SECURITYDATA
TU IDENTIDAD DIGITAL, EN UNA FIRMA.

SECURITY POLICY STATEMENT

marzo 4

2026

VERSION HISTORY

VERSION	DESCRIPTION	DATE	PREPARED BY	REVIEWED BY	APPROVED BY
V1	Initial Edition	02/11/2011	Technical Manager	Technical Manager	General Manager
V2	General update of the SPS in accordance with the Technical Regulations.	02/18/2026	Management System Coordinator	Chief Technology Officer (CTO) Legal Supervisor	General Manager

Contents

1. Legal Framework.

1.1. LEGAL BASIS.

Law on Electronic Commerce, Electronic Signatures and Data Messages, its Regulations; Organic Law on Consumer Protection, Organic Law on the Protection of Personal Data, Organic Law on Information Transparency and Accreditation of ARCOTEL.

1.2. VALIDITY.

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

1.3. LEGAL SUPPORT.

a) Law on Electronic Commerce, Electronic Signatures and Data Messages, published in Official Gazette No. 577 of April 17, 2002.
b) In accordance with the provisions of Article 37 of the Law on Electronic Commerce, Electronic Signatures and Data Messages, the National Telecommunications Council is the authorizing, registering and regulatory authority for Accredited Information and Related Services Certification Entities.
c) General Regulations to the Law on Electronic Commerce, Electronic Signatures and Data Messages, issued by Executive Decree No. 3496 published in Official Gazette No. 735 of December 31, 2002, and amendments made in Executive Decree No. 1356 of September 29, 2008, published in Official Gazette No. 440 of October 6, 2008.
d) Organic Law on the Protection of Personal Data, Official Register Supplement 459, May 26, 2021, which governs the treatment, storage and protection of the information of certificate holders.
e) That, the second enumerated article added by Article 4 of Executive Decree No. 1356 after Article 17 of the General Regulations to the Law on Electronic Commerce, Electronic Signatures and Data Messages, provides that accreditation as a certification entity for information and related services shall consist of an administrative act issued by CONATEL through a resolution that shall be registered in the National Public Registry of Information Certification Entities. Accredited and Related Third Party Information and Services.
f) Resolution 477-20-CONATEL-2008 of October 8, 2008, approved the model resolution for Accreditation as a Certification Entity for Information and Related Services.
g) 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 S.A. as a Certification Entity for Information and Related Services, for which SENATEL signed the respective administrative act, in accordance with the model approved by the National Telecommunications Council.

2. Introduction.

2.1. PRESENTATION.

This document includes the Security Policy Statement (SPS) of SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A., hereinafter Security Data.

This SPS contemplates the provisions of the SECURITY DATA DATA SECURITY AND DIGITAL SIGNATURE CPS, establishing a set of rules that indicate the procedures followed by the Certification authority in terms of security in its infrastructure.

This Security Policy Statement (SPS), along with the SECURITY DATA DATA SECURITY & DIGITAL SIGNATURE CPS, are intended for anyone who relies on this CA.

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

Name:	Security Policy Statement (SPS)
Code:	SD-ID-PE-15
Version:	2
Description:	Security Data Seguridad en Datos y Firma Digital S.A. Security Policy Statement
Publication Date:	February 18, 2026
Document Type:	Public

2.3. PARTICIPATING ENTITIES.

2.3.1. Accredited Entity (EA).

Security Data Seguridad en Datos y Firma Digital is an Accredited Entity (EA) that issues certificates recognized under the Electronic Commerce, Electronic Signatures and Messages Act of Data. Security Data Seguridad en Datos y Firma Digital is the entity that issues the certificates and is responsible for the operations of the certificate lifecycle. The functions of authorization, registration, issuance and revocation with respect to the personal certificates of the end entity may be performed by other entities by delegation contractually supported by Security Data Seguridad en Datos y Firma Digital, which will act as intermediaries. Security Data Seguridad en Datos y Firma Digital also offers electronic signature validation, time stamping and electronic seal services, governed by its particular policies, not included in this document.

2.3.2. Certificate Authority (CA).

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

2.3.3. Root Certification Authority.

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

2.3.4. Registration Authority (RA).

A Registration Authority (RA) for Security Data Seguridad en Datos y Firma Digital is the entity in charge of:

- To process requests for certificates.
- Identify the applicant and verify that they meet the necessary requirements for the application for the certificates.
- Validate the personal circumstances of the person who will be listed as the signatory of the certificate
- Manage key generation and certificate issuance.
- Deliver the certificate to the subscriber.

The following may act as RA of Security Data Seguridad en Datos y Firma Digital:

- Any legal entity that is a client of Security Data Seguridad en Datos y Firma Digital, for the issuance of certificates in the name of the corporation or to members of the corporation, and that complies with the technical and security requirements demanded by the entity and the control `authority`, for the issuance of certificates.
- Any trusted entity that enters into an agreement with Security Data Seguridad en Datos y Firma Digital to act as an intermediary on behalf of Security Data Seguridad en Datos y Firma Digital.
- Security Data Seguridad en Datos y Firma Digital directly.

Security Data Seguridad en Datos y Firma Digital will contractually formalise the relations between it and each of the entities that act as AR for Security Data Seguridad en Datos y Firma Digital.

The entity acting as the AR of Security Data Seguridad en Datos y Firma Digital may authorize one or more persons as an Operator of the AR to operate with the computer system for issuing Security Data certificates, Data Security and Digital Signature on behalf of the RA.

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 RA may delegate these functions to another trusted entity. This entity must have a special link with the RA and a close relationship with the subscribers of the certificates that justify the delegation. The trusted entity must sign a collaboration agreement with the HR in which the delegation of these functions is accepted. Security Data, Data Security and Digital Signature must be aware of and expressly authorize the agreement.

2.3.5. Applicant.

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

2.3.6. Subscriber.

The Subscriber is the natural or legal person who has contracted the Security Data Seguridad en Datos y Firma Digital certification services. Therefore, you will be the owner of the certificate. In general, the subscriber of a Security Data Seguridad en Datos y Firma Digital certificate will be a legal person (private company, public entity, natural person), the identity of which will appear on the certificate itself.

2.3.7. Signatory.

The Signatory is the person who owns a signature creation device and who acts on his or her own behalf or on behalf of a legal person he or she represents.

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

2.3.8. Custodian of the Keys.

The custody of the signature creation data associated with each electronic certificate of a legal entity will be the responsibility of the requesting natural person, whether legal representative or authorized delegate, whose identification will be included in the electronic certificate. The custodian has the unavoidable obligation to maintain exclusive control of their access codes and signature devices.

The custodian acknowledges that the use of your activation data and signature devices has the same legal effects as a handwritten signature, being solely responsible for their use and expressly prohibiting the transfer of keys to third parties.

2.3.9. Third Party Relies on Certificates.

A third party that trusts the certificates is understood to be any person or organization that voluntarily relies on a certificate issued by Security Data. For the trust to be valid, the third party must always verify the revocation status of the certificate through the mechanisms provided by Security Data.

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

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

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

2.4. USE OF THE CERTIFICATE.

2.4.1. Appropriate Uses of Certificates.

Appropriate uses of the Certificates shall be governed as defined in the Security Data CPS.

2.4.2. Prohibited Uses of Certificates.

Prohibited uses of the Certificates shall be governed as defined in the Security Data CPS.

2.5. POLICY MANAGEMENT.

2.5.1. Organization that administers the Document.

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. is the entity that manages and is the author of this Security Policy Statement and other regulatory documents.

2.5.2. Contact Person.

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

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

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

2.5.4. SPS approval procedures.

Publication of revisions to this SPS must be approved and signed by the Security Data CA Leader prior to publication.

The updated and approved versions of this SPS, as well as the other regulatory documents, will be submitted to the Supervisory Authority and subsequently published on the Security Data website.

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

2.6. DEFINITIONS AND ACRONYMS.

2.6.1. Definitions.

ARCOTEL: Telecommunications Regulation and Control Agency.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Integrity: Property that seeks to keep data free from unauthorized modification without being tampered with or altered unless it is planned to do so.

Availability: The quality of the information that it is accessible and usable at the time, for the persons authorized in each case.

Data security: A set of technical and organisational measures necessary to guarantee the confidentiality, integrity and availability of personal data.

Personal Data Security Breach: A security incident that affects the confidentiality, availability, or integrity of personal data.

2.6.2. Acronyms.

AC:	Certificate Authority
AC Sub:	Subordinate Certificate Authority
AR:	Registration Authority
PC:	Certification Policy
CPS:	Certification Practices Statement
CRL:	Certificate Revocation List
HSM:	Hardware Security Module
LDAP:	Lightweight Directory Access Protocol
OCSP:	Online Certificate Status Protocol.
PKI:	Public Key Infrastructure
PSC:	Certification Service Provider
TSA:	Time Stamp Authority
VA:	Validation Authority
ECI:	Information Certification Entity
OID:	Unique Object Identifier
DN:	Dinstinguished Name
C:	Country
CN:	Common Name, Attribute of the Distinctive Name
Or:	Organization, Attribute of the Distinctive Name
OU:	Organizational Unit, Attribute of the Distinctive Name

SN:	SurName, Attribute of Distinguished Name
ISO:	International Organizational for Standardization
PKCS:	Public Key Cryptography Standards, PKI Standards
UTF8:	Unicode Transformation Format – 8 bits.

3. Publishing and Repository Responsibilities.

3.1. REPOSITORIES.

Security Practices Statement: https://www.securitydata.net.ec/wp-content/downloads/Normativas/D_Practicas_Seguridad/sps.pdf

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

Subordinate CA Certificate: http://subca2.securitydata.net.ec/subca2sd/subca2.crt

CRL:

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

3.2. APPROVAL PROCEDURE.

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

Any substantial change that affects confidence or operability will be notified to the supervisory authority (ARCOTEL) at least 15 days prior to its publication.

3.3. TIME OR FREQUENCY OF PUBLICATION.

This SPS will be reviewed and, as appropriate, updated, annually or as we change.

3.4. ACCESS CONTROLS TO REPOSITORIES.

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

4. Identification and Authentication.

4.1. NAME.

4.1.1. Types of Names.

The name types for certificates are specified in the Security Data CPS.

4.1.2. Need for names to be meaningful.

It will be followed as defined in the Security Data CPS.

4.1.3. Rules for interpreting various name formats.

The rules are defined in the Security Data CPS.

4.1.4. Uniqueness of names.

It will be followed as defined in the Security Data CPS.

4.1.5. Recognition, authentication and function of trademarks.

Not applicable.

4.2. INITIAL IDENTITY VALIDATION.

The process defined in the Security Data CPS will be followed.

4.3. IDENTIFICATION AND AUTHENTICATION FOR KEY RENEWAL REQUESTS.

The process defined in the Security Data CPS will be followed.

4.4. IDENTIFICATION AND AUTHENTICATION FOR THE REVOCATION REQUEST.

The process defined in the Security Data CPS will be followed.

5. Certificate Life Cycle Operational Requirements.

5.1. APPLICATION FOR THE CERTIFICATE.

The application process is performed as defined in the Security Data CPS.

5.2. PROCESSING OF THE CERTIFICATE APPLICATION.

The processing process is carried out as defined in the Security Data CPS.

5.3. ISSUANCE OF THE CERTIFICATE.

The issuance process is performed as defined in the Security Data CPS.

5.4. ACCEPTANCE OF THE CERTIFICATE.

The acceptance process is performed as defined in the Security Data CPS.

5.5. USE OF KEY PAIRS AND CERTIFICATES.

The uses of keys and certificates are governed by what is defined in the Security Data CPS.

5.6. RENEWAL OF THE CERTIFICATE WITHOUT CHANGING THE PASSWORD.

This option is not contemplated.

5.7. RENEWAL WITH CHANGE OF CERTIFICATE KEY.

The renewal process is carried out as defined in the Security Data CPS.

5.8. MODIFICATION OF THE CERTIFICATE.

This option is not contemplated.

5.9. REVOCATION AND SUSPENSION OF THE CERTIFICATE.

The revocation process is performed as defined in the Security Data CPS.

5.10. CERTIFICATE STATUS SERVICE.

5.10.1. Operational Characteristics.

As indicated in the Security Data CPS.

5.10.2. Availability of Service.

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

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

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

5.10.3. Optional Features.

No stipulation.

5.11. END OF SUBSCRIPTION.

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

5.12. CUSTODY AND RECOVERY OF PASSWORDS.

5.12.1. Key Deposit and Recovery Policy and Practices.

Security Data does not store, nor does it have the possibility to store the private key of subscribers. Consequently, it is not possible to recover the holder's private key because there is no copy. The responsibility for the custody of the private key lies with the owner and the owner accepts and acknowledges this.

5.12.2. Session key encapsulation and retrieval policy and practices.

Not stipulated.

6. Facilities, Management and Operation Controls.

6.1. PHYSICAL CONTROLS.

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

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

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

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

6.1.1. Physical location and construction.

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

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

6.1.2. Physical Access.

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

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

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

6.1.3. Electric Power and Air Conditioning.

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

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

6.1.4. Water Exposure.

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

6.1.5. Fire Protection and Prevention.

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

6.1.6. Storage System.

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

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

6.1.7. Elimination of Information Carriers.

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

- Printed materials and paper: by means of shredders or in designated disposal bins to be subsequently destroyed under supervision.
- Storage media: before being discarded or reused, they must be processed for deletion physically destroyed or make the information contained illegible.

6.1.8. Enterprise Information Security.

Daily backups of the information are carried out.

6.2. PROCEDURAL CONTROLS.

6.2.1. Roles of Trust.

The trusted roles are those described in the respective Certification Policies and the personnel that are part of the Information Security Committee, so that a segregation of duties is guaranteed that disseminates control and limits internal fraud, not allowing a single person to control from start to finish all certification functions. The minimum roles established are:

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

6.2.2. Number of people needed per task.

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

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

6.2.3. Identification and authentication for each role.

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

Each person only controls the assets necessary for their role, thus ensuring that no one person has access to unallocated resources.
Access to resources is done depending on the asset through login/password, digital certificates, physical access cards and keys.

6.2.4. Roles that require separation of duties.

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

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

6.3. PERSONNEL CONTROLS.

6.3.1. Requirements on Qualification, Experience and Professional Knowledge.

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

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

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

Security Data Data Security and Digital Signature will remove an employee from their functions of trust when it becomes aware of the existence of the commission of a criminal act that could affect the performance of these functions.

6.3.2. Background Check Procedure.

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

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

6.3.3. Training Requirements.

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

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

6.3.4. Requirements and Frequency of Training Updates.

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

6.3.5. Frequency and Sequence of Task Rotation.

It is not stipulated.

6.3.6. Penalties for Unauthorized Actions.

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

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

6.3.7. Personnel Hiring Requirements.

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

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

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

6.3.8. Documentation Provided to Staff.

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

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

6.4. AUDIT TRAIL PROCEDURES.

6.4.1. Types of Events Recorded.

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

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

- Events associated with the use of the SECURITY DATA cryptographic module.
- Records of the destruction of the media containing the keys, activation data.

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

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

6.4.2. Frequency of Audit Log Processing.

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

6.4.3. Audit Log Retention Period.

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

6.4.4. Protection of Records.

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

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

The devices are operated at all times by authorized personnel.

6.4.5. Procedures for Supporting Audit Trails.

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

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

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

6.4.6. Audit Information Collection System.

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

6.4.7. Event Notification.

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

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

In the event of a security breach affecting personal data or the integrity of the CA, Security Data will notify the Data Protection Authority and ARCOTEL within a maximum of 72 hours, in accordance with Article 25 of the LOPDP.

6.4.8. Vulnerability Analysis.

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

6.5. LOG FILE.

6.5.1. Type of Archived Events.

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

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

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

6.5.2. Record Retention Period.

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

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

6.5.3. Protection of the Archive.

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

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

6.5.4. File Backup Procedures.

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

6.5.5. Requirements for the Time Stamping of Records.

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

6.5.6. Audit Information Filing System.

Not stipulated.

6.5.7. Procedures for obtaining and verifying information on file.

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

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

6.6. CHANGE OF KEY OF THE CA.

6.6.1. AC Raíz.

Before the Root CA certificate expires, a key change (rekeying) will be carried out and, where appropriate, changes will be made to the content of the certificate that better conform to current legislation and the reality of Security Data Seguridad en Datos y Firma Digital and the market. The old CA and its private key will only be used for CRL signing as long as they exist

active certificates issued by the old CA. A new CA will be generated with a new private key.

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

6.6.2. Subordinate AC.

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

6.7. DISASTER ENGAGEMENT AND RECOVERY.

6.7.1. Incident and Vulnerability Management Procedures.

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

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

In the event of an incident that alters or corrupts both hardware, software and data resources, Security Data Seguridad en Datos y Firma Digital will stop normal operations until a secure environment is established. At the same time, the relevant reviews will be carried out in order to identify the cause and arrange the necessary measures to avoid future repetitions.

In the event that digital certificates are issued during the uncertainty period and there is a risk that these certificates could be compromised, then these certificates will be revoked and subscribers will be notified of the need to reissue their certificates.

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

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

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

- It will inform all subscribers, users and other CAs with whom it has agreements or other types of relationship of the commitment, at least by publishing a notice on the CA's website.

- It will indicate that the certificates and information regarding the status of the revocation, signed using this key are invalid.

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

6.7.4. Business Continuity after a disaster.

For business continuity, Security Data has defined that:

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

6.8. TERMINATION OF CA OR RA.

6.8.1. Certification Authority.

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

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

6.8.2. Registration Authority.

In the event of the cessation of a registration authority for a specific group, Security Data Data Data Security and Digital Signature:

- It will stop issuing and renewing certificates of that RA.
- It will revoke the operator certificates of that RA.

- It will revoke the subscriber certificates issued by that RA, unless expressly decided otherwise.

7. Technical Security Controls.

7.1. KEY PAIR GENERATION AND INSTALLATION.

The generation and installation process will be performed as defined in the Security Data DPS.

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

7.2.1. Standards for Cryptographic Modules.

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

The keys of DSCF-recognized certificate subscribers and operators and administrators are securely generated by the data subject using a CC EAL4+, FIPS 140-1 Level 3, ITSEC E4 High or other equivalent level cryptographic device.

Cryptographic devices that safeguard the private key of the DSCF-recognized certificate subscriber and the operator or administrator provide a level of security.

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

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

7.2.3. Custody of the Private Key.

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

Subordinate CA private keys are held on secure FIPS 140-2 Level 3 certified cryptographic devices.

7.2.4. Backup of the Private Key of the CA.

There are devices that allow the restoration of the private key of the CA, which are stored securely and only accessible by authorized personnel according to the trusted roles, using at least a dual control on a secure physical medium.

Root CA keys can be restored in accordance with the Procedure for Ensuring Compliance with CA Operations.

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

7.2.5. Subscriber's Private Key File.

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

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

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

Security Data does not generate, store, or archive the subscriber's private signing key under any circumstances. Sole control of the private key resides solely with the subscriber.

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

There is an internal procedure for the CA key ceremony, which describes the processes of generating the private key 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 storage in the cryptographic module.

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

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

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

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

7.2.8. Private Key Activation Method.

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

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

7.2.9. Private Key Deactivation Method.

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

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

7.2.10. Private Key Destruction Method.

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

Criteria for destruction:

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

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

7.2.11. Classification of the cryptographic module.

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

7.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT.

7.3.1. Public Key File.

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

7.3.2. Certificate Operating Periods and Key Pair Usage Period.

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

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

7.4. ACTIVATION DATA.

7.4.1. Generation and Installation of Activation Data.

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

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

7.4.2. Protection of Activation Data.

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

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

7.4.3. Other aspects of activation data.

Not stipulated.

7.5. COMPUTER SECURITY CONTROLS.

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

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

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

7.5.1. Specific Technical Safety Requirements.

Each CA server includes the following functionality:

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

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

7.5.2. Computer Security Classification.

The security of the equipment is reflected by an initial risk analysis in such a way that the security measures implemented are a response to the probability and impact produced when a group of defined threats can take advantage of security breaches.
The physical protection of the environment is supported by the facilities mentioned above, while personnel management is efficiently handled due to the small group of staff operating in the data center of Security Data Seguridad en Datos y Firma Digital.

7.6. TECHNICAL CONTROLS OF THE LIFE CYCLE.

7.6.1. Systems Development Controls.

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

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

7.6.2. Security Management Controls.

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

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

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

a) General management of CA:

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

b) Certificate Generation:

- The CA facilities are equipped with continuous monitoring systems and alarms to detect, record and be able to act immediately in the event of an attempt to access their resources without authorization and/or irregularity.
- The authentication to carry out the issuance process is carried out by a system m of n operators for the activation of the private key of the AC.

c) Revocation management:

- Revocation refers to the loss of effectiveness of a digital certificate permanently. The revocation will be done by 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 AC operator.

d) Revocation Status:

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

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

7.6.3. Lifecycle Security Controls.

Security Data manages lifecycle security by:

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

7.7. NETWORK SECURITY CONTROLS.

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

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

7.8. TIME STAMPING.

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

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

8. Certificate, CRL and OCSP profiles.

8.1. CERTIFICATE PROFILE.

The profiles of the certificates are defined in the corresponding PC and CPS.

8.2. CRL PROFILE.

The CRL profile is defined in the Security Data CPS.

8.3. OCSP PROFILE.

The OCSP profile is defined in the Security Data CPS.

9. Compliance Audit and Other Assessments.

9.1. FREQUENCY OF AUDITS.

The frequency of audits is performed as defined in the Security Data CPS.

9.2. QUALIFICATION OF THE AUDITOR.

The process is carried out as defined in the Security Data CPS.

9.3. RELATIONSHIP BETWEEN THE AUDITOR AND THE AUDITED AUTHORITY.

The process is carried out as defined in the Security Data CPS.

9.4. ASPECTS COVERED BY THE CONTROLS.

The process is carried out as defined in the Security Data CPS.

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

The process is carried out as defined in the Security Data CPS.

9.6. COMMUNICATION OF RESULTS.

The process is carried out as defined in the Security Data CPS.

10. Other business and legal matters.

10.1. RATES.

The communication of the rates will be made as defined in the Security Data CPS.

10.2. FINANCIAL RESPONSIBILITY.

The insurance coverages are defined in the Security Data CPS.

10.3. CONFIDENTIALITY OF BUSINESS INFORMATION.

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

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

10.3.1. Scope of Confidential Information.

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

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

10.3.2. Non-Confidential Information.

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

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

10.3.3. Duty to Protect Confidential Information.

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

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

10.4. PRIVACY OF PERSONAL INFORMATION.

10.4.1. Privacy Policy.

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

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

10.4.2. Information treated as Private.

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

10.4.3. Information Not Classified as Private.

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

10.4.4. Responsibility for the Protection of Personal Data.

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

Owners may exercise their rights of access, deletion, rectification and opposition through the channels defined in the Privacy Policy published on the Security Data website.

10.4.5. Notice and Consent to Use Personal Data.

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

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

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

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

10.4.7. Other circumstances of disclosure of information.

It is not stipulated.

10.5. INTELLECTUAL PROPERTY RIGHTS.

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

10.6. REPRESENTATIONS AND WARRANTIES.

Representations and warranties are defined in the Security Data CPS.

10.7. DISCLAIMERS OF WARRANTIES.

Disclaimers of warranties are defined in the Security Data CPS.

10.8. LIMITATIONS OF LIABILITY.

The limitations of liability are defined in the Security Data CPS.

10.9. COMPENSATION.

Compensation will be made in accordance with the definition of the Security Data CPS.

10.10. TERM AND TERMINATION.

10.10.1. Term.

This Security Policy Statement document and any amendments to it will become effective upon publication on the SECURITY DATA website, and will remain in effect until it is replaced by a newer version.

10.10.2. Termination.

This Security Policy Statement document, and any amendments will remain in effect until modified or replaced by a newer version.

10.11. INDIVIDUAL NOTICES AND COMMUNICATIONS.

In general, the SECURITY DATA website will be used to make any type of notification and communication. In the event of security problems or loss of integrity that may affect a natural or legal person, SECURITY DATA will notify them of this incident. It may also notify the affected owners and the Data Protection Authority directly and expeditiously, in accordance with the established legal deadlines.

10.12. AMENDMENTS.

As defined in the Security Data CPS.

10.13. DISPUTE RESOLUTION.

As defined in the Security Data CPS.

10.14. GOVERNING LAW.

Law on Electronic Commerce, Electronic Signatures and Data Messages, its Regulations; Organic Law on the Protection of Personal Data (LOPDP) and its Regulations; Organic Code of the Social Economy of Knowledge in relation to intellectual property. Organic Law on Consumer Protection, Organic Law on Transparency of Information and Accreditation of ARCOTEL, Technical Standard for the Provision of Certification Services and Related Services, issued by the Agency for the Regulation and Control of Telecommunications (ARCOTEL).

10.15. COMPLIANCE WITH APPLICABLE LAW.

Certificates issued under SECURITY DATA will be used by subscribers and relying third parties only in accordance with the laws and regulations of the jurisdiction in which they are used or based.

10.16. MISCELLANEOUS PROVISIONS.

The provisions are defined in the Security Data CPS.

10.17. OTHER PROVISIONS.

No stipulation.

11. Control of Approvals.

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