certicámara.

Code:	IDI-L-001
Date:	11/11/2026
Version:	004
Labeling:	PUBLIC

CERTIFICATION PRACTICE STATEMENT

certicámara.

Certification Practice Statement

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

certicámara.

Code:	IDI-L-001
Date:	11/11/2026
Version:	004
Labeling:	PUBLIC

CERTIFICATION PRACTICE STATEMENT

Table of Contents

1. INTRODUCTION **8**
1.1 Identification of the Digital Certification Entity 8
1.2 Document Name and Identification 9
1.3 PKI Participants 9
1.3.1 Certification Authorities 9
1.3.2 Registration Authorities 11
1.3.3 Subscribers 11
1.3.4 Relying Parties 12
1.3.5 Other Participants 12
1.4 Certificate Use 13
1.4.1 Appropriate Uses of the Certificate 13
1.4.2 Prohibited Certificate Uses 13
1.5 Policy Administration 14
1.5.1 Organización que administra el documento 14
1.5.2 Contact Person 14
1.5.3 Procedure for the Update and Approval of the CPS 14
1.6 Definitions and Acronyms 15
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES **17**
2.1 Repositories 17
2.2 Subordinate CA Certicámara S.A. 18
2.3 Time or Frequency of Publication 19
2.3.1 Root CA Certificates 19
2.3.2 Certificate Revocation List (CRL) 19
2.3.3 OCSP Certificate Revocation Status 19
2.4 Repository Access Controls 19
3. IDENTIFICATION AND AUTHENTICATION **19**
3.1 Naming 20
3.1.1 Name Types 20
3.1.2 Need for Names to be Meaningful 20
3.1.3 Anonymity or Pseudonymity of Subscribers 20
3.1.4 Rules for Interpreting Various Name Forms 21
3.1.5 Uniqueness of Names 21
3.1.6 Recognition, Authentication, and Role of Trademarks 21
3.2 Initial Identity Validation 21
3.2.1 Method to Prove Possession of the Private Key 21
3.2.2 Authentication of Organization or Individual Identity 21

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

3.2.3 Verification of Representation Powers 22
3.2.4 Identity Validation Mechanisms 22
3.2.5 Unverified Subscriber Information 22
3.2.6 Interoperability Criteria 22
3.3 Identification and Authentication for Key Renewal Requests 22
4. CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENT 22
4.1 Certificate Application 22
4.1.1 ¿Who can submit a certificate application? 25
4.2 Certificate Issuance 26
4.2.1 CA Actions During Certificate Issuance 26
4.2.2 Subscriber Notification of Certificate Issuance by the CA 26
4.3 Physical Delivery of the Digital Certificate to Subscribers 26
4.3.1 Coverage 26
4.3.2 Delivery Requirements 26
4.3.3 Delivery Turnaround Time – Physical Certificates 27
4.3.4 Download Time 27
4.4 Certificate Acceptance 28
4.4.1 Certificate Publication by the CA 28
4.4.2 Notification of Certificate Issuance by the CA to Other Entities 28
4.5 Withdrawal 28
4.6 No Refund of Money 29
4.7 Use of Key Pairs and Certificates 29
4.7.1 Generation and Installation of Key Pairs 29
4.7.2 Subscriber Certificate and Private Key Use 29
4.7.3 Relying Party Certificate and Public Key Use 29
4.8 Certificate Renewal 29
4.8.1 Renewal Times 29
4.8.2 ¿Who can request a renewal? 30
4.8.3 Processing Certificate Renewal Requests 30
4.8.4 Notification of New Certificate Issuance to the Subscriber 30
4.9 Certificate Key Renewal 30
4.10 Certificate Modification 30
4.11 Certificate Revocation 30
4.11.1 Grounds for Revocation 31
4.11.2 ¿Who can request revocation? 32
4.11.3 Revocation Request Procedure 32
4.11.4 Revocation Request Grace Period 33

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

4.11.5 CRL Issuance Frequency 33
4.11.6 Availability of Online Status/Revocation Verification 33
4.11.7 Online Revocation Verification Requirements 34
4.11.8 Suspension Circumstances 34
4.12 Replacement of Digital Signature Certificates 34
4.12.1 Grounds for Replacement 35
4.13 Certificate Characteristics 36
4.13.1 Operational Characteristics 36
4.13.2 Service Availability 36
4.13.3 Optional Functions 37
4.14 Termination of the Subscription 37
4.15 Key Custody and Recovery 37
4.15.1 Key Custody and Recovery Policy and Practices 37
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 37
5.1 Physical Controls 37
5.1.1 Ubicación y construcción del sitio 37
5.1.2 Physical Access 37
5.1.3 Power and Air Conditioning 38
5.1.4 Water Exposure 38
5.1.5 Fire Prevention and Protection 38
5.1.6 Media Storage 38
5.1.7 Waste Disposal 39
5.1.8 Off-site Backup 39
5.2 Procedural Controls 39
5.2.1 Trusted Roles 39
5.2.2 Number of Persons Required per Task 39
5.2.3 Identification and Authentication for Each Role 39
5.2.4 Roles Requiring Segregation of Duties 40
5.3 Personnel Controls 40
5.3.1 Qualifications, Experience, and Authorization Requirements 40
5.3.2 Background Check Procedures 40
5.3.3 Training Requirements 40
5.3.4 Sanctions for Unauthorized Actions 40
5.3.5 Independent Contractor Requirements 41
5.3.6 Documentation Supplied to Personnel 41
5.4 Audit Logging Procedures (Logs) 41
5.4.1 Types of Events Recorded 41

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

5.4.2 Log Processing Frequency 41
5.4.3 Audit Log Retention Period 41
5.4.4 Protection of the Audit Log 41
5.4.5 Vulnerability Assessments 42
5.5 Records Archival 42
5.5.3 Archive Protection 42
5.5.4 Archive Backup Procedures 42
5.5.5 Procedures to Obtain and Verify Archive Information 42
5.6 Key Rollover (Change of Key) 42
5.7 Compromise and Disaster Recovery 43
5.7.1 Incident Handling and Compromise Procedures 43
5.7.2 Business Continuity Capabilities After a Disaster 43
5.8 Cessation of Activities 44
6. TECHNICAL SECURITY CONTROLS 44
6.1 Generation and Installation of Key Pairs 44
6.1.1 Delivery of Private Key to the Subscriber 45
6.1.2 Delivery of Public Key to the Certificate Issuer 45
6.1.3 Delivery of CA Public Key to Relying Parties 45
6.1.4 Key Sizes 45
6.1.5 Key Usage Purposes (according to the X.509 v3 Key Usage Field) 46
6.2 Private Key Protection and Cryptographic Module Engineering 46
6.2.1 Cryptographic Module Standards and Controls 46
6.2.2 Private Key (K of N) Multi-Person Control 47
6.2.3 Custody of the Private Key 47
6.2.4 Private Key Backup 47
6.2.5 Private Key Archival 47
6.2.6 Storage of Private Keys in a Cryptographic Module 47
6.2.7 Private Key Activation Method 47
6.2.8 Private Key Deactivation Method 48
6.2.9 Private Key Destruction Method 48
6.2.10 Cryptographic Module Rating 48
6.3 Other Aspects of Key Pair Management 48
6.3.1 Public Key Archival 48
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 48
6.4 Activation Data 48
6.4.1 Generation and Installation of Activation Data 48
6.4.2 Protection of Activation Data 48

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

6.5 Computer Security Controls 49
6.5.1 Specific Technical Computer Security Requirements 49
6.5.2 Computer Security Rating 49
6.6 Technical Lifecycle Controls 49
6.6.1 System Development Controls 49
6.6.2 Security Management Controls 50
6.6.3 Lifecycle Security Controls 50
6.7 Network Security Controls 50
6.8 Time-Stamping 50
7. CERTIFICATE, CRL, AND OCSP PROFILES 50
7.1 Certificate Profile 50
7.1.1 Version Number(s) 50
7.1.3 Algorithm Object Identifiers 51
7.1.4 Name Forms 51
7.1.5 Name Restrictions 51
7.1.6 Certificate Policy Object Identifier 51
7.1.7 Syntax and Semantics of Policy Qualifiers 52
7.2 Certificate Revocation List Profile 52
7.2.1 Version Number(s) 52
7.2.2 CRL and CRL Entry Extensions 52
7.3 OCSP Profile 52
7.3.1 Version Number(s) 52
7.3.2 OCSP Extensions 52
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 52
8.1 Frequency or Circumstances of Assessment 52
8.2 Identity/Qualifications of the Assessor 53
8.3 Relationship of the Assessor to the Assessed Entity 53
8.4 Actions Taken as a Result of a Non-Compliance 53
8.5 Communication of Results 53
9. OTHER LEGAL AND COMMERCIAL MATTERS 54
9.1 Fees 54
9.1.1 Certificate Issuance or Renewal Fees 54
9.1.2 Fees for Access to Revocation or Status Information 54
9.1.3 Refund Policy 54
9.2 Financial Liability 55
9.2.1 Insurance Coverage 55
9.3 Confidentiality of Information 55

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

9.3.1 Scope of Confidential Information 56
9.3.2 Information Outside the Scope of Confidential Information 56
9.3.3 Responsibility to Protect Confidential Information 57
9.3.4 Processing of Personal Data 57
9.3.5 Disclosure Pursuant to a Judicial or Administrative Process 58
9.4 Intellectual Property Rights 59
9.5 Obligations and Responsibilities of the Participating Parties 59
9.5.1 Obligations and Duties of Certicámara 59
9.5.2 Obligations and Duties of the Applicant 61
9.5.3 Obligations and Responsibilities of the Subscriber 61
9.5.4 Obligations and Responsibilities of the Relying Party 64
9.5.5 Contractor Obligations 64
9.6 Limits of Liability 65
9.7 Rights of Participating Parties 66
9.7.1 Rights of the Applicant 66
9.7.2 Rights of the Subscriber 66
9.8 Exclusion of Warranties / Disclaimers 66
9.9 Contract Templates 67
9.10 Management Policy for Other Services 67
9.11 Impartiality and Non-Discrimination 67
9.12 Petitions, Complaints, Claims, Suggestions, and Compliments Policy 68
9.13 Dispute Resolution Provisions 71
9.14 Applicable Law 72
9.15 Certification Policies 72
10. CHANGE CONTROL 73

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

certicámara.

Code:	IDI-L-001
Date:	11/11/2026
Version:	004
Labeling:	PUBLIC

CERTIFICATION PRACTICE STATEMENT

1. INTRODUCTION

This Certification Practice Statement (CPS) constitutes the public disclosure of the Open Digital Certification Authority, setting forth the rules and practices adopted by the Certification Authority for the provision of digital certification services. These practices are established in accordance with Law 527 of 1999 and its compiling and amending decrees (Decree 1074 of 2015, Decree 620 of 2020), as well as Law 2106 of 2019, Law 1581 of 2012, Law 1898 of 2018 (Article 13.10), and Decree-Law 019 of 2012 (specifically the activities outlined in Article 161).

This document details the practices for the accredited services offered by Sociedad Cameral de Certificación Digital Certicámara S.A.: Digital Signature Certificate Issuance, Time Stamping, Certified Biometric Fingerprint, Certified Email, Digital Signature Generation, and Certified Electronic Signature Generation.

The CPS is intended for natural and legal persons who request or use digital certification services, as well as relying parties who depend on their legal validity and evidentiary value across various application contexts.

This document has been structured in accordance with the RFC 3647 standard.

1.1 Identification of the Digital Certification Entity

Sociedad Cameral de Certificación Digital Certicámara S.A. (hereinafter, Certicámara) is a corporation established by the Chambers of Commerce of Bogotá, Medellín, Cali, Bucaramanga, Cúcuta, Aburrá Sur, and Confecámaras to provide digital certification services. As a subsidiary of the Bogotá Chamber of Commerce, Certicámara operates as an Open Digital Certification Authority, serving as a trusted third party to ensure the security of electronic products and services. Its primary purpose is to provide businesses and Internet users nationwide with the necessary tools to conduct electronic transactions with legal certainty.

Name:	Sociedad Cameral de Certificación Digital Certicámara S.A.
Tax ID (NIT):	830.084.433-7
Commercial Registration Number:	1079279
Certificate of Existence and Legal Representation:	https://web.certicamara.com/nosotros
Headquarters:	Bogotá
Address:	Carrera 7 N° 26-20 Pisos 18, 19 y 31

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

Teléfono (asuntos administrativos):	(601) 9157808
Email:	info@certicamara.com
Sales Phone:	(601) 7442725
Appointment Scheduling for Signature Installation:	https://zcal.co/t/agendate/certicamara/certicamara
Party Responsible for Handling Subscriber and User Petitions, Complaints, and Claims (PQRS):	Dirección de Implementación y Servicio
PQRS Portal/Email:	https://pqrf.certicamara.com/registrar
Website:	www.certicamara.com
Accreditation Certificate No.:	16-ECD-002
Accreditation Certificate:	https://onac.org.co/certificados/16-ECD-002.pdf

1.2 Document Name and Identification

For the provision of its various services, Certicámara sets forth the following information for this document.

Name:	Declaración de Prácticas de Certificación – DPC
Fecha de publicación:	11/11/2026
Version:	004
Code:	IDI-L-001
Location:	https://web.certicamara.com/marco-normativo

Note: Should you require access to a previous version of this document, it must be requested through the form at https://pqrf.certicamara.com/registrar in order for your request to be processed.

1.3 PKI Participants

1.3.1 Certification Authorities

It is a trusted entity that provides certification services. It is authorized to issue, manage, and revoke digital certificates, acting as a trusted third party between the subscriber and the certificate holder, or relying parties.

Certicámara has the following CA::

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

CERTIFICATION PRACTICE STATEMENT

Root Certification Authority (Root CA): The Root CA is the origin Certification Authority of the digital certification hierarchy. This component of Certicámara is responsible for issuing the digital certificates that accredit its issuance platform.

Its data structure is:

- Root Certificate Field
- Root Certificate Value
- Root CA Key: 4096 bits
- Validity: Until May 24, 2031, 01:39:46 PM
- Version: V3
- Certificate Serial Number: Unique certificate identifier. Less than 32 hexadecimal characters.
- Certificate Signature Algorithm: SHA256withRSAEncryption
- SHA1: 54 63 28 3b 67 93 ff 55 27 7c ed e3 90 98 e8 04 22 f9 12 f7
- Serial Number: 43 1c 28 c6 74 0f ed 25 57 44 9f f2 fd 0e 5e 14

Subordinate Certification Authorities

Within the Colombian regulatory framework, these are derived from the Root CA hierarchy, requiring the Root CA to sign their certificate so that they, in turn, can issue certificates to end subscribers, maintaining the chain of trust from Certicámara's root point as an Open Digital Certification Authority accredited by ONAC under Accreditation Certificate number 16-ECD-002.

For all CAs belonging to Certicámara's public key infrastructure, the provisions of the CPS apply, consistent with the general requirements established by the legal framework described in the regulatory references section.

The certificate data structure for subordinate authorities is:

- Root CA Certificate Field
- SUBORDINATE ENTITY Public Key: 4096 bits
- Version: V3
- Certificate Serial Number: Unique certificate identifier. Less than 32 hexadecimal characters.
- Certificate Signature Algorithm: SHA256withRSAEncryption
- Issuer Data
- CN: Root Certification Authority of the certification chain.
- SHA1: 26 c5 8f b4 36 4f f6 21 ce 2a 04 c7 3e bf b2 ac 09 c3 5f 56
- Serial Number: 58 1f 6a de 78 78 fe 8c 56 ac db d7 a6 77 58 10

Time Stamping Authority

"**Time stamping**" is provided by Certicámara in a secure and properly defined electronic format, integrated into the data message generated, transmitted, or received by the subscriber, thereby preventing its subsequent alteration. The "time stamp" of a data

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

message is unique to it and cannot be applied to any other data message or messages.

The **time stamping** service is located at the following URL:http://tsa.certicamara.com:9233/ where the subscriber must have a username and password to use the respective service.

This is explained as follows:(i) A user wants to obtain a time stamp for an electronic document they possess; (ii) A digital summary (technically a hash) is generated for the document on the device requesting the time stamp; (iii) This summary forms the request sent to the certification entity providing the **time stamping service**; (iv) The certification entity providing the **time stamping service** generates a time stamp (or chronological stamp) containing this digital summary, the date and time obtained from a reliable source, and the digital signature. In this way, by time-stamping this summarized representation of the document, the original document is effectively sealed; (v) The time stamp is sent back to the user; and (vi) The certification entity providing the time stamping services maintains a record of the issued stamps for future verification.

The structure of the TSA (Time Stamp Authority) Digital Time Stamping service is described in the RFC 3628 document, and the TSP (Time-Stamp Protocol) in RFC 3161.

1.3.2 Registration Authorities

Registration Authority (RA): It is responsible for receiving requests related to digital certification, registering applications submitted by applicants to obtain a certificate, verifying the veracity and correctness of the data provided by users in their requests, and forwarding compliant requests to a CA for processing.

Certicámara's registration authority is composed of:

- **RA Software:** Facilitates the registration of requests and enables the lifecycle management of the certification application.
- **RA Agents:** Privileged RA users responsible for reviewing and validating the information contained in the documents submitted by the applicant for the issuance of a digital certification entity (ECD) service.
- **RA Administrator:** The individual responsible for administering and configuring the RA.
- **System Auditor:** The individual responsible for auditing compliance with RA procedures and systems, validating that the provisions established in the Certification Practice Statement (CPS) and Certification Policies (CP) are met.

1.3.3 Subscribers

A Subscriber is the natural person to whom digital certification services are issued or activated and, therefore, acts as the subscriber and/or party responsible for it, with full

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

knowledge and acceptance of the rights and duties established and published in this CPS and the certification policy of the acquired service.

1.3.4 Relying Parties

Any natural or legal person, other than the subscriber and/or responsible party, who decides to accept and rely on the certification services provided by Certicámara.

1.3.5 Other Participants

a. Service Providers

Critical providers selected for the provision of Datacenter services satisfy the minimum requirements established in the Specific Accreditation Criteria document (CEA 3.0-7), available on the ONAC website. Therefore, they will be required to comply with the requirements detailed in said document where applicable.

Name:	Comunicación Celular S.A. Comcel S.A.
Tax ID (NIT):	800.153.993-7
Certificate of Existence and Legal Representation:	https://web.certicamara.com/nosotros
Headquarters:	Bogotá
Address:	Autopista Bogotá - Medellín, Km 7.5, Celta Trade Park, Funza, Cundinamarca, Colombia.
Phone (Administrative Matters):	(601) 7480000 - 7500300
Website:	www.claro.com.co

Name:	HostDime Colombia S.A.S.
Tax ID (NIT):	900.403.046-9
Certificate of Existence and Legal Representation:	https://web.Certicámara.com/nosotros
Headquarters:	Bogotá
Address:	Km 1.5 Vía Briceño Zipaquirá V Venganzo, Lote 9, Tocancipá, Cundinamarca
Phone (Administrative Matters):	3009108585
Email:	maria.diaz@sencinet.com
Website:	https://www.hostdime.com.co/

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

1.4 Certificate Use

1.4.1 Appropriate Uses of the Certificate

The root digital certificate may only be used for the identification of the root certification authority itself and for the secure distribution of its public key. The use of certificates issued by the Root CA shall be limited to signing digital certificates and signing the corresponding certificate revocation lists.

General uses applicable to digital certificates issued by Certicámara:

a) The **subscriber** may only use digital certificates for the purposes specified in the contract executed individually with Certicámara, those permitted under this **Certification Practice Statement and the Certification Policies**, and those allowed by virtue of Law 527 of 1999 and Decree 1074 of 2015 (which compiles Decree 333 of 2014). The contract entered into with the subscriber may limit the scope of use based on the environment in which the digital certificate is utilized or the special characteristics of the project being developed. Any other use shall be considered a violation of this **Certification Practice Statement and the Certification Policies**, constituting grounds for the revocation of the **digital signature certificate** and the termination of the contract with the subscriber, without prejudice to any corresponding criminal or civil actions.

b) The **subscriber** acknowledges and accepts that the advertised products and services are provided "as is" and as individually offered, that digital certificates primarily certify the identity of the natural person appearing as the service subscriber, that there is no implicit information implying additional services or benefits beyond those expressly mentioned, and that their use is the subscriber's exclusive responsibility, taking into account the provisions of Law 527 of 1999 and Decree 1074 of 2015 (which compiles Decree 333 of 2014).

c) The use of the digital certificate and the data messages digitally signed with it, including electronic monetary transactions regardless of their amount, are the sole responsibility of the corresponding subscriber. Therefore, Certicámara bears no liability whatsoever regarding the verification or public attestation of the signed data messages, as it does not know, nor does it have a legal obligation to know, the digitally signed messages or the amount of the transactions conducted using the digital certificate within third-party electronic transaction systems. In general, Certicámara, as an Open Digital Certification Authority and Trusted Third Party, does not assume liability for the subscriber's use of digital signature certificates; consequently, there are no financial limits applicable in this regard. To this end, the subscriber must comply with their duties as set forth in Law 527 of 1999 and Decree 1074 of 2015 (which compiles Decree 333 of 2014), and must bear the burden of liability imposed by said regulations.

1.4.2 Prohibited Certificate Uses

a) Digital certificates may not be used under any circumstances for illicit purposes or operations under any legal system in the world.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

b) Any use of digital certificates that is contrary to Colombian legislation, international treaties signed by the Colombian State, supranational regulations, public decency, sound commercial practices, or any provisions contained in this Certification Practice Statement and the contracts executed between Certicámara and the Subscriber is strictly prohibited.
c) Any use of digital certificates intended to violate any intellectual property rights of Certicámara or third parties is prohibited.
d) The physical medium of the digital certificate provided by Certicámara (if applicable) may only be used within the context of the Digital Certification System. No information other than that expressly authorized by Certicámara may be embedded into the provided physical medium, nor may it be used outside of the Digital Certification System.

1.5 Policy Administration

1.5.1 Organización que administra el documento

All information contained in this **Certification Practice Statement (CPS) and Certification Policies (CP)** constitutes the intellectual property of Certicámara, and its administration is carried out in accordance with the guidelines established herein.

1.5.2 Contact Person

Within Certicámara, it has been established that the contact person for matters related to this **Certification Practice Statement (CPS) and Certification Policies (CP)** is:

Position:	Process Director
Email:	angela.leandro@certicamara.com
Address:	Carrera 7 N° 26-20 Piso 18

1.5.3 Procedure for the Update and Approval of the CPS

The update of the Certification Practice Statement shall be carried out when required by legal, regulatory, and/or applicable requirements for the accredited services.

In this process, the individuals responsible for the various areas involved in providing the services within the scope will meet to evaluate the modifications to be made. Final approval of said changes is granted by the President.

The responsibility for managing the update of the CPS on Certicámara's website, specifically at the link https://web.certicamara.com/marco-normativo, rests with the Process Director.

FOR THE EXCLUSIVE USE OF CERTICAMARA S.A

1.6 Definitions and Acronyms

- **Algorithm:** A prescribed set of well-defined, ordered, and finite instructions or rules that allow an activity to be performed through successive steps without creating ambiguity for the person performing said activity. Given an initial state and following the successive steps, a final state is reached and a solution is obtained.
- **Certification Authority (CA):** A trusted entity responsible for issuing and revoking certificates.
- **Time Stamping Authority (TSA):** Time Stamp Authority.
- **Validation Authority (VA):** A trusted entity that provides information regarding the validity of digital certificates.
- **Root CA:** A first-level certification authority, the foundation of trust.
- **Subordinate CA:** A second-level or lower-level certification authority.
- **Digital Certificate:** An electronic data message signed by the digital certification entity, which identifies both the issuing certification entity and the subscriber, and contains the latter's public key.
- **Client:** In digital certification services, the term client identifies the natural or legal person with whom the digital certification entity (ECD) establishes a commercial relationship.
- **Signature Creation Data (Private Key):** Unique numerical values that, when used in conjunction with a known mathematical procedure, serve to generate the digital signature of a data message.
- **Signature Verification Data (Public Key):** Data, such as public cryptographic keys or codes, used to verify that a digital signature was generated using the subscriber's private key.
- **Certification Practice Statement (CPS):** Official document presented by the Digital Certification Entity, which defines the rules and practices of the Certification Authority for the provision of digital certification services.
- **Decline of Service Request:** The rejection of a digital certification service that falls outside the scope of the accreditation granted by ONAC or due to non-compliance with the law. In this scenario, there will be no opportunity for remediation by the user.
- **Open Certification Authority:** An entity that offers services inherent to an ECD to the general public, such that its use is not limited to the exchange of messages between the entity and the subscriber, and for which it receives remuneration.
- **Digital Certification Entity (ECD):** An entity authorized under the applicable law empowered to issue certificates related to individuals' digital signatures, offer or facilitate registration and time-stamping services for the transmission and reception of data messages, and fulfill other functions related to communications based on digital signatures.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

- **Time Stamping:** A digitally signed data message time-stamped by a TSA that links another data message to a specific point in time, providing evidence that this data existed at that moment and has not undergone any modification since the time stamp was applied.
- **ETSI:** European Telecommunications Standards Institute.
- **FIPS:** Federal Information Processing Standards are publicly announced standards developed by the United States government for use by all non-military government agencies and government contractors. Many FIPS standards are modified versions of standards used in wider communities (ANSI, IEEE, ISO, etc.).
- **Digital Signature:** A numerical value attached to a data message that, by utilizing a known mathematical procedure linked to the originator's key and the text of the message, allows it to be determined that this value was obtained exclusively with the originator's key and that the initial message has not been modified after the transformation was performed.
- **Electronic Signature:** Whenever any regulation requires the presence of a signature or establishes certain consequences in its absence regarding a data message, such requirement shall be deemed satisfied if:
    a) A method has been used to identify the originator of a data message and to indicate that the content has their approval;
    b) The method is both reliable and appropriate for the purpose for which the message was generated or communicated.
- **HASH Function:** An operation performed on a set of data of any size, such that the resulting output is another set of fixed-size data, regardless of the original size, which possesses the property of being uniquely associated with the initial data.
- **HSM:** Hardware Security Module.
- **LDAP:** Lightweight Directory Access Protocol.
- **Certificate Revocation List (CRL):** A list of digital certificates that have been revoked by the Certification Authority (CA), have not reached their scheduled expiration date, and should no longer be trusted.
- **Log:** An event recording service of the information system that preserves both previous and current information, identifying who performed the event and when.
- **Denial of Service Request:** A digital certification service will be denied due to reasons external to Certicámara S.A. and attributable to the user, provided that they can be remedied by the latter.
- **Technological Neutrality:** The principle of non-discrimination between information recorded on paper and information communicated or archived electronically, as well as the non-discrimination, preference, or restriction of any of the various techniques or technologies that can be used to electronically sign, generate, communicate, store, or archive information.
- **OID (Object Identifier):** An acronym for "Object Identifier," consisting of a unique identification number assigned based on international standards and commonly

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

used to identify documents, systems, equipment, etc., with the purpose, among other things, of determining the origin, ownership, and age of the identified object.

- **PKI (Public Key Infrastructure):** The set of hardware, software, policies, procedures, and technological elements that, through the use of a cryptographic key pair—a private key possessed exclusively by the service subscriber and a public key, which is included in the digital certificate.
- **Certificate Policies (CP):** The set of rules indicating the requirements of a certificate within a particular community and/or class, within the framework of legal and regulatory requirements, and with common security requirements.
- **Recommendation for Decision:** A communication issued by the Registration Authority (RA) to the Certification Authority (CA) to approve the request for the provision of services to the applicant by Certicámara S.A.
- **Revocation:** For the purpose of this document, the process by which an issued digital certificate is disabled and its period of validity for use is terminated as of the revocation date, occurring upon any of the causes established in the Certification Practice Statement.
- **Digital Certification Service:** A set of certification activities offered by the ECD to certify the origin and integrity of data messages, based on digital or electronic signatures, time stamping, as well as the applicability of accepted and current technical standards in Public Key Infrastructure (PKI).
- **Online Certificate Status Protocol (OCSP) Service:** A real-time query activity to the ECD system regarding the status of a digital certificate using the OCSP protocol.
- **Applicant:** A natural or legal person who, for the purpose of obtaining digital certification services from an ECD, demonstrates compliance with the requirements established in their CPS and CP to access the digital certification service.
- **Subscriber:** A natural or legal person in whose name a digital certificate is issued.
- **Token:** A cryptographic hardware device supplied by an ECD, which contains the digital certificate and the subscriber's private key.
- **Uptime:** A commitment in terms of the percentage of available time of an information system that the providing company undertakes to offer to its client per year.
- **Usability:** A term derived from the English word "Usability," used to denote the way in which a person can employ a particular tool effectively, efficiently, and satisfactorily to achieve a specific goal.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

The Root CA and Subordinate CA Certificates, as well as the Certificate Revocation List (CRL), will be available for consultation 365 days a year, 24 hours a day, 7 days a week. This service will be provided under a 99.8% availability agreement, and in the event of an interruption due to force majeure, the service will be restored within the timeframe established according to the availability percentage. For the PKI infrastructure, an availability of 99.8% is established.

2.2 Subordinate CA Certicámara S.A.

a) For the Certificate Revocation List (CRL):

- WEB:
- Root CA Certicámara S.A.
  http://www.certicamara.com/repositoriorevocaciones/ac_offline_raiz_certicamara_.cer

- Subordinate CA Certicámara S.A.
  http://www.certicamara.com/repositoriorevocaciones/ac_online_subordinada_certicamara_.crt
  http://www.certicamara.com/repositoriorevocaciones/ac_online_subordinada4096_certicamara_.crt

b) For the Certificate Revocation List (CRL):

- WEB:
  - Root CA Certicámara S.A.
    http://www.certicamara.com/repositoriorevocaciones/ac_raiz_certicamara.crl

  - Subordinate CA Certicámara S.A.
    http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara.crl
    http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_2014.crl
    http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica.crl

    http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_2014.crl

    http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_4096.crl?crl=crl

    http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_4096.crl?crl=crl

c) For the CPS:

- WEB:
  https://web.certicamara.com/marco-normativo

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

d) For Online Certificate Status Protocol (OCSP) certificate revocation status verification:

- WEB:
  http://ocsp.Certicamara.com

  http://ocsp.Certicamara.co

  http://ocsp4096.certicamara.co

Through this URL, the user can directly check the revocation status of a certificate; to do so, an OCSP client that complies with RFC 6960 is required. If the user does not have this OCSP client, they must download the full Certificate Revocation List (CRL).

The public repository of the Root CA does not contain any confidential or private information.

2.3 Time or Frequency of Publication

2.3.1 Root CA Certificates

The publication of the certificate will take place prior to its entry into force through Certicámara's website. The validity period is until Saturday, May 24, 2031, 13:39:46.

2.3.2 Certificate Revocation List (CRL)

The publication of the Certificate Revocation List (CRL) of the Subordinate CA Certicámara S.A. is carried out with a validity of three (3) days:

- Publication may occur a maximum of eight (8) hours after the last revocation, at any time of the day.

2.3.3 OCSP Certificate Revocation Status

The service is available continuously 24 hours a day, 365 days a year for web queries and updates automatically in the following cases:

- Every time a digital certificate is revoked.

2.4 Repository Access Controls

Access to the information published by the Root CA will be for consultation only, and its modification will be restricted to authorized personnel. The updating of public information will be carried out exclusively by Certicámara personnel assigned to this function.

Furthermore, consultation access to the CRL, issued certificates, the OCSP server, and the CPS in both their previous and updated versions is guaranteed.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

All certificates have a section called "Subject", the purpose of which is to allow the identification of the certificate subscriber. This section contains a DN (Distinguished Name) characterized by a set of attributes that form an unambiguous and unique name for each subscriber of the certificates issued by Certicámara.

3.1.1 Name Types

The attributes of each certificate type are established in the certificate issuance policy. Each certificate type will be identified by a unique OID (Object Identifier), included in the certificate as a policy identifier within the certificate properties.

OID	Policy Type
1.3.6.1.4.1.23267.50.1.1	Certificate of Affiliation with a Company / Entity on local and/or centralized devices
1.3.6.1.4.1.23267.50.1.2	Certificate of Representation of a Company / Entity on local and/or centralized devices
1.3.6.1.4.1.23267.50.1.3	Public Official Certificate on local and/or centralized devices
1.3.6.1.4.1.23267.50.1.4	Licensed Professional Certificate on local and/or centralized devices
1.3.6.1.4.1.23267.50.1.5	Natural Person Digital Certificate on local and/or centralized devices
1.3.6.1.4.1.23267.50.1.8.5	Natural Person Digital Certificate PKCS#10
1.3.6.1.4.1.23267.50.1.8.4	Legal Person Digital Certificate PKCS#10

3.1.2 Need for Names to be Meaningful

The defined policies ensure that the Distinguished Names (DN) of the certificates are sufficiently meaningful to link the public key with a specific identity.

3.1.3 Anonymity or Pseudonymity of Subscribers

Certicámara does not allow anonymous names or pseudonyms to identify a natural or legal person. In the case of an entity or legal person, the name must be exactly identical

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

to its corporate name (razón social); abbreviated names are not permitted. In the case of a natural person, the name must consist of the first and last names as they appear on their officially recognized identification document. Exceptionally, contractions or abbreviations may be used provided there is prior, express, and written consent from the holder, and documentary evidence of such authorization is preserved.

3.1.4 Rules for Interpreting Various Name Forms

The rules used to interpret the distinguished names in the issued certificates are described in ISO/IEC 9595 (X.500) Distinguished Name (DN). Additionally, all issued certificates use UTF-8 encoding for all attributes, in accordance with RFC 5280 ("Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile").

3.1.5 Uniqueness of Names

The Root CA defines the DN (Distinguished Name) field of the Authority Certificate as unique and unambiguous. To achieve this, the name or corporate name of the certificate holder will be included as part of the DN, specifically within the CN (Common Name) field.

3.1.6 Recognition, Authentication, and Role of Trademarks

The Digital Certification Entity (ECD) does not assume commitments regarding the use of a trademark by Subscribers during certificate issuance; therefore, the ECD is not obligated to search for evidence of trademark ownership prior to issuing certificates.

A certificate applicant retains all rights they possess (if any) in any trademark, service mark, or trade name contained in any certificate application and distinguished name within any certificate issued to said applicant.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of the Private Key

The certification system implemented and used by Certicámara to manage the life cycle of its certificates automatically controls and guarantees that the signed certificate is issued exclusively to the holder of the private key corresponding to the public key included in the request. This guarantee is achieved through the PKCS#10 format, which includes a digital signature of the request itself, generated using the private key corresponding to the public key of the certificate.

3.2.2 Authentication of Organization or Individual Identity

In the identity authentication process of the organization or individual, the applicant is required to provide the relevant documentation for each accredited service. Likewise,

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

the applicant must provide Certicámara with information that is truthful, sufficient, and appropriate in compliance with the established requirements.

3.2.3Verification of Representation Powers

The verification of the applicant's representation powers before Certicámara will be carried out by querying the Single Business and Social Registry (RUES) or by verifying the legal documents that, in accordance with Colombian legislation, accredit and authorize their role as a legal representative.

3.2.4 Identity Validation Mechanisms

3.2.4.1 Identity Verification

Certicámara, as an Open Digital Certification Authority, will perform identity verification through defined mechanisms, using reliable sources and data provided by third parties with whom Certicámara maintains a current contract for this purpose.

3.2.4.2 Biometric Identity Verification

If required, Certicámara may validate the applicant using established biometric identification to ensure that the applicant is who they claim to be.

3.2.5 Unverified Subscriber Information

Certicámara, in its capacity as an Open Digital Certification Authority, verifies the information provided by the applicant that can be supported by evidentiary documentation. Regarding information that lacks documentary support—such as physical address, email, and similar data—the applicant's principle of good faith will apply at the time of submission.

3.2.6 Interoperability Criteria

Certicámara, as an Open Digital Certification Authority, does not contemplate interoperability with external ECDs. It only contemplates the issuance of digital certificates within its own Subordinate CA.

However, should the need arise due to commercial and/or regulatory reasons to establish interoperability with another ECD, the different execution scenarios must be evaluated to guarantee proper service delivery.

3.3 Identification and Authentication for Key Renewal Requests

Certicámara does not include the renewal of digital certificates while maintaining the subscriber's original key pair within its processes. If it is necessary to renew a previously issued certificate, a new issuance request process must be carried out, which will include the generation of a new key pair.

4. CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENT

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

4.1 Certificate Application

The application process can be carried out through any of the following methods:

1. In-person by visiting Certicámara's facilities.
2. Through the Contact Center.
3. Through any other electronic means provided by Certicámara.

The received applications will be reviewed by the Registration Authority (RA) in accordance with the specific accreditation criteria established by ONAC and those defined internally by Certicámara. This review will be conducted within a maximum period of two (2) business days from the receipt of all required documents, proof of payment, and successful validation of the applicant's identity. Once the review is complete, the applications will be forwarded to the Certification Authority (CA) for issuance, which will take place within a maximum of one (1) business day.

According to the internal policies of Certicámara S.A., all documentation provided by the applicant must be in Spanish. If a document is submitted in another language, it must be accompanied by an official translation carried out by a translator certified by the Ministry of Foreign Affairs. The documentation will be preserved according to Certicámara's document retention schedules. The applicant's information will not be made public without their explicit consent.

By using and electronically signing the digital signature certificate of Certicámara S.A., the applicant fully and unreservedly accepts the following documents, which form an integral part of this CPS and the service agreement contract: the Terms and Conditions of the service, the Declarations and Commitments on the prevention of ML/FT/FPWMD and C/TS (Money Laundering, Terrorist Financing, Financing of the Proliferation of Weapons of Mass Destruction, and Smuggling / Transnational Bribery), the Certificate Policy (CP), personal data processing, and the organizational policies of Certicámara S.A., available on Certicámara's website.

The Terms and Conditions of the digital signature certification service are applicable from the moment the applicant expresses interest in acquiring the certificate and remain in force throughout its validity, along with the general service contracting conditions.

Applicants must take the following into account before requesting any service from Certicámara S.A.:

a) **Reading Documentation:** Having completely read the Terms and Conditions of the digital signature certification service, the Declarations and Commitments for the prevention of ML/FT/FPWMD and C/TS, this Certification Practice Statement (CPS), the Certificate Policy (CP), and the personal data processing policy.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

b) **Verification of Information:** Verifying the information mentioned by Certicámara S.A. to make an informed decision regarding the digital signature certificate application, in compliance with Law 527 of 1999, Decree 019 of 2012, Law 1341 of 2009, Law 1978 of 2019, Law 1581 of 2012, Decree 1074 of 2015, Decree 358 of 2020, Decree 1538 of 2020, and Decree 620 of 2020.

c) **Provision of Information:** The client must provide updated and available contact information that allows them to be contacted to carry out the processes associated with the issuance of the digital signature, ensuring that these do not have restriction configurations, security filters, or any other additional adjustments or authorizations in their domains. The email address and mobile phone number linked to a device provided in the application will be the authorized communication channels for sending notifications associated with the process; therefore, by submitting this data, authorization is granted to send communications for this purpose.

d) **Password Assignment:** To use the digital certificate, it is necessary for the holder to assign a password. The implications in the event that it is forgotten or lost are detailed below:

- **Virtual Token:** Password resetting can be performed through the website, at the link https://ventadigital.certicamara.com/reset-password at no additional cost for up to ten (10) times; subsequent requests will incur an associated fee.
- **Physical Token:** Because Certicámara S.A. does not possess recovery mechanisms, as it remains stored locally, purchasing a new certificate will be required, which carries an associated cost.

The holder must remember and securely safeguard the password. This password is the exclusive means to access the issued certificate.

e) **Technical and Security Knowledge:** Knowing the technological and security requirements for using the digital signature certificate. Being informed about the characteristics of the Certicámara S.A. certificate, its reliability level, limits of liability, customer obligations, and the security measures necessary for its use.

f) **Right to Non-Provision of Service:** Keeping in mind that Certicámara S.A. may reserve the right not to issue a digital signature certificate due to technical conditions, without this generating any liability.

g) **Identity Verification by Certicámara S.A.:** Certicámara S.A., as an Open Digital Certification Authority, will previously perform identity verification using reliable sources and data provided by third parties with a current contract for this purpose.

h) **Request for Additional Documents:** Certicámara reserves the right to request additional documents or copies of those required in the application form when it deems it necessary to verify the identity or any status of the applicant. It may also

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

waive the presentation of documents if the applicant's identity has been sufficiently verified by other means. These additional documents may include (without limitation):

- Commercial references of the company.
- Personal references of the applicant.
- Bank certifications.
- Valid driver's license.
- Military ID card.
- Health social security system affiliation document.
- Professional risk management company (ARL) affiliation document.
- Other documents that allow verifying the identity or powers of the subscriber or the entity for the issuance of any type of certificate.

i) **Database Querying:** Certicámara may query identity information databases of public or private entities to perform the validations necessary to issue the digital certificate.

j) **SAGRILAFT Compliance:** It will query the databases necessary to comply with SAGRILAFT, subject to the applicant's prior acceptance of the Declarations and Commitments for the prevention of ML/TF/FPWMD and S/TB (Money Laundering, Terrorist Financing, Financing of the Proliferation of Weapons of Mass Destruction, and Smuggling / Transnational Bribery), published on the Certicámara S.A. website.

k) **Certificate Validity:** Digital signature certificates will be issued with a maximum validity of two (2) years.

l) **Denial or Decline of the Application:** Certicámara S.A. may deny the issuance of a digital certificate when it falls outside the scope of the accreditation granted by ONAC, due to non-compliance with the law, and/or when in its judgment it threatens its good name as an ECD. In this case, there will be no opportunity for remediation by the user. If Certicámara decides to deny or decline the application, it will notify the applicant via email, indicating the reasons.

m) **Development for Mac OS:** Currently, Certicámara is developing the infrastructure for compatibility in the issuance of digital signature certificates for the Mac OS operating system.

4.1.1 ¿Who can submit a certificate application?

The application for a digital certificate may be made by any natural person in full exercise of their legal capacity, as well as by legal entities through their legal representative, a proxy, an employee, or a duly authorized third party, provided that such

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

status is proven with the documents required by the Registration Authority (RA). In the case of minors, the digital signature application must be submitted by their representative, attaching the minor's identification document and the document accrediting representation in accordance with current civil regulations.

4.2 Certificate Issuance

4.2.1 CA Actions During Certificate Issuance

Once the issuance request has been approved, the Certification Authority (CA) proceeds to generate the corresponding certificate, which is associated with a key pair and digitally signed using the CA's certificate, which forms part of the Certicámara chain of trust.

The issuance of certificates requires the authorization of the request by the Subordinate CA system. Following approval, the certificates are securely issued and made available to the subscriber.

During the issuance process, the Subordinate CA performs the following actions:

- Implements a certificate generation procedure that establishes a secure link between the certificate and the registration information, including the certified public key.
- Guarantees the protection of the confidentiality and integrity of the registration data.
- The validity of all certificates begins once the holder downloads or activates the digital signature; under no circumstances will a certificate be issued with a validity period that precedes the current date.

4.2.2 Subscriber Notification of Certificate Issuance by the CA

The subscriber will be notified of the successful issuance of their certificate via an email sent to their registered address.

4.3 Physical Delivery of the Digital Certificate to Subscribers

4.3.1 Coverage

The delivery of digital certificates will be carried out in accordance with the coverage matrix of the delivery service of the logistics operator that maintains a current contract with Certicámara for this purpose, or through direct delivery by a staff member from Certicámara's logistics department. In both scenarios, the physical device will be delivered, and the link to the download instructions will be shared in the approval email sent to the holder.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

4.3.2 Delivery Requirements

The physical device will be delivered by the logistics operator to the reported address or may be picked up by the subscriber at Certicámara's facilities, in accordance with what is indicated on the application form. When the holder authorizes a third party to claim the device at the facilities, the third party must physically present the authorized third-party form, which can be downloaded from Certicámara's website at the following link: https://web.certicamara.com/soporte/formatos

The form titled "Authorized Third Party" must be properly completed and signed by both parties. Additionally, photocopies of the identification documents of both the holder and the authorized third party must be presented.

The logistics operator's waybill will serve as evidence of acknowledgment of receipt of the physical device, and for deliveries at Certicámara's facilities, formal delivery documentation will be maintained.

4.3.3 Delivery Turnaround Time – Physical Certificates

The estimated delivery times from the issuance of the certificate are:

- **Bogotá and nearby municipalities:** Approximately two (2) business days.
- **Department capital cities:** Approximately two (2) to four (4) business days.
- **Other municipalities:** Approximately four (4) to five (5) business days.
- **Special municipalities or destinations:** Approximately six (6) to fifteen (15) business days.

In the event that delivery is not possible, a second attempt will be made. If this also fails, the logistics operator will return the digital certificate to Certicámara's facilities.

If delivery is not possible due to reasons attributable to the subscriber, Certicámara or the logistics operator will contact them to coordinate the delivery. However, it is important to keep in mind that if a delivery or pickup date is not coordinated within a period of three (3) months from the issuance date, the item will be considered abandoned. In this case, Certicámara will proceed to block the download link.

If the holder requires the digital signature after this period, they must initiate a new application process, which will incur a cost according to Certicámara's policies.

4.3.4 Download Time

Once the digital signature application is approved, the holder will automatically receive an email containing the download link, a detailed manual, and important recommendations.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

The download link will remain active for thirty (30) calendar days. After this period, the system will block it for security reasons. To reactivate it, the holder must formally request it and will have an additional two (2) months to download their signature.

If, after this three (3) month period, the signature has not been downloaded, the item will be considered abandoned and Certicámara will proceed to definitively block the link. In this case, if the holder wishes to obtain the digital signature certificate, they must initiate a new application process, which will incur a cost according to Certicámara's fees.

4.4 Certificate Acceptance

Confirmation by the subscriber is not required to accept the service received. It is understood that the digital signature certificate service is accepted from the moment its issuance is requested. Consequently, if the information contained in the service activation communication does not match its current status or was not provided correctly, the subscriber must inform Certicámara through any of the available customer service channels to carry out the relevant correction procedures, if applicable.

4.4.1 Certificate Publication by the CA

The registration authority, through its server, will incorporate the public keys of the digital certificates issued by the subordinate certification authority into the PKI's LDAP (Lightweight Directory Access Protocol) directory structure at the exact moment the certificate is issued.

In the event of any technical difficulty obstructing its publication, it will be carried out within the month following the certificate's issuance date, in accordance with the findings of the technical analysis that prevented its timely publication.

4.4.2 Notification of Certificate Issuance by the CA to Other Entities

Certicámara has an LDAP digital certificate repository through which entities, government agencies, private sector companies, and other interested parties can query the issuance of certificates. This repository is accessible at the following web address: https://ar.certicamara.com/. The information is published in this repository once the certificate has been issued.

4.5 Withdrawal

In the event that the user has made the payment for any of the services offered by Certicámara, but has not completed the submission of all required documentary requirements, a period of ninety (90) calendar days from the date of the service request is established for said information to be properly provided.

FOR THE EXCLUSIVE USE OF CERTICAMARA S.A

If the applicant does not complete the required information within the stipulated term, it will be understood that there is a withdrawal from the acquisition of the service. As a consequence, the amounts paid for the service will not be subject to a refund.

4.6 No Refund of Money

Certicámara will not be obligated to refund money to the applicant under any circumstances, except when expressly required by law.

4.7 Use of Key Pairs and Certificates

4.7.1 Generation and Installation of Key Pairs

The Root CA generates the key pair (Public and Private) using a hardware security module (HSM) that complies with the requirements established in a standardized certification authority secure electronic signature device protection profile, in accordance with FIPS 140-3 Level 3 or a higher security level, and the creation of CA keys utilizes a pseudo-random number generation algorithm.

4.7.2 Subscriber Certificate and Private Key Use

The **certification policy** details the uses and purposes for each of the types of certificates issued by Certicámara.

4.7.3 Relying Party Certificate and Public Key Use

Third parties in good faith may only place their trust in the certificates for the purposes defined in this CPS, the CP, and current regulations.

Said third parties may successfully carry out public key operations by relying on the certificates issued by the chain of trust. However, they must act with diligence and assume the responsibility of verifying the status of the certificates using the mechanisms detailed in this CPS.

4.8 Certificate Renewal

4.8.1 Renewal Times

Certicámara will notify its subscribers of the expiration of the validity of their digital certificate at least thirty (30) calendar days in advance. Such notification may be made via email to the address provided by the subscriber or through any other appropriate means of communication that Certicámara deems convenient.

However, it does not constitute an obligation for Certicámara to ensure the effectiveness of the notification regarding the end of the certificate's validity nor to confirm its receipt. It is the subscriber's duty to know the expiration date of their digital certificate and to

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

manage the relevant procedures before Certicámara for the issuance of a new signature.

Renewal shall be understood as the issuance of a new digital certificate, which entails the registration of a renewed application, the acceptance by the applicant of the Terms and Conditions of the digital signature certification service of Certicámara S.A., the Declarations and Commitments regarding the prevention of ML/TF/FPWMD and S/TB, the prior validation of identity, and the generation of a new key pair.

4.8.2 ¿Who can request a renewal?

Subscribers may request the renewal of their certificate when it is close to expiring and they wish to continue using a digital certificate that attests to the same conditions approved in the current certificate.

4.8.3 Processing Certificate Renewal Requests

For the purposes of renewing a certificate, the subscriber must undergo the identity validation process again. Consequently, the application procedure for the renewal of a certificate is identical to that of first-time issuance, with the exception that attaching documents to the application will not be required, unless they have expired (where applicable).

4.8.4 Notification of New Certificate Issuance to the Subscriber

The effective issuance of the new certificate will be communicated to the subscriber via an email sent to the address they provided.

4.9 Certificate Key Renewal

Certicámara does not contemplate the renewal of the key pair within the life cycle of its certificates. In all cases, the issuance of a certificate implies the generation of a new key pair.

4.10 Certificate Modification

During the validity of a certificate, the modification or update of the information it contains is not permitted. If it is required to change any data of the issued certificate, it will be necessary to revoke the current certificate, request the issuance of a new one with the correct data, and pay the corresponding fee.

4.11 Certificate Revocation

The revocation of a digital certificate constitutes the mechanism by which an issued certificate is disabled, concluding its validity period, either due to the expiration of its validity or upon the occurrence of any of the revocation events stipulated in this

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

Certification Practice Statement. It should be clarified that revocation does not have any associated cost.

Certicámara does not handle the suspension status for its digital certificates.

4.11.1 Grounds for Revocation

Certicámara will revoke the digital certificate in accordance with Article 37 of Law 527 of 1999, when it becomes aware that any of the following events have occurred:

a) Due to security compromise for any reason, manner, situation, or circumstance.

b) Compromise or loss of the subscriber's private key for any reason or circumstance.

c) The private key has been exposed or is at risk of being misused.

d) Due to the death of the subscriber.

e) Due to the supervening incapacity of the subscriber.

f) Due to the liquidation of the represented legal entity that appears on the digital certificate.

g) Due to the update of the information contained in the digital certificate.

h) Due to the confirmation that any information or fact contained in the digital certificate is false, as well as the occurrence of new facts that cause the original data to no longer reflect reality.

i) Due to the compromise of Certicámara's private key or its security system in a manner that affects the reliability of the digital certificate, under any circumstance, including fortuitous events.

j) Due to the cessation of activities of Certicámara, unless the issued digital certificates are transferred to another Certification Entity.

k) By order of a court or competent administrative entity.

l) Loss, destruction, or security compromise of the physical medium of the digital certificate that has been duly notified to Certicámara.

m) Due to the termination of the subscription contract, in accordance with the grounds established in the contract and in this Certification Practice Statement.

n) For any cause that reasonably leads to the belief that the certification service has been compromised to the point that the reliability of the digital certificate is called into question.

o) Due to improper handling of the digital certificate by the subscriber.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

p) Due to non-compliance by the subscriber or the legal entity they represent or to which they are linked through the Digital Certification service Contract provided by Certicámara.

q) Due to a past-due portfolio report caused by non-payment of the services being provided by Certicámara.

r) Per the subscriber's refund request, in accordance with Certicámara's refund policy.

s) For causes associated with Certicámara within the framework of regulatory or compliance requirements.

t) Due to the concurrence of any other cause specified in this Certification Practice Statement.

u) Due to the termination of the employment contract or contractual link of the subscriber with the entity for which the digital signature certificate was issued.

4.11.2 ¿Who can request revocation?

The subscriber is authorized to request the voluntary revocation of their digital certificate at any time. Such request may be submitted directly or through a duly authorized third party. The digital certificate revocation procedure will not generate any cost.

Certicámara may also process the revocation of a certificate if it comes to know or has reasonable suspicion of a compromise of the subscriber's private key, or any other decisive event that makes the revocation of the certificate imperative. In those cases where the revocation is attributable to reasons inherent to Certicámara, a new certificate will be issued to the subscriber under the same conditions and for the remaining validity period. For this purpose, previously provided documentation will be used in order not to affect service availability.

4.11.3 Revocation Request Procedure

Certicámara has established the following channels to receive revocation requests:

- **Virtual:** Complete the application form available on the website: https://web.certicamara.com/soporte/formatos and subsequently submit the request through the following link: https://pqr.certicámara.com/registrar. This mechanism applies when the digital certificate is associated with a legal entity or organization and the subscriber loses their affiliation with said organization.
- **Online:** Through the Certicámara website, by registering the request at the following URL: https://ventadigital.certicamara.com/revocar-certificado

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

If deemed necessary, Certicámara will carry out relevant inquiries, verifications, and procedures, either personally or through third parties, to verify the existence of the invoked grounds for revocation. These procedures may include direct communication with the subscriber and the physical presence of the third party invoking the grounds.

Certicámara will validate the identity of the subscriber invoking the grounds for revocation. If the person presenting the request is not the subscriber, or if they are but cannot identify themselves satisfactorily, they may go in person to Certicámara's offices during business hours from 8:00 a.m. to 05:00 p.m., Monday through Friday, providing proof of the existence of the respective grounds for revocation where applicable, without prejudice to any measures Certicámara may establish for the security of the Digital Certification System. It is clarified that once the revocation request is received and its veracity is verified, the certificate will be revoked immediately, with no grace periods for such revocations.

In cases where revocation is requested due to the termination of the employment contract or contractual relationship between the subscriber and the entity for which the digital signature certificate was issued, Certicámara will request a certification from the person in charge or responsible for the entity stating the termination of the employment relationship.

If the grounds are verified, Certicámara will include the digital signature certificate in the Database of Revoked Digital Certificates as a revoked digital certificate. Otherwise, it will terminate the digital certificate revocation process. It is clarified that Certicámara does not offer a certificate suspension service to subscribers.

4.11.4 Revocation Request Grace Period

Certicámara must inform the subscriber, within the following 24 hours, of the service cancellation or revocation of their certificate(s), in accordance with current regulations.

4.11.5 CRL Issuance Frequency

The publication of the Certificate Revocation List of the Subordinate CA Certicámara (CRL) and SUB CA CERTICÁMARA (CRL) is carried out with a validity of three (3) days:

- Periodically
- The publication may occur a maximum of eight (8) hours after the last revocation, at any time of the day.

4.11.6 Availability of Online Status/Revocation Verification

The Certificate Revocation Lists (CRL) and the Online Certificate Status Protocol (OCSP) validation service will be available for consultation 365 days a year, 24 hours a day, 7 days a week. This service will be provided under a 99.8% availability agreement.

Certicámara maintains the historical record of revoked certificates since the beginning of the service provision.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

4.11.7 Online Revocation Verification Requirements

Online certificate status verification must be performed using the OCSP service in accordance with RFC 6960. Through the use of this protocol, the current status of an electronic certificate is determined without requiring CRLs.

An OCSP client sends a certificate status request to the VA, which, after querying its Database, provides a response on the certificate status via HTTP through the addresses http://ocsp.certicamara.com, http://ocsp.certicamara.co y http://ocsp4096.certicamara.co

4.11.8 Suspension Circumstances

Certicámara does not include the temporary suspension of certificates within their lifecycle; in all cases, a revoked certificate cannot be reactivated.

4.12 Replacement of Digital Signature Certificates

Certicámara establishes that the replacement of a digital certificate consists of generating a new certificate, as defined in the lifecycle section of this Certification Practice Statement, the Certification Policy, and the values established in these documents.

Now, to make the replacement effective, it must be taken into account that the initial certificate acquired meets the following conditions:

- The validity of the digital certificate must be equal to or greater than one (1) year.
- No replacements will be made for digital certificates that are less than ninety (90) days from expiration.
- The same certification policy under which it was initially issued must be maintained.
- The digital signature certificate will be replaced for its remaining remaining time.

This new generation of the digital signature certificate will incur a cost associated with its commercial value at the time of issuance, in accordance with the rates stipulated in the Certification Policy. In the event that commercial agreements have been negotiated with the client, the rates to be applied will be those established in said document.

To manage the replacement of digital signature certificates, the following requirements must be met:

- The subscriber must generate the request on the Certicámara website: https://ventadigital.certicamara.com requesting the replacement of the digital certificate, taking into account the conditions mentioned in the previous section.

- The subscriber must perform the revocation of the digital signature certificate, as defined in the "Revocation Request Procedure" section of this document.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

Additionally, there are exceptional cases where, due to commercial agreements, Certicámara is obligated to maintain custody and management of quotas/slots; in this scenario, a communication from the contract supervisor and/or administrator must be provided, requesting the replacement of certificates and justifying it under any of the following grounds:

- Change of holder
- Change of position
- Change of certificate type (Physical/Digital)

Subsequently, the contract holder will send this request to the registration and use area through the form available on the website: https://pqr.certicámara.com/registrar, indicating the certificate to be replaced as well as the information corresponding to the respective revocation. Based on the information provided, the control of the entity's quotas will be carried out.

4.12.1 Grounds for Replacement

For each of the grounds set forth below, an internal analysis will be conducted by this company to determine the appropriateness of the replacement, in accordance with the defined procedure.

Certicámara will replace the digital signature certificate in accordance with the previous section when any of the following grounds occur:

i. Loss of the physical device.
ii. Exposure of the PIN (Password/key) of the digital certificate.
iii. Change in the information of the previously issued digital certificate. (Does not apply to a change in the identification number).
iv. Change in the corporate name of the company, regardless of whether it retains the same NIT.
v. Due to an error attributable to Certicámara.

Additionally, replacement will proceed when any of the following events occur, which are typified in Article 37 of Law 527 of 1999:

i. Due to the death of the subscriber.
ii. Due to the supervening incapacity of the subscriber.
iii. Due to the update of the information contained in the digital certificate.
iv. Due to the loss, destruction, or security compromise of the physical medium of the digital certificate that has been duly notified to Certicámara.

In the event that the replacement is due to an error attributable to Certicámara, it may use the information previously provided by the applicant for the issuance of the

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

certificate, without requiring the generation of a new request by the subscriber, and under the same conditions initially agreed upon.

4.13 Certificate Characteristics

4.13.1 Operational Characteristics

For the validation of digital certificates, several Validation Service providers are available to provide information regarding the status of certificates issued by the certification hierarchy. This is an online validation service (Validation Authority, VA) that implements the Online Certificate Status Protocol in accordance with RFC 6960. Through the use of this protocol, the current status of an electronic certificate is determined without requiring CRLs.

An OCSP client sends a certificate status request to the VA, which, after querying its Database, provides a response on the certificate status via HTTP through the addresses http://ocsp.Certicamara.com, http://ocsp.Certicamara.co y http://ocsp4096.certicamara.co.

The CRL files corresponding to each CA will also be available, published on the Certicámara website at the following URLs:

- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara.crl?crl=crl
- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica.crl?crl=crl
- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_2014.crl?crl=crl
- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_2014.crl?crl=crl
- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_4096.crl?crl=crl
- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_4096.crl?crl=crl

4.13.2 Service Availability

The certificate status checking service is available 24 hours a day, 365 days a year; the minimum availability level will be 99.8%.

4.13.3 Optional Functions

To make use of the Online Validation Service by querying the addresses http://ocsp.Certicamara.com; http://ocsp.Certicamara.co and

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

http://ocsp4096.certicamara.co, it is the responsibility of the third party in good faith to have an OCSP client that complies with RFC 6960.

4.14 Termination of the Subscription

The termination of a certificate subscription occurs in the following cases:

- Revocation of the certificate due to any of the grounds for revocation expressed in the following document.
- Expiration of the certificate's validity period.

4.15 Key Custody and Recovery

4.15.1 Key Custody and Recovery Policy and Practices

The private key of the Root CA is safeguarded by an HSM cryptographic device. For access to the private key repository, Shamir's threshold scheme (k, n) is used in both software and cryptographic devices.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Ubicación y construcción del sitio

All critical operations of the Root CA and the Subordinate CA are physically protected through the implementation of rigorous security measures and an uninterrupted 24/7 surveillance scheme. These systems operate independently from other Certicámara systems, restricting access exclusively to duly authorized personnel.

5.1.2 Physical Access

Certicámara has services and technologies that complement physical access controls to both its racks and its data centers, where normally a minimum of three (3) controls must be passed.

The Data Processing Centers of the Root CA and the Subordinate CA comply with the following physical requirements:

- Closed-circuit television (CCTV) in critical or restricted access areas.
- Access control based on biometrics and/or keys.
- Authorizations through systems.
- Fire protection and prevention systems: detectors, extinguishers, personnel training to act in the event of a fire, etc.
- Facilities are located away from smoke vents.
- Video captures and/or photographs.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

5.1.3 Power and Air Conditioning

The facilities where the equipment is located comply with the power and ventilation conditions required to prevent interruptions in the electrical supply or other anomalies of an electrical nature.

The equipment cabling is protected to prevent interception or physical damage. Additionally, specific measures have been adopted to mitigate information loss caused by the interruption of the electrical supply flow, by connecting essential components to UPS systems that guarantee a continuous electrical supply with sufficient capacity to sustain the electrical network during controlled system shutdown procedures and to safeguard the equipment against electrical fluctuations that could compromise its integrity.

The air conditioning systems maintain the spaces where the equipment is located at optimal humidity and temperature levels for its proper operation and preservation.

5.1.4 Water Exposure

The facilities of the Root CA and the Subordinate CA are protected to prevent exposure to water through the implementation of moisture and flood detectors and other security mechanisms suitable for the environment.

5.1.5 Fire Prevention and Protection

The installation of the Root CA and Subordinate CA features an intelligent detection and extinction system. It consists of:

- Intelligent control panel.
- Extension nozzles on the ceiling.
- Fire detectors on the ceiling and false ceiling.
- Alarm system that activates fire detectors.

5.1.6 Media Storage

Information related to the infrastructure of the Root CA and Subordinate CA is stored securely in fireproof cabinets and safes, according to the classification of the information contained therein.

This information is housed in separate physical locations in order to minimize associated risks.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

5.1.7 Waste Disposal

All waste generated from the operation of digital certification services is treated in accordance with applicable regulations to contribute to environmental protection and guarantee information security.

5.1.8 Off-site Backup

All backup copies are stored in entities distant from the Root CA and Subordinate CA. These facilities are protected by security means and mechanisms aligned with international security best practices.

5.2 Procedural Controls

5.2.1 Trusted Roles

The Root CA and the Subordinate CA have personnel who, due to their essential responsibilities for the operation of Certicámara S.A., are subjected to special control procedures and are considered trusted roles:

- **RA Agent:** Responsible for reviewing and validating the information in the applicant's documents for the issuance of digital certificates by the ECD.
- **CA Agent:** Responsible for the approval, activation, and revocation of ECD services.
- **PKI/TSA Infrastructure Specialist:** Responsible for the operation of the systems (hardware and base software) of the Root CA and Subordinate CA.
- **System Auditor:** The Director of Processes is internally responsible for the audit management process, establishing guidelines to evaluate compliance with applicable requirements through a specialized third party.

5.2.2 Number of Persons Required per Task

As a security measure, collaborators have been assigned to the different roles, ensuring proper segregation of duties, independence, and impartiality in their actions within the accredited services.

5.2.3 Identification and Authentication for Each Role

Collaborators assigned to each role have the necessary permissions for their functions, authenticating through personal and non-transferable access credentials to the platform.
Authentication is supplemented by the corresponding authorizations to access specific information assets of the Certicámara system.

5.2.4 Roles Requiring Segregation of Duties

The responsibilities of personnel performing roles corresponding to the Registration Authority (RA) and the Certification Authority (CA) are duly segregated, thereby guaranteeing independence and impartiality in the development of their functions.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

CERTIFICATION PRACTICE STATEMENT

In consideration of the functions inherent to the Registration Authority (RA) and the Certification Authority (CA), and in accordance with the Specific Accreditation Criteria (CEA), these activities are carried out by personnel who maintain a direct employment relationship with Certicámara S.A

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Authorization Requirements

Certicámara implements a reliability background study process for collaborators who perform activities in the provision of digital services. This process comprises the validation of references, work experience, background checks, home visits, and qualifications, among other evaluation criteria.

5.3.2 Background Check Procedures

In the background verification process, Certicámara relies on a specialized company to conduct queries in defined lists, with the objective of determining the suitability of its collaborators.

5.3.3 Training Requirements

Certicámara implements an annual training plan for its collaborators, designed based on the training needs identified within the framework of their responsibilities. This plan may contemplate, among others, the following topics:

- Legal framework relating to the provision of certification services.
- Information security and personal data protection.
- Operational and technical characteristics of the accredited services.
- Operating and administration procedures.
- Business continuity.
- Technological evolution of the environment.
- Implementation of new tools.
- Modification of operating procedures.

5.3.4 Sanctions for Unauthorized Actions

Certicámara has established a procedure to carry out investigations and apply the corresponding disciplinary sanctions in the event that its collaborators contravene the directives issued by the organization. Upon suspicion by Certicámara that an employee is executing an unauthorized action, the automatic suspension of their access permission will proceed, with the possibility of terminating their employment contract.

5.3.5 Independent Contractor Requirements

Certicámara maintains the contracting support and documentation proving compliance with both administrative and technical requirements by independent contractors who provide the data center service.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

5.3.6 Documentation Supplied to Personnel

Certicámara will make available to all personnel the documentation related to the functions associated with the position they hold, the policies and practices governing these processes, and security documentation.

5.4 Audit Logging Procedures (Logs)

Certicámara features a log analysis tool that allows monitoring transactional and security audit records and, in turn, issues automatic alerts in order to identify failures or risk events requiring remediation in a timely manner. Likewise, it safeguards its records generated in the systems during this period for a minimum period of three (3) years.

5.4.1 Types of Events Recorded

Certicámara contemplates the recording of the following events:

- Warning: Indicates that an action performed within the involved systems presents an abnormal situation, but it is not necessarily a failure.
- Informational: Indicates that an action performed within the systems involved in providing the accredited services has been completed correctly.
- Error: Indicates that an action performed within the involved systems presents an unexpected behavior that results in the failure to complete the action as expected.

5.4.2 Log Processing Frequency

The processing of logs is performed permanently, ensuring that the information derived from actions within the involved information systems is safeguarded.

5.4.3 Audit Log Retention Period

It is defined that the retention period for the different audit logs is three (3) years, a period after which, and in accordance with the given guidelines, their destruction can proceed.

5.4.4 Protection of the Audit Log

Logs derived from actions performed in the information systems will be safeguarded in one copy within Certicámara's facilities and another copy off-site, always ensuring that a copy is available for consulting the information if necessary.

5.4.5 Vulnerability Assessments

Security tests including risk analysis, vulnerability scanning, and ethical hacking are conducted at least once a year. These are contracted to a specialized third party that complies with the assurance requirements defined in ONAC's specific accreditation criteria and internally by the company.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

5.5 Records Archival

5.5.1 Types of Records Archived

For digital signature certificate services, the documentation will be defined in the information system according to each type of policy. For other accredited services, they will be viewed in the respective certification policies.

5.5.2 Archive Retention Period

The retention period for documents will be in accordance with Article 38 of Law 527 of 1999, Certicámara's document retention schedules, and current regulations.

5.5.3 Archive Protection

The defined security measures are intended to protect the archives from unauthorized access (internal or external), so that only certain individuals can consult, modify, or delete the files. Archives are stored using physical and logical security measures to protect them.

5.5.4 Archive Backup Procedures

Copies of the files composing the archives to be retained are made in accordance with defined backup policies. The copy is generated and stored in a secure location within the primary data center of the Subordinate CA, which complies with environmental and physical security conditions.

5.5.5 Procedures to Obtain and Verify Archive Information

Recorded events are protected using cryptographic techniques, such that no one except the event viewing and management applications themselves can access them. Only authorized personnel have access to physical media archives and computer files to perform integrity verifications or others.

5.6 Key Rollover (Change of Key)

The keys of certificates issued by the Root CA will cease to be valid at the exact same moment that its self-signed certificate expires. Once expired, the Root CA will generate a new key pair that it self-signs to generate the new root certificate. Certicámara will notify the external auditor and/or accreditation body established by current regulations at the time of performing the key rollover, in order to determine the technical, procedural, and legal conditions applicable to this procedure prior to its execution, ensuring compliance with the regulations applicable to the process from a security standpoint. For this purpose, Certicámara will present the document titled Key Ceremony (Ceremonia de cambio de clave), which will be drafted and adjusted for presentation ahead of the proposed date for the key rollover.

FOR THE EXCLUSIVE USE OF CERTICAMARA S.A

5.7 Compromise and Disaster Recovery

Certicámara S.A. plans and prepares Business Continuity to have the capacity to continue operating during emergency events or any event causing an interruption or malfunction. To this end, it identifies and manages risks that could impact business continuity and takes measures against their materialization, striving for compliance with the legal, regulatory, statutory, and contractual requirements of our stakeholders related to business continuity.

Certicámara S.A. establishes and applies guidelines, directives, and commitments in order to respond quickly to an interruption or disruptive events, properly managing risks and conducting tests that consider critical processes, suppliers, services, and activities.

5.7.1 Incident Handling and Compromise Procedures

Certicámara has defined the procedure for incident management that ensures operational continuity, prevention, and timely reaction to possible failures in the normal operation of services, guaranteeing a minimum of interruptions in the provision and availability of platforms.

The business continuity plan ensures that Certicámara can continue providing the service in adverse situations, after identifying, evaluating, managing, and minimizing any type of risk events, where at least the following are contemplated:

- When the security of the certification authority's private key has been compromised.
- When the certification authority's security system has been breached.
- When failures occur in the certification authority's system that compromise service delivery.
- When encryption systems lose validity because they do not offer the security level contracted by the subscriber.

Certicámara will strive to follow the recommendations given by:

https://csrc.nist.gov/projects/hash-functions

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-57pt3r1.pdf

5.7.2 Business Continuity Capabilities After a Disaster

Certicámara's business continuity capabilities are defined in the business continuity plan, which establishes the resources necessary for its execution.

5.8 Cessation of Activities

In accordance with the provisions of Article 163 of Decree-Law 019 of 2012, which amends Article 34 of Law 527 of 1999, ECDs (Digital Certification Entities) accredited by

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

ONAC "may cease the exercise of activities, provided that they guarantee the continuity of the digital certification service to those who have already contracted it, directly or through third parties, without additional costs to the services already paid for." Consequently, Certicámara will inform ONAC of the cessation of services thirty (30) days in advance, as established in Chapter 48 of the DURSCIT, Article 2.2.2.48.3.8. Cessation of activities.

Therefore, Certicámara has defined a business continuity and contingency plan for all accredited services, ensuring high-availability continuity of the provided infrastructure and guaranteeing an appropriate cessation of its activities as an ECD.

Certicámara will report the cessation by sending an email addressed to all subscribers with active accredited services and through two notices published in newspapers or media of wide national circulation, with a 15-day interval, regarding:

i. The termination of its activity or activities and the precise date of cessation.
ii. The legal consequences of the cessation regarding the accredited services.
iii. The possibility for a subscriber to obtain a refund equivalent to the value of the remaining validity period of the contracted service.
iv. The authorization issued by ONAC for the ECD to cease the service, and if applicable, the CRL operator responsible for publishing the certificates issued by the ECD until the last one expires.
v. Any other obligation established by law.

In any case, subscribers may request revocation and a refund equivalent to the value of the remaining validity period of the services, provided they request it within two (2) months following the second publication.

The termination of the activity or activities will be carried out in the manner and following the schedule presented by Certicámara to the monitoring and control entity and approved by the latter.

6. TECHNICAL SECURITY CONTROLS

6.1 Generation and Installation of Key Pairs

The Root CA generates the key pair (Public and Private) using a hardware security module (HSM) that complies with the requirements established in a standardized certification authority secure electronic signature device protection profile, in accordance with FIPS 140-3 Level 3 or a higher security level, and the creation of CA keys utilizes a pseudo-random number generation algorithm.

The key generation procedure for the Subordinate CAs accredited before Certicámara is identical, performed within their own HSM.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

6.1.1 Delivery of Private Key to the Subscriber

The algorithm used for the generation of the subscribers' key pair is RSA of no less than 4096 bits, using SHA256 as the cryptographic digest or hash function. Subscribers may use the following means to generate their digital certificates and safeguard them:

- Physical USB hardware token devices to generate their private key, which comply with the FIPS 140-3 Level 3 standard.
- Virtual Token, utilizing Certicámara's HSMs (Hardware Security Modules).
- PKCS#10, when the subscriber previously creates their own keys and requests Certicámara to sign the digital certificate; the request must guarantee:
    - Minimum key size of 4096 bits.
    - The request must be sent in PKCS#10 format.

The risks to which the utilized cryptographic devices would be exposed include:

- Fluctuations outside normal environmental operating ranges, such as voltage or temperature.
- Unauthorized physical access attempts outside the manufacturer's technical specifications.

To know the level of associated risks of cryptographic devices, the document can be consulted NIST.FIPS.140-3.pdf

6.1.2 Delivery of Public Key to the Certificate Issuer

Public keys generated by the end entity under its responsibility are sent to Certicámara as part of a certificate request (.csr) requested to be signed by the Subordinate CA.

6.1.3 Delivery of CA Public Key to Relying Parties

The public key of any Certicámara subscriber will be permanently available in the active directory for consultation by relying parties who require it.

6.1.4 Key Sizes

- For Root CA certificates, the RSA algorithm with a size of 4096 bits is used.
- For Subordinate CA certificates, the RSA algorithm with a size of 4096 bits is used.
- For end-entity certificates, the RSA algorithm with a minimum key size of 2048 bits is used.

6.1.5 Key Usage Purposes (according to the X.509 v3 Key Usage Field)

The private key and certificate can only be used for the purposes authorized in this CPS and CP. Certicámara issues certificates with private key usage fields limited to certificate signing and CRL signing.

The intended uses for the keys of the CA certificates are:

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

- Certificate Signing
- Off-line CRL Signing
- Certificate Revocation List (CRL) Signing

The intended uses for the keys of end-entity certificates are:

- Digital Signature

- Digital Signature
- Non-Repudiation
- Key Encipherment
- Data Encipherment
- Key Agreement

- Enhanced Key Usage:
  - Subscriber Authentication (OID 1.3.6.1.5.5.7.3.2) – Applies to all certificates.
  - Secure Email (OID 1.3.6.1.5.5.7.3.4) – Applies to all certificates.
  - Server Authentication (OID 1.3.6.1.5.5.7.3.1) – Applies to Company / Entity Representation and Legal Person certificates.

6.2 Private Key Protection and Cryptographic Module Engineering

The private key of the Root CA is protected by a security scheme generated by a cryptographic device. In order to safeguard the private keys of the self-signed certificate, the private key is never decrypted outside the HSM.

Backup copies maintain the secrecy of the private key in the same manner as the original private key is safeguarded.

6.2.1 Cryptographic Module Standards and Controls

The HSM used by the Root CA to generate its keys is FIPS 140-3 Level 3 certified.

The public key has been stored in a signed electronic format, ensuring protection against electronic failures and/or power supply issues.

Therefore, the commissioning of a CA involves the following tasks:

- Initialization of the HSM module state.
- Creation of administrator and operator cards.
- Generation of the CA keys.

6.2.2 Private Key (K of N) Multi-Person Control

The Root CA generates its key pair using a hardware security module (HSM). Authentication against the HSM requires at least 2 out of 3 operators. This procedure follows the K of N scheme, using the non-persistent mode of the cryptographic device.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

In this mode, it is necessary to guarantee the physical connection of the last set of cards in the HSM reader to open the private key of the Root CA.

6.2.3 Custody of the Private Key

The private key of the Root CA and Subordinate CA is housed in a cryptographic device. This device complies with the requirements established in a standardized certification authority secure electronic signature device protection profile, in accordance with FIPS 140-3 Level 3 security.

The remaining private keys of operators and administrators are contained in cryptographic smartcards held by the administrators of each entity; Certicámara's private key is not held in escrow by a third party.

6.2.4 Private Key Backup

Private key backups are performed in accordance with the security guidelines and recommendations indicated by the PKI software manufacturer. These security guidelines describe the use of cryptographic devices complying with FIPS 140-3 Level 3, a card set complying with the k/n requirement for protection, and require at least the collaboration of the PKI/TSA infrastructure lead, the custodian of cryptographic material, and designated personnel from the Operations Management.

6.2.5 Private Key Archival

Backup copies of private keys will be held in encrypted form in the alternate data center. Backup copies of private keys are kept in secure, fireproof files.

6.2.6 Storage of Private Keys in a Cryptographic Module

Private keys are created inside the cryptographic module at the time it is initialized; subsequently, the private key generated within the HSM is exported in an encrypted form.

6.2.7 Private Key Activation Method

The sole activation method for the private key consists of using smart cards to distribute access across different people and roles. Explicitly, the unique combination required to activate the private key involves two out of three HSM administrators, three out of eight HSM operators, and one application Operating System administrator.

6.2.8 Private Key Deactivation Method

An operating system administrator can proceed to deactivate the private key of the Root CA and Subordinate CA. After being activated by the combination described in the previous section, the operator can proceed with deactivation by stopping the Certification Authority application.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

6.2.9 Private Key Destruction Method

The RSE component of Certicámara's PKI infrastructure will delete the identity associated with the private key of the subscriber's certificate issued on a Virtual Token upon expiration of its validity period or if it has been revoked. The destruction will be carried out using established commands to physically erase from the HSM memory the section where the key was recorded.

6.2.10 Cryptographic Module Rating

The Root CA and Subordinate CA use commercially available hardware and software cryptographic modules developed by third parties. The Root CA and Subordinate CA only use cryptographic modules with FIPS 140-3 Level 3 certification (nShield Edge, nShield 5c, nShield solo XC).

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The public key of the Root CA and Subordinate CA is archived according to the standard PKCS#7 format for a period of 20 years.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The key pair of the Root CA will remain valid until Saturday, May 24, 2031. On the other hand, the operational periods of the certificates will be ten years.

The key pair of the Subordinate CA will remain valid until Saturday, May 24, 2031. On the other hand, the operational periods of the certificates will be ten years.

6.4 Activation Data

6.4.1 Generation and Installation of Activation Data

Activation data for the Root CA and Subordinate CA must be generated and stored on smart cards. Their protection is guaranteed by a PIN held by authorized personnel.

6.4.2 Protection of Activation Data

Only authorized personnel possess the cryptographic cards capable of activating the CA private keys, and likewise, they know the PINs required for their use.

- The personal access code (PIN) is confidential, personal, and non-transferable, and it is the parameter that protects the private keys, allowing the use of the Root CA and Subordinate CA certificates; therefore, certain security rules must be taken into account for their custody and use:
- The PIN must not be sent or communicated to any person.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

- Operators and administrators must change the PIN when they suspect that it is known by another person.
- It is recommended to change the PIN periodically.

6.5 Computer Security Controls

6.5.1 Specific Technical Computer Security Requirements

For the respective provision of the service, a series of technical controls has been established, aiming for its proper functioning and guaranteeing its adequate operation. Among the aspects taken into account are:

- Equipment configuration
- Application configuration
- User configuration
- Application of network access profiles
- Information on the security system to protect the information collected for the purpose of issuing certificates.

6.5.2 Computer Security Rating

Currently, as part of its organizational approach, Certicámara is certified under the ISO/IEC 27001:2022 Standard – Information Security Management System, according to the scope defined in the certificate, which is available on Certicámara's website.

6.6 Technical Lifecycle Controls

6.6.1 System Development Controls

Security requirements for system development for the Root CA and the SUBORDINATE ENTITY are enforceable.

A security design analysis must be performed during the design and specification phases of new requirements for any component to be used in the Root CA and Subordinate CA applications. This is to ensure that the involved systems are secure.

The technological infrastructure of the Root CA and Subordinate CA must be equipped with clearly differentiated and independent development and production environments. Change control procedures must be used for new versions and updates.

6.6.2 Security Management Controls

Certicámara maintains an inventory of all IT assets and classifies them according to their protection needs; the guidelines for this will be dictated by the results of the risk analysis performed.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

System configuration must be periodically audited, and the growth in resource needs must be tracked according to demand.

6.6.3 Lifecycle Security Controls

Throughout the entire lifecycle, security controls must be implemented to instrument and audit each phase of the Root CA and Subordinate CA systems.

6.7 Network Security Controls

The technological infrastructure of the Root CA and Subordinate CA features a network with all the security mechanisms necessary to guarantee a reliable and integral service. Firewalls or encrypted data exchange between networks are used to ensure integrity. On the other hand, redundancy and high-availability technologies are used to ensure reliable and high-performance operation. Additionally, the infrastructure must be audited periodically by internal and external personnel of Certicámara.

6.8 Time-Stamping

The synchronization of the CA and RA clocks is performed based on the Legal Time of the Republic of Colombia, taken directly from the reference standards of the National Institute of Metrology (INM) of Colombia, in accordance with the provisions of Article 14 of Decree 4175 of 2011, amended by Decree 62 of 2021.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

The certificates of the Root CA and the SUBORDINATE ENTITY are issued in accordance with the regulatory or technical documents defined in the scope accredited by ONAC, which is published at https://onac.org.co/directorio3/index.php/acreditaciones/16-ECD-002

7.1.1 Version Number(s)

The certificates issued by Certicámara comply with the X.509 v3 standard.

7.1.2 Certificate Extensions

The extensions of the Root CA and Subordinate CA certificates allow additional information to be encoded in the certificates.

The standard X.509 extensions define the following fields:

- SubjectKeyIdentifier

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

- AuthorityKeyIdentifier
- BasicConstraints. Marked as critical
- Certificate Policies. Marked as critical
- KeyUsage. Marked as critical
- CRLDistributionPoint. Marked as critical
- SubjectAlternativeName. Marked as critical
- AuthorityInformationAccess

The following are the fields of the certificates issued to subscribers:

- Date and time of signing
- Document name
- Subject
- Certification Authority
- Certificate Serial Number
- Thumbprint
- Certificate valid from
- Certificate valid until

7.1.3 Algorithm Object Identifiers

- OID of the signature algorithm SHA256withRSAEncryption 1.2.840.113549.1.1.11
- OID of the public key algorithm RSAEncryption 1.2.840.113549.1.1.1

7.1.4 Name Forms

Certificates issued by Certicámara feature a DN, in X.500 format, containing the names of the issuer and the certificate holder in the issuer and subject fields.

7.1.5 Name Restrictions

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

7.1.6 Certificate Policy Object Identifier

The Root CA has a defined OID assignment policy within its private numbering tree.

7.1.7 Syntax and Semantics of Policy Qualifiers

The description of the syntax and semantics is found inside the generated digital certificates, within the certificate policies section, which displays a URL where Certicámara's CPS is published.

7.2 Certificate Revocation List Profile

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

7.2.1 Version Number(s)

The Subordinate CA issues CRLs in X.509 format.

7.2.2 CRL and CRL Entry Extensions

The extensions of the CRLs issued by the Root CA are those defined in accordance with RFC 5280, namely:

- Authority Key Identifier
- CRL Number
- Issuing Distribution Point

7.3 OCSP Profile

The validity status of a specific certificate issued to a subscriber may be verified using the Online Certificate Status Protocol (OCSP), which is implemented in accordance with RFC 6960.

7.3.1 Version Number(s)

Version 1 of the OCSP protocol is used, as established in RFC 6960.

7.3.2 OCSP Extensions

In accordance with the operational mechanics of digital certificate generation, the use of OCSP extensions is not established.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

In accordance with the definitions of the National Accreditation Body of Colombia – ONAC, Certicámara has established an annual audit program for the evaluation of its various accredited services.

The accreditation system of the Root CA and the Subordinate CA will be subject to a third-party audit on an annual basis, in accordance with the audit program defined by Certicámara. This process guarantees the alignment of its functioning and operation with the provisions contained in this CPS.

Additionally, Certicámara reserves the right to conduct internal audits under its own criteria or at any time when there is a suspicion of non-compliance with any security measure or a potential compromise of the keys.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

Likewise, an external audit will be conducted annually to evaluate the level of compliance with the WebTrust principles and criteria for Digital Certification Authorities of AICPA/CICA.

8.2 Identity/Qualifications of the Assessor

In the case of the third-party audit, the auditing firm must comply with the minimum assurance requirements stipulated in the specific accreditation criteria that ONAC has published on its website, in addition to those defined in Certicámara's internal procedures for contracting third parties.

8.3 Relationship of the Assessor to the Assessed Entity

The interaction between the auditor and the entity subject to audit will be strictly limited to the processes and information required to perform the audit. Consequently, the audited party (whether the Root CA or the subordinate entity) must not maintain any relationship of a financial, legal, or any other nature, whether current or projected, that could result in a conflict of interest with the auditor. Regarding internal auditors, the absence of any functional relationship with the area subject to the audit will be required.

8.4 Actions Taken as a Result of a Non-Compliance

The identification of any non-compliance during audits will trigger the internal improvement actions management process, the objective of which is the elimination of the detected root cause. In the event of a critical non-compliance, Certicámara will be empowered to determine the temporary suspension of the operations of the Root CA or the Subordinate CA until the deficiencies are remedied in the shortest possible timeframe.

8.5 Communication of Results

All audit results are presented to the executive presidency committee in order to determine the corrective and improvement actions to be implemented.

9. OTHER LEGAL AND COMMERCIAL MATTERS

9.1 Fees

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

9.1.1 Certificate Issuance or Renewal Fees

The fees established by Certicámara for each of the accredited services are defined in each of the certification policies published on the website.

9.1.2 Fees for Access to Revocation or Status Information

Certicámara does not include in its fee policies any charge for access to revocation or status information of certificate-related services. Both consultation and revocation will be free of charge.

9.1.3 Refund Policy

Subscribers may request a money refund through the Certicámara S.A. website via the form at https://pqrf.certicamara.com/registrar in the following cases:

- Withdrawal from the digital signature acquisition process: The subscriber may request the cancellation of the digital certificate acquisition process and the corresponding refund of the amount paid, provided that the digital certificate has not been issued or the physical token has not been delivered. The request must be submitted within ninety (90) calendar days following the date on which the payment was made.

- Subscriber Right of Rescission (Retracto): Applies when exercised within 5 business days counted from the delivery of the good, the provision of the service, or the conclusion of the contract. Its applicability will be evaluated considering the specific characteristics of the product or service acquired.

  Subscribers who acquire digital signature certificates issued by Certicámara S.A. through non-traditional or distance mechanisms (including electronic, telephone, or virtual channels) may exercise their right of rescission within five (5) business days following the conclusion of the contract, provided that the performance of the service has not begun.

  Given that digital signature certificates constitute customized services, exclusively associated with the holder, and whose execution is perfected upon the issuance or download of the certificate, the right of rescission will not apply once the technical activation process of the certificate has begun.

  Therefore, the right of rescission will only be applicable if: i) It is exercised within the legal term of five (5) business days from contracting, and ii) The certificate has not been issued, downloaded, activated, or linked to the user.
- Payment Reversal: Right exercised in cases of fraud, unsolicited transactions, defective products, products acquired but not received, and non-conforming products, within 5 business days.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

- Refund for duplicate payment, overpayment, or erroneous payment: A request made by the subscriber when a payment is made twice (2 times) for the same invoice or digital certificate, when an amount greater than the amount due was paid, or when an erroneous deposit was made. The subscriber or client user has a maximum period of ninety (90) days, counted from the date of payment.

- Refund for Taxes: In this case, the client paid a tax amount that they were not required to pay, and therefore a refund must be processed. The subscriber or user has a maximum period of ninety (90) days, counted from the date of payment.

- Refund for incompatibility: In these cases, the client requests a refund because the digital certificate is not compatible with their equipment or system. The subscriber or user has a maximum term of ninety (90) days, provided that the digital signature has not been downloaded.

- Refund due to breach of the duty of information: Occurs in cases involving sanctions or fines for non-compliance with this duty, provided there is a judicial or administrative decision, in which case the refund must proceed regardless of the timeframe in which it is presented.

This policy shall apply without prejudice to the rights legally vested in the subscriber or consumer in accordance with current Colombian legislation.

Note: Certicámara S.A. informs its subscribers that international payments and bank transfers abroad will not be processed for funds, refunds, or reimbursements. Any approved balance in favor or reimbursement, in accordance with the policies established in this document, must be processed and disbursed solely and exclusively through bank accounts located in Colombia.

9.2 Financial Liability

9.2.1 Insurance Coverage

a) In accordance with the provisions of numeral 5 of Article 2.2.2.48.2.3 of Decree 1074 of 2015 (which compiles Decree 333 of 2014, Article 7) and Article 2.2.2.48.2.5 of Decree 1074 of 2015 (which compiles Decree 333 of 2014, Article 9), Certicámara has taken out an insurance policy with an authorized insurance entity according to Colombian legislation, covering contractual and extra-contractual damages of subscribers and third parties in good faith exempt from fault, derived from errors and omissions, or bad faith acts of administrators, legal representatives, or employees of Certicámara in the development of their activities.
b) The insured amount complies with the provisions of these regulations, covering 197,347.6 UVT per event.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

c) The general conditions of the policy can be consulted on the website in the following section: https://web.certicamara.com/marco-normativo/poliza-de-garantias.

9.3 Confidentiality of Information

Certicámara commits to protecting all data to which it has access as a consequence of its activity as a certification authority.

However, Certicámara reserves the right to disclose the confidential data necessary to perform activities within Certicámara to external or internal employees and consultants. In this case, employees and/or consultants are informed about confidentiality obligations.

These obligations do not apply if the information classified as "confidential" is required by the Courts or competent administrative bodies or imposed by law, in which case the confidential information provided by the subscriber will be disclosed in accordance with current regulations.

The confidential information of the digital certification services subscriber may be exposed at the request of the subscriber, in their capacity as the owner of the information. When the ECD is required by law or authorized by contractual provisions to disclose confidential information, the subscriber or person involved must be notified of the information provided, unless prohibited by law.

9.3.1 Scope of Confidential Information

The following is considered confidential information:

- Documents containing information related to the administration, management, and control of the PKI infrastructure.
- Business information supplied by its suppliers and other persons with whom Certicámara has a legal or conventional duty to maintain secrecy.
- Information resulting from queries made to credit bureaus or other private or public sector entities.
- Employment information containing related data of the subscriber.
- All information submitted to Certicámara that has been labeled as "Confidential" by the sender.
- Information about the subscriber obtained from sources external to them (for example, from a claimant or regulators) must be treated as confidential, except when it is of a public nature.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

9.3.2 Information Outside the Scope of Confidential Information

The following is considered non-confidential information:

- Content of issued certificates
- Certificate Revocation List (CRL)
- Public key of the Root CA and Subordinate CA
- Certification Practice Statement (CPS)
- Organizational policies

9.3.3 Responsibility to Protect Confidential Information

As an accredited open digital certification authority, Certicámara S.A. has established a commitment to safeguard the confidentiality, integrity, and availability of all information it manages within the framework of certification services. This includes, but is not limited to, the personal information of subscribers, private keys, digital certificate data, and any other information that, by its nature, must be treated with the utmost discretion.

To guarantee the protection of this information, we commit to:

- Implement and maintain strict information security policies and procedures that comply with national and international standards, including ONAC requirements and current legislation regarding data protection.
- Continuously train all our personnel on information security best practices, the importance of confidentiality, and their individual responsibilities in data protection.
- Use robust and updated security technologies and systems, including data encryption, strict access controls, intrusion detection systems, and information backup and recovery mechanisms.
- Limit access to confidential information solely to authorized personnel who require such information to perform their duties. All access is monitored and logged.
- Establish confidentiality agreements with all our employees, contractors, and third parties who may have access to sensitive information.
- Securely and responsibly manage the information of subscribers' private keys, ensuring their protection against unauthorized access, disclosure, alteration, or destruction.
- Timely notify competent authorities and affected parties of any security incident that compromises the confidentiality, integrity, or availability of information, in accordance with applicable regulatory frameworks.
- Conduct regular internal and external audits to evaluate the effectiveness of our security controls and ensure continuous compliance with our policies and regulatory requirements.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

CERTIFICATION PRACTICE STATEMENT

The trust of our users is fundamental. Therefore, the protection of their confidential information is an essential pillar of our operations.

9.3.4 Processing of Personal Data

At Certicámara S.A., the processing of personal data is governed by the principles of legality, purpose, freedom, truthfulness or quality, transparency, access and restricted circulation, security, and confidentiality, in strict compliance with current Colombian legislation on data protection, including Law 1581 of 2012 and its regulatory decrees.

To guarantee the proper processing of personal data collected or accessed by Certicámara S.A., it commits to:

- Collect personal data only when necessary and relevant for the provision of its digital certification services, identity verification, issuance, renewal, suspension, or revocation of certificates, and compliance with our legal and contractual obligations.
- Inform data subjects about the specific purpose for which their data will be collected and processed, obtaining their prior, express, and informed consent, unless otherwise required or permitted by law.
- Use personal data exclusively for the informed and authorized purposes, refraining from using them for purposes other than those established in its personal data processing policy, authorizations, or privacy notice provided at the time of collection.
- Guarantee the truthfulness, updating, and completeness of the information residing in our databases, implementing the necessary mechanisms so that data subjects can update or rectify their data.
- Implement rigorous technical, human, and administrative measures to safeguard the security of personal data, preventing its alteration, loss, unauthorized or fraudulent consultation, use, or access.
- Allow data subjects access to their personal data and information regarding their processing, as well as facilitate the exercise of their rights to know, update, rectify, and delete their data, and to revoke the authorization granted.
- Maintain the confidentiality of personal data, even after the relationship with the data subject has ended, except in cases where the information is required by a judicial or administrative authority in the exercise of its legal functions.
- Not transfer or communicate personal data to third parties without the express authorization of the data subject, except in cases permitted or required by law for the fulfillment of a legal or contractual function.

Certicámara makes the personal data processing policy available to the applicant and subscriber on the website at the following online location:

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

9.3.5 Disclosure Pursuant to a Judicial or Administrative Process

Information is not available to nor disclosed to unauthorized individuals, entities, or processes. It may only be disclosed upon requirement by a judicial or administrative authority in the exercise of its functions.

In accordance with the provisions of Law 1581 of 2012, the subject's authorization is not required when information is requested by a public or administrative entity in the exercise of its legal functions or by court order.

9.4 Intellectual Property Rights

The subscriber must respect and comply with intellectual property regulations, which include both industrial property and copyright. To this end, they shall comply with the provisions of the Code of Commerce, Decision 486 of 2000, Decision 351 of 1993, and other complementary regulations on these matters.

By means of this provision, it is established that all information contained in the Certification Practice Statement (CPS) belongs solely and exclusively to the Sociedad Cameral de Certificación Digital Certicámara S.A., which reserves all rights related to the intellectual property of this document (CPS), including information, techniques, models, internal policies, processes, and procedures, in accordance with national and international regulations related to the matter.

9.5 Obligations and Responsibilities of the Participating Parties

9.5.1 Obligations and Duties of Certicámara

Certicámara has the following obligations in the provision of its services:

a) Implement and maintain security systems that are reasonable based on the service provided and, in general, the necessary infrastructure for the provision of the Digital Certification service.
b) Comply with the Certification Practice Statement (CPS), Certification Policies (CP), and agreements made with subscribers.
c) Inform the subscriber of the characteristics of the service provision, limits of liability, and obligations assumed as a participant in the digital certification process. In particular, Certicámara must inform the subscriber or third parties requesting it about the time and computational resources required to validate the digital signature carried out with the signature certificates it issues to its subscribers.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

d) Verify, directly or through Registration Entities duly accredited before Certicámara, the information defined in this Certification Practice Statement as verifiable for the issuance of digital certificates.
e) Refrain from accessing or storing the subscriber's private key. For certificates issued on a virtual token, the private key will be automatically deleted from our infrastructure upon expiration of the certificate's validity period or following its revocation for the reasons set forth in this document.
f) Maintain, by itself or through an intermediary, the custody of the physical medium of the digital certificate until its effective delivery to the subscriber (if applicable).
g) Permit and facilitate the conduct of audits by the National Accreditation Body of Colombia.
h) Issue digital certificates in accordance with the provisions of the digital certificate issuance procedure section of this Certification Practice Statement and the specifications agreed upon by the subscriber in the subscription contract.
i) Publish issued digital certificates and maintain the Registry of Issued Certificates.
j) Inform the National Accreditation Body of Colombia of the occurrence of any event established in the Certification Practice Statement that compromises service provision.
k) Inform the National Accreditation Body of Colombia of the introduction of new requirements or changes in the PKI infrastructure that may affect service provision.
l) Notify the subscriber of any change in status of their digital certificate, explaining the reasons for the decisions taken in accordance with the provisions of the Certification Practice Statement.
m) Maintain control and confidentiality of its private key and establish reasonable security measures so that it is not disclosed or compromised.
n) Diligently strive for the permanent and uninterrupted provision of digital certification services.
o) Permit access for subscribers, relying parties, and third parties to this Certification Practice Statement and to the repository of the Certification Authority.
p) Update the Database of Revoked Digital Certificates under the terms established in this Certification Practice Statement and make the notices and publications established by law therein.
q) Revoke digital certificates as required in accordance with the provisions of section 4.7 of this Certification Practice Statement.
r) Inform the subscriber, within the following 24 hours, of the revocation of their digital certificate in accordance with current regulations.
s) Remove administrators or representatives who fall within the grounds established in literal c of Article 29 of Law 527 of 1999.
t) Provide a telephone customer service line for subscribers and third parties to allow queries and prompt requests for certificate revocation by subscribers.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

u) Supply information required by competent administrative or judicial authorities in relation to issued digital signatures and certificates, and in general regarding any data message under its custody and administration.
v) Maintain physically or electronically the documentation backing the issued digital certificates for the term provided by law for merchants' records, and take the necessary measures to guarantee their proper integrity and confidentiality.
w) Address requests, complaints, and claims made by subscribers, in accordance with the provisions of this Certification Practice Statement.
x) Provide the information supplied by the subscriber with the treatment established in the certificate request section of this Certification Practice Statement.
y) Comply with the Specific Accreditation Criteria published on the ONAC website.
z) Advise on the security measures that subscribers of digital signatures and certificates must observe for the use of these mechanisms.
aa) Certicámara will provide digital certification services without any discrimination to any applicant who meets the requirements established in this CPS and current legal regulations; however, Certicámara may decline a digital certification request to an applicant or subscriber when involvement in illegal activities is evidenced.
bb) Comply with the provisions of Statutory Law 1581 of 2012 on Personal Data Protection and its developing regulations; provided personal data will be processed according to the procedures defined by Certicámara S.A. for such purpose and with the goal of providing a Digital Certification service or related services.
cc) Notify the subscriber in advance regarding subcontracting activities to provide them with the opportunity to object in accordance with current Colombian regulations; for this purpose, Certicámara provides a system on its website for receiving Requests, complaints, claims, suggestions, and appeals (PQRSA).
dd) Critical suppliers contracted for the data center service provision comply with the minimum requirements established in the Specific Accreditation Criteria document CEA 3.0-7 published on the ONAC website. To this effect, compliance with the requirements described in Specific Accreditation Criteria CEA 3.0-7 published by ONAC will be extended to them where applicable.
ee) Any others established in Article 32 of Law 527 of 1999 and Article 2.2.2.48.3.6 of Decree 1074 of 2015 (which compiles Decree 333 of 2014).

Compliance with all or part of the obligations or procedures for issuing digital certificates or the general provision of the digital certification service may be carried out directly by Certicámara or through its Registration Entities.

CERTICÁMARA HAS NO ADDITIONAL OBLIGATIONS BEYOND THOSE PROVIDED IN THIS SECTION EXCEPT THOSE PROVIDED BY CURRENT REGULATIONS, NOR SHALL IT

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

BE UNDERSTOOD THAT THERE ARE IMPLICIT OBLIGATIONS IN ADDITION TO THOSE EXPRESSLY CONSECRATED IN THIS CERTIFICATION PRACTICE STATEMENT.

9.5.2 Obligations and Duties of the Applicant

Applicants for Certicámara's certification services will have the following obligations and responsibilities:

a) Supply the required information in accordance with the requested digital certification service.

9.5.3 Obligations and Responsibilities of the Subscriber

The subscriber has the following obligations toward Certicámara and third parties:

a) Use the private key and the issued digital certificate solely for the established purposes and in accordance with the conditions established in the contract entered into with them individually and in this Certification Practice Statement and the corresponding certification policy. The subscriber will be responsible for any improper use made by them or third parties.

b) Use the private key and the digital certificate to sign data messages, clarifying to relying parties under what capacity they are signing (either as a natural person or as a natural person linked to a specific capacity at the time of issuance of the digital certificate), provided that the relying party's information system does not verify the capacity in which the subscriber is acting. The data message or electronic document that the subscriber signs with their digital certificate will determine the context of the capacity in which the subscriber signs, and whether or not they are using the capacity associated with the digital certificate (if applicable).

c) Be responsible for safeguarding the private key and its physical medium (if applicable), preventing its loss, disclosure, modification, or unauthorized use. Especially, the subscriber must refrain, regardless of the circumstance, from writing the activation code or private keys on the physical medium of the digital certificate or on any other document that the subscriber keeps or carries with them or with the physical medium.

d) Request the revocation of the issued digital certificate whenever any of the conditions set forth for the revocation of digital certificates are met.

e) Refrain in all circumstances from disclosing the private key or the activation code of the digital certificate, as well as refrain from delegating its use to third parties.

f) Ensure that all information contained in the digital certificate is true and immediately notify Certicámara if any incorrect or inaccurate information has been included or if, due to any subsequent circumstance, the digital certificate information no longer corresponds to reality. Likewise, they must immediately

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

communicate any change or variation suffered by any of the data provided to acquire the digital certificate, even if these were not included in the digital certificate itself.

g) Immediately inform Certicámara about any situation that may affect the reliability of the digital certificate, and initiate the digital certificate revocation procedure when necessary. Especially, they must immediately notify the loss, theft, or forgery of the physical medium and any attempt to perform these acts upon it, as well as the awareness by other persons of the activation code or private keys, requesting the revocation of the digital certificate in accordance with the procedure established in the Certification Practice Statement.

h) Destroy the physical medium when so required by Certicámara, when it has been replaced by another for the same purposes, or when the period of the digital certificate service acquired from Certicámara ends, following Certicámara's instructions in all cases.

i) Return the physical medium of the digital certificate when so required by Certicámara.

j) Respect the intellectual property rights (Industrial Property and Copyright) of Certicámara and third parties in the application for and use of digital certificates. Certicámara will not include information in the digital certificate whose inclusion could constitute in any way a violation of the intellectual or industrial property rights of Certicámara and third parties.

k) Any other derived from current regulations, the content of this Certification Practice Statement, or the Certification Policy.

l) Refrain from monitoring, altering, reverse engineering, or interfering in any other way with the provision of digital certification services.

m) Refrain from using the digital certificate in situations that may cause a poor reputation and damages to Certicámara.

n) Refrain from using the name of the ECD and the certification mark or in all promotional material containing any reference to the digital certification service provided by Certicámara immediately after its cancellation or termination, and undertake the actions required by the digital certification service and any other required measures.

o) Comply with the logo usage manual established by Certicámara.

p) Comply with the requirements established by the digital certification service in relation to the use of trademarks in the provision of services and consequently respect the trademark rights held by Certicámara.

q) Any others established in Article 39 of Law 527 of 1999.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

THE SUBSCRIBER MAY USE THEIR CERTIFICATE TO: (I) IDENTIFY THEMSELVES AS A NATURAL PERSON, OR (II) ASOCIATE THEIR PERSONAL IDENTIFICATION WITH A SPECIFIC CAPACITY VERIFIED BY CERTICÁMARA AT THE TIME OF ISSUANCE OF THE DIGITAL CERTIFICATE (IF APPLICABLE). THE USE OF THE DIGITAL CERTIFICATE IN EITHER CASE WILL DEPEND DIRECTLY ON THE CONTEXT IN WHICH THE DIGITAL CERTIFICATE IS BEING USED AND ON WHETHER OR NOT THE RELYING PARTY'S INFORMATION SYSTEM CAN VERIFY THE SUBSCRIBER'S IDENTIFICATION.

IT WILL BE THE ELECTRONIC DOCUMENT OR DATA MESSAGE THAT THE SUBSCRIBER DIGITALLY SIGNS THAT WILL PROVIDE THE CONTEXT WITHIN WHICH THE SUBSCRIBER MAKES USE OF THE CERTIFICATE AND WHETHER OR NOT THEY USE THE CAPACITY ASSOCIATED WITH THE DIGITAL CERTIFICATE.

9.5.4 Obligations and Responsibilities of the Relying Party

Certicámara's Digital Certification System comprises the use of a set of integrated elements surrounding the provision of a service to both subscribers and those who use and rely on the digital certificates issued by Certicámara. When a third party relies on a digital certificate, they accept the use of said system in its entirety and therefore agree to be governed by the rules established for it, which are contained essentially but not exclusively in this Certification Practice Statement. That third party becomes a participant in the Digital Certification System as a relying party, and therefore assumes the obligations established below:

a) erify the reliability of the digital signature and the digital certificate, checking especially that it is not in Certicámara's database of revoked digital certificates available on the internet site or at Certicámara's offices. The reliability of the digital signature and the digital certificate must in all cases conform to the provisions of the Reliability of Signatures and Digital Certificates section.
b) Accept and recognize digital certificates only for the use permitted in accordance with the provisions of the Use of Digital Certificates section.
c) Thoroughly understand and comply at all times with the Certification Practice Statement in the use of Certicámara's signatures and digital certificates. Especially, the relying party must keep in mind and act at all times in accordance with the limitations of liability and guarantees offered by Certicámara.
d) Inform Certicámara of any irregularity or suspicion thereof that arises in the use of the Digital Certification System.
e) Refrain from monitoring, altering, reverse engineering, or interfering in any other way with the provision of digital certification services.

9.5.5 Contractor Obligations

In the event that Certicámara externally contracts services or products related to the activities accredited within the scope, compliance with the requirements established in CEA 3.0-7 will be extended based on the nature of the contracted service, this

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

Certification Practice Statement, and the requirements of the current Colombian regulatory framework according to their contracted function for digital certificates.

Certicámara will determine whether the external approval entity provides compliance levels as established contractually, without prejudice to higher-ranking legal, technical, operational, and procedural regulations in force for the approval process, which will be available for review and comparison in Certicámara's management systems, which allow access to be established according to their confidentiality classification, and in any case will be available for third-party audits and by the National Accreditation Body.

9.6 Limits of Liability

a) The obligations listed in Certicámara's obligations section are of means and not of results. This means that Certicámara will use its knowledge and experience in providing the digital certification service, and will be professionally liable for ordinary negligence (*culpa leve*) in its actions as a Digital Certification Authority. Certicámara cannot ensure that the certification activity will have a specific result. Certicámara will only be liable for those errors that, having occurred, could have been avoided by its professional diligence.

b) Damages produced or related to the non-performance or defective performance of obligations by the **subscriber**, the relying party, or both, will be borne by them, as well as any harm caused by the improper use of **digital certificates** or violations of their established use limitations herein, in the Use of Digital Certificates section, or in any other document regulating the **Digital Certification System**. In addition to the foregoing, in the case of subscribers, what current regulations establish in terms of subscriber liability will be taken into account.

c) Certicámara will not be liable for damages caused by non-compliance with its obligations due to force majeure, fortuitous events, or, in general, any circumstance beyond reasonable control, including but not limited to: natural disasters, public order disturbances, power and/or telephone supply cuts, computer viruses, deficiencies in telecommunications services (Internet, communication channels, etc.), or the compromise of asymmetric keys derived from unpredictable technological risk.

d) Regardless of the cause or origin of its liability, Certicámara fixes the maximum amount for indemnification of damages caused per issued digital certificate according to what is set in the professional civil liability policy. Consequently, Certicámara will only indemnify persons harmed by a digital certificate issued by it, regardless of the number of times it has been used or the number of persons harmed by such uses. If there are multiple harmed parties, the maximum indemnifiable amount will be distributed pro-rata among them. If, after the indemnification has been distributed, new harmed parties arise, they must

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

proceed against the persons already indemnified in order to obtain their pro-rata indemnification.

e) Certicámara will only be liable for damages caused by the use of digital certification services within the year following the expiration or revocation of the digital certificate. Certicámara does not offer any type of guarantee that is not expressly stipulated in this Certification Practice Statement, nor will it be liable for any event not expressly contemplated in this section.

f) It will be liable in accordance with the provisions of Articles 16 and 19 of Decree 333 of 2014 compiled by Decree 1074 of 2015.

g) In the event that applicable laws to the digital certification service establish the impossibility of limiting liability in any of the aspects described here or in this **Certification Practice Statemen**t, these clauses will be given the greatest scope that the law allows regarding the limitation of Certicámara's liability.

9.7 Rights of Participating Parties

9.7.1 Rights of the Applicant

Applicants for Certicámara's certification services will have the following rights:

a) That their application be addressed according to the timeframes defined by the entity.

b) That the provisions established in the certification policies be fulfilled.

c) Receive assistance to resolve doubts or concerns regarding the digital certification service.

9.7.2 Rights of the Subscriber

Subscribers of Certicámara's certification services will have the following rights:

a) Be able to properly use the acquired digital certification service.
b) Inform relying third parties that Certicámara is their ECD providing the acquired service.
c) Request the revocation of the digital certification service when required.
d) Request the rectification and/or revocation of information in accordance with the personal data processing policy.
e) Receive support for the digital certification service(s) in accordance with the terms and conditions established between the parties.
f) To rescind (retractarse) the acquisition of certification services, provided they comply with the requirements established in Law 1480 of 2011.
g) To reverse the payment when it involves one of the events determined in Decree 587 of 2016.

FOR THE EXCLUSIVE USE OF CERTICAMARA S.A

9.8 Exclusion of Warranties / Disclaimers

Certicámara will not be held liable for:

a) The truthfulness of the information provided by the subscriber or applicant.
b) Cybercrimes suffered by the subscriber
c) The fraudulent use of certified services or CRLs
d) Damages and losses arising from the erroneous interpretation of the Certification Practice Statement (CPS).
e) Non-compliance with the obligations of the subscriber or applicant.
f) The content of messages or documents in which digital certification services are used.
g) Fortuitous events or force majeure.
h) The use of certificates when it exceeds the provisions of current regulations, the CPS, and CPs.

9.9 Contract Templates

The contract model used by Certicámara for the provision of the digital signature certificate service consists of two (2) documents, which are available at the following links:

- Términos y condiciones del servicio de certificación de firma digital Certicámara S.A.
- Condiciones generales de contratación del servicio de certificación de firma digital de Certicámara S.A.

On the other hand, the contract model used by Certicámara for the provision of the other accredited services consists of two (2) documents, which are available at the following links:

- Términos y condiciones de productos, servicios y/o soluciones de Certicámara S.A.
- Condiciones generales de contratación de productos, servicios y/o soluciones de Certicámara S.A.

In the event of specific commercial situations with the client, a contract detailing such situations may be signed between Certicámara and the client.

9.10 Management Policy for Other Services

Not applicable.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

9.11 Impartiality and Non-Discrimination

Certicámara recognizes the importance of safeguarding impartiality and independence to prevent both internal and external conflicts of interest. Therefore, the Presidency declares its commitment to guaranteeing compliance with independence, impartiality, and integrity requirements in all its services. The main mechanism to ensure impartiality is the impartiality management process and the formation of the impartiality committee.

The impartiality policy is available at: https://web.certicamara.com/politicas

Certicámara has carried out an exhaustive process of identification, analysis, and evaluation of risks likely to compromise objectivity and impartiality in the provision of its digital certification service. Consequently, information is provided regarding the actions implemented with the purpose of minimizing any circumstance that could jeopardize objectivity and impartiality in the provision of its services:

- With the aim of preventing risks associated with misleading advertising, its web portal has been carefully designed to ensure that its clients and/or subscribers can clearly discern which of its products and/or services hold accreditation from the National Accreditation Body of Colombia (ONAC).
- To mitigate risks in contracting Datacenter services, the providers supplying this service are comprehensively managed (from selection and contracting to performance evaluation) in strict compliance with its provider management procedure, thereby ensuring fulfillment of the admissible technical requirements defined in the specific accreditation criteria.
- The policies and procedures governing the operation of Certicámara, as well as its administration, are applied in a non-discriminatory manner. Certicámara refrains from using procedures that could hinder or restrict applicants' access to its services.

The digital certification services offered by Certicámara are accessible to all applicants whose requests fall within the scope of its accreditation, consistently applying the principle of technological neutrality, which is duly recorded in the definitions and conventions of this document.

Access to Certicámara's digital certification services is not conditioned by any particular characteristic of the applicant or subscriber other than those expressly defined in the Certification Policy (CP), nor by membership in any association or group, nor by the number of certifications previously issued. There are no undue conditions, whether of a financial or any other nature.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

9.12 Petitions, Complaints, Claims, Suggestions, and Compliments Policy

Certicámara establishes the guidelines, processes, and communication channels for the receipt, management, monitoring, and timely response to Petitions, Complaints, Claims, Suggestions, and Compliments submitted by clients, users, and other stakeholders. In this manner, the continuous improvement of services and products, as well as the satisfaction of all interest groups, is guaranteed.

To this end, the following channels have been provided to file a PQRSF:

- **In person:** At our Bogotá office, Carrera 7 No. 26-20, 18th Floor.
- **PQRSF System:** https://pqrf.certicamara.com/registrar

The procedure for addressing Petitions, Complaints, Claims, Requests, and Compliments is framed as follows:

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

certicámara.

Code:	IDI-L-001
Date:	11/11/2026
Version:	004
Labeling:	PUBLIC

CERTIFICATION PRACTICE STATEMENT



FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

9.13 Dispute Resolution Provisions

All differences arising between the parties by reason of the conclusion of the contract, during its execution, or due to its interpretation, will be resolved between the Digital Certificate Holder and Certicámara S.A. in the first instance, by means of conciliation, settlement (*transacción*), or amicable resolution (*amigable composición*). For this purpose, the aggrieved party shall send a duly substantiated written communication to the other PARTY, who will evaluate the grounds for disagreement and send a response within five (5) business days from the date of receipt (it will be the responsibility of the party sending the communication to ensure that the other party receives the sent communication, taking into account security and information integrity parameters).

If, after the aforementioned period, fifteen (15) days elapse and the difference(s) persist(s), it/they shall be resolved by an Arbitration Tribunal, regardless of the nationality of the Digital Certificate holder, which shall be subject to the current regulations on the matter and shall be governed specifically by the following rules:

a) The Tribunal shall consist of one (1) arbitrator appointed by THE PARTIES by mutual agreement. If this is not possible, their appointment is delegated to the Director of the Arbitration and Conciliation Center established by Certicámara S.A. Upon accepting the appointment, the arbitrator must declare in writing to THE PARTIES their independence and impartiality to act as arbitrator for the dispute.

b) The arbitrator must be a Colombian lawyer, registered on the lists of arbitrators of the Arbitration and Conciliation Center.

c) The internal organization of the Tribunal shall be subject to the rules provided for that purpose by the Arbitration and Conciliation Center, in matters not regulated in this clause.

d) The Tribunal shall operate in the city of Bogotá, at the Arbitration and Conciliation Center.

e) The Tribunal shall decide in law, and its award shall have the effects of material *res judicata* of last instance and, consequently, shall be final and binding for THE PARTIES.

f) The costs incurred by reason of the summoning of the Tribunal shall be borne by the losing PARTY.

g) The applicable regulations shall be Colombian.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

9.14 Applicable Law

Certicámara has identified the following regulations within the scope of the provision of accredited services in compliance with:

- Single Decree of the Commerce, Industry, and Tourism Sector - DURSCIT, 1074 of 2015
- Law 527 of 1999
- Decree 019 of 2012
- Decree 620 of 2020
- Law 2106 of 2019
- Law 1581 of 2012
- Law 1898 of 2018
- Decree 333 of 2014
- Law 1341 of 2009
- Decree 1595 of 2015

- **Activity 1.** Issuance of certificates in relation to the digital signatures of natural or legal persons.
- **Activity 2.** Issuance of certificates on the verification regarding alteration between the sending and receiving of data messages and transferable electronic documents.
- **Activity 3.** Issuance of certificates in relation to the person holding a right or obligation with respect to the documents set forth in literals f) and g) of Article 26 of Law 527 of 1999.
- **Activity 4.** Offering or facilitating services for the generation of creation data for certified digital signatures.
- **Activity 6.** Offering or facilitating services for the generation of creation data for electronic signatures.
- **Activity 9.** Any other activity related to the creation, use, or utilization of digital and electronic signatures.

9.15 Certification Policies

The interrelation between this CPS and the Certification Policies applicable to the different types of certification services is based on the following:

- This CPS is structured based on the recommendations of RFC 3647 and establishes the practices adopted by Certicámara for the provision of the services accredited by ONAC, containing detailed information on its security, support, administration, and certificate issuance systems, as well as the trust relationship among Applicant, Subscriber, Responsible Party, Providers, Third Parties in good faith, and the ECD.
- Certification Policies establish the specific procedures and requirements applicable to the Certification services provided by Certicámara. Each Certification Policy defines the requirements for service applications,

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

responsibilities, commercial conditions, and in general, the specific conditions for each certification service.

Certicámara details the requirements applicable to each service in the following Certification Policies:

- CP Digital Signature Certificate
- CP Time-Stamping
- CP Associated Information Services

Which are available at https://web.certicamara.com/marco-normativo

10. CHANGE CONTROL

Date	Reason for Update
12/09/2019	The following adjustments are made to the document: • Job titles and department names are updated in accordance with the current organizational structure. • URLs are updated. • According to the new operating model, the person responsible for keeping the CPS updated on the website is the Product Management Director. Likewise, those responsible for reviewing and approving changes to the certification practice statement are the Commercial and Marketing Manager and the Product Management Director. • The responsibilities and trusted roles defined by the organization for the administration and control of the PKI infrastructure are aligned. • In the section "Vulnerability analysis", it is clarified that they are managed by a third party that complies with the specific accreditation criteria of ONAC through the Administrative and Financial Management. • In the section "Auditors", it is clarified that, for third-party audits, the auditing firm must comply with the minimum assurance requirements established in the specific accreditation criteria published on the ONAC website. • The fee table by certificate type is updated.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

CERTIFICATION PRACTICE STATEMENT

Date	Reason for Update
	• The data regarding Certicámara's physical facilities is updated. • The log management performed by the organization for its monitoring and control is updated at a general level. • The requirements for each type of certificate are aligned with what is internally defined by the organization. • The code and version change in accordance with the documentary structure.
11/06/2020	The following adjustments are made to the document: • The positions responsible for making adjustments, reviewing, and approving the certification practice statements are updated in accordance with changes in the organizational structure. Likewise, the person responsible for their publication on the website is updated. • The roles requiring segregation of duties and the requirements for independent contractors are included.
30/06/2020	The following updates are made to the document: • Clarification that the certification policies (CP) are embedded within the chapters of this Certification Practice Statement (CPS) document, with the objective of facilitating the management and consultation of the information for interested parties. • The update and/or modification of the Certification Practice Statement (CPS) will be carried out through the procedure established by Certicámara, which contemplates a first stage of reviewing the changes and/or adjustments where the impacts are analyzed jointly with those involved from each management department. Subsequently, they are presented to the Executive President for approval.
02/09/2020	The following adjustments are made to the document: • Clarification regarding the mechanisms for the delivery of digital certificates, described in section 6.1.8. Generation of the subscribers' key pair. Based on the above, the Certification Practice Statement for Centralized Signature

FOR THE EXCLUSIVE USE OF CERTICAMARA S.A

CERTIFICATION PRACTICE STATEMENT

Date	Reason for Update
	Services is deactivated, given that it is unified with this document. • Requirements for the issuance request for each certification policy, regarding the subscriber's identification document.
22/10/2020	The document is updated in the following aspects: • Keywords and their definition, for a better understanding of the document. • For adult Colombian citizens, attaching a copy of the citizenship card (cédula de ciudadanía) to the application is required for all mentioned certification policies. • In section 1.2 “La Sociedad Cameral de Certificación Digital Certicámara S.A”, the company's identification data and the person responsible for the Petitions, Queries, and Claims of subscribers and users are included. • For the modification/updating of the information contained in the certificates, the wording is adjusted to provide clarity to the subscriber regarding the steps to follow in this regard. • As part of section 10 of “Digital Certificate Management Policies” issued by Certicámara, it is clarified that the issued certificates may have a maximum validity of 2 years in accordance with the provisions of CEA-4.1.10. • The section “Contract Model and Templates” is added.
27/10/2020	Se actualiza el documento, en los siguientes aspectos: • Modification of the name of the building where Certicámara is located. • Inclusion of the procedure for handling PQRSAF. • Inclusion of the link to consult the certificate of existence and legal representation of the ECD and the DataCenters. • Inclusion of identification information related to the DataCenters. • Adjustment of the link to the ECD's accreditation certificate. • Reference documents and activities of certification entities that fall within the scope of the service.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

certicámara.

Code:	IDI-L-001
Date:	11/11/2026
Version:	004
Labeling:	PUBLIC

CERTIFICATION PRACTICE STATEMENT

Date	Reason for Update
22/02/2021	The document is updated in the following aspects: • Change of corporate name of the Datacenter Bt Latam to SENCINET LATAM COLOMBIA S.A. • In the glossary, the definition of Registration Authority (RA) is included and that of Time Stamping is adjusted. • Wording of the sections related to the business continuity plan for greater clarity. • Adjustment in the policies of the types of digital certificates. • Inclusion of Annex 1 where the information available in the different digital certificates is described. • Updating of fees.
22/09/2021	The document is updated in the following aspects: • Area code and contact number for Certicámara's administrative matters. • In section 1.5.1 Root CA Certification Authority and Subordinate Certification Authorities, the serial number and hash of the root CA and Subordinate CA certificates are included respectively. • In section 4.1 Certificate application, it is included that Certicámara will consult the necessary databases to comply with SAGRILAFT. • In section 4.6.1 Root CA and Subordinate Key Usage, the key usages are updated in accordance with those declared in the digital certificate. • Clarification: "Certicámara will annually follow the recommendations given by: https://csrc.nist.gov/projects/hash-functions ". • Fee update for digital certificates on physical tokens with a validity period of two (2) years. • Adjustment in the stages and communication channels of the Procedure for handling Petitions, Complaints, Claims, Suggestions, Appeals, and Compliments.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

certicámara.

Code:	IDI-L-001
Date:	11/11/2026
Version:	004
Labeling:	PUBLIC

CERTIFICATION PRACTICE STATEMENT

Date	Reason for Update
	• In Annex 1 – Digital Certificates, Email Address (E) is removed from the OIDs. • Update of responsible job titles according to the new organizational structure. • Adjustment in the wording to make the information clearer for the user and subscriber.
12/05/2022	The following changes are made to the document: • Rewording of the description of the Public Function (*Función Pública*) policy to provide a better understanding of its application. • In the natural person policy, aspects related to legal person guidelines are incorporated in accordance with the service accreditation by ONAC. • Inclusion of the OIDs for the legal person policy. • Updating of the fees for 2022.
01/09/2022	• Within the framework of compliance with the provisions of Chapter 48 of the DURSCIT, Article 2.2.2.48.3.1. Certification Practice Statement (CPS) and the RFC 3647 standard, the sections are aligned with what is established in these documents and the wording is adjusted to provide greater clarity to the applicant and subscriber regarding the provisions, information, guidelines, controls, and other aspects applicable to the services accredited by the National Accreditation Body of Colombia ONAC. Based on the above, a comprehensive CPS and independent certification policies (CP) are defined for the services: Digital signature certificate, time-stamping, and associated services, which are published on the website in the same section.
22/09/2022	In section 1.1 Identification of the digital certification entity, the positions responsible for the following are updated: • Receipt of petitions, queries, and claims from subscribers and users • Review and approval of responses to petitions, queries, and claims from subscribers and users.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

certicámara.

Code:	IDI-L-001
Date:	11/11/2026
Version:	004
Labeling:	PUBLIC

CERTIFICATION PRACTICE STATEMENT

Date	Reason for Update
29/09/2022	In section 4.9.6 Availability of online status/revocation verification, it is included that Certicámara has the history of revoked certificates since the beginning of the service provision.
16/02/2023	Section 4.10 is included for the definition of the replacement of digital signature certificates, where it is clarified that a new certificate must be generated and the conditions that the subscriber must take into account for its management.
21/07/2023	The document is updated in the following aspects: • Inclusion of sections: "4.5 Withdrawal" and "4.6 No refund of money", in order to inform applicants and subscribers of the conditions they must take into account for each of these matters. • Updating of the URLs of the new 4026 distribution points for the CRL certificate revocation list.
18/09/2023	The document is updated in the following aspects: Inclusion of the definitions: • Inclusion of the definitions: Declination of the application, denial of the application, and recommendation for the decision. • Updating of the concepts of declination and denial of the application in section "4.1 Certificate application". Likewise, clarity is provided regarding the language of the documents submitted by the applicant. • In section "4.12.1 Grounds for replacement", clarity is provided regarding the guidelines to be taken into account for the management of this type of requests. • Clarification in section "5.2.4 Roles requiring separation of duties" regarding the functions performed by the Registration Authority (RA) and Certification Authority (CA) in accordance with the Specific Accreditation Criteria – CEA, which are carried out by personnel directly employed by Certicámara S.A. • Inclusion in section "9.1.3 Refund policy" of the authorized channel to request the refund and payment reversal

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

CERTIFICATION PRACTICE STATEMENT

Date	Reason for Update
	through the Certicámara S.A. website in the PQRSAF section or payment reversal tab. • In section "9.11 Impartiality and non-discrimination", clarity is provided regarding the policies and procedures related to non-discrimination and the application of the principle of technological neutrality.
15/01/2024	The following changes are made to the document: • In section "1.3.5 Other participants, service providers", the providers for the provision of the Datacenter service are updated. • In section "3.2 Identity validation mechanisms", identity verification from the web portal when the applicant files their application is included. • Inclusion in section "4.1 Certificate application" of the full, unreserved, and complete acceptance of the Terms and Conditions of the service, as well as the Declarations and Commitments regarding the prevention of money laundering, terrorist financing, financing of the proliferation of weapons of mass destruction, corruption, and transnational bribery. • Clarification in section "4.8.1 Renewal times" that the issuance of a new digital certificate previously implies the acceptance of the Terms and Conditions of the service, the Declarations and Commitments regarding the prevention of money laundering, terrorist financing, financing of the proliferation of weapons of mass destruction, corruption, and transnational bribery, and identity validation in the registration of a new application.
18/03/2024	Se realizan los siguientes cambios en el documento: • Eliminación del servicio de Digitalización certificada con fines probatorios del alcance de los servicios acreditados.

FOR THE EXCLUSIVE USE OF CERTICAMARA S.A

certicámara.

Code:	IDI-L-001
Date:	11/11/2026
Version:	004
Labeling:	PUBLIC

CERTIFICATION PRACTICE STATEMENT

Date	Reason for Update
	• En el numeral 4.1 solicitud de certificado, se aclara que la validación de la identidad hace parte de los requisitos que debe cumplir el suscriptor. • Actualización de los links de acuerdo con los cambios en la página web.
26/04/2024	• Clarification of the general contracting conditions for digital certification services in section 9.9 *Contract templates*.
09/09/2024	The following changes are made to the document: • Updating of the delivery management times for digital certificates in physical media. • Clarification on the replacement in case of an error attributable to Certicámara. • Adjustment of the service channels for technical support. • Updating of the key length to 4096 bits in the issuance of digital certificates. • Inclusion of the grounds for revocation due to termination of the employment contract or contractual relationship of the subscriber. • Inclusion of the policies: Natural person digital certificate PKCS#10 and Legal person digital certificate PKCS#10
05/08/2025	The following changes are made to the document: • Comprehensive adjustment of wording to provide greater clarity and precision in the information. • Updating of the position and area responsible for handling PQRSAF, as well as the procedure to follow. • Adjustment of the approval procedure for changes to the CPC. • Adjustment of the download time conditions • Inclusion that the digital certificate revocation procedure does not generate any cost. • Clarity of the conditions to be taken into account for the refund due to withdrawal. • Elimination of the toll-free national line. • Updating of links.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

certicámara.

Code:	IDI-L-001
Date:	11/11/2026
Version:	004
Labeling:	PUBLIC

CERTIFICATION PRACTICE STATEMENT

Date	Reason for Update
26/09/2025	The following changes are made to the document: • Updating of the contact person data in section 1.5.2. • Adjustment of the guideline to reset the virtual token password, which does not generate any cost for up to ten requests.
20/04/2026	The following changes are made to the document: • Service channels are comprehensively updated. • Updating of responsible positions in accordance with changes in the organizational structure. • Modification of the PQR handling procedure. • Updating of the requirements for delivering a physical token to a third party. • Change of document code and version in accordance with changes in processes.
01/06/2026	The following changes have been made to this document: • Updated certificate policy names in alignment with the latest revision of the ONAC accreditation certificate. • Comprehensive update of all hyperlinks to reflect the recent changes to the website. • Updated the method for resetting virtual token passwords. • Clarified the available channels for submitting revocation requests.
21/09/2026	The following document changes have been made: • Update of Datacenter details. • Technical standards adjustment for FIPS 140-3 certificates throughout the document. • Adjustment of revocation causes in accordance with the operating model. • Inclusion of a clarifying note in the "Refund Policy" section stating that disbursements will be made solely and exclusively through bank accounts located in Colombia. • Update of job title names in accordance with the current organizational structure.

FOR THE EXCLUSIVE USE OF CERTICAMARA S.A

certicámara.

Code:	IDI-L-001
Date:	11/11/2026
Version:	004
Labeling:	PUBLIC

CERTIFICATION PRACTICE STATEMENT

Date	Reason for Update
11/11/2026	The following changes are made to the document: • In Section 6.2.9, "Private Key Destruction Method," the method used for the destruction of keys for digital certificates issued on a physical token is adjusted. • In Section 9.2.1, "Insurance Coverage," the insured amount that the policy must cover is adjusted in accordance with current regulations in UVT. • In Section 9.5.1, "Obligations and Duties of Certicámara," provisions regarding the destruction of subscriber keys on virtual tokens are clarified. • Adjustments to the wording of the refund policy to provide greater clarity regarding the timeframe the subscriber has to submit a request.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A