CERTIFICATION PRACTICES STATEMENT (CPS)

OF

SECURITY DATA, SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A.

Version 10.2

Index

1. LEGAL FRAMEWORK

1.1. Legal base

Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos, its Regulations; Organic Law on Consumer Protection, Organic Law on Transparency of Information and Accreditation of CONATEL.

1.2. Validity

This document will become effective from the date of its approval.

1.3. Legal Support

1. Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos, published in the Official Register No. 577 of April 17, 2002.

2. In accordance with the provisions of Article 37 of the Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos, the National Telecommunications Council is the Agency for the authorization, registration and regulation of Accredited Information Certification Entities and Related Services.

3. General Regulations to the Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos, issued by Executive Decree No. 3496 published in the Official Gazette 735 of December 31, 2002, and constant reforms in Executive Decree 1356 of September 29, 2008, published in the Official Gazette No. 440 of October 6, 2008.

4. That, the second article listed added by article 4 of Executive Decree No. 1356 after article 17 of the General Regulations to the Law of Electronic Commerce, Electronic Signatures and Data Messages, provides that the accreditation as an entity of certification of information and related services, will consist of an administrative act issued by CONATEL through a resolution that will be registered in the National Public Registry of Accredited Information and Related Services Certification Entities and Related Third Parties.

5. Resolution 477-20-CONATEL-2008 of October 8, 2008, approved the resolution model for Accreditation as an Information and Related Services Certification Entity.

6. Resolution No. TEL-640-21-CONATEL-2010 of October 22, 2010, approved the request for Accreditation of the Company SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL SA as Information and Services Certification Entity

   Related, for which SENATEL signed the respective administrative act, according to the model approved by the CONATEL.

1.4. Conflict Resolution Process

The differences that arise between the parties on this Service during its execution or due to its interpretation will be resolved in the first instance directly between the User and SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL SA

If there is no such agreement, they may submit the dispute to the mediation process as an alternative conflict resolution system recognized constitutionally, for which the parties stipulate to go to the Mediation Center of the State Attorney General's Office.

The mediation process will be subject to the Arbitration and Mediation Law and the Operating Regulations of the Mediation Center of the State Attorney General's Office.

If an Act of total agreement is signed, it will have the effect of an enforceable judgment and res judicata and its execution will be in the same way as the judgments of last resort following the enforcement route, as provided in Art. 47 of the Law of Arbitration and Mediation.

If there is no agreement between the parties, they will sign the respective act of impossibility of agreement, and the controversy will be heard before the competent District Court of Contentious-Administrative Matters.

In the case of subscribing minutes of partial agreement, they will have the effect of res judicata on the agreed matters; and in the case of aspects on which there is no agreement, these will be resolved before the competent District Court of Administrative Litigation.

The applicable legislation is Ecuadorian.

1.5. Protection of Intellectual Property Rights

Public key certificates and CRLs issued by the CA are the property of the CA. This CPD and related certificate policies are the property of the CA

2. INTRODUCTION

2.1. Presentation

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 for electronic signatures and digital certificates.
Security Data is a company constituted according to Ecuadorian legislation, registered in the commercial register under number 2246 on July 13, 2010, with legal existence until July 13, 2060.
The Information Certification Services and Related Electronic Services offered by Security Data Seguridad en Datos y Firma Digital S.A are aimed at individuals, Public and Private Corporations (such as companies, public entities) and their objective is to accredit the digital identity of corporations and companies. natural persons acting through the Web.

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

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

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

2.2.Document Name

2.2.1. ID

Name:	CERTIFICATION PRACTICES STATEMENT (CPS)
Version:	10.2
Description:	Statement of Security Data Certification Practices Data Security and Digital Signature SA

Date of issue:	18 March 2021
Contact person:	Lenin Alberto Vasquez Gonzalez
Email:	Lenin.vasquez@securitydata.net.ec
Address:	Alonso de Torres y Av. Del Parque
Telephone number:	023922169 Ext 5001
Website:	www.securitydata.net.ec
Name: Company:	Security Data Seguridad en Datos y Firma Digital S.A
Email:	info@securitydata.net.ec
Address:	Alonso de Torres y Av. Del Parque
C8 Telephone number:	023922169 Ext 5001
Website:	www.securitydata.net.ec

2.2.2. Publication

This document can be obtained free in the following link.
https://www.securitydata.net.ec

The types of certificate issued by Security data can be found at the following URLs:

Persona Natural-Natural Person
https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/Politicas%20de%20Certificado%20Persona%20Natural.pdf

Representante Legal-Legal Representative
https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/Politicas%20de%20Certificado%20Representante%20Legal.pdf

Miembro de Empresa- Company Member
https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/Politicas%20de%20Certificado%20Miembro%20de%20Empresa.pdf

2.2.3. State certificates

2.2.3.1. root CA certificate

https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema_Windows/cacert.cer

2.2.3.2. CA subordinate root certificate

https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema_Windows/subcert.cer

2.2.3.3. Subordinate root certificate SUBCA-1

https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema_Windows/SUBCA-1.cer

2.2.3.4. CA-2 root certificate

https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema_Windows/SECDATA-CA-2.cer

2.2.3.5. Subordinate root certificate SUBCA-2

https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema_Windows/SECDATA-SUBCA2.cer

2.3.Definitions and Acronyms

2.3.1. Definitions

- **Electronic Certificate:** It is a electronic document signed by a certification service provider that links signature verification data to a signatory and confirms their identity.
- **Recognized Certificate:** Certificate issued by an Accredited Entity that meets the requirements established in the Law regarding verification of the identity and other circumstances of the applicants and the reliability and guarantees of the certification services they provide.
- **Public Key and Private Key:** The asymmetric cryptography on which PKI is based uses a pair of keys (it could be two pairs of keys), what is encrypted with one of them can only be decrypted with the other and vice versa. One of these keys is called public and is included in the electronic certificate, while the other is called private and is only known by the holder of the certificate.

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

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

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

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

- **Advanced Electronic Signature:** It is that electronic signature that allows establishing the

personal identity of the subscriber in regard to the signed data and verifying the integrity of the same, as it is exclusively linked to both the subscriber and the data to which it refers, and for having been created by means that it maintains under its exclusive control.

- **Hashing function:** It is an operation that is performed on a data set of any size, so that the result obtained is another data set of fixed size, regardless of the original size, and that has the property of being uniquely associated with the initial data.
- **Certificate Revocation Lists (CRL):** list that contain the relationships of revoked or suspended certificates.
- **Hardware Cryptographic Module (HSM):** Module hardware used to perform cryptographic functions and store keys in secure mode.
- **Time stamp:** Electronic annotation signed electronically and added to a data message that includes at least the date, time and identity of the person making the annotation.
- **Time Stamping Authority (TSA):** Trusted entity that issues time stamps.
- **Validation Authority (VA**): Trusted entity that provides information on the validity of digital certificates and electronic signatures.
- **Linked Third Party:** Trusted entity that provides and/or manages certification services.

2.3.2. Acronyms

CA:	Certification Authority
Sub CA:	Subordinate Certification Authority
RA:	Registration Authority
CP:	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
CSP:	Certification Services Provider
TSA:	Time Stamp Authority
VA:	Validation Authority
ECI:	Information Certification Entity
OID:	Unique object identifier
DN:	Distinguished Name
C:	Country
CN:	Common name
O:	Organization
OU:	Organizational Unit
SN:	Surname
ISO:	International Organization for Standardization
PKCS:	Public Key Cryptography Standards,
UTF8:	Unicode Transformation Format – 8 bits.

2.4.General features

2.4.1. Obligations

2.4.1.1. Obligations of the CA

- Issue Certificates in accordance with this CPS and the corresponding CPs and the application standards.
- Issue Certificates whose minimum content is defined in the current Certificate Policies.
- Issue Certificates according to the information in their possession and free of data entry errors.
- Keep your own private keys under your exclusive control using reliable systems and products to store them in a way that guarantees 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 CPs of each type of Certificate and, where appropriate, of the corresponding certification service provision contracts and in the Agreement for the Registration Authority.
- Facilitate access to the current versions of the CPS and PCs of each type of Certificates.

- Offer and maintain the necessary infrastructure for the certification services, as well as the physical, procedures and personal security controls necessary for the practice of the certification activity.
- Use reliable systems and products that were protected against alteration and that guarantee the technical security, and where appropriate, cryptography of the certification processes that they serve as support.
- Publish the certificates issued in accordance with the provisions of the Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos.
- Protect personal data as established in the Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos and Ley Organica de Protección de Datos.
- Use reliable systems to store recognized certificates that allow their authenticity to be verified and prevent unauthorized persons from altering the data.
- The revocation information available to those who wish to verify an electronic signature with reference to said certificates, can be found at the URL which will be published on the website https://www.securitydata.net.ec/firma-electronica-en-ecuador/
- 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 the forgery of certificates and guarantee the confidentiality of the signature creation data during the generation process, as well as its delivery by a secure procedure to the subscriber.
- Do not copy or store the subscriber's signature creation data.
- Inform about the modifications of the Certificate Policies and the Certification Practices Statement to the Subscribers and related Third Parties.
- Comply with the obligations of this CPS.
- All those obligations imposed by this CPS and, where appropriate, in the Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos.
- Approve or deny requests for the issuance of electronic signature digital certificates, in accordance with the provisions of this CPS and in the CPs.
- Make available to usersthe list of revoked certificates (CRL), the exact url are detailed in point 5.11.1 of this document.
- Custody by any secure means all the information and documentation related to a recognized certificate and the declarations of certification practices in force at any time, for at least 15 years from the time of issue, so that the signatures made with the certificate can be verified. same. For these purposes, the SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A stores in digital or paper format all the published versions of the CPS and a copy of the contract for the provision of services between the Information Certification Entity and the subscriber.
- Immediately notify the holders of the certificates issued by the ECI, the compromise of their private key, loss, disclosure, modification, unauthorized use, in order to revoke them.
- Carry out the identification and authentication of users as steps prior to the revocation of electronic signature certificates.
- Protect the personal data of applicants and users of digital certificates or electronics.
- Carry out each of the steps described in the procedure for issuing electronic signature

certificates.

- Implement and maintain the security requirements imposed on the private key of the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A, in accordance with this CPS and PCs.
- Offer and maintain the necessary technological infrastructure to establish a structure, both in hardware and software, to operate in accordance with international standards.
- Present the updated list of linked third parties that are part of the Security data certification entity approved by Arcotel, which can be consulted at the following link:
  either https://www.securitydata.net.ec/wp-content/downloads/terceros_vinculados.pdf

2.4.1.2. Obligations of the Linked Third Party

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

- Correctly identify and authenticate the Subscriber and/or Applicant and/or the organization they represent, in accordance with the procedures established in this CPS and in the specific Certification Practices for each type of Certificate, using any of the means admitted by law.
- Formalize the certificate issuance contracts with the Subscriber under the terms and conditions established by the CA.
- Safely store and for a period never less than 15 years the documentation provided in the process of issuing the Certificate and in the process of suspension / revocation of the same, under the terms and conditions established in this CPS, in the PC of each type of certificate and, if applicable, in the agreement for the Linked Third Party
- Carry out any other function that corresponds to them, through the personnel that is necessary in each case, as established in this CPS and in the CP of each type of certificate and, where appropriate, the Agreement for the Linked Third Party
- In any case, the Linked Third Party will allow ECI SECURITY DATA SECURITY IN DATA AND DIGITAL SIGNATURE access to the files and the file conservation procedures assumed by the Linked Third Party and will give it the right to investigate any suspected breach of the CPS and/or PCs by the Linked Third Party or any holder of a Certificate. The Linked Third Party and the holders of any Certificate must immediately inform ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A of any suspected infringement.

2.4.1.3. Applicant Obligations

- Pay the registration fees that correspond by virtue of the services they request.
- Provide the Linked Third Party or the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A with the necessary information to carry out a correct identification.
- Confirm the accuracy and veracity of the information provided.
- Notify any change in the data provided for the creation of the certificate during its validity period.

- Request the certificate as stipulated in the terms and conditions established in the CP of each type of Certificate and, where appropriate, in the Contract for the provision of certificate services signed with the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A .

2.4.1.4. Subscriber Obligations

- Comply at all times with the rules and regulations issued by the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A in its CPS and the corresponding Certificate Policies.
- Communicate to the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A any modification or variation of the data provided to obtain the Electronic Signature Certificate.
- Verify, through the List of Revoked Certificates, the status of the electronic signature Certificates.
- Protect and conserve the Secure-Token Portable Device and the access to the software certificate.
- Request the revocation of the certificate and the issuance of a new one to the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A in case of forgetting the protection key of the Electronic Signature Certificate.
- Respond for the use of the Electronic Signature Certificate and the consequences arising from its use.
- Comply with the provisions of article 17 of the Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos.

2.4.1.5. Obligations of the Users

- Users who intend to trust and use the Certificates issued by the CA must verify the validity of the signatures issued by the Subscribers.
- In the event that Users would not proceed to verify the signatures through the CRL (List of Revoked Certificates), ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A is not responsible for the use and trust that users make of these Certificates. .
- Every person shall have the right to rely on an electronic signature issued through an ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A certificate to the extent that it is reasonable to do so.
- To determine if it is reasonable to trust; The following must be taken into account:
- The nature of the corresponding operation that the firm intends to guarantee. It will not be considered reasonable to trust a signature issued by an ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A certificate if said operation can be considered improper use.
- Whether the relying party has taken appropriate steps to determine the reliability of the signature, and in particular whether it has verified that the certificate is not expired, suspended, or revoked. The expiration will be stated in the Certificate itself. The possible suspension or revocation of the certificate must be consulted in the list of revocation or

suspension of certificates (CRL).

- Whether the relying party knew or should have known that the signature was compromised or had been revoked or suspended.
- The policies and procedures that govern the activity of the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A in relation to the different Electronic Signatures made with the types of certificates issued by the ECI SECURITY

- DATA SECURITY IN DATA AND DIGITAL SIGNATURE, policies and procedures that are specified in this CPS and in the CPs for each different type of certificate.

2.4.2. Responsibilities

2.4.2.1. CA Responsibility

- Guarantee compliance with the responsibilities and obligations described in this CPS; and the provisions of the Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos, and its Regulations.
- The ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A, solely and exclusively, will be liable for damages caused to any person, when he fails to comply with his legal obligations derived from the legislation in force in the Republic of Ecuador or when he acts with negligence in the provision of certification services.
- ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A shall not be liable for any damage arising from or related to the non-execution or faulty execution of the obligations by the Applicant, Subscriber and/or User.
- The ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A will not be responsible for the negligent or malicious use of the certificates and keys.
- The ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A shall not be liable for damages arising from negligent or malicious actions by third parties in relation to the certificates issued by it in favor of a specific subscriber.
- The ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A will not be responsible for any inaccuracies in the Certificate resulting from the information provided by the Subscriber, provided that they have always acted with the maximum negligence required.
- The ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A will not be responsible for the damages derived from those operations in which the limitations of use that are indicated in the CPs corresponding to each type of certificate have been breached.
- The ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL will not assume any responsibility for the non-execution or the delay in the execution of any of the obligations under this CPS if such non-execution or delay resulted or was the consequence of an assumption of force majeure, fortuitous event or, in general, any circumstance over which ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A cannot have reasonable control.
- ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A will not be responsible for the content of digitally signed electronic documents. Neither the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL nor its registration

authorities will be responsible in any case for the damages caused by the employment of its public certification services in these environments.

- The ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A has the proper guaranteed policy, which is renewed every year and delivered to the regulatory body in accordance with the regulations and requirements of ARCOTEL
- The conditions general of the policy I know they can consult the following linkhttp://www.securitydata.net.ec/ayuda-security-data-ecuador/in the regulations section, item 17. "Guarantee" where you will find the updated information of the policy.

2.4.2.2. Responsibility of the Linked Third Party

- The Linked Third Party will be responsible for the functions that correspond to it in accordance with this CPS and will assume all responsibility for the correct identification and validation of the Applicant/Subscriber, with the same limitations established in the previous section in relation to the ECI. SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A.
- The Linked Third Party shall be liable to the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL for any damages that may arise from the execution of these functions arranged negligently or in a manner other than that contemplated in this CPS and in the CPs issued for each type of certificate.
- However, the Linked Third Party is not responsible, in any case, for the identity or identification of the applicant and/or subscriber in the event of falsification of the documentation or other data provided, by himself or by the third party that impersonates him.

2.4.2.3. Subscriber Responsibility

- The Subscriber will be responsible for the damages caused by the breach of their respective obligations listed in this CPS.
- The Subscriber will be responsible for complying with all those obligations imposed by this CPS, the CPs of each type of Certificate, and by current regulations regarding the provision of certification services.
- The Subscriber undertakes to indemnify ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL for damages that may be caused by any culpable or intentional act or omission on its part, also assuming the procedural costs in which ECI SECURITY DATA SEGURIDAD EN DATOS Y DIGITAL SIGNATURE may incur for this reason, including the professional fees of Lawyers and Solicitors.
- The Subscriber shall indemnify and hold ECI SECURITY DATA SECURITY IN DATA AND DIGITAL SIGNATURE harmless for any damage that it may suffer due to the total, partial or defective fulfillment of the obligations assumed and based on any claim directed against it by any third party with the that the subscriber had contracted.

2.4.2.4. User Responsibility

- The User will be responsible for the damages caused by the breach of their respective obligations listed in this CPS.
- The User will be responsible for complying with all those obligations imposed by this CPS, the CPs of each type of Certificate, and by current regulations regarding the provision of certification services.
- In any case, the User will assume all the responsibility and risks derived from the acceptance of a Certificate without having observed the obligations contained in the CPS and, where appropriate, in the specific CPs of each certificate, guaranteeing full indemnity of the ECI SECURITY DATA SECURITY IN DATA AND DIGITAL SIGNATURE for said concept.

2.4.3. Participating Entities

2.4.3.1. Accredited Entity (AE)

Security Data Security in Data and Digital Signature is an Accredited Entity (EA) that issues recognized certificates according to the Law of Electronic Commerce, Electronic Signatures and Data Messages. Security Data Security in Data and Digital Signature is the issuing entity of the certificates and responsible for the life cycle operations of the certificates. The functions of authorization, registration, issuance and revocation with respect to the personal certificates of the final entity, may be carried out by other entities by delegation supported contractually with Security Data Seguridad en Datos y Firma Digital S.A, which will act as intermediaries. Security Data Seguridad en Datos y Firma Digital S.A also offers electronic signature validation and time stamping services, governed by its policies, not included in this document.

2.4.4. Certification Authority (CA)

The Security Data Security Data and Digital Signature certification system is made up of various Certification Authorities (in English CA or Certificate Authority) organized under a Certification Hierarchy.

2.4.4.1. Root Certification Authority

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

2.4.4.2. Linked Third Party

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

- Process certificate requests.
- Identify the applicant and verify that they meet the necessary requirements for requesting 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 issuing the certificate to the subscriber and, if applicable, deliver the cryptographic device

They may act as a Linked Third Party of Security Data Seguridad en Datos y Firma Digital S.A:

- Any trusted entity that reaches 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 itself Security in Data and Digital Signature directly.

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

The entity that acts as a Linked Third Party of Security Data Seguridad en Datos y Firma Digital S.A may authorize one or several persons as Operator of the Linked Third Party to operate with the Security Data Security Data Security and Digital Signature certificate issuing computer system on behalf of the Linked Third Party.

Where the geographical location of the subscribers represents a logistical problem for the identification of the subscriber and in the request and delivery of certificates, the Linked Third Party or Security Data may delegate these functions to another entity or trusted person called a mobile agent. 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 Linked Third Party or with Security Data accepting the delegation of these functions. Security Data Seguridad en Datos y Firma Digital S.A must know and expressly authorize the agreement.

2.4.5. Applicant

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

2.4.6. 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, it will be the owner of the certificate.

2.4.7. Signatory

The Signatory is the person who has a signature creation device or access to the software signature certificate and who acts on their own behalf or on behalf of a legal person they represent.

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

2.4.8. Keeper of the Keys

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

2.4.9. Third party that trusts the Certificates

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

The recognized certificates issued by Security Data Seguridad en Datos y Firma Digital S.A are universal in nature and are accepted by 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 that voluntarily trust the certificates will be limited to those included in this CPS

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

2.5.Types of Certificates

2.5.1. Recognized Corporate Certificates

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

- Corporate Certificates of Legal Representative: These are recognized certificates of a natural

person that identify the subscriber as a corporation and the signer as the legal representative of said corporation.

- Company Member Corporate Certificates: These are recognized certificates of a natural person that identify the subscriber as a corporation and the signer as linked to that corporation as an employee.

2.5.2. Private Certificates

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

2.5.3. Secure Server Certificates

Secure Server Certificates: These are certificates that link an Internet domain with a legal entity or a specific registered merchant.

2.6.Support Types

Corporate, Public Administration or Private Certificates can be generated in two types of hardware support, software:

2.6.1. Secure Signature Creation Device (DSCF)

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

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

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

To activate the DSCF it will be necessary to enter the activation code (PIN). If the PIN is entered incorrectly six times in a row, the device will be locked and therefore unusable. To proceed with the unlocking, you must approach the Linked Third Party where you purchased the certificate with the locked device or send it to it, where the unlocking will take place. The PIN is secret and personal for the user, an initial PIN will be given to the user, which must be modified later by the user using the corresponding applications.

2.6.1.1. DSCF Distribution

The DSCF distributed by Security Data after validating the identity of the subscriber is delivered in

two ways:

- directly to the subscriber
- To a third party authorized by the subscriber

2.6.1.2. DSCF life cycle

The life cycle of the DSCF depends on the technical sheet provided by the supplier.

2.6.2. Software Support

2.6.2.1. Certificates, Public and private keys in Software

This service allows the user, after having made the request and being approved by the Certifying Entity and after having received the generation codes, to access the Security Data portal and be able to generate the digital certificate with their public and private keys, storing it in the Windows CAPI of the client's PC or as an EPF file or as a file with a .p12/.pfx extension in it, being the use of these certificates to sign and encrypt documents and for encrypted mail.

2.6.2.2. Certificates, public and private keys for Secure Web server - SSL

This service allows the user, after having made the request and being approved by the Certifying Entity, to relate an Internet domain with a Legal Entity or a registered merchant and once he has received the generation codes, he can access the Security Data portal and can generate the digital certificate, once it has generated the request on the Web Server, allowing it to be stored on the Server in a .CER format. Being the use of these certificates for the implementation of Secure Web servers.

2.7.Private use of certificates

2.7.1. Appropriate uses of certificates

- The certificates do not have a technical, administrative, financial, etc. limitation. for your use.
- The subscriber may use the Electronic Signature certificate as established in this certificate policy, in the service provision contract signed with ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A, and the CPS.
- It will be considered that a Certificate is misused when it is used to carry out unauthorized operations according to the Certificate Policies applicable to each of the Certificates, and the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A contracts with its subscribers. As a consequence of this, the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A may revoke the certificate and terminate the contract.
- The authorized uses of the Certificates issued by the ECI SECURITY DATA SEGURIDAD

EN DATOS Y FIRMA DIGITAL S.A may be specified in each type of certificate.

- If the subscriber's certificate is found to be compromised during the validity period, that is, its private key, it must initiate the revocation procedure as mentioned in this CP, and in the CPS.
- The electronic signature certificate issued by ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A 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 illicit actions, in accordance with the provisions of Ecuadorian legislation.
- The electronic signature certificates present the following guarantees:

    - **Authenticity:** The information on the document and its electronic signature undoubtedly correspond to the person who signed it.
    - **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 their authorship.
    - **Confidentiality:** The information contained has been encrypted and by the will of the issuer, only the receiver is allowed to decrypt it.
- The purpose of using the ac keys is established in the x509 v3 standard.
- The root digital certificate can only be used for the identification of the root certification authority itself and for the distribution of its public key in a secure manner.

2.8.Unauthorized Uses of Certificates

Use that is contrary to Ecuadorian and community regulations, international conventions ratified by the Ecuadorian state, customs, morality and public order is not allowed. The use other than what is established in this Certification Practices Statement and in its corresponding Certification Policy is also not allowed.

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

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

2.9.Policy Administration

2.9.1. Responsible Organization

The Technical Department of Security Data Seguridad en Datos y Firma Digital S.A is responsible

for the administration of this CPS and the Certification Policies.

2.9.2. Review Frequency

The CPS and the different CPs will be reviewed and, if applicable, updated, annually or when a change occurs.

2.9.3. Approval Procedure

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

3. REPOSITORIES AND PUBLICATION OF INFORMATION

3.1.Repositories

The Security Data Seguridad en Datos y Firma Digital S.A repositories are referenced by the URLhttps://repository.securitydata.net.ec/security1/ . Any change in the URLs will be notified to all entities that may be affected. The IP addresses corresponding to each URL may be multiple and dynamic, and may be modified without prior notice.

3.2.Publication of information

3.2.1. Certification Policies and Practices

Both the current CPS and the Certification Policies for each type of certificate will be available in electronic format on the Security Data website Data Security and Digital Signature.

Previous versions will be withdrawn from online consultation but may be requested by interested parties at the Security Data Seguridad en Datos y Firma Digital S.A contact address.

3.2.2. Terms and Conditions

The contractual relationship between Security Data Seguridad en Datos y Firma Digital S.A and the Subscribers is based on the signing of a Certification Services Provision Contract and the acceptance of the General Contracting Conditions of Security Data Seguridad en Datos y Firma Digital S.A published in its Web.

3.2.3. Dissemination of Certificates

The Subscriber of the certificate will be responsible for sending their certificate to any third party that wishes to authenticate a user or check the validity of a signature. This shipment will generally be made automatically, attaching the certificate to any electronically signed document.

Security Data Seguridad en Datos y Firma Digital S.A is not obliged to publish the issued certificates in a public access repository. However, in order to improve customer services, Security Data Seguridad en Datos y Firma Digital S.A could offer Directory and search and download services for some certificates issued under its certification hierarchy.

3.3.Posting Frequency

The Root CA will issue a List of Revoked CAs (ARL) at least every six months, or extraordinarily, when an authority certificate is revoked.

Each Subordinate CA will issue a List of Revoked Certificates (CRL) daily, and extraordinarily, each time a certificate is suspended or revoked.

Security Data Seguridad en Datos y Firma Digital S.A will immediately publish any changes in the certification policies and practices.

3.4.Repository access control

The CPS, the Certification Policies, the General Conditions of Contract, the CA certificates and the lists of revoked certificates (CRL) will be published in public access repositories without access control.

The issued certificates may be published in public or restricted access repositories according to the needs. The validation services for the OCSP protocol and time stamping for the TSP protocol will be services with restricted access and payment.

4. IDENTIFICATION AND AUTHENTICATION

4.1.Name Registry

4.1.1. Types of Names

All certificates require a distinguished name (DN or distinguished name) according to standard X.500. Additionally, 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 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile",
- RFC 3739 "Qualified Certificates Profile".

4.1.2. Need for names to be meaningful

The fields of the DN referring to the Name and Surname 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.

In the event that the data consigned in the DN is fictitious or its invalidity is expressly indicated (eg "TEST" or "INVALID"), the certificate will be considered without legal validity, only valid to carry out technical interoperability tests.

4.1.3. Rules for interpreting various name formats

Security Data Seguridad en Datos y Firma Digital S.A attends in any case to what is marked by the standard X.500 referenced in ISO/IEC 9594.

4.1.4. uniqueness of names

The distinguished name (DN) of the issued certificates will be unique for each subscriber or signer. The CIF or NIF attribute is used to distinguish between two identities when there is a problem of name duplication.

4.1.5. Naming conflict resolution

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

4.1.6. Verification of the powers of representation

The verification of the representation of the applicant before Security Data will be carried out by verifying the documentation according to the type of certificate established in the regulations through its regulatory body, Arcotel.

4.2.Initial Identity Validation

4.2.1. Private Key Possession Proof Method

When a certificate is issued on a hardware device, the private key is created just before the certificate is generated, through a procedure that guarantees its confidentiality and its link to the applicant's identity.

Each Linked Third Party is responsible for ensuring that the device is safely delivered to the applicant.

In other cases, the method of proof of the possession of the private key by the subscriber will be the delivery of PKCS#10 or an equivalent cryptographic proof or another method approved by Security Data Seguridad en Datos y Firma Digital S.A.

4.2.2. Authentication of the Identity of a Legal Entity

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

- The data related to the name or company name of the organization.
- The data related to the constitution, and legal personality of the subscriber.
- Data relating to the extension and validity of the powers of representation of the applicant.
- The data related to the tax identification code of the RUC organization.

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

4.2.3. Authentication of the identity of a natural person

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

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

The Linked Third Party will verify, either by displaying sufficient original documentation, or with its own sources of information, photography and the rest of the data and attributes to be included in the certificate (distinguished name of the certificate), and must keep the documentation accrediting the validity of data that you cannot verify using your own data sources.
If it is a professional natural person, the data of the profession will be verified with the competent Entity.

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

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

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

- Security Data Seguridad en Datos y Firma Digital S.A will verify the existence of the entity through its own sources of information.
- An authorized representative of the organization must sign a contract with Security Data Seguridad en Datos y Firma Digital S.A, specifying the specific aspects of the delegation and the responsibilities of each agent.
- In addition, the Linked Third Party will be required to comply with the following with respect to the operators of the Linked Third Party:
    - Verify and validate the identity of the new operators of the Linked Third Party. The Linked Third Party must send Security Data Seguridad en Datos y Firma Digital S.A the documentation corresponding to the new operator, as well as its authorization to act as a Linked Third Party operator.
    - Ensure that the operators of the Linked Third Party have received sufficient training to perform their duties, attending at least one operator training session.
    - Ensure that the communication between the Linked Third Party and Security Data Seguridad en Datos y Firma Digital S.A is carried out securely through the use of operator digital certificates.

4.2.5. Email Validation

In general, the signatories are people linked with the Registration Authority (for example, banks, organizations, etc.)

One of the generation codes of the electronic signature certificate is sent to the email address provided by the applicant, in this way said address would be validated.

4.3.Identification and Authentication in the Renewal of Certificates

The subscriber can be identified and authenticated in the process renewal if the following is true:

- The Linked Third Party has authorized the renewal.
- The certificate you want to renew has not expired (up to one day before the expiration date).
- The subscriber meets the requirements to renew a certificate. The documents for renewal that are detailed in the "Certification Policy" of each specific type of certificate.

4.4.Identification and Authentication in the Revocation of Certificates

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

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

5. OPERATIONAL REQUIREMENTS FOR THE LIFE CYCLE OF CERTIFICATES

5.1.Certificate Request

5.1.1. Who can apply for a Certificate

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

5.1.2. Certificate Request Processes

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

- Necessary documentation to present for the processing of your request and to verify the identity of the subscriber.
- Availability to complete the registration process.
- Information on the issuance and revocation process, on the custody of the private key, as well as the responsibilities and conditions of use of the certificate and the device.
- How to access and consult this document and the certification policies.

The documentation required for the request of each type of certificate is specified in the certification policies (CP).

5.2.Validity of the Electronic Signature Certificate

According to the Regulation to the Law of electronic commerce, electronic signatures and data messages (Decree No.3469):

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

5.3.Processing of Certificate Requests

5.3.1. Performing identification and authentication functions

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

5.3.2. Face-to-face validation of identity and documentation

The validation of the identity and of the documentation presented will be done in person before a Linked Third-Party operator, who will validate the identity of the applicant through the identification documents and will review the validity of the requested documents. Once the identity and the documents have been validated, the token will be delivered to the subscriber.

5.3.2.1. Identity validation via video conference

The validation of the identity may be carried out by videoconference before an operator of the Linked Third Party, which will validate the identity of the applicant through the identification documents. The validation of the documentation will be done in person or online before an operator of the Linked Third Party. Once the identity and the documents have been validated, the token will be delivered to the subscriber, sending it securely to the place where the subscriber is located.

5.3.3. Approval or denial of certificate requests

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

If the information is not correct, the Linked Third Party will deny the request, contacting the applicant to inform them of the reason.

If it is correct, the service will proceed, or the applicant will receive an email indicating that their

request has been approved and that they must approach the Registration Authority and appear in person to confirm the data, 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 Security Data Seguridad en Datos y Firma Digital S.A. The certificate will then be issued.

5.4. Issuance of Certificates

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

Once the request is approved, the certificate will be issued, which must be delivered securely to the subscriber.

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

a) For certificates in hardware support:

- The Linked Third Party will deliver the token. If the applicant provides their own device, it must be approved by Security Data Seguridad en Datos y Firma Digital S.A prior to its use. The Linked Third Parties will have a list of approved devices.
- Activation of the device: In the event that the applicant does not have them, the activation data of the device and access to the private key that it will contain will be generated.
- Generation of the pair of keys: The generation codes will be generated in the AC.
- The Linked Third Party will deliver one of the generation codes. The second-generation code will be sent to the applicant to the email that has been provided in the application.

b) For Software certificates:

The applicant will receive by email the download link for the issuance of their electronic signature and one of the keys for its issuance. The second key will be entered by the subscriber at the time of its generation.

5.4.2. Delivery of the certificate.

When the Subscriber has the two generated keys (Authorization Code and Reference Number, for Hardware issue), he can generate the certificate.

a) In hardware

The registry operator or linked third party will enter the following linkhttps://emision.securitydata.net.ec/cda-cgi/clientcgi.exe?action=start and will place the two keys for issuance.

b) In Software

Once the notification by email has been received by the subscriber, they will have to generate their certificate through the indicated portal, filling out the download form with the following data:
ID number
RUC number (legal entity only) Reference
number
Password that the subscriber will create at the time of download.

5.4.3. Key pair lifetime

The validity of the pair of keys will be according with what is requested by the subscriber based on the following parameters:

- For natural persons

From 1 day to 5 years

- For legal persons

From 1 to 5 years the maximum allowed by the appointment of the legal representative

5.4.4. Using the private key of the certificate

The pair of electronic signature keys issued by Security Data has no restrictions for its use, since they are multipurpose, having the following bits enabled in accordance with the x509 V3 standard:

- Digital signature
- without repudiation
- encryption key

5.5. Certificate Acceptance

5.5.1. Form in which the Certificate is Accepted

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

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

The acceptance document must be delivered to the Physically Linked Third Party and it must be digitally signed once the subscriber has the corresponding digital signature. The physical file will proceed to be destroyed.

5.5.2. Certificate Publication

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

5.6. Uses of the Keys and the Certificate

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

Certificates may be used as stipulated in this CPS and in the corresponding Certification Policy. The Key Usage extension may be used to establish technical limits to the uses of the private key of the corresponding certificate. The application of these limits will largely depend on their correct implementation by third-party computer applications, their regulation being outside the scope of this document.

5.6.2. Use of the Public Key and the Certificate by Third Parties that trust the Certificates

Third parties that trust the certificates may use the certificates for what is established in this CPS and the corresponding 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 S.A specifically for this purpose and specified in this document.

5.7. Renewal of Certificates without Change of Keys

This option is not considered.

5.8. Renewal with Change of Keys

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

5.8.1. Certificate expiration notification to a subscriber for renewal

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

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

5.8.2. Notification of the issuance of the certificate by the CA to other entities

Security Data will notify entities, government agencies and private companies of the renewal of a certificate through the Security Data website.

5.9. Modification of Certificates

In case of need to modify any data, the Linked Third Party must proceed to the revocation and the issuance of a new certificate.
If the certifying entity, in accordance with changes in legislation or lines of business, requires updating the data in the client's electronic signature certificate, the following process will be considered:

- 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 by email to the client.

5.10. Revocation and Suspension of Certificates

The revocation of a certificate supposes the loss of its validity, and it is irreversible. The suspension supposes the temporary loss of validity of a certificate, and it is reversible.

Revocations and suspensions take effect from the moment they appear published in the CRL, which are detailed in point 5.11.1 of this document.

5.10.1. Causes for revocation

A certificate may be revoked for the following reasons:

a) Circumstances that affect 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 relationship of the signatory with the Corporation.

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

- Compromise of the private key or of the infrastructure or systems of the CA, as long as it affects the reliability of the certificates issued from that incident.

- Infringement, by the CA or the Linked Third Party of the requirements set forth 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.
- The irregular use of the certificate by the subscriber or signatory.
- Failure by the subscriber or signatory to comply with the rules of use of the certificate set forth in this CPS or in the binding legal instrument between Security Data Seguridad en Datos y Firma Digital S.A and the subscriber.

c) Circumstances that affect the security of the cryptographic device:

- commitment or suspected compromise of the security of the cryptographic device.
- Loss or disablement 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 of use of the certificate set forth in this CPS or in the binding legal instrument between Security Data Seguridad en Datos y Firma Digital S.A and the subscriber.

d) Circumstances affecting the subscriber:

- Termination of the legal relationship between Security Data Seguridad en Datos y Firma Digital S.A and the Subscriber.
- Modification or termination of the underlying legal relationship or because that allowed the issuance of the certificate to the signatory.
- Violation by the applicant of the certificate of the pre-established requirements for the applicationof the same.
- Infraction by the subscriber of his obligations, responsibility and guarantees, established in the corresponding legal instrument or in the CPS.
- The supervening disability, total or partial.
- Due to the death of the subscriber or signatory.

e) Others circumstances:

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

5.10.2. Who can Request the Revocation

They can request the revocation of a certificate:

- The subscriber himself, who must request the revocation of the certificate in the event of having knowledge of any of the above circumstances.

- Any person may request the revocation of a certificate if they become aware of any of the circumstances.

They may process the revocation of the certificate:

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

5.10.3. Revocation Request Procedures

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

In any case, at the time the certificate is suspended or revoked, a communication will be sent to the subscriber.

5.10.3.1. Revocation during Office Hours

The subscriber or signatory must contact the certifying entity or the Linked Third Party of Security Data Seguridad en Datos y Firma Digital S.A either via email, in person or by telephone.
If the subscriber or signatory attends personally, it will be authenticated by means of their 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 the event of suspension of the certificate. subscriber can request prior data validation from the AC.
If you do so by telephone at 023922169-04392169, the certificate will be suspended until the subscriber or signatory personally appears before the Linked Third Party 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 you do it via email tosupport@securitydata.net.ec ,the certificate will be suspended until the subscriber personally submits to the linked third party or sends a letter requesting the revocation of the certificate, in case the revocation request is electronically signed, the definitive revocation proceeds, otherwise the certificate will be suspended and the applicant or signatory can cancel the suspension and the revocation procedure.
Depending on the type of request received, the operator will carry out the respective revocation within the Security Data income portal, which has the revocation option in which it can suspend or revoke the certificate prior to loading the letter delivered by the subscriber, for the different aforementioned means.
Revocations and suspensions take effect from the moment they appear published in the CRL.

5.10.3.2. Suspension criteria

A certificate may be suspended due to the following causes:

a) Circumstances that affect 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 relationship of the signatory with the Corporation.

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

- Compromise of the private key or of the infrastructure or systems of the CA, as long as it affects the reliability of the certificates issued from that incident.
- Infringement, by the CA or the Linked Third Party of the requirements set forth 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.
- The irregular use of the certificate by the subscriber or signatory.
- Failure by the subscriber or signatory to comply with the rules of use of the certificate set forth in this CPS or in the binding legal instrument between Security Data Seguridad en Datos y Firma Digital S.A and the subscriber.

c) Circumstances that affect the security of the cryptographic device:

- commitment or suspected compromise of the security of the cryptographic device.
- Loss or disablement 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 of use of the certificate set forth in this CPS or in the binding legal instrument between Security Data Seguridad en Datos y Firma Digital S.A and the subscriber.

d) Circumstances affecting the subscriber:

- Termination of the legal relationship between Security Data Seguridad en Datos y Firma Digital S.A and the Subscriber.
- Modification or termination of the underlying legal relationship or because that allowed the issuance of the certificate to the signatory.
- Violation by the applicant of the certificate of the pre-established requirements for the application of the same.
- Infraction by the subscriber of his obligations, responsibility and guarantees, established in the corresponding legal instrument or in the CPS.
- The supervening disability, total or partial.
- Due to the death of the subscriber or signatory.

e) Others circumstances:

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

5.10.3.3. Suspension Lift Criteria

The client will be the only entity authorized to lift the suspension, according to the subscriber's criteria, and it cannot be delegated to a third person, the procedure for suspension or lifting is the same as detailed in point 5.10.3.1

5.10.3.4. Revocation Outside Office Hours

The customer will request the revocation by email to soporte@securitydata.net.ec,It will be processed the next business day after 9:00 a.m.

5.10.4. Term in which the CA must resolve the Revocation Request

Once the identity of the subscriber has been authenticated as stated above, and the revocation duly processed by the Linked Third Party, the revocation will be effective immediately.

5.10.5. Obligation to Verify Revocations by Third Parties

The verification of the status of the certificates is mandatory for each use of the certificates, either by consulting the revocation list (CRL) or the OCSP service.

5.10.6. Frequency of Issuance of CRLs

The CRL of the end entity certificates are issued every 24 hours or when a revocation occurs and for quick reference the certification entity issues a delta CRL every 4 hours.

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

5.10.7. Maximum time between generation and publication of CRLs

Since the publication of the CRLs is carried out at the moment of its generation, considers elapsed time to be zero or null.

5.10.8. Availability of the Online Certificate Status Verification System

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

week.

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

5.10.9. Online Revocation Check Requirements

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

- In any case, the last CRL issued must be verified, 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's certification chain.
- The user must ensure that the revocation list is signed by the authority that has issued the certificate to be validated.
- Revoked certificates that expire will be removed from the CRL.

5.10.10.Circumstances for Suspension

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

- If the compromise of a key is suspected, until this fact is confirmed or denied.
- If the subscriber has incurred in non-payment of his certificate.
- If they do not have all the information necessary to determine the revocation of a certificate.
- Be arranged by ARCOTEL, in accordance with the provisions of the Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos
- It is verified by the information certification entity, falsity in the data consigned by the holder of the certificate.
- The breach of the contract between the information certification entity and the owner of the electronic signature occurs.

5.10.11.Who can Request the Suspension

They may only carry out the suspension of the certificate:

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

5.10.12.Suspension Period Limits

The limit is established by the client itself or by the validity of the certificate.

5.10.13.Circumstances for lifting the suspension

Under no circumstances Security Data Seguridad en Datos y Firma Digital S.A makes copies of the certificates in case of expiration, revocation or suspension.

Once the suspension has been carried out, the unique serial number of the certificate goes to the list of CRL's in revocation status, 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 certificate from the certificate. subscriber of the CRL's, and in case the certificate has expired or is no longer valid, a new one will be issued.

5.11. Certificate Status Information Services

5.11.1. Operating Characteristics

Security Data Seguridad en Datos y Firma Digital S.A offers a free Web publication service of Certificate Revocation Lists (CRL) without access restrictions, which contain the revocation list since its creation and are signed by the Root CA, the query is made via LDAP protocol.

The CRL can be downloaded from the official pagehttps://www.securitydata.net.ec/firma-electronica-en-ecuador/ in the option "Signature and CRL Expiration" URL: https://www.securitydata.net.ec/firma-electronica-en-ecuador/

The download links can be found at the following addresses: CRLS

- Subca- 2011
https://direct.securitydata.net.ec/~crl/autoridad_de_certificacion_sub_security_data_entidad_de_certificacion_de_informacion_curity_data_s.a._c_ec_crl file.crl

https://direct.securitydata.net.ec/~crl/

- SUBCA-1
- https://portal-operador.securitydata.net.ec/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN%3DAUTORIDAD+DE+CERTIFICACION+SUBCA-1+SECURITY+DATA%2COU%3DENTIDAD+DE+CERTIFICACION+DE+INFORMACION%2CO%3DSECURITY+DATA+S.A.+1%2CC%3DEC
-
- https://portal-

operador.securitydata.net.ec/ejbca/publicweb/webdist/certdist?cmd=deltacrl&issuer=CN%3DAUTORIDAD+DE+CERTIFICACION+SUBCA-1+SECURITY+DATA%2COU%3DENTIDAD+DE+CERTIFICACION+DE+INFORMACION%2CO%3DSECURITY+DATA+S.A.+1%2CC%3DEC

- SUBCA-2
- https://portal-operador2.securitydata.net.ec/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN%3DAUTORIDAD+DE+CERTIFICACION+SUBCA-2+SECURITY+DATA%2COU%3DENTIDAD+DE+CERTIFICACION+DE+INFORMACION%2CO%3DSECURITY+DATA+S.A.+2%2CC%3DEC
-
- https://portal- operador2.securitydata.net.ec/ejbca/publicweb/webdist/certdist?cmd=deltacrl&issuer=CN%3DAUTORIDAD+DE+CERTIFICACION+SUBCA-2+SECURITY+DATA%2COU%3DENTIDAD+DE+CERTIFICACION+DE+INFORMACION%2CO%3DSECURITY+DATA+S.A.+2%2CC%3DEC
-
- Security Data has all the revocation lists published.

Additionally, Security Data Seguridad en Datos y Firma Digital S.A offers the service of validation of certificates through the OCSP protocol (Online Certificate Status Protocol). Information on this can be found in the OSCP DCP published at the following link:

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

5.11.1.1. Publication of documents

The publication of the certificate will be carried out prior to its entry into force through the Security Data website. The validity period depends on the implemented CAs, which are detailed below:
CA ENTRUST
Valid until Sunday, February 16, 2031 17:18:50 CA 2
Valid until Thursday, October 6, 2039 16:20:12

5.11.1.2. CRL issuance parameters

The certificate revocation lists (CRL) are signed by the Root CA with a sha256RSA signature algorithm, which are valid for one day after they are updated.

5.11.1.3. OCSP Message Digital Signature Parameters

OCSP 1
Ou: INFORMATION CERTIFICATION ENTITY,o=SECURITY DATA SA,c=ECSerial: 4D5D28E4

Issue date: Thursday, November 1, 2012 16:44:56 Expiration

date: Tuesday, November 1, 2022 16:50:20

OCSP 2
Ou: INFORMATION CERTIFICATION ENTITY,o=SECURITY DATA SA,c=ECSerial: 4D5D59C9

Issue date: Tuesday, March 19, 2013 11:03:29
Expiration date: Sunday, March 19, 2023 11:30:06

OCSP 3
CN: SUB SECURITY DATA CERTIFICATION AUTHORITY, ou=INFORMATION CERTIFICATION ENTITY,o=SECURITY DATA SA,c=EC
Serial: 4D5D59E3

Issue date: Tuesday, March 19, 2013 17:14:31
Expiration date: Sunday, March 19, 2023 17:16:52

OCSP 4
CN=CERTIFICATION AUTHORITY SUBCA-1 SECURITY DATA,OU=INFORMATION CERTIFICATION ENTITY,O=SECURITY DATA SA 1,C=EC
Serial: 1A0900B2

Issue date: 2019-03-18 16:39:00-05:00
Expiration date: 2024-07-31 17:30:43-05:00

5.11.2. Availability of the Service

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

In case of system failure, or any other factor that is not under the control of the CA, it will make every effort to ensure that this information service is available within a period of no more than 24 hours.

5.11.3. Termination of Subscription

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

6. PHYSICAL SECURITY, FACILITIES, MANAGEMENT AND OPERATIONAL CONTROLS

6.1. Physical controls

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

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

- Unauthorized physical access
- Natural disasters
- Fires
- Failure of support systems (electronic energy, telecommunications, etc.)
- collapse of the structure
- floods
- Stole
- Unauthorized exit of equipment, information, supports and applications related to components used for the services of the Accredited Entity

The facilities have preventive and corrective maintenance systems with assistance 24 hours a day, 365 days a year, with assistance within 24 hours of notification. The location of the facilities guarantees the presence of security forces within a period not exceeding 30 minutes

6.1.1. Physical Location and Construction

The AC facilities are built with materials that guarantee protection against brute force attacks and are located in an area with low risk of disasters and allow quick access.

Specifically, the room where the cryptographic operations are carried out is a cage with protection against external radiation, a double floor, fire detection and extinction, anti-humidity systems, a double cooling system and a double electrical supply system.

6.1.2. Physical Access

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

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

Access to the rooms is done with identification card and fingerprint readers, managed by a computer system that maintains an automatic entry and exit log.

6.1.3. Electric Power and Air Conditioning

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

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

6.1.4. Water Exposure

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

6.1.5. Fire Protection and Prevention

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

6.1.6. Storage System

Each removable storage medium (tapes, cartridges, diskettes, etc.), containing classified information, is labeled with the highest level of classification of the information it contains and remains only accessible to authorized personnel.

Information classified as Confidential, regardless of the storage device, is permanently stored in fireproof cabinets or under lock and key, requiring express authorization for removal.

6.1.7. Elimination of Information Carriers

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

- Printed matter and paper: through shredders or in bins arranged for this purpose to be destroyed later, under control.
- Storage media: before being discarded or reused, they must be processed for erasure physically destroyed or make the information contained unreadable.

6.1.8. Business information security

Daily data backups are established

6.2. Procedural Controls

6.2.1. Roles of those responsible

The trusted roles are those described in the respective Certification Policies of the hierarchy in such a way as to guarantee a segregation of functions that spreads control and limits internal fraud, not allowing a single person to control all the functions from start to finish. certification functions. The minimum established roles are:

- **Security Officer:** Maintains overall responsibility for the administration and implementation of security policies and procedures
- **Certification System Administrators:** Authorized to make changes to the system configuration, but without access to system data.
- **System Operators:** Responsible for the day-to-day management of the system (monitoring, backup, recovery,...)
- **Internal Auditor (System Auditor):** Authorized a access the system logs and verify the procedures carried out on it.
- **AC Operator - Certification Operator:** Responsible for activating the CA keys in the Online environment, or for the certificate signing processes and CRL's in the Root Offline environment.
- **Linked Third Party Operator (Registration Officer):** Responsible for approving, issuing, suspending and revoking the final Entity certificates.

6.2.2. Number of People Required per Task

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

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

6.2.3. Identification and Authentication by Role

The people assigned to each role are identified by the internal auditor who will ensure that each person performs the operations for which they are assigned.

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

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

6.2.4. Roles Requiring Segregation of Duties

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

The people involved in Systems Administration may not carry out any activity in the Audit or Certification tasks.

6.3. Personnel Controls

6.3.1. Requirements Regarding Professional Qualification, Knowledge and Experience

All personnel who perform tasks classified as reliable without supervision, have been working at the production center for at least six months and have a permanent employment contract.

All personnel are qualified and have been suitably instructed to carry out the operations assigned to them.

The CA ensures that the registry personnel are reliable personnel of a corporation to carry out the registry tasks. To this end, a statement to that effect is required from the Entity that assumes functions of the Linked Third Party.

The registry employee will have completed a preparation course to carry out the tasks of registering and validating requests. At the end of this course, an external auditor will proceed to evaluate your knowledge of the process.

Security Data Seguridad en Datos y Firma Digital S.A will remove an employee from their functions of trust when there is knowledge of the existence of the commission of a criminal act that could affect the performance of these functions.

6.3.2. Background Check Procedures

Security Data Seguridad en Datos y Firma Digital S.A carries out the pertinent investigations before hiring any person.

The Linked Third Parties may establish different criteria, being responsible for the action of authorized persons.

6.3.3. Training Requirements

Security Data Seguridad en Datos y Firma Digital S.A carries out the necessary courses to ensure the correct performance of the certification tasks, especially when substantial modifications are made to them and based on the personal knowledge of each operator.

6.3.4. Training Update Requirements and Frequency

Updates will be made on an annual basis, except for modifications to the CPS, which will be notified as they are approved.

6.3.5. Third Party Hiring Requirements

Employees hired to perform reliable tasks must previously sign the confidentiality clauses and the operational requirements used by the CA. Any action that compromises the safety of the accepted critical processes may lead to the termination of the employment contract.

6.4. Security Audit Procedures

6.4.1. Logged Event Types

Security Data Seguridad en Datos y Firma Digital S.A registers and saves the logs of all the events related to the security system of the CA. These include the following events:

- On and off of the system.
- Attempts to create, delete, set passwords or change privileges.
- Login and logout attempts.
- Unauthorized access attempts to the AC system through the network.
- Unauthorized access attempts to the AC's internal network.
- Unauthorized access attempts to the file system.
- Physical access to the logs.
- Changes in system configuration and maintenance.
- Records of the applications of the Certification Authority.
- AC application on and off.
- Changes in the details of the CA and/or its keys.
- Changes in the creation of certificate profiles.
- Generation of own keys.
- Certificate lifecycle events.
- Events associated with the use of the CA cryptographic module.
- Records of the destruction of the media containing the keys, activation data.

Additionally, Security Data Seguridad en Datos y Firma Digital S.A retains, either manually or

electronically, the following information:

- CA key creation ceremonies and key management databases.
- Physical access logs.
- Maintenance and system configuration changes.
- Changes in the personnel that carry out tasks of trust in the CA.
- Reports of commitments and discrepancies.
- Records of the destruction of material containing key information, activation data, or personal subscriber information, if such information is managed.
- Possession of activation data, for operations with the private key of the CAs.

6.4.2. Audit Record Processing Frequency

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

6.4.3. Period of Conservation of Audit Records

The information of the audit logs will be stored for the time considered necessary to guarantee the security of the system based on the importance of each specific log.

6.4.4. Protection of Audit Records

The system logs are protected from being manipulated by signing the files that contain them.

They are stored in fireproof devices. Its availability is protected through storage in facilities outside the center where the Certification Authority is located.

Devices are always handled by authorized personnel.

6.4.5. Audit Log Backup Procedures

Security Data Seguridad en Datos y Firma Digital S.A has an adequate backup procedure, so that, in case of loss or destruction of relevant files, the corresponding backup copies of the logs are available in a short period of time.

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

Additionally, a copy of the audit logs is kept in an external custody center.

6.4.6. Audit Information Collection System

The event audit information is collected internally and automatically by the operating system and by the certification software.

6.4.7. Vulnerability scan

The CA carries out an annual review of discrepancies in the information in the logs and suspicious activities.

6.5. Log File

6.5.1. Type of Archived Events

The events that take place during the life cycle of the certificate, including its renewal, will be preserved. It will be stored by the CA or, by delegation of the latter in the Linked Third Party:

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

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

6.5.2. Record Retention Period

All system data related to the life cycle of the certificates will be kept for the period established by current legislation when applicable. The certificates will be kept published in the repository for at least one year after their expiration. The contracts with the subscribers and any information related to the identification and authentication of the subscriber will be kept for at least 15 years or the period established by current legislation.

6.5.3. File Protection

The AC ensures the correct protection of the files by assigning qualified personnel for their treatment and storage in fireproof safes and external facilities in cases where this is required.

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

6.5.4. File Backup Procedures

The AC has an external storage center to guarantee the availability of the copies of the electronic file archive. Physical documents are stored in secure places with access restricted only to authorized personnel.

6.5.5. Requirements for Time Stamping Records

The records are dated with a reliable source.

Within the technical and configuration documentation of the CA, there is a section on the time configuration of the equipment used in the issuance of certificates.

6.5.6. Audit Information File System

Not stipulated.

6.6. Procedures for Obtaining and Verifying Filed Information

During the audit required by this CPS, the auditor will verify the integrity of the information filed.

Access to archived information is done only by authorized personnel.

The CA will provide the information and means to the auditor to be able to verify the information filed.

6.7. Change of Keys of the AC

6.7.1. AC Root

Before the Root CA certificate expires, a key change (rekeying) will be carried out and, where appropriate, changes will be made to the content of the certificate that better adjust to current legislation and the reality of Security Data Seguridad en Datos y Firma Digital S.A and the market. The old CA and its private key will only be used to sign CRLs while there are active certificates issued by the old CA. A new CA will be generated with a new private key.

The technical and security documentation of the CA details the process of changing the keys of the CA. The keys of the certificates issued by Root CA will cease to be valid at the same time that your self-signed certificate does. Once expired, the Root CA will generate a new pair of keys that self-signs to generate the

new root certificate. The change of keys is not a recurring operation of a Certification authority and must be planned in accordance with the technical and regulatory conditions that are established. Find in force.

6.7.1.1. Action procedure before the vulnerability of the private key of an authority

The compromise or suspicion of your private key is considered as an incident and will be treated as a major incident in the provision of services.digital certification services.

6.7.2. AC Subordinate

In the case of subordinate CAs, you can choose to renew the certificate with or without a change of keys. Only when the change is made, what is described in the previous point will be applied.

6.8. Disaster Recovery Plan

6.8.1. Incident and Vulnerability Management Procedures

Based on its infrastructure, the CA can recover all the systems in less than 48 hours, although the revocation and publication of information on the status of the certificates is ensured in less than 24 hours.

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

In the event that an incident occurs that will alter or corrupt both hardware, software and data resources, Security Data Seguridad en Datos y Firma Digital S.A will proceed as stipulated in the "Security Policy" document.

6.8.3. Procedure of Action before the Vulnerability of the Private Key of a Certification Authority

In case of compromise of the private key of the CA, Security Data Seguridad en Datos y Firma Digital S.A:

- It will inform all subscribers, users and other ACs with which it has agreements or another type of relationship of the commitment, at least by publishing a notice on the AC's website.
- It will indicate that the certificates and revocation status information signed using this key are not valid.

6.8.4. Business continuity after a disaster

- The CA will restore critical services (Revocation and publication of certificates revoked) in accordance with this CPS within 24 hours after a disaster or unforeseen emergency
- The AC has an alternative center, if necessary, for the start-up of operation of certification systems.

- Restoration is done logically.
- Backups run daily at the logical level with a 7-day retention.

6.9. Cessation of Activity

6.9.1. Certification Authority

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

- It will provide the necessary funds (to continue the completion of the revocation activities until the definitive cessation of the activity, if that is the case.
- It will inform all subscribers, applicants, users, other AC's or entities with which it has agreements or another type of relationship of the termination at least 2 months in advance, or the period established by current legislation.
- It will revoke any authorization to subcontracted entities to act on behalf of the CA.
- It will inform the competent administration, with the indicated notice, of the cessation of its activity and the destination that will be given to the certificates, specifying, where appropriate, if the management is going to be transferred and to whom.
- CA records will be archived and transferred to a specific custodian.
- In the event that the CA is terminated, all certificates issued under the CA will be revoked and the CA will no longer issue certificates.

6.9.2. Registration Authority

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

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

7. TECHNICAL SECURITY CONTROLS

7.1. Generation and Installation of the Key Pair

7.1.1. Key Pair Generation

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

a) In hardware (physical support)

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

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

signature verification.

b) in software

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

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

7.1.2. Delivery of the Private Key to the Subscriber

c) In hardware (physical support)

The private key will be delivered together with the certificate in the signature creation device. The Linked Third Party will be responsible for guaranteeing the delivery of the device to the subscriber, thus ensuring that the latter is in possession of the signature creation data corresponding to the verification data contained in the certificate.

The cryptographic device uses an activation key to access the private keys, or, in turn, it will be accessed by means of the fingerprint in case of having a biometric device.

d) in software

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

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

The sending of the public key to the CA for the generation of the certificate is done through a standard format, preferably in self-signed PKCS#10 or X.509 format, using a secure channel for transmission.

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

The certificate of the CAs of the certification chain and their fingerprint (digital footprint) will be available to users on the Security Data Seguridad en Datos y Firma Digital S.A website.

7.1.5. Supported Key Usages (X.509v3 Key Usage field)

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

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

7.1.6. 7.1.5.1. Extended Key Usage (EKU)

The EKUs that are included in the Security Data Seguridad en Datos y Firma Digital S.A are the following:

Server Auth	1.3.6.1.5.5.7.3.1
Client Auth	1.3.6.1.5.5.7.3.2
OCSP	1.3.6.1.5.5.7.4
Timestamping	1.3.6.1.5.5.7.3.88.1

7.1.7. name restriction

The names contained in the certificates are restricted to distinguished names (DN) X.500, unique and unambiguous.

7.1.8. CA key pair lifetime

The validity of the key pair will have a validity period of 20 years.

7.1.9. CA Public Key Distribution

The certificate and public key of the CA is located on the official page of Security Data, which has perimeter security and proactive monitoring against cyber-attacks.

7.2. Protection of the Private Key and Engineering Controls of the Cryptographic Modules

7.2.1. Standards for Cryptographic Modules

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

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

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

7.2.2. Multiperson Control (k of n) of the Private Key

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

7.2.3. Custody of the Private Key

The root CA's private key is guarded by a FIPS 140-2 level 3 certified hardware cryptographic device, ensuring that the private key is never in the clear outside of the cryptographic device. The activation and use of the private key requires the multi-person control detailed above. After the operation performed, the session is closed, leaving the private key deactivated.

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

7.2.4. Backup of the Private Key of the CA

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

The keys of the Root CA can be restored in accordance with what is indicated in the Procedure of

Recovery, backup and storage of private keys of the CA.

7.2.5. Subscriber Private Key File

The CA will not file the certificate signing private key after the expiration of its validity period.

The private keys of the internal certificates used by the different 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.

The private keys of the subscribers can be archived by themselves, through the conservation of the signature creation device or other methods, because they may be necessary to decrypt the historical information encrypted with the public key, as long as the custody device allows the operation.

7.2.6. Transfer of the Private Key to or from the Cryptographic Module

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

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

7.2.7. Private Key Activation Method

The CA Root keys are activated by a process that requires the simultaneous use of 3 out of 5 cryptographic devices (cards). The keys of the Subordinate CAs are activated by a process that requires the use of 1 of 4 cryptographic devices (cards).

Access to the subscriber's private key is done through a PIN or, if applicable, through a fingerprint. The pin device has a protection system against access attempts that block it when an incorrect access code is entered more than six times.

7.2.8. Private Key Deactivation Method

The private key of the certificate subscriber with DSCF will be deactivated once the cryptographic signature creation device is removed from the reading device.

7.2.9. Private Key Destruction Method

The method of destruction must be governed in accordance with what is indicated in the Procedure for Archiving, Access and Destruction of private keys archived by the AC.

7.2.10. Other Aspects of Key Pair Management

7.2.10.1. archive of the Public Key

The CA will keep all the public keys during the period required by current legislation, when applicable, or while the certification service is active and at least 6 months more, in any other case.

7.2.10.2. Operating Periods of the Certificates and Period of use for the Key Pair

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

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

7.3. Activation Data

7.3.1. Generation and Installation of Activation Data

The activation data is generated at the time of initialization of the cryptographic device.

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

7.3.2. Activation Data Protection

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

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

7.4. Computer security controls

The CA uses reliable systems and commercial products to offer its certification services.

The equipment used is initially configured with the appropriate security profiles by the Security Data systems personnel Data Security and Digital Signature in the following aspects:

- Operating system security settings.
- Application security settings.
- Sizing system correct.

- Configuration of Users and permissions.
- Log events configuration.
- Backup and recovery plan.
- Virus settings.
- Network traffic requirements.

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

7.4.1. Specific Technical Security Requirements

Each CA server includes the following functionalities:

- Access control to AC services and privilege management.
- Imposition of separation of tasks for the management of privileges.
- Identification and authentication of roles associated with identities.
- Archiving of subscriber and CA history and audit data.
- Audit of events related to security.
- Security self-diagnosis related to AC services.
- Mechanisms of recovery of keys and of the AC system.

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

7.4.2. Computer Security Assessment

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

Physical security is guaranteed by the facilities already defined above and personnel management is easy due to the reduced number of people who carry out their work in the Security Data Seguridad en Datos y Firma Digital S.A data center.

7.5. Lifecycle Security Controls

7.5.1. System Development Controls

The CA has a procedure to control changes in versions and applications that imply an improvement in its security functions or that correct any vulnerability detected.

7.5.2. Security Management Controls

7.5.2.1. Security Management

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

The CA requires by contract, security measures equivalent to any external provider involved in the certification work.

7.5.2.2. Classification and Management of Information and Assets

The CA maintains an inventory of assets and documentation and a procedure for the management of this material to guarantee its use.

The security policy of the CA details the information management procedures where it is classified according to its level of confidentiality.

The documents are cataloged in three levels: PUBLIC, INTERNAL and CONFIDENTIAL.

7.5.2.3. Management Operations

The AC has an adequate incident management and response procedure, through the implementation of an alert system and the generation of periodic reports. In the technical documentation of the CA and the CPD procedures, the incident management process is developed in detail.

The AC has fireproofed safes for the storage of physical media.

The CA has documented the entire procedure related to the functions and responsibilities of the personnel involved in the control and handling of elements contained in the certification process.

7.5.2.4. Treatment of Supports and Security

All supports will be treated safely in accordance with the requirements of the information classification. Supports containing sensitive data are safely destroyed if they are not going to be required again.

7.5.2.5. System Planning

The technical department of the AC maintains a record of the capabilities of the equipment. Together with the resource control application of each system, a possible resizing.

7.5.2.6. Incident Reports and Response

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

7.5.2.7. Operational Procedures and Responsibilities

The CA defines activities assigned to people with a role of trust other than the people in charge of carrying out day-to-day operations that are not confidential.

7.5.2.8. Access System Management

The CA performs use reasonable efforts to confirm that access to the system is limited to authorized persons. In particular:

a) General AC management:

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

b) Certificate generation:

- The AC facilities are equipped with continuous monitoring and alarm systems to detect, record and be able to act immediately in the event of an unauthorized and/or irregular access attempt to its resources.
- The authentication to carry out the issuance process is carried out through a system m of n operators for the activation of the CA's private key.

c) Revocation management:

- The revocation refers to the permanent loss of effectiveness of a digital certificate. The revocation will be done through strong card authentication to the applications of an

authorized administrator. The log systems will generate the evidence that guarantees the non-repudiation of the action carried out by the CA operator.

d) Revocation Status
   - The revocation status application has an access control based on certificate authentication to avoid attempts to modify the revocation status information.

7.5.2.9. Cryptographic Hardware Life Cycle Management

- The CA ensures that the cryptographic hardware used for signing certificates is not tampered with during transport.
- The cryptographic hardware is built on supports prepared to prevent any manipulation.
- The CA registers all the pertinent information of the device to add to the Security Data Seguridad en Datos y Firma Digital S.A asset catalog
- The use of cryptographic certificate signing hardware requires the use of at least two trusted employees.
- Security Data Seguridad en Datos y Firma Digital S.A performs periodic tests to ensure the correct functioning of the device.
- The cryptographic device is only manipulated by trusted personnel.
- The CA's signing private key stored in the cryptographic hardware will be deleted once the device is removed.
- The AC has a maintenance contract for the device for its correct maintenance. Changes or updates are authorized by the person responsible for security and are reflected in the corresponding work records. These settings will be made by at least two trustworthy people.

7.6. Network Security Controls

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

Confidential information transferred over unsecured networks is encrypted.

8. PROFILE OF THE CERTIFICATES

8.1. Certificate Profile

The profile of the certificates corresponds to that proposed in the corresponding certification policies, and is consistent with the provisions of the following standards:

- ETSI TS 101 862 known as “European profile for Qualified Certificates”
- RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile",
- RFC 3739 “Qualified Certificates Profile”.

The profile common to all subscriber certificates is as follows:

Certificate field	Name	Description
Version	version number	V3 (version of the standard X509)
serial number	serial number	Code unique to the name distinguished from issuer
Signature Algorithm	algorithm of signature	signature algorithmsha256RSA
signature hash Algorithm	HASH algorithm of signature	Sha256
Issuer	Transmitter	DN of the CA issuing the certificate
Valid from	Valid since	Start date validity, UTC time
Valid to	Valid until	Ending date validity, UTC time
Subject	Subject	Distinguished name of the subscriber.
Public Key	Key code public	public key of the subscriber
Key Usage the	Use of key code	extensions of the certificates.
Access to authority information	Access to authority information	Information indicating that OCSP will be used

8.1.1. Version number

The certificates follow the X.509 version 3 standard for subscribers and version 2 for those specified in this CPS.

8.1.2. Certificate Extension (OID-Object Identifier)

The extensions presented here correspond to all those that the issued certificates may contain. The required extensions will be specified in the certification policy for each type of certificate.

Extension	Criticism	Possible Values
X509v3 Key Usage	Yes	Digital Signature Non-Repudiation Key Encipherment, Data Encryption, Key Agreement
X509v3 Authority Information Access	-	URI where find the CA certificate
X509v3 Certificate Policies	-	OID of the certification policy corresponding to the certificate. CPS URI User Notice: Text note that can be displayed on the user screen
1.3.6.1.4.1.37746.2.1		Certificate Policies – Natural Person
1.3.6.1.4.1.37746.2.2		Certificate Policies– Legal Entity- Company
1.3.6.1.4.1.37746.2.3		Certificate Policies – Legal Representative
1.3.6.1.4.1.37746.2.4		Certificate Policies – Company Member
1.3.6.1.4.1.37746.2.5		Certificate Policies – Public Official
1.3.6.1.4.1.37746.2.6		Certificate Policies – SSL
1.3.6.1.4.1.37746.2.7		Type of Natural Person Certificate
1.3.6.1.4.1.37746.2.8		Type of Certificate Legal Entity
1.3.6.1.4.1.37746.2.9		Type of Legal Representative Certificate
1.3.6.1.4.1.37746.2.10		Type of Certificate Company Member
1.3.6.1.4.1.37746.2.11		Type of Public Official Certificate
1.3.6.1.4.1.37746.2.12		SSL Certificate Type

1.3.6.1.4.1.37746.2.13		Certificate Type DEMO
1.3.6.1.4.1.37746.3.1		Citizenship ID or Passport No.
1.3.6.1.4.1.37746.3.2		Names
1.3.6.1.4.1.37746.3.3		Surname
1.3.6.1.4.1.37746.3.4		Second Surname: (if it does not have it, it is left blank)
1.3.6.1.4.1.37746.3.5		Position
1.3.6.1.4.1.37746.3.6		Institution
1.3.6.1.4.1.37746.3.7		Address
1.3.6.1.4.1.37746.3.8		Telephone
1.3.6.1.4.1.37746.3.9		City
1.3.6.1.4.1.37746.3.10		Business name
1.3.6.1.4.1.37746.3.11		RUC
1.3.6.1.4.1.37746.3.12		Country
1.3.6.1.4.1.37746.3.26		Representative Name Legal
1.3.6.1.4.1.37746.3.29		OR
1.3.6.1.4.1.37746.3.27		Domain
1.3.6.1.4.1.37746.3.28		Ecuador Legal Time
X509v3 Subject Alternative Name	-	subscriber (or CA) email
X509v3 CRL Distribution Points	-	CRL URI
X509v3 Private Key Usage Period	Yes	Private key usage period
X509v3Authority Key Identifier	-	id of the public key of the CA certificate, obtained from its hash
X509v3 Subject Key Identifier	-	id of the public key of the certificate, obtained from its hash
X509v3 Basic Constraints	Yes	2 possible values depending on whether it is a CA certificate: CA: FALSE CA:TRU E
1.2.840.113533.7.65.0	-	entrust version extension
X509v3 Extended Key Usage	-	TLS Web Client Authentication Email

		Protection
thumbprint algorithm	Yes	Certificate fingerprint creation algorithm
thumb print	Yes	certificate fingerprint

8.1.1. name formats

DN field	Name	Description
CN, Common Name	Subscriber Name	Name and surname of the subscriber,
CN, Common Name	CA Name	Names and Surnames of the CA
OU, Organizational Unit	Organizational Unit	Information Certification Entity
Or Organization	Organization	CA name
C Country	Country	country code two digits according to ISO 3166-1. By default, “ES”.

8.1.3. CRL Profile

The CRL's profile corresponds to the one proposed in the corresponding certification policies, and to the X.509 version 3 standard of RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". The CRL's are signed by the certification authority that has issued the certificates

8.1.4. Version number

The CRLs issued by the CA are version 2.

8.1.5. CRL and Extensions

8.1.5.1. Root Authority CRL (Root AC)

FIELDS	VALUES
Version	two
CRL number	incremental number
signature algorithm	Sha1WithRSAEncryption
Issuer	Distinguished Name (DN) of the sender

Effective date of issue	(CRL issue date, UTC time)
next update date	Effective date of issue + 6 months
Authority Key Identifier	Issuer key hash
Contains only User Certificates	NO
It only contains Certificates of the issuing entity	NO
Indirect Certificate Revocation List (CRL)	NO
CRL Entries	Certificate serial number Revocation date reason code

8.1.5.2. CRL of Subordinate Certification Authorities

FIELDS	VALUES
Version	two
CRL number	incremental number
signature algorithm	Sha1WithRSAEncryption
Issuer	Distinguished Name (DN) of the sender
Effective date of issue	(CRL issue date, UTC time)
next update date	Effective date of issue + 7 days
Authority Key Identifier	Issuer key hash
Contains only User Certificates	NO
It only contains Certificates of the issuing entity	NO
Certificate Revocation List (CRL) indirect	NO
CRL Entries	Certificate serial number Revocation date reason code

9. COMPLIANCE AUDITS AND OTHER CONTROLS

9.1. Audit Frequency

Internal audit plans will be carried out with the presentation of monthly reports, in order to have control over the life cycle of the certification entity and external audits will be carried out as long as it is requested by the regulatory entity.

9.2. Auditor Qualification

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

9.3. Relationship between the Auditor and the Audited Authority

The companies that carry out the external audits never represent any conflict of interest that could undermine their actions in their relationship with Security Data Seguridad en Datos y Firma Digital S.A.

However, Security Data Seguridad en Datos y Firma Digital S.A will carry out planned internal audits with monthly reports to the AC of the hierarchy to guarantee at all times its adaptation to the requirements set by the certification policies of the hierarchy.

9.4. Aspects Covered by 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 said statements.
b) Service Integrity. That the CA maintains effective controls to reasonably ensure that:

- The 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:

- The information of subscribers and users is restricted to authorized personnel and protected from uses not specified in the business practices of the company. AC published.
- The continuity of the operations related to the management of the life cycle of

the keys and certificates is maintained.
- The tasks of exploitation, development and maintenance of the CA systems are duly authorized and carried out to maintain their integrity.

9.4.1. Audit in Registration Authorities

The Registration Authorities that have access to the software/system provided by Security Data Seguridad en Datos y Firma Digital S.A for the management of certificates are audited by a third party prior to its effective implementation. Additionally, audits are carried out to verify compliance with the requirements demanded by the certification policies for the development of the registration tasks set forth in the signed service contract. The frequency of the audits will be determined by the agreement between Security Data Seguridad en Datos y Firma Digital S.A and the Registration Authority, always considering the activity planned for develop by the Registration Authority in terms of the number of certificates or specific security requirements.

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

9.5. Actions to be taken as a result of Incident Detection

In the event that incidents or non-conformities are detected, the appropriate measures will be enabled for their resolution in the shortest possible time. For serious non-conformities (affecting critical services, namely, REVOCATION SERVICES, CERTIFICATE ACTIVATION/SUSPENSION SERVICES, PUBLICATION SERVICES OF CRL), Security Data Security in Data and Digital Signature is committed to its resolution within a maximum period of sixty days.
In any case, a resolution committee will be formed made up of personnel from the affected areas and another for training follow-up by those responsible for the affected areas and the General Directorate.

9.6. Communication of Results

The auditor will communicate the results to the technical director and the General Director, whileHead of Security Data Seguridad en Datos y Firma Digital S.A.

10. OTHER LEGAL AND ACTIVITY ISSUES

10.1. Rates

10.1.1. Certificate Issuance or Renewal Fees

The prices of the certification services or any other service will be provided to clients or potential clients by the Commercial Department of Security Data Seguridad en Datos y Firma Digital S.A or through the website https://www.securitydata.net.ec/wp-content/downloads/listas/lista_precios.pdf

10.1.1.1. Change of rates or exceptions

The prices indicated in point 10.1.1, may be subject to revision or modification without prior notice, by the management or commercial department of Security Data, in the same way the prices may be variable considering promotions or legal regulations in force in the country. Promotions and price changes will be approved by general management, and communicated to the marketing department, which will be disseminated by the different media.

10.1.2. Certificate Access Fees

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

10.1.3. Fees for Access to Status Information or Revocation

Security Data Seguridad en Datos y Firma Digital S.A provides free access to information regarding the status of certificates or revoked certificates, through the publication of the corresponding CRL.
Security Data Seguridad en Datos y Firma Digital S.A offers other commercial certificate validation services (such as OCSP).

10.1.4. Other Services Rates

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

10.1.5. refunds

Certificate subscribers may request money reimbursement under the following guidelines:

- When an excess deposit has been made
- When the service has not been provided and the client does not want to continue with the process

For these cases, the client must demonstrate the evidence of the payment made, once the circumstances for making the reimbursement have been analyzed, the financial department

will proceed with the respective refund.

In these cases, the customer must send an email indicating the reason for the refund toreturns@securitydata.net.ec ,Once analyzed whether or not the refund applies, the client is notified.

The value of the refund will be that of the requested service, and the value deposited in excess.

10.2. Confidentiality of information

Security Data Seguridad en Datos y Firma Digital S.A has an adequate information treatment policy and agreement models that must be signed by all persons who have access to confidential information.

10.2.1. Scope of Confidential Information

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

- The private signing keys of the subscribers are confidential and are not provided to the CA or to related third parties. The specific information for the operation and control of the CA, such as security parameters and audit trails, is kept confidential. confidentially by the CA and is not disclosed outside the CA organization unless required by law, Subscriber information held by the CA or related third parties, excluding that published in certificates, CRLs, certificate policies or this CPS is considered confidential and will not be disclosed outside the CA unless required by the Certification Policy or by law.
- Release of Information Requested by Law Enforcement Officials
- Publication of information at the request of management.
- Other Information Disclosure Circumstances.
- Publication of information concerning the revocation.

10.2.2. Non-Confidential Information

The following information will be considered non-confidential:

- That contained in this CPS.
- That contained in the different Certification Policies (PC).
- The information contained in the certificates, since for their issuance the subscriber previously grants their consent, including the different states or situations of the certificate.
- The certificate revocation lists (CRL's), as well as the rest of the revocation status information.

- Information contained in the certificate deposits.
- Any information whose publicity is legally imposed.

10.2.3. Responsibility in the Protection of Confidential Information

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

1. Reviews

Document: Certification Practices Statement (CPS)										
Review	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Posted	09/03/2011	03/31/2011	06/24/2011	09/01/2011	09/26/2011	12/13/2011	07/04/2011	09/13/2013	09/13/2019	04/18/2022
Author(s)	LV/XC	XC	XC	DC/XC	XC	XC	XC	XC	XC	MF
Review Date	02/18/2011	05/16/2011		09/14/2011			07/04/2011			
Reviewed by	XC	XC		XC						
Approved date	02/18/2010	05/16/2011		09/16/2011	09/26/2011	12/13/2011	07/04/2011	09/13/2013	09/13/2019	04/18/2022
Approved by	CS	CS	CS	CS	CS	CS	CS	CS	CS	CS