.	Key Pair Generation.	46
6.1.2.	Delivery of Private Key to the Subscriber.	46
6.1.3.	Delivery of Public Key to the issuer of the Certificate.	46

CODE	SD-ID-PE-1 7
VERSION	V10
APPROVAL DATE	03/04/2026
PAGES	8

6.1.4.	Delivery of CA Public Key to Trusted Parties.	46
6.1.5.	Key Sizes.	47
6.1.6.	Generation of Public Key Parameters and quality control.	47
6.1.7.	Purposes of Use of the Key.	47
6.2.	PROTECTION OF PRIVATE KEYS AND ENGINEERING OF CRYPTOGRAPHIC MODULES.	47
6.2.1.	Standards for Cryptographic Modules.	47
6.2.2.	Multi-person control (k of n) of the Private Key.	47
6.2.3.	Custody of the Private Key.	47
6.2.4.	Backup of the Private Key of the CA.	47
6.2.5.	Subscriber's Private Key File.	47
6.2.6.	Transfer of the Private Key to/or from the Cryptographic Module.	48
6.2.7.	Private key storage in the cryptographic module.	48
6.2.8.	Private Key Activation Method.	48
6.2.9.	Private Key Deactivation Method.	48
6.2.10.	Private Key Destruction Method.	48
6.2.11.	Classification of the cryptographic module.	48
6.3.	OTHER ASPECTS OF KEY PAIR MANAGEMENT.	48
6.3.1.	Public Key File.	48
6.3.2.	Certificate Operating Periods and Key Pair Usage Period.	49
6.4.	ACTIVATION DATA.	49
6.4.1.	Generation and Installation of Activation Data.	49
6.4.2.	Protection of Activation Data.	49
6.4.3.	Other aspects of activation data.	49
6.5.	COMPUTER SECURITY CONTROLS.	49
6.5.1.	Specific Technical Safety Requirements.	50
6.5.2.	Computer Security Classification.	50
6.6.	TECHNICAL CONTROLS OF THE LIFE CYCLE.	50
6.6.1.	Systems Development Controls.	50
6.6.2.	Security Management Controls.	50
6.6.3.	Lifecycle Security Controls.	50
6.7.	NETWORK SECURITY CONTROLS.	50
6.8.	TIME STAMPING.	50
7.	Certificate, CRL and OCSP profiles.	50

CODE	SD-ID-PE-1 7
VERSION	V10
APPROVAL DATE	03/04/2026
PAGES	9

7.1.	CERTIFICATE PROFILE.	50
7.1.1.	Version Number.	56
7.1.2.	Certificate Extensions.	56
7.1.3.	Algorithm Object Identifiers.	56
7.1.4.	Forms of names.	56
7.1.5.	Name Restrictions.	56
7.1.6.	Certificate Policy object identifier.	56
7.1.7.	Use of the Policy Restrictions extension.	57
7.1.8.	Syntax and Semantics of the Qualifiers of Politics.	57
7.1.9.	Processing Semantics for Critical Certificate Policy Extension.	57
7.2.	CRL PROFILE.	57
7.2.1.	Version Number.	57
7.2.2.	CRLs and CRL input extensions.	58
7.2.3.	OCSP PROFILE.	58
7.2.4.	Version Number.	58
7.2.5.	OCSP extensions.	58
7.3.	CRL PROFILE.	59
7.4.	OCSP PROFILE.	59
8.	Compliance Audits and Other Controls.	59
8.1.	FREQUENCY OR CIRCUMSTANCES OF THE EVALUATION.	59
8.2.	QUALIFICATIONS OF THE EVALUATOR.	60
8.3.	RELATIONSHIP BETWEEN THE AUDITOR AND THE AUDITED AUTHORITY.	60
8.4.	ASPECTS COVERED BY THE CONTROLS.	60
8.5.	ACTIONS TO BE TAKEN AS A RESULT OF THE DETECTION OF INCIDENTS.	60
8.6.	COMMUNICATION OF RESULTS.	60
9.	Other Legal and Activity Issues.	61
9.1.	RATES.	61
9.1.1.	Certificate Issuance or Renewal Fees.	61
9.1.2.	Certificate Access Fees.	61
9.1.3.	Status Information Access or Revocation Fees.	61
9.1.4.	Fees for Other Services.	61
9.1.5.	Refunds.	61
9.2.	FINANCIAL RESPONSIBILITY.	62
9.2.1.	Insurance Coverage.	62

CODE	SD-ID-PE-1 7
VERSION	V10
APPROVAL DATE	03/04/2026
PAGES	10

9.2.2.	Other Assets.....	62
9.2.3.	Insurance or Guarantee of Coverage for Final Entities.....	62
9.3.	CONFIDENTIALITY OF INFORMATION.....	62
9.3.1.	Scope of Confidential Information.	62
9.3.2.	Non-Confidential Information.	62
9.3.3.	Responsibility for the Protection of Confidential Information.	63
9.4.	PRIVACY OF PERSONAL INFORMATION.....	63
9.4.1.	Privacy Policy.....	63
9.4.2.	Information treated as Private.	63
9.4.3.	Information Not Classified as Private.	63
9.4.4.	Responsibility for the Protection of Personal Data.	63
9.4.5.	Notice and Consent to Use Personal Data.....	64
9.4.6.	Disclosure in the framework of an administrative or judicial process.....	64
9.4.7.	Other circumstances of disclosure of information.	64
9.5.	INTELLECTUAL PROPERTY RIGHTS.	64
9.6.	REPRESENTATIONS AND WARRANTIES.	64
9.6.1.	CA Representations and Warranties.	64
9.6.2.	RA Representations and Warranties.	64
9.6.3.	Subscriber Representations and Warranties.....	64
9.6.4.	Representations and Warranties of the Relying Party.	64
9.6.5.	Representations and Warranties of Other Participants.	65
9.7.	DISCLAIMERS OF WARRANTIES.	65
9.8.	LIMITATIONS OF LIABILITY.	65
9.9.	COMPENSATION.....	65
9.10.	TERM AND TERMINATION.....	65
9.10.1.	Term.....	65
9.10.2.	Termination.....	65
9.11.	INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS.	66
9.12.	AMENDMENTS.	66
9.13.	DISPUTE RESOLUTION PROVISIONS.	66
9.14.	GOVERNING LAW.....	66
9.15.	COMPLIANCE WITH APPLICABLE LAW.....	66
9.16.	MISCELLANEOUS PROVISIONS.	66

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-17
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	11

9.16.1.	Entire Agreement.....	66
9.16.2.	Assignment.....	66
9.16.3.	Severability.....	67
9.16.4.	Execution.....	67
9.16.5.	Force Majeure.....	67
9.17.	OTHER PROVISIONS.....	67
10.	Control of Approvals.....	67

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	12

1. Introduction.

1.1. GENERAL DESCRIPTION.

This document includes the Certification Policy (PC) of the Certification authority of SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. for the certificates of Legal Entity for Company Member.

This PC specifies and contemplates the provisions of the Certification Practices Statement (DPC) of the Certification Entity of SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. establishing a set of rules that indicate the procedures followed by this entity in the provision of its services for the request, identification, acceptance, issuance, revocation of digital certificates as well as the limits of use, the scope and technical characteristics of this type of certificate.

This Certification Policy (PC), together with the CPS of the Certification authority of SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A., are aimed at anyone who trusts this type of certificate.

1.2. NAME AND IDENTIFICATION OF THE DOCUMENT.

Name:	Certification Policy (PC)
Version:	10
Description:	Policy for the Certification of Legal Entities for Company Members.
Date of issue:	2 February 4, 2026
Website:	www.securitydata.net.ec
Company Name:	Security Data Seguridad en Datos y Firma Digital S.A.
Email:	info@securitydata.net.ec
Address:	Alonso de Torres and Av. Del Parque administrative offices C8
Phone:	023922169

1.3. PKI PARTICIPANTS.

1.3.1. Accredited Entity (EA).

Security Data Seguridad en Datos y Firma Digital S.A. is an Accredited Entity (EA) that issues certificates recognized according to the Law of Electronic Commerce, Electronic Signatures and Data Messages, Security Data is the entity issuing the certificates and responsible for the operations of the life cycle of the certificates.

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 Data Security and Digital Signature, which will act as intermediaries. Security Data Data Security and Digital Signature also offers electronic signature validation and time-stamping services, governed by its particular policies, not included in this document, it may issue 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

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	13

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.

1.3.2. Certificate Authority (CA).

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

1.3.3. 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.

1.3.4. Registration Authority (AR).

Security Data Data Security and Digital Signature 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.

1.3.5. Related Third Party.

A Related Third Party of Security Data Seguridad en Datos y Firma Digital S.A., is the entity in charge of:

- 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 Related Third Party of Security Data Seguridad en Datos y Firma Digital S.A.:

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	14

- Any trusted entity that enters into an agreement with Security Data Seguridad en Datos y Firma Digital S.A. to act as a third party on behalf of Security Data Seguridad en Datos y Firma Digital S.A.
- Security Data Seguridad en Datos y Firma Digital S.A. itself, directly.

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

The entity acting as a Related Third Party of Security Data Seguridad en Datos y Firma Digital S.A. may authorize one or more persons as Operator of the Related Third Party to operate with the computer system for issuing certificates of Security Data Seguridad en Datos y Firma Digital S.A. on behalf of the Related Third Party.

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 and Firma Digital S.A. must be aware of and expressly authorize the agreement.

1.3.6. 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 Data Data Security and Digital Signature. 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.

1.3.7. Subscriber.

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

1.3.8. 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.

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	15

1.3.9. Custodian of the keys.

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

1.3.10. Third, who trusts the certificates.

A third party that trusts in certificates (in English, relaying party) is understood to be any person or organization that voluntarily trusts a certificate issued by Security Data Data Security and Digital Signature S.A.

The recognized certificates issued by Security Data Seguridad en Datos y Firma Digital S.A. are universal and are accepted by the public bodies of the Ecuadorian state, such as Ministries, Secretariats, etc.

The obligations and responsibilities of Security Data Seguridad en Datos y Firma Digital S.A. with third parties who voluntarily rely on the certificates will be limited to those set out in this DPC.

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

1.4. USE OF THE CERTIFICATE.

1.4.1. Appropriate Uses of the Certificate.

- 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 DPC, in the service provision contract signed with SECURITY DATA DATA SECURITY AND DIGITAL SIGNATURE, and the PC.
- The authorized uses of the Certificates issued by SECURITY DATA DATA SECURITY AND DIGITAL SIGNATURE may be specified in each type of certificate.
- If the subscriber's certificate in the validity period is compromised, i.e. their private key, they must initiate the revocation procedure as mentioned in the Security Data DPC.
- Certificates must be used in accordance with the provisions of the Law on Electronic Commerce, Electronic Signatures and Data Messages for the use of keys and certificates.
- The use of the certificates of Legal Representation before the Public Administration is limited to those that allow the powers of representation.
- The electronic signature certificate issued by SECURITY DATA DATA SECURITY AND DIGITAL SIGNATURE 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.

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	16

- 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.

1.4.2. Prohibited Uses of the Certificate.

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.

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.

1.5. POLICY MANAGEMENT.

1.5.1. 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 PC, CPS and other regulatory documents.

1.5.2. Contact person.

Contact person:	Lenin Alberto Vásquez González
Email:	cto@securitydata.net.ec
Address:	Alonso de Torres and Av. Del Parque administrative offices C8
Phone Number:	023922169
Website:	www.securitydata.net.ec

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	17

1.5.3. Person who determines the adequacy of the Certification Policies.

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.

1.5.4. Procedures for approving Certification Policies.

The Certification Policies will be reviewed and, if appropriate, updated, will be done annually or when any changes are presented.

The Certification Policies of Security Data Seguridad en Datos y Firma Digital S.A. will be approved by the General Manager once it has been reviewed and corroborated that the requirements of the law and compliance are met.

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.

1.6. DEFINITIONS AND ACRONYMS.

1.6.1. Definitions.

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

Recognised Certificate: A certificate issued by an Accredited Entity that meets the requirements established in the Law in terms of verifying the identity and other circumstances of 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.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	18

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.

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.

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.

1.6.2. Acronyms.

AC:	Certificate Authority
AC Sub:	Subordinate Certificate Authority
AR:	Registration Authority
PC:	Certification Policy
CPS:	Certification Practices Statement
CRL:	Certificate Revocation List
HSM:	Hardware Security Module
LDAP:	Light weight Directory Access Protocol
OCSP:	Online Certificate Status Protocol.
PKI:	Public Key Infrastructure
PSC:	Certification Service Provider

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	19

TSA:	Time Stamp Authority
VA:	Validation Authority
ECI:	Information Certification Authority
OID:	Unique Object Identifier
DN:	Distinguished Name
C:	Country
CN:	Common Name (Common Name)
Or:	Organization
OU:	Unity Organizational (Organizational Unit)
SN:	SurName
ISO:	International Organization for Standardization
PKCS:	Public Key Cryptography Standards, PKI Standards
UTF8:	Unicode Transformation Format – 8 bits.

2. Publishing and Repository Responsibilities.

2.1. REPOSITORIES.

The repositories are located on the website of Security Data Seguridad en Datos y Firma Digital S.A., which are referenced at the following URL <https://repositorio.securitydata.net.ec/security1/>.

Certification Practice Statement:

https://www.securitydata.net.ec/wp-content/downloads/Normativas/p_certificacion/certification.pdf

Company Member Certification Policy:

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

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>

Certificate consultation:

<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

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	20

notice.

2.2. PUBLICATION OF CERTIFICATION INFORMATION.

Both the Statement of Certification Practices and the Certification Policies will be available in electronic format on the Security Data Data Data Seguridad en Datos y Firma Digital S.A. website.

The previous versions will be removed from your on-line consultation, but may be requested by interested parties at the contact address of Security Data Seguridad en Datos y Firma Digital S.A.

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 Data Security and Digital Signature is not required to publish certificates issued in a publicly accessible repository. However, in order to improve services to customers, Security Data Data Security and Digital Signature may offer Directory services and search and download of some certificates issued under its certification hierarchy.

2.3. TIME OR 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 Data Security and Digital Signature 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.

2.4. ACCESS CONTROLS TO REPOSITORIES.

Certification Policies, Statement of Certification Practices, General Terms and Conditions of Contract, CA certificates, and revoked certificate lists (CRLs) will be published in publicly accessible repositories without access control.

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

The administration of the repositories will be in charge of Security Data Seguridad en Datos and Firma Digital S.A.

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	21

3. Identification and Authentication.

3.1. NAME.

3.1.1. 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".

3.1.2. Need for names to have meaning.

Security Data shall ensure that the names assigned to the digital certificates, both of the holder (Subject) and the issuer (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.

3.1.3. 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.

3.1.4. Rules for the interpretation of the different forms of names.

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

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	22

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.

3.1.5. 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.

3.1.6. 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.

3.2. INITIAL IDENTITY VALIDATION.

For the validation of the identity of a Legal Entity as a Member of the Company, 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.

3.2.1. Method to prove 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.

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	23

3.2.2. Authentication of the organization's identity.

Organization Certificates are electronic signature certificates issued in favor of a Legal Entity, whose holder may be a company, organization or entity of the Public Administration. These certificates allow the legal entity to be electronically identified as a subscriber and are recognized in accordance with current regulations.

- Corporate Company Member Certificates: These are recognized certificates that identify the subscriber as a legal entity and the signatory as linked to that company as an employee.

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.
- Data relating to their powers within the organisation.

In addition, the company member of the legal entity must present the identity card, passport or other legally recognized means that identifies him.

Security Data Data Security and Digital Signature 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.

3.2.3. Authentication of individual identity.

Not applicable.

3.2.4. 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 entities.

3.2.5. Authority validation.

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

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.

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	24

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

3.2.6. 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.

3.3. IDENTIFICATION AND AUTHENTICATION FOR KEY RENEWAL REQUESTS.

3.3.1. 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, as a new process of acquisition of electronic signature, and the validation will be carried out as a new one.

3.3.2. Identification and authentication for key renewal after revocation.

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.

3.4. IDENTIFICATION AND AUTHENTICATION FOR THE REVOCATION REQUEST.

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

- a) The subscriber, by identifying and authenticating themselves on the Security Data Seguridad en Datos y Firma Digital website through the Account Administration section.
- b) A Registry operator in person.
- c) Any Third Party Authorized by Security Data Seguridad en Datos y Firma Digital: must identify the subscriber in the event of a revocation request using the means it considers necessary.

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	25

4. Operational requirements of the certificate life cycle.

4.1. APPLICATION FOR THE CERTIFICATE.

4.1.1. Who can submit a certificate application.

The application for an electronic signature certificate can be submitted or processed by a natural person as a member of a company.

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

4.1.2. 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 website of the CA, in person, communication channels of the CA 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 identity of the subscriber and the organization.
- 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 CPS.

The Certification Authority shall register the application and proceed to verify the identity of the applicant, the completeness and sufficiency of the information and documentation provided, in accordance with the requirements established for certificates of Legal Entity as a Member of a Company.

For these purposes, 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, in case the services have failed, the registry operator will ask the applicant for their identification document and the Single Taxpayer Registry (RUC) to carry out the identity verification manually. Likewise, all the qualifying requirements for company members will be reviewed. Once the validation process has been completed, the Certification authority will notify the applicant of the approval or rejection of the application, in accordance with the criteria defined in the Certification Practices Statement.

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

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	26

registration process in a secure, reliable manner and in compliance with applicable technical and regulatory standards.

4.2. PROCESSING OF THE CERTIFICATE APPLICATION

4.2.1. Performing identification and authentication functions

It is the responsibility of the CA and the Related 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 Related 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 Related Third Party will carry out the review and validation of the information provided. Once the identity and documents have been validated, the electronic signature certificate will be issued.

The documents that will be verified depending on the type of signature that the subscriber will request will be the following:

Legal Persons (Company Member).

- A process of validation of the identity of the applicant will be carried out as mentioned in the section INITIAL IDENTITY VALIDATION for Ecuadorian citizens, in the case of foreigners the passport will be requested, it will not perform biometric validation, they will be asked for a video that allows them to confirm their identity and will regarding the obtaining or renewal of the certificate, in accordance with the internal procedures established by Security Data.
- The certification authority will validate the RUC before the SRI and store a screenshot of its status, in case the SRI page is not available, the certificate is not granted until the manual validation of the RUC is carried out.
- Legible copy of the appointment or power of attorney granted by the legal representation with its due registration when appropriate or registration of directives as the case may be.
- Copy of the incorporation, bylaws or creation document as applicable of the applicant Company.
- Letter of authorization, appointment, or registration of directives when appropriate as the case may be.

4.2.2. Approval or rejection of certificate requests.

Once the certificate request has been made, the Registry operator or Linked Third Party must

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	27

verify the information provided by the applicant, including the validation of the subscriber's identity. Additionally, if the application is made online, the Applicant must accept the terms 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, in case the services are not available, the registry operator must carry out these verifications manually with the enabling documents issued by the competent entities.

In the case of legal persons, the registration operator and related third party must verify all the documents enabling the position held within the company as a member of the company.

If the information is not correct, the registry operator will deny the request communicating the reason and likewise, the Linked Third Party will deny the request, contacting the requester to inform him or her 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 Data Security and Digital Signature. 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 and the information provided.
- Repeated failure in the life tests (biometrics) without the user accepting the validation by video or in person.

4.2.3. 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 applications in person will be 15 minutes, if you meet all the requirements and conditions indicated in this section.

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	28

4.3. ISSUANCE OF THE CERTIFICATE.

4.3.1. Actions of the CA during the issuance of the certificate.

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.

The following actions will be carried out for the issuance of certificates:

For certificates on hardware support:

- The registry operator or linked third party will deliver the empty DSCF to you, i.e. regardless of the certificate within the device. In the event that the applicant provides their own device, it must be a DSCF previously delivered by Security Data Data Security and Digital Signature. 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 CA 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 CA will provide the procedure for changing the DSCF password or pin.

For certificates in software support:

- The CA 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 CA will send the security PIN to their email for the signature download.
- The CA will send the email the backup of the signature key that the subscriber placed at the time of download.

4.3.2. Notification to the subscriber by the CA of the issuance of the certificate

The CA, after approving the application, will notify the subscriber by email that the electronic

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	29

signature certificate is in the customer portal ready for download.

a) In Hardware

- The CA or the Related 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 CA will issue the certificate on the DSCF device if the customer 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.

4.4. ACCEPTANCE OF THE CERTIFICATE.

4.4.1. Conduct that constitutes acceptance of the certificate.

The certificate will be accepted at the time the subscriber has accepted terms and conditions at the time of download and the binding legal instrument 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.

4.4.2. Publication of the certificate by the CA.

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

4.4.3. Notification of the issuance of certificates by the CA to other entities.

Not stipulated

4.5. USE OF KEY PAIRS AND CERTIFICATES.

4.5.1. Use of the subscriber's private key and certificate.

The use of the private key and certificate is subject to the terms of the subscriber's agreement and as specified herein and the CPSs, the use of a private key is only permitted after the subscriber has accepted the corresponding certificate.

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	30

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 Data Data and Digital Signature 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.

4.5.2. Use of the trusting party's public key and certificate.

Third parties relying on certificates may use certificates for the purposes of the CPS and this applicable Certification Policy.

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 , specifically for this purpose and specified in this document.

4.6. RENEWAL OF THE CERTIFICATE.

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

4.6.1. Circumstance for the renewal of the certificate.

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 offer certificate rekey services.

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

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

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	31

4.6.2. Who can apply for renewal.

The renewal of the electronic signature certificate can be requested by the holder or a duly authorized third party and the requirements that must be met for certificates from legal entity to company member are specified in the section *Performing identification and authentication functions*.

4.6.3. Processing of applications for renewal of certificates.

The processing of the renewal of certificates will be carried out through the means authorized by the CA for the issuance of certificates, the applicant must contact Security Data Seguridad en Datos y Firma Digital , these means can be online through the website, authorized means of communication or in person.

The CA will receive the request and register it for subsequent verification of the data, the subscriber must have the following:

- Documentation necessary to submit for the processing of your application and to verify the identity of the subscriber, the requirements will be found in this document in the section PROCESSING OF THE CERTIFICATE REQUEST, Performance of identification and authentication functions
- 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.

The validation of the identity will be carried out based on the INITIAL IDENTITY VALIDATION section of this document.

4.6.4. 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 subscriber's certificate renewal.

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

If the subscriber proceeds with the renewal, when the new certificate has been issued, the CA will notify the subscriber by email of the issuance of the certificate so that it can proceed with the download.

4.6.5. Conduct that constitutes acceptance of a renewal certificate.

The certificate will be accepted at the time the subscriber has accepted terms and conditions at the time of download and the binding legal instrument 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

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	32

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.

4.6.6. Publication of the renewal certificate by the CA.

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.

4.6.7. Notification of the issuance of certificates by the CA to other entities.

Security Data does not notify other entities of certificate issuance.

4.7. CHANGE OF CERTIFICATE KEY.

4.7.1. Circumstances for the renewal of the certificate key.

The certificate key may be renewed under the following circumstances:

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

4.7.2. Who can request certification of a new public key.

The certification of a new public key may be requested by the holder or a duly authorized third party and the requirements that must be met will depend on the type of certificate requested.

4.7.3. Processing certificate key renewal requests.

Renewal process, which will be carried out in the same way as the issuance of a new certificate, since the subscriber has in his 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.

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 CA or the Related Third Party, which will validate the identity of the applicant through the identification documents.

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	33

The validation of the documentation will be done in person or online before an operator of the CA or the Related Third Party. Once the identity and documents have been validated, the electronic signature certificate will be issued.

4.7.4. Notification of the issuance of a new certificate to the subscriber.

When the new certificate has been issued, the CA will notify the subscriber of the issuance of the new certificate so that they can proceed with the download, this notification will be made by email.

Security Data will notify the subscriber of the certificate expiration by email 30 days in advance.

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

4.7.5. Conduct that constitutes acceptance of a certificate with a new key.

The certificate will be accepted at the time the subscriber has accepted terms and conditions at the time of download and the binding legal instrument 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.

4.7.6. Publication of the certificate with a new key by the CA.

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.

4.7.7. Notification of the issuance of certificates by the CA to other entities.

Security Data does not notify other entities of certificate issuance.

4.8. MODIFICATION OF THE CERTIFICATE.

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.

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	34

4.8.1. 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.

4.8.2. Who can request the modification of the certificate.

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

4.8.3. Processing of certificate modification requests.

If the subscriber detects any error in the data of his electronic signature, he must approach the offices of the AR with the respective evidence for correction or contact the entity by the approved means for the correction of the data.

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

4.8.4. Notification of the issuance of a new certificate to the subscriber.

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

4.8.5. Conduct that constitutes acceptance of the modified certificate.

The certificate will be accepted at the time the subscriber has accepted terms and conditions at the time of download and the binding legal instrument 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.

4.8.6. Publication of the certificate modified by the CA.

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.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	35

4.8.7. Notification of the issuance of certificates by the CA to other entities.

Security Data does not notify other entities of certificate issuance.

4.9. REVOCATION AND SUSPENSION OF THE CERTIFICATE.

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.

4.9.1. Circumstances of Revocation.

A certificate may be revoked due to the following causes:

- 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 Corporation.

- Circumstances affecting the security of the private key or certificate:
 - Compromise of the private key or the infrastructure or systems of the CA, whenever it affects the reliability of the certificates issued from that incident.
 - Infringement, by the CA or the Related Third Party, of the requirements provided for 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 and the subscriber.

- 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 the subscriber's activation data.
 - Failure by the subscriber or signatory to comply with the rules for the use of the certificate set out in the CPS or in the binding legal instrument between Security Data Seguridad en Datos y Firma Digital and the subscriber.

- Circumstances affecting the subscriber:
 - Termination of the legal relationship between Security Data Seguridad en Datos y Firma Digital and the Subscriber.
 - Modification or termination of the underlying legal relationship or cause that

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	36

- 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.
 - By the death of the subscriber or signatory.
- 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.

4.9.2. Who can request the revocation.

The following can request the revocation of a certificate:

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

The following may process the revocation of the certificate:

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

4.9.3. Procedure for the request for revocation.

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. **Legal Person Holder:** The holder, in his or her capacity as a 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

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	37

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 CA 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.

II. **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:

- 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

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	38

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 CA.

If you call 02-3922169/04-3922169, the subscriber will receive information to carry out the certificate revocation process. The certificate will be suspended until the subscriber or signatory personally appears before the Tied Third Party or at the office, or sends a letter requesting the revocation of the certificate. The certificate will be suspended and the applicant or signatory can cancel the suspension and the revocation procedure.

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.
2. A third party who, through the use of false, outdated documentation or acting maliciously, misleads the CA 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 CA 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.

4.9.4. Grace period for the request for revocation.

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.

4.9.5. Period within which the CA 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.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	39

4.9.6. Revocation check 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.

4.9.7. CRL emission frequency.

The CRL of end-entity certificates is issued every 24 hours or when a revocation occurs, and for quick query, the CA issues a delta CRL every 2-4 hours.

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

4.9.8. 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.

4.9.9. Online health check/revocation availability.

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 CA, the CA shall make every effort to ensure that this information service is not unavailable for longer than the maximum period of 24 hours.

4.9.10. 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.

4.9.11. Other forms of revocation notices available.

Not applicable.

4.9.12. Special key compromise requirements.

Not applicable.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	40

4.9.13. Circumstances of suspension.

Security Data Data Security and Digital Signature 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.

4.9.14. 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 CA.
- The same users.

4.9.15. 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.

4.9.16. Limits on the suspension period.

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.

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	41

4.10. CERTIFICATE STATUS SERVICES.

4.10.1. Operational characteristics .

Security Data Seguridad en Datos y Firma Digital 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 CA, the query is carried out by LDAP protocol.

The 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>

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

4.10.2. Service Availability.

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

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.

4.10.3. Optional features.

Not applicable

4.11. END OF 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.

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	42

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.

4.12. CUSTODY AND RECOVERY OF PASSWORDS.

4.12.1. Key Deposit and Recovery Policy and Practices.

Security Data does not store, nor does it have the possibility to store the private key of subscribers and, therefore, does not provide key recovery services.

4.12.2. Session key encapsulation and retrieval policy and practices.

The CA 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.

5. Facilities, Management and Operation Controls.

5.1. PHYSICAL CONTROLS.

5.1.1. Site location and construction.

Site location and construction controls will be enforced as defined in the CPS and Safety Policy Statement (DPS).

5.1.2. Physical Access.

Physical access controls will be enforced as defined in the CPS and SPS.

5.1.3. Energy and Air Conditioning.

Energy and air conditioning controls will be applied as defined in the CPS and SPS.

5.1.4. Water Exposure.

Water exposure controls will be applied as defined in the CPS and SPS.

5.1.5. Fire Protection and Prevention.

Fire protection and prevention controls shall be applied as defined in the CPS and SPS.

 <p>SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.</p>	<p align="center">CERTIFICATION POLICIES COMPANY MEMBER</p>	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	43

5.1.6.Storage System.

The controls for the storage system will be applied as defined in the CPS and SPS.

5.1.7.Elimination of Information Carriers.

Controls for waste disposal will be applied as defined in the CPS and SPS.

5.1.8.External Backup.

The controls for offsite backups will be applied as defined in the CPS and SPS.

5.2. PROCEDURAL CONTROLS.

5.2.1.Roles of Trust.

The controls for defining trust roles will be applied as defined in the CPS and SPS.

5.2.2.Number of people needed per task.

The controls for defining the number of people required per task will be applied as defined in the CPS and SPS.

5.2.3.Identification and authentication for each role.

The controls for identification and authentication for each role will be applied as defined in the CPS and SPS.

5.2.4.Roles that require separation of duties.

The controls for defining functions that require separation of duties will apply as defined in the CPS and SPS.

5.3. PERSONNEL CONTROLS.

5.3.1.Requirements on Qualification, Experience and Professional Knowledge.

The requirements are defined in the CPS and SPS of Security Data.

5.3.2.Background Check Procedure.

The procedure for background checks will be applied as defined in the CPS and SPS.

5.3.3.Training Requirements.

The controls will be applied as defined in the CPS and SPS.

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	44

5.3.4. Requirements and Frequency of Training Updates.

They will be applied as defined in the CPS and SPS.

5.3.5. Frequency and Sequence of Task Rotation.

They will be applied as defined in the CPS and SPS.

5.3.6. Penalties for Unauthorized Actions.

The process for the enforcement of sanctions shall be followed as defined in the CPS and SPS.

5.3.7. Personnel Hiring Requirements.

It will be followed as defined in the CPS and SPS.

5.3.8. Documentation Provided to Staff.

All personnel incorporated within Security Data Seguridad en Datos y Firma Digital Signature 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, and not limited to the following documentation:

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

5.4. AUDIT TRAIL PROCEDURES.

5.4.1. Types of Events Recorded.

The types of events are defined in the CPS and SPS.

5.4.2. Frequency of Audit Log Processing.

The processing frequency is defined in the CPS and SPS.

5.4.3. Audit Log Retention Period.

The retention period is defined in the CPS and SPS.

5.4.4. Protection of Records.

The protection of records is defined in the CPS and SPS.

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	45

5.4.5. Procedures for Supporting Audit Trails.

The supporting procedures are defined in the CPS and SPS.

5.4.6. Audit Information Collection System.

It will be followed as defined in the CPS and SPS.

5.4.7. Event Notification.

Event reporting will be done as defined in the CPS and SPS.

5.4.8. Vulnerability Analysis.

The analysis will be performed as defined in the CPS and SPS.

5.5. LOG FILE.

5.5.1. Type of Archived Events.

As defined in the CPS and SPS.

5.5.2. Record Retention Period.

The record retention period is defined in the CPS and SPS.

5.5.3. Protection of the Archive.

File protection is defined in the CPS and SPS.

5.5.4. File Backup Procedures.

The procedures will be followed as defined in the CPS and SPS.

5.5.5. Requirements for the Time Stamping of Records.

The requirements are defined in the CPS and SPS.

5.5.6. Audit Information Filing System.

The controls are defined in the CPS and SPS.

5.5.7. Procedures for obtaining and verifying information on file.

The procedures are defined in the CPS and SPS.

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	46

5.6. CHANGE OF KEY OF THE CA.

The process for changing the key is defined in the Security Data CPS.

5.7. DISASTER ENGAGEMENT AND RECOVERY.

5.7.1. Incident and Vulnerability Management Procedures.

The procedure is defined in the CPS and SPS.

5.7.2. Alteration of Hardware, Software and/or Data Resources.

It will be followed as defined in the CPS and SPS.

5.7.3. Procedure for Action in the Face of the Vulnerability of the Private Key of the CA.

It will be followed as defined in the CPS and SPS.

5.7.4. Business Continuity after a disaster.

It will be followed as defined in the CPS and SPS.

5.8. TERMINATION OF CA OR RA.

The procedure as defined in the CPS and SPS will be followed.

6. Technical Security Controls.

6.1. KEY PAIR GENERATION AND INSTALLATION.

6.1.1. Key Pair Generation.

Key pair generation is performed as defined in the CPS.

6.1.2. Delivery of Private Key to the Subscriber.

The delivery of the private key to the subscriber is carried out in accordance with what is defined in the CPS.

6.1.3. Delivery of Public Key to the issuer of the Certificate.

The delivery of the public key is carried out in accordance with what is defined in the CPS.

6.1.4. Delivery of CA Public Key to Trusted Parties.

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	47

The delivery of the public key is carried out in accordance with what is defined in the CPS.

6.1.5. Key Sizes.

It is defined in the CPS.

6.1.6. Generation of Public Key Parameters and quality control.

The procedure is carried out according to what is defined in the CPS.

6.1.7. Purposes of Use of the Key.

The purposes of use are defined in the CPS.

6.2. PROTECTION OF PRIVATE KEYS AND ENGINEERING OF CRYPTOGRAPHIC MODULES.

6.2.1. Standards for Cryptographic Modules.

The standards are defined in the CPS and SPS.

6.2.2. Multi-person control (k of n) of the Private Key.

As defined in the CPS and SPS.

6.2.3. Custody of the Private Key.

As defined in the CPS and SPS.

6.2.4. Backup of the Private Key of the CA.

As defined in the CPS and SPS.

6.2.5. Subscriber's Private Key File.

The CA will not archive 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

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	48

mechanism.

6.2.6. Transfer of the Private Key to/or from the Cryptographic Module.

The transfer is carried out as defined in the CPS and SPS.

6.2.7. 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 authorized and duly authorized personnel in accordance with the provisions of the CPS and 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.

6.2.8. Private Key Activation Method.

The process is carried out as defined in the CPS and SPS.

6.2.9. Private Key Deactivation Method.

The process is carried out as defined in the CPS and SPS.

6.2.10. Private Key Destruction Method.

For the destruction of the private key, the process defined in the CPS and SPS will be followed.

6.2.11. Classification of the cryptographic module.

As defined in the CPS and SPS.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT.

6.3.1. Public Key File.

The CA shall retain all public keys for the period required by applicable law, where applicable, or for as long as the certification service is active and at least 6 months further, otherwise.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	49

6.3.2. Certificate Operating Periods and Key Pair Usage Period.

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

A certificate should not be used after the validity period of the certificate, even if trusted third parties may use it to verify historical data, bearing in mind that there will be no valid online verification service for that certificate.

6.4. ACTIVATION DATA.

6.4.1. 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 the confidentiality of the same before third parties.

6.4.2. Protection of Activation Data.

Only authorized personnel are aware of the activation data of the root CA and subordinate CA private keys.

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.

6.4.3. Other aspects of activation data.

Not stipulated.

6.5. COMPUTER SECURITY CONTROLS.

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 Data Security and Digital Signature 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.

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	50

- Network traffic requirements.

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

6.5.1. Specific Technical Safety Requirements.

The necessary technical requirements are specified in the CPS and SPS of Security Data.

6.5.2. Computer Security Classification.

The classification is specified in the CPS and SPS of Security Data.

6.6. TECHNICAL CONTROLS OF THE LIFE CYCLE.

6.6.1. Systems Development Controls.

The necessary controls are defined in the CPS and SPS of Security Data.

6.6.2. Security Management Controls.

The necessary controls are defined in the CPS and SPS of Security Data.

6.6.3. Lifecycle Security Controls.

The necessary controls are defined in the CPS and SPS of Security Data.

6.7. NETWORK SECURITY CONTROLS.

The necessary controls are defined in the CPS and SPS of Security Data.

6.8. TIME STAMPING.

As defined in the Security Data CPS.

7. Certificate, CRL and OCSP profiles.

7.1. CERTIFICATE PROFILE.

Electronic signature certificates make it possible to unequivocally identify the holder and link their identity with a cryptographic key, making it possible to sign electronic documents with guarantees of authenticity, integrity and non-repudiation, in accordance with current regulations.

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	51

Security Data, within the framework of its electronic signature certificate service, issues certificates of Legal Entity as a Member of a Company.

These certificates can be issued in the following formats:

- **On File**, in the custody of the holder, or
- **DSCF Secure Signature Creation Device**, in accordance with the security requirements established in current regulations.

In order to identify the certificates, Security Data has assigned the following object identifiers (OIDs), as stipulated by the Technical Regulations:

a. Company Member Certificate on File:

Field	on File	Oblig.	Crit.	Observations OID 1.3.6.1.4.1.oid_AC.2.2.1
Of Natural Person	Authentication and Signing			
1. Basic structure				
1.1. Version	"2"	YES		Item "2" corresponds to version 3. X.509 v3
1.2. Serial Number	Automatically set by the CA Unique Identification Number of the certificate.	YES		It cannot be a negative number or 0.
1.3. Signature Algorithm		YES		
1.3.1. Algorithm	SHA-256 with RSA Signature	YES		1.2.840.113549.1.1.11
1.3.2. Parameters	Not applicable	No		
1.4. Issuer		YES		
1.4.1. Country Name (C)	Country Code "EC" (ISO 3166)	YES		OID 2.5.4.6
1.4.2. Organization Name(O)	Name of the Subordinate CA "Organization"	YES		OID 2.5.4.10
1.4.5. Common Name (CN)	Name of the Subordinate CA	YES		OID 2.5.4.3
1.4.6. Organizational Unit Name (OU)	Name of the Organizational Unit of the Subordinate CA E.g. ELECTRONIC SIGNATURE UNIT	No		OID 2.5.4.11
1.5. Validity		YES		
1.5.1. Not Before	Validity Start Date	YES		YYMMDDHHMMSSZ
1.5.2. Not After	Expiration Date	YES		YYMMDDHHMMSSZ
1.6. Subject		YES		
1.6.1. Country Name (C)	Country where the "EC" Signatory resides (ISO 3166)	YES		OID 2.5.4.6
1.6.2. Locality Name (L)	Location of the Signatory (City) e.g. QUITO	YES		OID 2.5.4.7
1.6.3. Organization Name (O)	The name of the Natural Person or Legal Person (Public or Private) to which the Signatory belongs or with whom he or she has a relationship of dependency is specified. E.g. FAVORITE CORPORATION	YES		OID 2.5.4.10
1.6.4. Organization Unit Name (OU)	The Department or Area to which the Signatory belongs or the type of relationship with the Natural Person or Legal Person (Public or Private) that has a relationship of dependency is specified	No		OID 2.5.4.11

1.6.5. Organization Identifier	Unique Taxpayer Registration Number of the legal entity (Public or Private) to which the Signatory "VAT(CÓDIGO_PAIS)-RUC Eg. ("VATEC-1716151413001") is linked.	No		OID 2.5.4.97coding according to ETSI EN 319 412-1RFC 5280 establishes as non-mandatory
1.6.6. Title	The name of the title or position (position) that the Signatory Occupies is specified	YES		OID 2.5.4.12
1.6.7. Surname	Last Name of the Signatory (as stated in the official document)	YES		OID 2.5.4.4
1.6.8. Given Name	Names of the Signatory (as stated in the official document)	YES		OID 2.5.4.42
1.6.9. Serial Number	Identity card number (IDC "Country"-1716151413) or passport (PAS "Country"-A6362611) of the SignatoryEx. IDCEC-1716151413 or PASEC-A6362611	YES		OID 2.5.4.5Official document number coded according to ETSI EN 319 412-1
1.6.10. Common Name (CN)	Names and Surnames of the Signatory	YES		OID 2.5.4.3
1.7. Subject Public Key Info		YES		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	YES		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	Not applicable	NO		
1.7.2. SubjectPublicKey	Signatory Public Key	YES		ETSI TS 119 312 Accord
2. Extensions				
2.1. Authority Key Identifier	Issuer Key Identifier	No	NO	OID 2.5.29.35(Marked as NOT critical according to EN 319412-2) Not Mandatory as long as the public key of the CA is distributed in "SELF-SIGNED" certificate format
2.1.1. KeyIdentifier		No		Derived from the public key
2.2. Subject Key Identifier	Subject key identifier	YES	NO	OID 2.5.29.14(Marked as NOT critical according to EN 319412-2)
2.2.1. KeyIdentifier		YES		Derived from the public key
2.3. Key Usage		YES	YES	OID 2.5.29.15
2.3.1. Digital Signature	Selected "1"	YES		
2.3.2. Content commitment	Selected "1"	YES		
2.3.3. Key Encipherment	Selected "1"	YES		
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"			
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		YES		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.2.1	YES		CA Policy ID
2.4.1.2. Policy Qualifiers		YES		

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	53

2.4.1.1.1 CPS URI	(https://www.repo_example.com/dpc/)	YES		OID 1.3.6.1.5.5.7.2.1 URL of the Certificate Policy of the Accredited Entity
2.4.1.1.2. User Notice/Explicit text	"CERTIFICATE OF MEMBER OF THE COMPANY OR IN A RELATIONSHIP OF DEPENDENCY ON FILE"	YES		OID 1.3.6.1.5.5.7.2.2 Indicative text
2.5. Subject Alternative Names		NO	NO	OID 2.5.29.17(Marked as NOT critical according to EN 319412-2)
2.5.1. rfc822Name	Signatory Email "nombreadellido@example.com.ec"	YES		
2.6. Extended Key Usage		YES	NO	OID 2.5.29.37(Marked as NOT critical according to EN 319412-2)
2.6.1. clientAuth	Present (1.3.6.1.5.5.7.3.2)	YES		Transport Layer Security (TLS) World Wide Web (WWW) client authentication
2.6.2. Email protection	Present (1.3.6.1.5.5.7.3.4)	NO		Only activated if the Signatory's email address is included
2.7. cRLDistributionPoint		YES	NO	OID 2.5.29.31 (Marked as NOT critical according to EN 319412-2)
2.7.1. distributionPoint	(http://crl1.example.com/example1subordinada.crl)	YES		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	(http://crl2.example.com/example2subordinada.crl)	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		YES	NO	OID 1.3.6.1.5.5.7.1.1(Marked as NOT critical according to EN 319412-2)
2.8.1. Access Description		YES		
2.8.1.1. Access Method	id-ad-ocsp	Yes		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	(http://ocsp1.example.com/ocsp/)	Yes		OCSP(http://) access URL IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.1.1.2. Access Location	(http://ocsp2.example.com/ocsp/)	No		OCSP Access URL (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.2. Access Description		No		Not Required as long as you include the OCSP access location
2.9. Basic Constraints		YES	YES	OID 2.5.29.19
2.9.1. cA	FALSE	YES		

b. DSCF Company Member Certificate:

Field	in Secure Signature Creation Device DSCF	Oblig.	Crit.	Observations
Of Natural Person	Authentication and Signing			OID 1.3.6.1.4.1.oid_AC.2.2.2
1. Basic structure				
1.1. Version	"2"	YES		Paragraph "2" corresponds to version 3. X.509 v3
1.2. Serial Number	Automatically set by the CA Unique Identification Number of the certificate.	YES		It cannot be a negative number or 0.

1.3. Signature Algorithm		YES		
1.3.1. Algorithm	SHA-256 with RSA Signature	YES		1.2.840.113549.1.1.11
1.3.2. Parameters	Not applicable	No		
1.4. Issuer		YES		
1.4.1. Country Name (C)	Country Code "EC" (ISO 3166)	YES		OID 2.5.4.6
1.4.2. Organization Name(O)	Name of the Subordinate CA "Organization"	YES		OID 2.5.4.10
1.4.5. Common Name (CN)	Name of the Subordinate CA	YES		OID 2.5.4.3
1.4.6. Organizational Unit Name (OU)	Name of the Organizational Unit of the Subordinate CA E.g. ELECTRONIC SIGNATURE UNIT	No		OID 2.5.4.11
1.5. Validity		YES		
1.5.1. Not Before	Validity Start Date	YES		YYMMDDHHMMSSZ
1.5.2. Not After	Expiration Date	YES		YYMMDDHHMMSSZ
1.6. Subject		YES		
1.6.1. Country Name (C)	Country where the "EC" Signatory resides (ISO 3166)	YES		OID 2.5.4.6
1.6.2. Locality Name (L)	Location of the Signatory (City) e.g. QUITO	YES		OID 2.5.4.7
1.6.3. Organization Name (O)	The name of the Natural Person or Legal Person (Public or Private) to which the Signatory belongs or with whom he or she has a relationship of dependency is specified. E.g. FAVORITE CORPORATION	YES		OID 2.5.4.10
1.6.4. Organization Unit Name (OU)	The Department or Area to which the Signatory belongs or the type of relationship with the Natural Person or Legal Person (Public or Private) that has a relationship of dependency is specified	No		OID 2.5.4.11
1.6.5. Organization Identifier	Unique Taxpayer Registration Number of the legal entity (Public or Private) to which the Signatory "VAT(CÓDIGO_PAIS)-RUC Eg. ("VATEC-1716151413001") is linked.	No		OID 2.5.4.97coding according to ETSI EN 319 412-1RFC 5280 establishes as non-mandatory
1.6.6. Title	The name of the title or position (position) that the Signatory Occupies is specified	YES		OID 2.5.4.12
1.6.7. Surname	Last Name of the Signatory (as stated in the official document)	YES		OID 2.5.4.4
1.6.8. Given Name	Names of the Signatory (as stated in the official document)	YES		OID 2.5.4.42
1.6.9. Serial Number	Identity card number (IDC "Country"-1716151413) or passport (PAS "Country"-A6362611) of the SignatoryEx. IDCEC-1716151413 or PASEC-A6362611	YES		OID 2.5.4.5Official document number coded according to ETSI EN 319 412-1
1.6.10. Common Name (CN)	Names and Surnames of the Signatory	YES		OID 2.5.4.3
1.7. Subject Public Key Info		YES		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	YES		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	Not applicable	NO		
1.7.2. SubjectPublicKey	Signatory Public Key	YES		ETSI TS 119 312 Accord
2. Extensions				
2.1. Authority Key Identifier	Issuer Key Identifier	No	NO	OID 2.5.29.35(Marked as NOT critical according to EN 319412-2) Not Mandatory as long as the public key of the

				CA is distributed in "SELF-SIGNED" certificate format
2.1.1. KeyIdentifier		No		Derived from the public key
2.2. Subject Key Identifier	Subject key identifier	YES	NO	OID 2.5.29.14(Marked as NOT critical according to EN 319412-2)
2.2.1. KeyIdentifier		YES		Derived from the public key
2.3. Key Usage		YES	YES	OID 2.5.29.15
2.3.1. Digital Signature	Selected "1"	YES		
2.3.2. Content commitment	Selected "1"	YES		
2.3.3. Key Encipherment	Selected "1"	YES		
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"			
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		YES		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.2.2	YES		CA Policy ID
2.4.1.2. Policy Qualifiers		YES		
2.4.1.1.1 CPS URI	(https://www.repo_example.com/dpc/)	YES		OID 1.3.6.1.5.5.7.2.1 URL of the Certificate Policy of the Accredited Entity
2.4.1.1.2. User Notice/Explicit text	"CERTIFICATE OF MEMBER OF THE COMPANY OR IN A RELATIONSHIP OF DEPENDENCY IN SECURE SIGNATURE CREATION DEVICE -DSCF"	YES		OID 1.3.6.1.5.5.7.2.2 Indicative text
2.5. Subject Alternative Names		NO	NO	OID 2.5.29.17(Marked as NOT critical according to EN 319412-2)
2.5.1. rfc822Name	Signatory Email "nombreaellido@example.com.ec"	YES		
2.6. Extended Key Usage		YES	NO	OID 2.5.29.37(Marked as NOT critical according to EN 319412-2)
2.6.1. clientAuth	Present (1.3.6.1.5.5.7.3.2)	YES		Transport Layer Security (TLS) World Wide Web (WWW) client authentication
2.6.2. Email protection	Present (1.3.6.1.5.5.7.3.4)	NO		Only activated if the Signatory's email address is included
2.7. cRLDistributionPoint		YES	NO	OID 2.5.29.31 (Marked as NOT critical according to EN 319412-2)
2.7.1. distributionPoint	(http://crl1.example.com/example1subordinada.crl)	YES		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	56

2.7.2. distributionPoint	(http://crl2.example.com/example2subordinada.crl)	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		YES	NO	OID 1.3.6.1.5.5.7.1.1(Marked as NOT critical according to EN 319412-2)
2.8.1. Access Description		YES		
2.8.1.1. Access Method	id-ad-ocsp	Yes		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	(http://ocsp1.example.com/ocsp/)	Yes		OCSP(http://) access URL IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.1.1.2. Access Location	(http://ocsp2.example.com/ocsp/)	No		OCSP Access URL (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.2. Access Description		No		Not Required as long as you include the OCSP access location
2.9. Basic Constraints		YES	YES	OID 2.5.29.19
2.9.1. cA	FALSE	YES		

7.1.1. Version Number.

The version number is specified within each certificate profile.

7.1.2. Certificate Extensions.

The certificate extension is specified within each profile.

7.1.3. Algorithm Object Identifiers.

OIDs are specified within each certificate profile.

7.1.4. Forms of names.

The shapes of the names are specified within each certificate profile.

7.1.5. 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.

7.1.6. Certificate Policy object identifier.

The OID of the certificates is:

- OID of Company Member file: 1.3.6.1.4.1.37746.2.2.1
- DSCF Company Member OID: 1.3.6.1.4.1.37746.2.2.2

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	57

- Electronic Seal OID on file: 1.3.6.1.4.1.37746.2.4.1
- Electronic Seal OID in DSCF: 1.3.6.1.4.1.37746.2.4.2
- Timestamp OID: 1.3.6.1.4.1.37746.2.5.1

7.1.7. Use of the Policy Restrictions extension.

Not applicable.

7.1.8. Syntax and Semantics of the Qualifiers of Politics.

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 1: 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 ID
2.4.1.2. Policy Qualifiers		YES	-	-
2.4.1.1.1 CPS URI	(https://www.repoexchange.com/dpc/) – CPS or PC URI	YES	-	OID 1.3.6.1.5.5.7.2.1 Certificate Authority Certificate Policy URL
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

7.1.9. Processing Semantics for Critical Certificate Policy Extension.

It is not stipulated.

7.2. CRL PROFILE.

The profile of the CRLs corresponds to the one proposed in the corresponding certification policies, and to the X.509 standard 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.

7.2.1. Version Number.

The CRLs issued by the CA are version 2.

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	58

7.2.2. CRLs and CRL input extensions.

CRLs and extensions are defined in the Security Data CPSs.

7.2.3. OCSP PROFILE.

Certificates issued for the OCSP validation service follow an X.509 v3 certificate profile intended exclusively for OCSP response signing. The certificate does NOT act as a CA, where CA=FALSE and its use is restricted by EKU to the OCSPSigning purpose.

Characteristic elements of the profile:

- Subject DN identifies OCSP Responder
- Basic Constraints: CA=FALSE.
- EKU: OCSPSigning with OID 1.3.6.1.5.5.7.3.9
- It contains the OCSP No Check extension, to allow trusting parties to not require additional revocation verification of this certificate during OCSP validation.
- Publishes CRL Distribution Points and Authority Information Access for string and issuer fetching.

7.2.4. Version Number.

The OCSP certificate is issued as X.509 Version 3, to allow the use of critical and non-critical extensions necessary for OCSP service operation.

7.2.5. OCSP extensions.

The following are the extensions present in the OCSP certificate and their semantics of use within this profile:

- Critical Extensions:
 - Key Usage with OID 2.5.29.15 – CRITICAL
 - digitalSignature = TRUE OCSP response signature.
 - contentCommitment / nonRepudiation = TRUE
 - All other KeyUsage bits are kept at FALSE, no encryption, certificate signing, or CRL signing is allowed.
 - Basic Constraints with OID 2.5.29.19 – REVIEW
 - CA = FALSE.
 - No pathLenConstraint.
 - Confirms that the certificate is an end-entity certificate and cannot issue certificates.
- Non-Critical Extensions:
 - Extended Key Usage with OID 2.5.29.37 – NON-CRITICAL
 - Includes id-kp-OCSPSigning with OID 1.3.6.1.5.5.7.3.9.
 - Restricts the use of the certificate to OCSP response signing.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	59

- OCSP No Check with OID 1.3.6.1.5.5.7.48.1.5 – NON-CRITICAL
 - Indicates that relying parties can bypass the CRL/OCSP revocation check of this OCSP certificate when validating OCSP responses, according to common practices for OCSP responder certificates.

- Certificate Policies with OID 2.5.29.32 – NON-CRITICAL
 - Includes the policy OID applicable to the OCSP certificate: 1.3.6.1.4.1.37746.2.6.1
 - In addition, the documentary reference of policy is published:
 - CPS: <https://www.securitydata.net.ec/normativas/dpcocsp.pdf>
 - User Notice: "OCSP VALIDATION CERTIFICATE"

- Subject Alternative Name with OID 2.5.29.17 – NON-CRITICAL
 - Includes rfc822Name with service contact email.

- CRL Distribution Points with OID 2.5.29.31 – NON-CRITICAL
 - Publish issuer CRL distribution points.

- Authority Information Access with OID 1.3.6.1.5.5.7.1.1 – NON-CRITICAL
 - Publish calssuers for download of the issuer certificate (issuer HTTP URL).

- Subject Key Identifier with OID 2.5.29.14 – NON-CRITICAL
 - Subject key identifier to facilitate string construction and validation.

- Authority Key Identifier with OID 2.5.29.35 – NON-CRITICAL
 - Key identifier of the issuing CA for easy string construction and validation.

7.3. CRL PROFILE.

The CRL profile is defined in the Security Data CPS.

7.4. OCSP PROFILE.

The OCSP profile is defined in the Security Data CPS.

8. Compliance Audits and Other Controls.

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

8.1. FREQUENCY OR CIRCUMSTANCES OF THE EVALUATION.

Internal audit plans will be carried out with reporting, in order to have control over the life cycle

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	60

of the certification authority and external audits will be carried out whenever requested by the regulatory authority.

Webtrust seal maintenance audits are conducted annually.

8.2. QUALIFICATIONS OF THE EVALUATOR.

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

8.3. 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 Seguridad en Datos y Firma Digital.

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.

8.4. ASPECTS COVERED BY THE CONTROLS.

The audit verifies the following principles:

- a) Publication of Information: That the CA publishes the Business and Certificate Management Practices (this CPS), as well as the information privacy and personal data protection policy, and provides its services in accordance with such 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: That 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.

8.5. ACTIONS TO BE TAKEN AS A RESULT OF THE DETECTION OF INCIDENTS.

The actions are defined in the Security Data CPS.

8.6. COMMUNICATION OF RESULTS.

The communication process is defined in the Security Data CPS.

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	61

9. Other Legal and Activity Issues.

9.1. RATES.

9.1.1. 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.

9.1.2. 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.

9.1.3. 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 commercial certificate validation services (such as OCSP).

9.1.4. 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.

9.1.5. 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 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

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	62

certificate within a maximum period of 72 hours.

9.2. FINANCIAL RESPONSIBILITY.

9.2.1. Insurance Coverage.

The insurance coverages are defined in the Security Data CPS.

9.2.2. Other Assets.

No stipulation.

9.2.3. Insurance or Guarantee of Coverage for Final Entities.

The insurance coverages are defined in the Security Data CPS.

9.3. 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.

The holder's private key is confidential and under his or her exclusive control; Security Data does not have access to it, but protects the confidentiality of generation processes when they occur on your premises.

9.3.1. Scope of Confidential Information.

All non-public information is considered confidential and therefore of restricted access:

- Confidentiality of the Certification Authority's private key.
- Confidentiality of the holder's private key.
- Confidentiality of the information provided by the owner.
- Records of transactions.
- Audit trail logs.
- Security policies.
- Contingency Plan.
- Business continuity plans.
- Any other information relating to the subscriber or SECURITY DATA, which may be confidential in nature.

9.3.2. Non-Confidential Information.

The CA will keep the following as non-private information:

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	63

- That contained in this SPS, CP and CPS.
- All information contained in issued certificates and certificate revocation lists (CRLs), including all such information that can be obtained.
- Certificate information (as authorized by the subscriber in the subscriber's agreement) and certificate status information.
- All information expressly classified as "PUBLIC".
- Information regarding the revocation of a certificate.
- Any other information whose publication is required by law.

9.3.3. Responsibility 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.

9.4. PRIVACY OF PERSONAL INFORMATION.

9.4.1. 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.

9.4.2. 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.

9.4.3. Information Not Classified as Private.

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

9.4.4. 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.

Owners may exercise their rights of access, deletion, rectification and opposition through the

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	64

channels defined in the Privacy Policy published on the Security Data website.

9.4.5. Notice and Consent to Use Personal Data.

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

9.4.6. 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.

9.4.7. Other circumstances of disclosure of information.

Not stipulated

9.5. 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.

9.6. REPRESENTATIONS AND WARRANTIES.

9.6.1. CA Representations and Warranties.

The representations and warranties of the CA are set forth in the CPS.

9.6.2. RA Representations and Warranties.

The RA's representations and warranties are set forth in the CPS.

9.6.3. Subscriber Representations and Warranties.

Underwriters' representations and warranties are set forth in the CPS.

9.6.4. Representations and Warranties of the Relying Party.

The relying party's representations and warranties are set forth in the CPS.

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	65

9.6.5. Representations and Warranties of Other Participants.

No stipulation.

9.7. 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.

9.8. LIMITATIONS OF LIABILITY.

To the extent that the SECURITY DATA CA 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 PC and its corresponding CPS, 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 fully complies with the provisions of this PC and CPS.

SECURITY DATA's liability to any person for damages arising under, out of, or in connection with this PC and its CPS, 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.

9.9. COMPENSATION.

The cases of compensation are defined in the contracts of the holders.

9.10. TERM AND TERMINATION.

9.10.1. Term.

This Certification Policy 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.

9.10.2. Termination.

This Certification Policy document, and any amendments, will remain in effect until modified or

	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	66

replaced by a newer version.

9.11. 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, and may also notify the affected owners and the Data Protection Authority directly and expeditiously, in accordance with the established legal deadlines.

9.12. 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.

9.13. DISPUTE RESOLUTION PROVISIONS.

As defined in the Security Data CPS.

9.14. GOVERNING LAW.

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

9.15. 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.

9.16. MISCELLANEOUS PROVISIONS.

9.16.1. Entire Agreement.

No stipulation.

9.16.2. Assignment.

Issuing CAs, subscribers, relying third parties, Registration Entities, or any other entity operating under this Certification Policy, have no right to assign any of their rights or obligations hereunder without the prior written consent of SECURITY DATA.

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	CERTIFICATION POLICIES COMPANY MEMBER	CODE	SD-ID-PE-1 7
		VERSION	V10
		APPROVAL DATE	03/04/2026
		PAGES	67

9.16.3. Severability.

If any of the provisions of the Certification Policy and your CPS are held to be invalid by a competent authority in the applicable jurisdiction, the remainder of the Statement of Practice and Certification Policy shall remain valid and enforceable.

9.16.4. Execution.

No stipulation.

9.16.5. Force Majeure.

Security Data accepts no liability for any delay or failure to perform an obligation under its Practices Statement and Certification Policy, to the extent that such delay or failure is caused by events beyond its reasonable control.

9.17. OTHER PROVISIONS.

No stipulation.

10. Control of Approvals.

PREPARED BY	COORDINATOR OF THE MANAGEMENT SYSTEM	
REVIEWED BY	CHIEF TECHNOLOGY OFFICER (CTO)	
	LEGAL SUPERVISOR	
APPROVED BY	GENERAL MANAGER	