SECURITY DATA
TU IDENTIDAD DIGITAL, EN UNA FIRMA.

ELECTRONIC SEAL CERTIFICATION POLICY

marzo 4

2026

VERSION HISTORY

VERSION	DESCRIPTION	DATE	PREPARED BY	REVIEWED BY	APPROVED BY
V1	Initial Edition	12/22/2025	Legal Supervisor	Chief Technology Officer (CTO)	General Manager
V2	General update of the PC in accordance with the Technical Regulations and RFC 3647.	02/12/2026	Management System Coordinator	Chief Technology Officer (CTO) Legal Supervisor	General Manager

Contents

1. Introduction.

1.1. GENERAL DESCRIPTION.

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

Security Data Seguridad en Datos y Firma Digital S.A. (hereinafter Security Data), is a company incorporated in accordance with Ecuadorian legislation, registered in the commercial registry under number 2246 on July 13, 2010 with legal existence until July 13, 2060.

This document is the Certification Policy (PC) corresponding to the certificates issued by Security Data of the type "Electronic Seal File" and "Electronic Seal DSCF". These certificates may be issued with the consideration of qualified in accordance with the provisions of the Technical Standard for the Provision of Certification Services and Related Services, issued by the Telecommunications Regulation and Control Agency (ARCOTEL), relating to electronic identification and trust services for electronic transactions in the internal market. and with the consideration of qualified as defined in current legislation.

The Certification Policy is mandatory for the CA, its personnel, suppliers and other parties involved in the provision of the Electronic Seal issuance service, and constitutes a public document, except for those sections that, for security reasons, must be classified.

This Certification Policy (PC), together with the CPS of Security Data Seguridad en Datos y Firma Digital S.A., are aimed at anyone who relies on this type of certificate.

1.2. NAME AND IDENTIFICATION OF THE DOCUMENT.

Name:	Electronic Seal Certification Policy
Document Code:	SD-ID-PE-13
Version:	2
Description:	Electronic Seal Certification Policy of Security Data Seguridad en Datos y Firma Digital S.A.
Publication date:	February 12, 2026
Document Type:	Public
OID:	File OID: 1.3.6.1.4.1.37746.2.4.1 DSCF OID: 1.3.6.1.4.1.37746.2.4.2

1.3. PKI PARTICIPANTS.

1.3.1. Certification Authority.

The Certification Authority, hereinafter "AC", is the person authorised and empowered to issue certificates in relation to the electronic signatures of individuals, to offer or facilitate the services of registration and chronological stamping of the transmission and reception of data messages, as well as to perform other functions related to communications based on electronic signatures.

1.3.2. Certification Service Provider.

The Electronic Certification Service Provider (PSC) is the legal entity that provides one or more certification services. Security Data is a PSC in compliance with its Certification Practices Statement (CPS) that issues certificates recognized under the Electronic Commerce, Electronic Signatures and Data Messaging Act.

1.3.3. Subscribers.

The subscribers of the certification service are the end users of the electronic certificates issued by SECURITY DATA. Subscribers can be natural or legal persons.

1.3.4. Parties that trust.

They are the natural or legal persons who voluntarily trust and make use of the certificates issued by SECURITY DATA.

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

1.3.5. Electronic Seal Certificate.

It is a certificate for a legal entity, which subscribes to the terms and conditions of use of a certificate, and whose identity is linked to the Seal Verification Data (Public Key) of the certificate issued by Security Data. Therefore, the identity of the certificate subscriber is linked to what is electronically stamped by the seal creator, using the Seal Creation Data (Private Key) associated with the certificate issued by Security Data.

1.4. USE OF THE CERTIFICATE.

1.4.1. Appropriate Uses of the Certificate.

These certificates must be used in accordance with the legal regulations in force governing certain aspects of electronic trust services. The use of the keys and certificate by the subscriber presupposes acceptance of the terms of use set out in the Security Data CPS.

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 which Security Data may revoke the certificate and terminate the contract unilaterally.

If the subscriber's certificate in the validity period is compromised, that is, its private key, it must initiate the revocation procedure as mentioned in this PC and CPS.

1.4.2. Unauthorized Uses of Certificates.

Use that is contrary to Ecuadorian and Community regulations, international conventions ratified by the Ecuadorian State, customs, morals and public order is not permitted. Nor is use other than that established in this Certification Policy and in the established CPS´s allowed.

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.

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 Certification Policy and other regulatory documents.

1.5.2. Contact Person.

Name:	SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A.
Address:	Alonso de Torres and Edmundo Carvajal "El Bosque" Shopping Center Administrative Offices 1st floor.
Address:	Quito - Ecuador
Email:	cto@securitydata.net.ec
Phone:	(02) 3922169
Website:	www.securitydata.net.ec

1.5.3. Person who determines the suitability of the CPS for the Policy.

This document is digitally signed by the Head of the Security Data CA before being published, and its versions are controlled, in order to avoid unauthorized modifications and impersonations.

1.5.4. CPS approval procedures.

The publication of the revisions of this PC and CPS must be approved and signed by the Security Data CA manager before publication.

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.

Public Key and Private Key: The asymmetric cryptography on which PKI is based employs a pair of
(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 by the holder of the certificate.

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.

Electronic seal: A set of data in electronic format, created by secure cryptographic means and associated with an electronic seal certificate, which allows the issuing entity to be identified and guarantees the integrity and authenticity of the electronic data to which it is applied.

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): A 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.

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.

1.6.2. Acronyms.

AC:	Certificate Authority
AC Sub:	Subordinate Certificate Authority
PC:	Certification Policy
CPS:	Certification Practices Statement
CRL:	Certificate Revocation List
HSM:	Hardware Security Module
LDAP:	Lightweight Directory Access Protocol
OCSP:	Online Certificate Status Protocol.
PKI:	Public Key Infrastructure
PSC:	Certification Service Provider
VA:	Validation Authority
ECI:	Information Certification Authority
OID:	Unique Object Identifier
DN:	Dinstinguished Name
C:	Country
CN:	Common Name
Or:	Organization
OU:	Organizational Unit
SN:	SurName
ISO:	International Organizational for Standardization
PKCS:	Public Key Cryptography Standards, PKI Standards
UTF8:	Unique Transformation Format – 8-bit.

2. Publishing and Repository Responsibilities.

2.1. REPOSITORIES.

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

Certification Policy: https://www.securitydata.net.ec/normativas/pc_se.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

2.2. APPROVAL PROCEDURE.

The publication of the revisions of this Electronic Seal PC must be approved by the Senior Management of Security Data, after verifying compliance with the requirements expressed in them.

2.3. TIME OR FREQUENCY OF PUBLICATION.

This Electronic Seal PC will be reviewed and, if appropriate, updated, annually or when any change is presented.

2.4. ACCESS CONTROLS TO REPOSITORIES.

The repositories available on the aforementioned Security Data website are freely accessible to the public.

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 EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles.
- RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile",
- ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

3.1.2. Need for names to be meaningful.

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 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.

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.

3.1.3. Pseudonyms.

Alias may not be used in the Owner fields, Security Data does not issue pseudonymous certificates.

3.1.4. Rules for interpreting that names are meaningful.

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

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

3.1.5. Singularity of Names.

The DN of the certificates issued is unique for each subscriber and/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.

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.

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.

3.2.2. Authentication of the Identity of an Organization (Legal Entity).

Security Data will need to verify the following data before you can authenticate your organization's identity:

- 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 single taxpayer register of the RUC organisation.

In addition, the legal representative or company member of the legal entity must present the identity card, passport or other legally recognized means that identifies them or a biometric validation process or other legally recognized means will be carried out that identifies them.

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 to natural persons.

3.2.4. Unverified Owner 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 authority, faculty or legal representation necessary to act on behalf of the legal entity, position or function to which the requested certificate will be associated.

The CA validates that the applicant has a current appointment, power of attorney or authorization, granted in accordance with the applicable legal regulations, which empowers him or her to request and use the certificate on behalf of the entity, in accordance with the provisions of the section Authentication of the Identity of a Legal Entity.

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

The validation of the authority is carried out prior to the issuance of the certificate, 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 seal 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 CA; 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.

For electronic seal certificates, no renewals are made, but new issuances of certificates are made.

3.3.2. Identification and Authentication for the renewal of keys after revocation.

Once electronic seal certificates have been revoked, they cannot be renewed; instead, a new certificate must be issued.

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

4. Operational Requirements for the Life Cycle of Certificates.

4.1. REQUEST FOR CERTIFICATES.

4.1.1. Who can apply for a Certificate.

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, with full legal capacity to act.

4.1.2. Certificate Request Processes.

The applicant must go to the offices of de Security Data Seguridad en Datos y Firma Digital, having in their possession the documentation required to manage the application for the certificate, in whose presence they will proceed to sign the application form that must be duly completed.

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 CP and CPS. The CA is responsible for managing the enrollment process in a secure, reliable manner and in compliance with applicable technical and regulatory standards.

4.1.3. Validity of the Electronic Seal Certificate.

The duration of the electronic seal certificate will be contractually established between the holder of the electronic seal and Security Data.

4.2. PROCESSING PROCEDURE.

4.2.1. Performing Identification and Authentication functions.

The subscriber must prove their identity and present, in force, the original or authentic copy of the following documentation:

a) Physical address and other data that allow contact with Him, for which the RUC will be requested.
b) The CA, as accreditation of the face-to-face act and in order to make it impossible to repudiate the procedure carried out, may obtain a set of biometric evidence: photograph and/or video validation.
c) Identity card or passport in the case of foreign citizens, whose photograph allows the identity of the person appearing to be verified.
d) The Representative must have sufficient power of representation, delivering documents such as: appointment, power of attorney, appointment registered with the regulatory entity, and other enabling documents that Security Data deems necessary.

To authenticate a Certificate Manager, the same procedure as that specified in the previous section will be followed, with the particularity that, in this case, the power of representation required of the subscriber will be replaced by the signing of a letter of Authorization. The letter must be signed by the Legal Representative.

4.2.2. Approval or rejection of the certificate request.

Once the certificate request has been made, the Registry Operator shall verify the information provided by the applicant, including the validation of the subscriber's identity.

After obtaining the evidence to verify identity, the registration operator will review the identification process and check the evidence to accept or reject the validity of the identification process, in accordance with the applicable regulations on the causes of rejection of video identification.

The Legal Department and the Technical Department will intervene in the validation process, which will review and technically validate the petition certificate.
If the information is incorrect, the registry operator will deny the request, and the requestor will be informed of the reason.

If it is correct, the attention, payment or confirmation of the payment of the certificate and the signing of the binding legal instrument between the subscriber and/or the applicant and de Security Data Seguridad en Datos y Firma Digital will be carried out. The certificate will then be issued.

4.2.3. Processing time for Certificate requests.

The issuance of a certificate involves the final and complete approval of an application by Security Data. The certificate must be issued within a maximum period of 48 hours, once the request has been made as defined in the Security Data CPS.

4.3. ISSUANCE OF THE CERTIFICATE.

The issuance of the certificate will be carried out as defined in the Security Data CPS.

4.3.1. Actions of the CA during the Issuance of the Certificates.

As defined in the Security Data CPS.

4.3.2. Delivery of the Certificate.

As defined in the Security Data CPS.

4.4. ACCEPTANCE OF THE CERTIFICATE.

As defined in the Security Data CPS.

4.4.1. Form in which the Certificate is Accepted.

The certificate will be accepted at the time the legal instrument binding between the subscriber and de 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.

4.4.2. Publication of the Certificate.

The certificate is published in the Security Data repositories, within a maximum period of 24 hours from the time it has been issued.

4.4.3. Notification of the Issuance of the Certificate by the CA to third parties.

No notification is made to third parties.

4.5. USE OF KEY PAIRS AND CERTIFICATES.

4.5.1. Use of the Subscriber's Private Key and Certificate.

Certificates may be used as stipulated in this CP and in the CPS.

4.5.2. Use of Public Key and Certificate of the relying party.

Third parties relying on certificates may use certificates for the purposes of this CP and the CPS.

It is the responsibility of third parties to verify the status of the certificate through the services offered by Security Data, Data Security and Digital Signature, specifically for this purpose and specified in this document.

4.6. RENEWAL OF CERTIFICATES.

Security Data does not renew certificates, as the renewal process is carried out in the same way as issuing a new certificate.

4.7. CHANGE OF CERTIFICATE KEY.

As defined in the Security Data CPS and identity validation as defined in this PC.

4.7.1. Circumstances for Certificate Renewal.

The Electronic Seal certificate may be renewed under the following circumstances:

- The certificate has expired.
- The certificate has been revoked.

4.7.2. Persons authorized to apply for renewal.

The renewal application form must be signed by the subscriber himself, either the subscriber himself or the legal representative who processes the certificate application.

The subscriber's personal circumstances must not have changed, in particular his or her capacity for legal representation.

4.7.3. Approval or rejection of renewal applications.

The same procedure as that carried out in the issuance process specified in this document will be followed.

4.7.4. Notification of Certificate Renewal.

The same procedure as that carried out in the issuance process specified in this document will be followed.

4.7.5. Acceptance of Certificate Renewal.

As defined in the Security Data CPS.

4.7.6. Publication of the Renewed Certificate.

The same procedure as that carried out in the issuance process specified in this document will be followed.

4.7.7. Notification of the issuance of Certificates to other entities.

Security Data does not notify other entities of certificate issuance.

4.8. MODIFICATION OF CERTIFICATES.

Not applicable.

4.9. REVOCATION AND SUSPENSION OF CERTIFICATES.

The entire process of revocation and suspension will be carried out in accordance with the provisions of the Security Data CPS.

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 "Signature Expiration and CRL" option URL: https://www.securitydata.net.ec/firma- electronica-en-ecuador/

Download links can be found at the following addresses: CRLS

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

4.10.2. Availability of Service.

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.

No stipulation.

4.11. END OF SUBSCRIPTION.

The subscription will end at the time of expiry or revocation of the electronic certificate used in the provision of the Electronic Seal service.

4.12. CUSTODY AND RECOVERY OF PASSWORDS.

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.

5. Facilities, Management and Operation Controls.

Security Data will implement technical and organisational measures to ensure:

- Physical and logical security of the facilities.
- Access control.
- Separation of duties.
- Event logging and monitoring.
- Continuity of service.

The application of the practices will be carried out in accordance with what is defined in the CPS of Security Data and established internal procedures.

a) Control and Detection of Incidents.

Any interested party can communicate their complaints or suggestions through the following means:

a. By phone: 023922169.
b. By email: info@securitydata.net.ec
c. By filling in the electronic form available on the website: https://www.securitydata.net.ec/quejas-sugerencias-security-data/

b) Incident Log.

Security Data has an Incident Registry in which any incident that has occurred with the certificates issued, and the evidence obtained, is recorded. These incidents are recorded, analyzed, and remedied according to Security Data's Information Security Management System procedures.

The Chief Technology Officer (CTO) determines the severity of the incident and appoints a person in charge and, in the event of relevant security incidents, reports to the PKI Security Committee.

5.1. PHYSICAL SECURITY CHECKS.

As defined in the CPS and SPS of Security Data.

5.2. PROCEDURAL CONTROLS.

As defined in the CPS and SPS of Security Data.

5.3. PERSONNEL CONTROLS.

As defined in the CPS and SPS of Security Data.

5.4. AUDIT LOG PROCEDURE

5.4.1. Types of Events Recorded.

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

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

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

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

5.4.2. Frequency of Audit Log Processing.

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

5.4.3. Audit Log Retention Period.

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

5.4.4. Protection of Records.

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

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

The devices are operated at all times by authorized personnel.

5.4.5. Procedures for Supporting Audit Trails.

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

SECURITY DATA has implemented a secure backup procedure for audit logs, making a weekly copy of all logs on an external medium. The external medium is stored in a fireproof cabinet under security measures that guarantee that access is only allowed to authorized personnel. Daily, incremental, and full weekly copies are made.

In addition, a copy of the audit logs is kept in an external custody center of SECURITY DATA.

5.4.6. Audit Information Collection System.

SECURITY DATA's event audit information is collected internally and automatically by the operating system and by the certification software.

5.4.7. Event Notification.

SECURITY DATA establishes that the possibility of allowing notification to a holder is taken into consideration in cases where it is established that the event is of an accidental nature and it is likely that it may occur again.

5.4.8. Vulnerability Analysis.

SECURITY DATA performs an annual review of discrepancies in log information and suspicious activities.

5.5. LOG FILES.

As defined in the CPS and SPS of Security Data.

5.6. CHANGE OF PASSWORD.

As defined in the CPS and SPS of Security Data.

5.7. DISASTER ENGAGEMENT AND RECOVERY.

As defined in the CPS and SPS of Security Data.

5.8. TERMINATION OF CA.

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

- Protecting audit trails.
- Notify subscribers, holders and trusted third parties of the cessation of operations at least thirty (30) days in advance.
- Inform ARCOTEL at least sixty (60) days in advance.

Security Data takes steps to transfer audit logs to the Competent Authority for a period of 10 years after the log is generated.

All existing applications and contracts of subscribers and holders will be transferred to the Competent Authority or to another PSC designated by it, in compliance with the previously established guarantees and responsibilities.

All subscribers, holders and trusted third parties will be warned of the changes and any type of condition associated with the continuity of the use of the certificates issued by a CA that terminates or transfers its operations, through a communication published on the Security Data website.

6. Technical Security Controls.

6.1. KEY PAIR GENERATION AND INSTALLATION.

The generation and installation process will be carried out as defined in the CPS and SPS of Security Data.

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

Controls are stipulated as defined in the Security Data CPS and SPS.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT.

Controls are stipulated as defined in the Security Data CPS and SPS.

6.4. ACTIVATION DATA.

Controls are stipulated as defined in the Security Data CPS and SPS.

6.5. COMPUTER SECURITY CONTROLS.

Controls are stipulated as defined in the Security Data CPS and SPS.

6.6. TECHNICAL CONTROLS OF THE LIFE CYCLE.

Controls are stipulated as defined in the Security Data CPS and SPS.

6.7. NETWORK SECURITY CONTROLS.

Controls are stipulated as defined in the Security Data CPS and SPS.

6.8. TIME STAMPING.

Not applicable.

7. Certificate, CRL and OCSP profiles.

7.1. CERTIFICATE PROFILE.

These certificates serve as proof that an electronic document has been issued by a legal entity, providing certainty about the origin and integrity of the document. Security Data, within the framework of its service of qualified electronic seal certificates, issues the following types:

- **Electronic Seal Certificate for Legal Persons**, intended to identify private entities and guarantee the integrity and origin of electronic data.
- **Institutional Electronic Seal Certificate**, intended for public entities or bodies, when applicable.

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) Electronic seal on file:

Field	on File	Oblig.	Crit.	Observations OID 1.3.6.1.4.1.oid_AC.2.4.1
ELECTRONIC SEAL	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. Locality Name (L)	Locality of the Subordinate CA (City) Ex. QUITO	YES		OID 2.5.4.7
1.4.3. 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 Legal Entity (Public or Private) Holder of the Signature "EC" (ISO 3166) is registered	YES		OID 2.5.4.6
1.6.2. Locality Name (L)	Location of the Legal Entity (Public or Private) Owner of the Firm (City) e.g. QUITO	YES		OID 2.5.4.7
1.6.3. Organization Name (O)	Name of the Legal Entity (Public or Private) Owner of the Firm. 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 is specified	No		OID 2.5.4.11
1.6.5. Organization Identifier	Unique Taxpayer Registration Number of the legal entity (Public or Private) Holder of the Signature to which the Electronic Seal "VAT(CÓDIGO_PAIS)-RUC is linked Ex. VATEC-1716151413001	No		OID 2.5.4.97coding according to ETSI EN 319 412-1RFC 5280 establishes as non-mandatory
1.6.6. Serial Number	Unique Taxpayer Registration Number of the Legal Entity (Public or Private)E.g. "1716151413001"	YES		OID 2.5.4.5
1.6.7. Common Name (CN)	Description of the use that will be given to the Electronic Seal. RECEIPT OF DOCUMENTS AT A SINGLE WINDOW	YES		OID 2.5.4.3
1.6.8. Surname	Surname of the Signatory that will be linked to the seal (as stated in the official document)	YES		OID 2.5.4.4
1.6.9. Given Name	Names of the Signatory who will be linked to the seal (as stated in the official document)	YES		OID 2.5.4.42

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 commintment	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.102.2.4.1	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	"ELECTRONIC SEAL CERTIFICATE 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	Email of the Legal Entity (Public or Private) Holder of the Signature (electronic seal) "info@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		It is only activated if the email address of the Legal Entity (Public or Private) Holder of the Signature (electronic seal) 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://) IETFRFC 4516 [4] scheme
2.7.2. distributionPoint	(http://crl2.example.com/example2subordinada.crl)	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETFRFC 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
2.8.2.1. Access Method	id-ad-caIssuers	no		OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	(http://www.example.com/subordinate1.crt)	No		URL Access to AC(http://) IETF RFC 7230-7235 [3] or (https://) IETF RFC 2818 [5] certificate
2.9. Basic Constraints		YES	YES	OID 2.5.29.19
2.9.1. cA	FALSE	YES		

b) Electronic seal in DSCF Secure Signature Creation Device:

Field	in Secure Signature Creation Device DSCF	Oblig.	Crit.	Observations OID 1.3.6.1.4.1.oid_AC.2.4.2
ELECTRONIC SEAL	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. Locality Name (L)	Locality of the Subordinate CA (City) Ex. QUITO	YES		OID 2.5.4.7
1.4.3. Organization Name(O)	Name of the Subordinate CA "Organization"	YES		OID 2.5.4.10

1.4.4. Organization Identifier	Subordinate CA identifier "VAT(CÓDIGO_PAIS)-IDENTIFICAR_ORGANIZACIÓN" e.g. VATEC-1716151413001	NO		2.5.4.97coding according to ETSI EN 319 412-1 RFC 5280 establishes as non-mandatory
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 Legal Entity (Public or Private) Holder of the Signature "EC" (ISO 3166) is registered	YES		OID 2.5.4.6
1.6.2. Locality Name (L)	Location of the Legal Entity (Public or Private) Owner of the Firm (City) e.g. QUITO	YES		OID 2.5.4.7
1.6.3. Organization Name (O)	Name of the Legal Entity (Public or Private) Owner of the Firm. 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 is specified	No		OID 2.5.4.11
1.6.5. Organization Identifier	Unique Taxpayer Registration Number of the legal entity (Public or Private) Holder of the Signature to which the Electronic Seal "VAT(CÓDIGO_PAIS)-RUC is linked Ex. VATEC-1716151413001	No		OID 2.5.4.97coding according to ETSI EN 319 412-1RFC 5280 establishes as non-mandatory
1.6.6. Serial Number	Unique Taxpayer Registration Number of the Legal Entity (Public or Private)E.g. "1716151413001"	YES		OID 2.5.4.5
1.6.7. Common Name (CN)	Description of the use that will be given to the Electronic Seal. RECEIPT OF DOCUMENTS AT A SINGLE WINDOW	YES		OID 2.5.4.3
1.6.8. Surname	Surname of the Signatory that will be linked to the seal (as stated in the official document)	YES		OID 2.5.4.4
1.6.9. Given Name	Names of the Signatory who will be linked to the seal (as stated in the official document)	YES		OID 2.5.4.42
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 commintment	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.102.2.4.2	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	"ELECTRONIC SEAL CERTIFICATE 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	Email of the Legal Entity (Public or Private) Holder of the Signature (electronic seal) "info@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		It is only activated if the email address of the Legal Entity (Public or Private) Holder of the Signature (electronic seal) 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://) IETFRFC 4516 [4] scheme
2.7.2. distributionPoint	(http://crl2.example.com/example2subordinada.crl)	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETFRFC 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
2.8.2.1. Access Method	id-ad-calssuers	YES		OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	(http://www.example.com/subordinate1.crt)	No		URL Access to AC(http://) IETF RFC 7230-7235 [3] or (https://) IETF RFC 2818 [5] certificate
2.9. Basic Constraints		YES	YES	OID 2.5.29.19
2.9.1. cA	FALSE	YES		

7.1.1. Version Number.

Specified in the Certificate Profile.

7.1.2. Certificate Extensions.

Specified in the Certificate Profile.

7.1.3. Algorithm Object Identifiers.

Specified in the Certificate Profile.

7.1.4. Forms of names.

Specified in the 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.

Name limitation is done by issuance profile, subject template, and allowed fields, so certificates issued under this policy must: Contain a Subject DN aimed at identifying the electronic seal service that includes C, L, O, CN, OU, Serial Number, and Organization Identifier fields.

7.1.6. Certificate Policy object identifier.

The OID of the certificates is:

- File OID: 1.3.6.1.4.1.37746.2.4.1
- DSCF OID: 1.3.6.1.4.1.37746.2.4.2

7.1.7. Use of the Policy Restrictions extension.

The X.509 "Policy Constraints" extension under OID 2.5.29.36 is not used in the certificates in this policy. Therefore, no technical restrictions of "requireExplicitPolicy" or "inhibitPolicyMapping" are applied within the final certificate.

7.1.8. Syntax and Semantics of the Qualifiers of Politics.

Certificates include the Certificate Policies extension with OID 2.5.29.32 with: a SECURITY DATA's own policy OID for the certificate type, and qualifiers to document and explain the applicable policy.

Supported qualifiers and meaning:

- CPS URI with OID 1.3.6.1.5.5.7.2.1: Public URL to the specific PC document applicable to the certificate.
- User Notice with OID 1.3.6.1.5.5.7.2.2: Informational text that describes the use or type of the certificate.

- Electronic seal on file
  - Policy OID: 1.3.6.1.4.1.37746.102.2.4.1
  - CPS: https://www.securitydata.net.ec/normativas/pc_se.pdf
  - User Notice: "ELECTRONIC SEAL CERTIFICATE ON FILE"

- Electronic Seal in DSCF
  - Policy OID: 1.3.6.1.4.1.37746.102.2.4.2
  - CPS: https://www.securitydata.net.ec/normativas/pc_se.pdf
  - User Notice: "ELECTRONIC SEAL CERTIFICATE ON SECURE SIGNATURE CREATION DEVICE - DSCF

7.1.9. Processing Semantics for Critical Certificate Policy Extension.

On attached certificates, the Certificate Policies extension with OID 2.5.29.32 is issued as NOT critical.

If an application/verifier does not process Certificate Policies because it is non-critical, it can accept the string following standard validations of signature, validity, revocation, EKU/KU, etc., as long as the use case does not require policy validation.

If the use case requires e-seal policy validation, the certificate must be verified to contain the expected policy OID for that use.

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.

7.2.2. CRLs and CRL input extensions.

CRLs and extensions are defined in the Security Data DPCs.

7.3. 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
- Contains the OCSP No Check extension to allow relying parties not to require additional revocation verification of this certificate during OCSP validation.
- Publishes CRL Distribution Points and Authority Information Access points for string and issuer fetching.

7.3.1. 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.

7.3.2. 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.
    - 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 caIssuers 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.

8. Compliance audits and other controls.

The SECURITY DATA Certificate issuance system is audited to keep the Webtrust Seal active.

8.1. FREQUENCY OF AUDITS.

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

Webtrust seal maintenance audits are conducted annually.

8.2. QUALIFICATION OF THE AUDITOR.

Audits can be internal or external. In this second case, they are carried out by companies of recognised 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.
However, SECURITY DATA 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 makes public the Business and Certificate Management Practices in the 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 the management of the life cycle of keys and certificates 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 TAKEN AS A RESULT.

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

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

8.6. COMMUNICATION OF RESULTS.

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

9. Other Business and Legal Matters.

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. Revocation or status Information Access 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. Fee 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. Refund Policy.

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 certificate within a maximum period of 72 hours.

9.2. FINANCIAL RESPONSIBILITY.

9.2.1. Insurance Coverage.

The insurance covers all contractual and non-contractual damages of SECURITY DATA's client holders, who trust SECURITY DATA to be free of fault arising from errors and omissions, or acts of bad faith by the administrators, legal representatives or employees of the SECURITY DATA Certification authority in the development of the activities for which it is authorised.

9.2.2. Other Assets.

No stipulation

9.2.3. Insurance or Guarantee of Coverage for Final Entities.

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

9.3. CONFIDENTIALITY OF BUSINESS 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:

- That contained in this PC 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 publicity is required by law

9.3.3. Duty to Protect 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 that established in current regulations, in the terms and conditions published. With regard to the protection of personal data, the applicable regulations in this area will apply, especially the Organic Law on the Protection of Personal Data (LOPDP), its regulations and other provisions issued by the competent authority.
Security Data will also implement appropriate technical and organisational measures to ensure the security of the personal data processed.

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 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.

It is 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.

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

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

- Issue Certificates in accordance with this PC and the provisions of the CPS and the applicable standards.
- Issue Certificates whose minimum content is defined in the current PC and CPS.
- Issue Certificates according to the information in their possession and free of data entry errors.
- To keep your own private keys under your sole control by using reliable systems and products to store them in a way that ensures their confidentiality and makes them inaccessible to unauthorized persons, preventing their loss or disclosure.
- Issue the requested Certificates in accordance with the provisions of the CPS, in the PC and, where appropriate, in the corresponding certification service provision contracts.
- Likewise, it issues the electronic seals according to the information in its possession and free of data entry errors, delivering the services with the reliability and accuracy established in the respective contracts and in this document.
- Use reliable systems and products that are protected against alteration and that guarantee the technical security, and where appropriate, cryptography of the certification processes to which they support.
- Publish the certificates issued in accordance with the provisions of the Law on Electronic Commerce, Electronic Signatures and Data Messages.
- Protect personal data as established in the Law on Electronic Commerce, Electronic Signatures and Data Messages, and the Organic Law on the Protection of Personal Data.
- Use reliable systems to store recognised certificates to verify their authenticity and prevent unauthorised persons from altering data.

9.6.2. RA Representations and Warranties.

The responsibilities of the registry entity are as follows:

- Verify the identity of certificate applicants, as well as the veracity of the information and documents provided.
- Respect the provisions of the CPS and PC.
- Provide the minimum information necessary for the use of the certificates to the applicant, whose information must be transmitted free of charge, in writing or electronically.

- Take measures against certificate forgery and ensure the confidentiality of signature creation data during the generation process, as well as its delivery by a secure procedure to the subscriber.
- Do not copy or store subscriber signature creation data.
- Protect the personal data of applicants and users of digital or electronic certificates.

9.6.3. Subscriber Representations and Warranties.

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

- Comply at all times with the rules and regulations issued by Security Data in its CPS and the corresponding Certificate Policies.
- Notify Security Data of any modification or variation of the data provided to obtain the Electronic Seal Certificate.
- Verify, through the List of Revoked Certificates, the status of the Electronic Seal Certificates.
- Protect and preserve the Secure Signature Creation Device.\or in turn access to the certificate in software.
- The revocation of the certificate and the issuance of a new one to Security Data in case of forgetting the protection key of the Electronic Seal Certificate.
- To be responsible for the use of the Electronic Seal Certificate and the consequences arising from its use.
- Comply with the provisions of Article 17 of the Law on Electronic Commerce, Electronic Signatures and Data Messages.
- Respect the provisions of the legal instruments binding on the CA.
- The Subscriber shall be liable for any damages caused by the failure to perform its respective obligations listed in this PC.

9.6.4. Representations and Warranties of the Relying Party.

The responsibilities of trusted third parties are as follows:

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

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 PC and CPS.

9.8. LIMITATIONS OF LIABILITY.

To the extent that the SECURITY DATA CA has issued and managed the time-stamping certificate in accordance with the PC/CPS, 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 CPS or for any other liability they may incur in contract, tort or other, including liability for negligence by subscriber or trusted third party or third party by certificate, provided that the subscriber, trusted third party, or third party is in full compliance with such CP and CPS.

SECURITY DATA's liability to any person for damages arising under, outside or in connection with this PC and 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 CPS and Certification Policy document, and any amendments will remain in effect until amended or 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.

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 owners and subscribers, in accordance with the means specified in their contracts.

9.13. DISPUTE RESOLUTION PROVISIONS.

The dispute resolution procedure will be defined in the contracts of the holders.

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 and are not entitled to assign any of their rights or obligations hereunder without the prior written consent of SECURITY DATA.

9.16.3. Severability.

If any provision of this Certification Policy and Practices Statement is held 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 responsibility for any delay or failure to perform an obligation under its Statement of Practice 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	