V20 CERTIFICATION PRACTICE STATEMENT

Standard

Code	Name	Version	Information classification
POP-DT-58	Certification Practice Statement	20	Public

Document Title	Certification Practice Statement
Version	20
Working Group	Management Committee
Document status	Final
Date of issue	01/11/2016
Effective date	09/12/2025
OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.1.20
DPC Location	https://gse.com.co/documentos/calidad/DPC/Declaracion_de_Practicas_de_Certificacion_V20.pdf
Prepared by	Operations Coordinator
Reviewed by	Integrated Management System
Approved by	Management Committee

Change Control

Version	Date	Change/Modification
1	01-11-2016	Initial document
2	04-10-2017	• ECD Contact Information Update and Logo • Enrollment Entities Update • Update contact information for certification service providers • Information regarding the General Director of GSE. GSE TSA data update.
3	03-04-2018	Update information and adjustments in relation to CEA-4.1-10 in accordance with the review of the requirements matrices.
4	27-11-2018	The version was changed from V3 to V4 on 11/27/2018. This included updating the table of contents, providing information and adjustments related to new charges, rates, website access paths, correcting the subordinate clause, including the phrase "established and tested," expanding section 8.7.4 by naming the technological mechanisms used for data protection, linking all certification policies, changing terms, and updating the legal representative.
5	12-04-2019	The EE section was removed, and it was clarified that the use of the centralized signature certificate requires the acquisition of a technological platform with additional costs. This clarification is made in section 1.6.2 of the RA requirements and restrictions. Criteria and methods for evaluating applications. The roles of the RA were updated.
6	07/06/2019	Clarification of the scope of accreditation within the framework of DPC 1.1 Summary 4.1 Certificate application, the procedure for accessing the service is clarified. 4.1.1 Clarification of non-discrimination when accessing the service. 8.9.3 Clarification of subscriber or responsible party rights
7	31/03/2020	The DPC is adjusted to the changes generated by the new platforms, the objective and scope sections are added, the price list is adjusted, the links are modified to point to the new routes, the Legal Representative is changed, and the services accredited by ONAC are related in a more specific way.
8	14/08/2020	Everything related to the Digital Signature Generation service is removed, another condition is added in section 5.2.2 Authentication of the identity of an entity, for the renewal of digital signature certificates and the services used for identity validation are mentioned.
9	12/02/2021	The link to consult online the Certificate of Existence and Legal Representation for the current ECD and CA (Paynet SAS) was included. Detailed information on current CAs (Paynet) was included SAS) and historical (Indenova) in accordance with the established in item 1 of section 10.7 of CEA 4.1-10. The data center information was modified according to as established in the ONAC accreditation certificate. The paragraph regarding the renewal of certificates was removed. digital from numeral 5.2.2 and 5.2.3. The following sections were updated: • 6.4.2 Approval or rejection of applications for

10	16/07/2021	certificate • 6.4.3 Timeframe for processing certificate applications • 7.10.1 Trust Roles • 8.1.4 Delivery of the ECD public key to third-party acceptors The links have been updated to point to the new routes The following sections were updated: 3.6.1 Certification Authority (CA), data center provider data. 4.1 Repositories. Section 6.5.6 was also updated. 6.5.7 Timeframe for processing certificate applications 6.8.2 Use of the private key and certificate by third parties bona fide 6.12 Revocation and suspension of certificates 6.12.3 Revocation request procedure 6.13.1 Description of the content of the certificates Subordinate Authority 01 GSE 6.13.1.8 Algorithm Object Identifiers (OIDs) 6.14.1.3 CRL Availability 6.14.1.7 OCSP Availability 6.14.3 Optional Features 7.10.1 Trust Roles 8.1.4 Delivery of the ECD public key to third parties acceptors 8.1.5 Key size 8.1.6 Public key generation parameters and quality verification 8.2.4 Backup of the private key 8.2.5 Private key file 8.2.6 Transfer of the private key from the module cryptographic 8.2.7 Storing private keys in a module cryptographic 8.5.3 Actions in case of an event or incident of information security 10. DESCRIPTION OF PRODUCTS AND SERVICES, Service
11	5/10/2021	of Archiving, Registration, Conservation, Custody and Annotation for Electronic Documents 11.7.1 Personal Data Processing Policy 11.3 Impartiality and Non-Discrimination 14. ANNEX 1 DPC MATRIX TECHNICAL PROFILE CERTIFICATES DIGITAL 15. ANNEX 2 TERMS AND CONDITIONS OIDs and query links are updated for: • Certification Practice Statement • Certificate Policies for Digital Certificates • Certificate Policies for Time Stamping Service • Certificate Policies for Archiving, Registration, Preservation, Custody and Annotation of Transferable Electronic Documents and Data Messages. • Certificate Policies for Certified Email Service • The sections were updated to include electronic signatures: 6.1 Certificate Application 6.5 Initial identity validation 6.5.1 Method for demonstrating possession of the private key 10 Description of Products and Services 11.1.1 Fees for issuing or renewing certificates 11.9.3 Obligations of the Subscriber and/or Responsible Party. • The following sections were included, referring to electronic signatures: 5.1.1.1.1 Electronic Signature 5.1.1.2.2 ECD GSE Subscriber Certificates (Profile Matrix) electronic signature certificate technician) 13 Certification Policies 16 Annex 3 DPC technical profile matrix certificates electronic signature • include an explanatory note on the OCSP validation in sections 4.1, 4.3, 6.12.9, 6.12.10, 6.14.3. • Section 6.12.3 Revocation request procedure was updated by adding a new online revocation channel. • Section 8.3.2 was updated to clarify the period ofValidate the root and subordinate keys of the RSA algorithm and ECDSA • OIDs and query links are updated
12	27/10/2021	• Modified section 6.5 of Identity Validation • The OIDs and the link to the Digital Certificates PC were updated. • The OID and DPC link were updated with this new version.
13	31/05/2022	According to the new version of CEA, the following sections were adjusted: • 3.1 Summary: ItI remove 4.1-10 leaving only CEA. • 3.2. Petitions, complaints, claims and requests: The following was removed:appeal ends. • 3.6 PKI Participants: Eliminated as CAIndenova. • 5.1.1.1 - 5.1.1.2 Name Types: Root and subordinate certificates are removed fromIndenova and includes those related to elliptic curves. • 6.5 Initial identity validation: A final paragraph regarding the use of identity verification (confronta) services was added.. • 6.13.1 Description of certificate content:I include the subject's alternative name field.

JOSÉ F. JARAMILLO SANINT
Traductor e Intérprete Oficial
Inglés Español Inglés
Resolución Nro. 0499
Ministerio de Justicia

		• 6.13.1.7 Three purposes of the key were removed. • 7.10.1 Trust Roles: The roles of RA Agents, RA Administrator, and RA Auditor were modified: • 7.16 Cessation of an ECD: ItI am modifying it in accordance with the requirements of the new CEA. • 9.2 Auditor identity/qualification: Assurance requirements were modified. • 10. Description of products and services: The centralized signature certificate was removed, the Archive service name was changed, and the electronic signature generation service was modified in accordance with the accreditation certificate. • 11.4. The exemption provisions were modified due to liability limits. • 11.9.6 Obligation of other participants: Item (r) was modified by removing "4.1-10", leaving only "CEA". • 15. The title of the annex regarding Terms and Conditions was modified. • 16. This item from the technical annex for the electronic signature certificate was included. • The OIDs and the link to the Certificate Policy (CP) for Digital Certificates were updated. • The OID and the link to the Certification Practice Statement (CPS) were updated in this new version. • The quality code was added to the document header..
14	23/09/2022	• Section 3.6.4 was amended by replacing "Responsible Party" with "Third Party Acting in Good Faith". • Section 3.6.4.1 "Precautions to be observed by third parties" was added. • Section 6.4.1 "Performance of identification and authentication functions" was amended. • Section 6.5.1 "Method to demonstrate possession of the private key" was amended, clarifying the process in cases where applicants generate the key pair within their own infrastructure. • Section 6.5.5 "Interoperability criteria" was amended. • Section 6.12.7 "Update frequency of CALs" was amended in accordance with the availability percentage established in the new CEA. • RFC 2560 was replaced with RFC 6960 in the following sections: 6.12.10 "Online revocation checking requirements", 6.14.1.4 "OCSP profile", and 6.14.1.5 "Version number". • Section 7.7 "Storage system" was amended to clarify that the servers are hosted in cloud environments. • Section 7.4 "Exposure to water" was amended to clarify that it refers to the PKI data centers. • Section 7.16 "Termination of an ECD" was amended by adding a paragraph regarding the security plan for the cessation of operations. • Section 11.4 "Liability limits" was amended to include: Subscriber liability for the accuracy of the information provided; liability regarding service availability; liability regarding service functionality within the Subscriber's infrastructure; and liability related to cybercrime. • Section 11.9.1 "Obligations of the GSE ECD" was amended to include items (o) through (y). • Sections 12.3 "Notification and communication", 12.5 "Dispute prevention and resolution", 12.6 "Governing law", and 12.7 "Compliance with applicable law" were added. • The OIDs and the link to the Certificate Policy (CP) for Digital Certificates were updated. • The OID and the link to the Certification Practice Statement (CPS) were updated in this new version. • The entire structure of the document was reorganized in accordance with the sections of RFC 3647.
15	10/05/2023	• Paynet SAS was removed as the CA authority, as the PKI was transferred to GSE's ECD. • The position title "Director of Operations" was replaced with "Operations Manager."
16	24/10/2023	• The information regarding the primary and alternate data centers was updated, designating HostDime and Claro, respectively. • Section 11.6.2 "Acronyms" was amended to include the acronym RNEC. • Section 1.3.1.3 was amended to include the terms "pseudonymous" and "pseudo-anonymous", and to expand the list of nicknames. • Section 1.3.2 was amended and the section information was updated. • Section 1.3.2.3 was amended to include requirements for the identification and authentication of an individual's identity. • Section 1.3.2.4 was amended and the section information was updated. • Section 1.3.2.5 was amended by removing the word "recommendation". • Section 1.3.3.1 was amended by adjusting the identification and authentication requirements for routine key generation.

JOSÉ F. JARAMILLO SANINT
Traductor e Intérprete Oficial
Inglés Español Inglés
Resolución Nro. 0499
Ministerio de Justicia

		• Section 1.4.1 is modified to include the ECD and information from fully trusted databases. • Section 1.4.2.1 is modified. The word information is included. • Section 1.4.3.2 is modified to include the words defined and authorized • Section 1.4.4.1 is modified to include the word "inform it" and/or • Section 1.4.7.2 is amended: The term duly authorized and/or attorneys-in-fact is included • Section 1.4.7.3 is modified. The means or mechanisms for collecting ECD information are updated. • Section 1.4.7.4 is modified. The means of notifying the subscriber are updated. • Section 1.4.9.3 is modified. The online revocation request information is updated. • Section 1.4.9.11 is modified. The means of notifying the subscriber are updated. • Section 1.4.12.3 is modified to include the service desk for cases of forgotten PIN. • Section 1.5.2.2 is modified. The information of the people required by role is adjusted. • Section 1.5.7.2 is modified. GSE is included. • Section 1.5.7.3 is modified. GSE is included. • Section 1.7.1 is modified. The information in section 1 is updated. • Section 1.9.3.4 is modified. Information relating to the TRD is updated. • Section 1.9.4.1 is modified. Rules related to the processing of personal data are included. • Section 1.9.4.5 is modified. The wording of the section is adjusted. • Section 1.9.4.6 is modified. The wording of the section is adjusted. • Section 1.9.11.2 is modified. Literal c is adjusted. • Section 1.14 is modified. The OID and location of the Certificate Policy for Digital Certificates are updated. • Section 1.1 is modified; the telephone code is updated. • Section 1.1 is modified to remove the fax • OIDs for the entire document are updated • The numbering and order are updated according to section 6 of the RFC 3647 Scheme. • The name of the IT process is updated to "technology".
17	08/07/2024	• Section 3.2 Initial identity validation is modified (Information verification method included) • Section 3.2 is modified. Information on verification mechanisms is adjusted. • Section 4.1 Application for certificate is modified: procedure code is updated • Section 4.10.2 is modified. Service availability information is included and related numbering is adjusted. • Section 4.12 is modified. The text "storage of the private key to a responsible party" is removed as it was repeated.
18	01/10/2024	• Section 1.3 PKI Participants, 1.3.1 Certification Authority (CA) is adjusted, removing "GSE Root Electronic Signature". • Section 3.1.1 Types of names is modified, and the electronic signature is removed.
19	22/10/2025	1.5.2 Contact (ECD Manager): Legal Representative adjusted by President. • 1.5.3 Person who determines the suitability of the DPC for the policy: Operations Manager is replaced by Operations Coordinator. • 3.2.4 Unverified subscriber information: The wording of the section is adjusted. . ^4.1 Certificate request: The procedure name is updated • 4.3.2 Notification mechanisms authorized by subscribers: The wording of section 4.12.1 Policy and practices regarding key custody and recovery / 6.1.1 Key pair generation / 6.2.1 Standards and controls for the use of cryptographic modules / 6.2.4 Private key backup / 6.2.5 Private key archiving is adjusted. This includes compliance with FIPS 140-2 Level 3 or higher. •5.8 Cessation of CA or RA: Regulatory information is updated 1.3.1 Certification Authority (CA): Information associated with the Datacenter is updated. 5.8 Termination of the CA or RA. In accordance with the provisions of External Circular No. 30-2021, the notification to the Superintendency of Industry and Commerce is eliminated.
20	09/12/2025	

Table of Contents
Table of Contents

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. January 29th, 2026.

JOSÉ F. JARAMILLO SANINT
Traductor e Intérprete Oficial
Inglés Español Inglés
Resolución Nro. 0499
Ministerio de Justicia

Registration Authority (RA).
Subscribers
Trusted parties.
Other participants.
1.4 Use of the certificate.
Proper use of certificates
Prohibited use of certificates
1.5 Policy administration.
Organization that manages the document.
Contact (ECD Manager):
Person who determines the suitability of the DPC for the policy.
DPC approval procedures.
1.6 Definitions and acronyms.
Definitions.
Acronyms.
Standards and Standardization Bodies.
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES.
Repositories.
Publication of information on certification.
Publication schedule or frequency.
Access controls to repositories.
3. IDENTIFICATION AND AUTHENTICATION.
3.1 Names.
Types of names.ECD GSE root certificates.Elliptical Curve (ECDSA).Certificates of Subsidiaries.Elliptical Curve (ECDSA).
ECD GSE Subscriber Certificates (Technical Certificate Profile Matrix).
ECD GSE subscriber certificates (Technical Profile Matrix of Electronic Signature Certificates).
The need for names to make sense.
Anonymity or pseudonymization of subscribers.
Rules for interpreting the different forms of the name.
Uniqueness of Names.
Recognition, authentication and role of trademarks.
3.2 Initial identity validation.
Method to prove possession of the private key.
Authentication of the organization's identity.
Authentication of individual identity.
Unverified subscriber information.
Authority validation.
Interoperability criteria.
3.3 Identification and Authentication for key renewal.
Identification and authentication for the key reuse routine.
Identification and authentication for the key reuse routine after revocation.
3.4 Identification and authentication for the revocation request.
4. CERTIFICATE LIFECYCLE OPERATIONAL REQUIREMENTS.
4.1 Certificate application.
Who can request a certificate?
Application, registration and liability process.
4.2 Certificate application processing.
Procedure for processing the application/ identification and authentication.
Criteria for acceptance or rejection of the application.
Deadline for processing certificate applications
4.3 Issuance of the Certificate.
ECD GSE actions during certificate issuance.
Notification mechanisms authorized by subscribers.
4.4 Acceptance of the Certificate.
4.4.1 Subscriber acceptance mechanism for the certificate. 4.4.2 Publication of the certificate by the CA
4.4.3 Notification of the issuance of certificates by the ECD GSE to other entities.
4.5 Use of key pairs and certificates.
Subscriber Responsibilities Regarding the Use of the Private Key and Certificate.
Responsibilities of the trusted third party related to the use of the subscriber's private key and certificate.
4.6 Certificate renewal
Circumstances for certificate renewal.
Who can request a renewal without changing the keys?
Procedures for requesting renewal of certificates.
Notification to the subscriber or person responsible for issuing a new certificate without changing the keys.
How a certificate renewal is accepted.
Publication of the certificate renewed by the ECD.
Notification of the issuance of a renewed certificate by the ECD to other entities.
4.7 Re-use of certificate key
Circumstance for the reuse of certificate keys.
Who can request certification of a new public key?
Processing of certificate key reuse requests.
Notification to the subscriber of the issuance of a new certificate.
Conduct that constitutes acceptance of a certificate with key reuse.
Publication of the certificate with key reuse by the CA
Notification of the issuance of certificates by the CA to other entities
4.8 Certificate Modification.
Circumstance for the modification of the certificate.
Who can request a change to the certificate?
Processing of requests for modification of certificates.
Notification to the subscriber of the issuance of a new certificate
Conduct that constitutes acceptance of a modified certificate.
Publication of the certificate modified by the CA.
Notification of the issuance of certificates by the CA to other entities.
4.9 Revocation and Suspension of the Certificate.
Circumstances for revocation.
Who can request the revocation of a certificate
Procedure for requesting revocation of a certificate.

Grace period to request revocation of a certificate.
Time within which the CA must process the revocation request.
Revocation verification requirement for relying parties.
CRL emission frequency.
Maximum latency of the CRLs.
Availability of online revocation/status verification
Online revocation verification requirements.
Other forms of revocation notices are available.
Special requirements for renewal of compromised keys.
Circumstances for suspension
Who can request the suspension
Suspension application procedure
Limits of the suspension period
4.10 Certificate Status Services.
Operational characteristics
Service availability
Optional features.

End of Subscription.
Key Custody and Recovery

Policy and practices regarding key custody and recovery.
Session key encapsulation and recovery policies and practices.
5. FACILITIES, MANAGEMENT AND OPERATIONAL CONTROLS.
5.1 Physical Security Controls.
Physical location of the ECD construction.
Physical access control mechanisms.
Energy and air conditioning.
Exposure to water.
Fire prevention and protection.
Backup copy system - Media storage.
Waste disposal
Off-site backup.
5.2 Procedural Controls.
ECD Trust Roles.
Number of people required in each role.
Identification and authentication of each role.
Roles that require segregation of duties.
5.3 Personnel controls.
Requirements regarding qualification, experience and licensing requirements.
Background check procedure.
Training requirements.
Training requirements and frequency of updates.
Frequency and sequence of task rotation.
Penalties for unauthorized actions.
Controls for contracting third parties.
Documentation provided to staff.
5.4 Audit Recording Procedures.
Type of events recorded.
Log processing frequency.
Audit record retention period.
Protection of audit records.
Procedure for backing up audit logs.
Audit record collection system (internal or external)
Notification to the person responsible for the security incident.
Vulnerability analysis.
5.5 Records Archive.
Types of archive records.
Retention period for archiving
File protection
File backup copy procedures
Requirements for time-stamping records.
File collection system (internal or external).
Procedures for obtaining and verifying file information.
Key Change.
Commitment and Disaster Recovery.
Incident and engagement management procedures
Procedure in case of damage to computer resources, software and/or data.
Recovery procedure in the event of a compromise of the ECD private key.
Disaster recovery capacity.
5.8 Termination of the CA or the RA.
6. TECHNICAL SECURITY CONTROLS.
6.1 Generation and Installation of Key Pairs.
Key pair generation
Delivery of the private key to subscribers.
Delivery of the public key to the certificate issuer.
Delivery of the public key of the CA to the trusting parties.
Key Size.
Public key generation parameters and quality control.
Purposes of use of the key (according to the field of use of the X.509 v3 key).
6.2 Private key protection and cryptographic module engineering controls.
Standards and controls for the use of cryptographic modules.
Multi-person control (n of m) of the private key.
Custody of the ECD private key.
Backup copy of the private key.
Private key file.
Transfer of private keys to or from a cryptographic module.
Storing the private key in the cryptographic module.
Private key activation method.
Method for deactivating the private key.
Method to destroy the private key.
Cryptographic module classification.
6.3 Other Aspects of Key Pair Management.
6.3.1 Public key file.

6.3.2 Operating periods of the certificates and period of use of the key pair.
6.4 Activation Data.
Generation and installation of activation data.
Protection of activation data.
Other aspects of activation data.
6.5 Information Security Controls.
Specific technical requirements for computer security.
Classification of computer security.
6.6 Technical Lifecycle Controls.
Systems development controls.
Security management controls.
Lifecycle safety controls.

Network Security Controls.
Chronological Print.
7. CERTIFICATE, CRL AND OCSP PROFILES.
7.1 Certificate Profile.
Version numbers.
Certificate extensions.
Algorithmic object identifiers.
Forms of names.
Name restrictions.
Certification Policy Object Identifier.
Using the Policy Constraints extension.
Syntax and semantics of Policy Qualifiers
Semantic treatment for the Certificate Policies extension.
7.2 CRL profile.
Version number(s)
CRL and CRL input extensions
7.3 OCSP profile.
Version number(s)
OCSP Extensions
8. COMPLIANCE AUDIT AND OTHER EVALUATIONS.
Frequency or Circumstances of the Evaluation.
Evaluator identity and qualifications.
Relationship of the evaluator with the entity being evaluated.
Topics subject to evaluation.
Actions taken as a result of the deficiency.
Communication of Results.
9. OTHER COMMERCIAL AND LEGAL MATTERS.
9.1 Fee.
Certificate issuance or renewal fees
Certificate access fees
Rates for access to information on revocation or status
Fees for other services
Refund policy
9.2 Financial Responsibility.
Insurance or guarantee of coverage for subscribers, responsible parties and bona fide third parties.
Other assets.
Insurance coverage or guarantee for end entities
9.3 Confidentiality of Commercial Information.
Scope of confidential information.
Non-confidential information.
Duty to protect confidential information.
9.4 Privacy of Personal Information.
Privacy Plan - Personal Data Processing Policy.
Information treated as private.
Information that is not considered private.
Responsibility to protect private information.
Notice and consent to use private information.
Disclosure pursuant to a judicial or administrative proceeding.
Other circumstances of information disclosure.
Intellectual Property Rights.
Representations and Guarantees.
CA Declarations and Guarantees
RA Declarations and Guarantees
Subscriber Representations and Warranties
Representations and warranties of the trusting party
Representations and warranties of other participants
Warranty Disclaimers.
Limitations of Liability.
Compensation.
Duration and Termination.
Duration.
Termination.
Termination effect, notification and communication.
Procedure for Change in the DPC and PC.
9.11 Individual notifications and communications to participants.
ECD GSE Obligations.
Obligations of the RA.
Obligations (Duties and Rights) of the Subscriber and/or Responsible Party.
Obligations of Third Parties in Good Faith.
Obligations of the Entity (Client).
Obligations of other participants in the ECD.
9.12 Amendments.
Amendment procedure.
Notification mechanism and deadline.
Circumstances in which an OID must be modified.
Notification to the subscriber or person responsible for issuing a new certificate.
How a certificate modification is accepted.
Publication of the certificate modified by the ECD.
Notification of the issuance of a certificate by the ECD to other entities.
9.13 Provisions on dispute resolution.

Applicable legislation.
Compliance with applicable legislation.
Various provisions.
Full agreement
Assignment
Divisibility
Enforcement (attorney fees and waiver of rights)
Force Majeure
9.17 Other Provisions.
DESCRIPTION OF PRODUCTS AND SERVICES FEES.
Fees for issuing or renewing certificates.
Certificate access fees.
Fees for revocation or access to status information.
Rates for other services.
Returns policy. Impartiality and non-discrimination certification policies.
ANNEX 1 DPC TECHNICAL PROFILE MATRIX DIGITAL CERTIFICATES.
ANNEX 2 DPC MODELS AND MINUTES OF TERMS AND CONDITIONS DOCUMENTS. ANNEX 3 DPC TECHNICAL PROFILE MATRIX ELECTRONIC SIGNATURE CERTIFICATES.

1. INTRODUCTION.
1.1 General Description
The Certification Practice Statement (CPS) - Global Certification Authority Root GSE (hereinafter CPS) is a document prepared by Gestión de Seguridad Electrónica SA (hereinafter GSE) acting as a Digital Certification Authority, containing the standards, statements on policies and procedures that the Digital Certification Authority (hereinafter CDA GSE) as a Digital Certification Service Provider (CSP) applies as a guideline to provide digital certification services in accordance with the provisions of Law 527 of 1999, Decree Law 0019 of 2012, Decree 333 of 2014, Decree 1471 of 2014 and the regulations that modify or complement them, in the territory of Colombia.
The DPC agrees with the following guidelines:
1.Specific Accreditation Criteria for Digital Certification Entities (hereinafter CEA) that must be met to obtain Accreditation as a Digital Certification Entity - ECD, before the National Accreditation Body of Colombia - ONAC;
2.The DPC is organized under the structure defined in the document RFC3647 Internet x.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework of the IETF - The Internet Engineering Task Force working group, (which replaces RFC2527) http://www.ietf.org/rfc/rfc3647.txt?number=3647.
3.ETSI EN 319 411-1 V1.2.0 (2017-08).
4.Chapters 47 and 48 of Title 2 of Part 2 of Book 2 of the Single Decree of the Trade, Industry and Tourism Sector - DURSCIT
The updating and/or modification of the DPC will be carried out through the procedure established by GSE for documented information; any change or adjustment to the document must be reviewed, analyzed and approved by the Management Committee.
This document applies to products and services accredited by the National Accreditation Body of Colombia - ONAC. ELECTRONIC SECURITY MANAGEMENT DATA SA:

Company Name:	ELECTRONIC SECURITY MANAGEMENT SA
Initials:	GSE SA
Tax Identification Number:	900.204.272 - 8
Commercial Registry No: Certificate of Existence and Legal Representative:	01779392 of February 28, 2008 https://gse.com.co/documentos/marco-regulatorio/Certificado-de-Existencia-y-Representante-Legal-GSE.pdf
Commercial register status:	Asset
Company address and correspondence:	77th Street No. 7 - 44 Office 701
City / Country:	Bogotá DC, Colombia
Phone:	+57 (601) 4050082
Email:	inforagse.com.co
Web page:	www.gse.com.co

1.2 Name and identification of the document.
The DPC for ECD GSE will be called "Certification Practice Statement (DPC)". The version changes according to the modifications on the same document.
GSE is a registered private enterprise with the international organization IANA (Internet Assigned Numbers Authority), under private code No. 31136 in branch 1.3.6.1.4.1 (iso.org.dod.internet.private.enterprise). This information can be found at the following URL by searching for code 31136: http://www.iana.org/assignments/enterprise-numbers
The OIDs hierarchy was established by ECD GSE starting from the root 1.3.6.1.4.1.31136 defined by IANA and conforms to the following parameters:

OID HIERARCHY	DESCRIPTION	NAME
1	ISO format	It does not vary
3	Organization	It does not vary
6	Public	It does not vary
1	Internet	It does not vary
4.1 (31136)	Organization Identification	It does not vary, as defined by IANA
1	Document type	It varies depending on whether they are policies, procedures, manuals, among others.
1	Document number	This is the number assigned to the document within your group
20	Document version	It is modified according to each version of the document

In accordance with this hierarchy, the present DPC has been identified with the OID: 1.3.6.1.4.1.31136.1.1.20

1.3 PKI Participants.

1.3.1 Certification Authority (CA).
It is that legal entity, accredited in accordance with Law 527 of 1999 and Decree 333 of 2014, authorized by the Colombian government or the National Accreditation Body in Colombia to provide digital certification services in accordance with the provisions of Law 527 of 1999, Decree Law 0019 of 2012, Decree 333 of 2014, Decree 1471 of 2014 and the regulations that modify or complement them, is the origin of the digital certification hierarchy that allows it to provide services related to communications based on public key infrastructures.
Hierarchy of the CA's.
The GSE certification hierarchy is comprised of the following Certification Authorities (CAs):

GSE SA CERTIFICATION HIERARCHY		
GSE Root Authority		
Subordinate Authority 01 GSE	GSE ECDSA Subordinate	GSE Intermediate Electronic Signature

GSE has two data centers: the (Active) data center with Sencinet Latam Colombia SA ICD Nimbus, located at Carrera 106 No. 15A25 Manzana 4 Lote 38 Zona Franca, Bogotá, Colombia, and the (Active) data center with Claro located at Autopista Medellin Km 7.5 Celta Trade Park - Datacenter Triara, Cota, Cundinamarca, Colombia.
1. PUBLISHING AND REPOSITORY RESPONSIBILITIES. a. PKI Repositories.
GSE ECD Root Certificates https://certs2.gse.com.co/CA ROOT.crt https://certs2.gse.com.co/CA ECROOT.crt
List of Revoked Certificates ECD GSE Root (CRL) https://crl2.gse.com.co/CA ROOT.crl https://crl2.gse.com.co/CA ECROOT.crl
ECD GSE Subordinate Certificateshttps://certs2.gse.com.co/CA SUB01.crhttps://certs2.gse.com.co/CA ECSUB01.crt https://certs2.gse.com.co/CA FESUB01.crt
- List of Revoked Certificates ECD GSE Subordinates (CRL)

https://crl2.gse.com.co/CA SUB01.crlhttps://crl2.gse.com.co/CA ECSUB01.crlhttps://crl2.gse.com.co/CA FESUB01.crl
Online validation of digital certificates https://ocsp2.gse.com.co
Note: Online validation of digital certificates using OCSP must be performed with a tool that implements the OCSP protocol and is capable of understanding the responses generated by the service, such as OPENSSL.
This ECD GSE repository does not contain any confidential or private information.
The ECD GSE repositories are referenced by URL. Any changes to these URLs will be notified to all potentially affected entities. The IP addresses associated with each URL may be multiple and dynamic, and may be modified by ECD GSE without prior notice.
Registration Authority (RA).
This is the GSE area responsible for verifying the validity of the information provided by the applicant for a digital certification service. This is done by verifying the identity of the subscriber or the entity responsible for the digital certification services. The RA (Registration Authority) decides on the issuance or activation of the digital certification service. To this end, it has defined the criteria and methods for evaluating applications.
Under this DPC, the RA figure is part of the ECD itself and may act as a Subordinate of ECD GSE.
GSE does not under any circumstances delegate the functions of Registration Authority (RA).
Subscribers
Subscriber is the natural person to whom the digital certification services are issued or activated and therefore acts as subscriber or responsible for it, trusting in it, with knowledge and full acceptance of the rights and duties established and published in this DPC.
The Subscriber status will differ depending on the services provided by the ECD GSE as established in the Certificate Policies for digital certificates.
Trusted parties.
The responsible party is the natural person to whom the digital certification services of a legal entity are activated and therefore acts as the responsible party, trusting in him, with knowledge and full acceptance of the rights and duties established and published in this DPC.
The role of the responsible party will differ depending on the services provided by the ECD GSE as established in Annex 1 of this DPC.
Precautions that third parties should observe:
Verify the scope of the certificate in the associated certification policy.
Consult the regulations associated with digital certification services
Verify the ECD's accreditation status with ONAC.
Verify that the digital signature was generated correctly.

Verify the origin of the certificate (Certification chain)
Verify its conformity with the content of the certificate.
7. Verify the integrity of a digitally signed document.
Applicant.
The term Applicant shall refer to the natural or legal person interested in the digital certification services issued under this DPC. This may coincide with the role of the Subscriber.
Entity to which the subscriber or responsible party is linked.
In this case, the legal entity or organization to which the subscriber or responsible party is closely related through the accredited link in the digital certification service.

1.3.5 Other participants.
Management Committee.
The Management Committee is an internal body of ECD GSE, made up of the CEO and Directors who are responsible for approving the DPC as an initial document, as well as authorizing the changes or modifications required on the approved DPC and authorizing its publication.
Service providers.
Service providers are third parties that provide infrastructure or technological services to ECD GSE, when GSE so requires, and guarantee the continuity of service to subscribers, entities for the entire time that the digital certification services have been contracted.
Reciprocal Digital Certification Entities.
In accordance with the provisions of Article 43 of Law 527 of 1999, digital signature certificates issued by foreign certification entities may be recognized under the same terms and conditions required by law for the issuance of certificates by national certification entities, provided that such certificates are recognized by an authorized certification entity that guarantees, in the same way as it does with its own certificates, the regularity of the certificate details, as well as its validity and validity.
Currently, ECD GSE does not have any reciprocity agreements in place.
Petitions, Complaints, Claims and Requests.
Petitions, complaints, claims and requests regarding services provided by ECD GSE or subcontracted entities, explanations regarding this DPC and its policies; are received and handled directly by GSE as ECD and will be resolved by the relevant and impartial persons or by committees that have the necessary technical competence, for which the following channels are available for the attention of subscribers, responsible parties and third parties.
Telephone: +57 (601) 4050082
Email:pqrs@gse.com.co
Address: Calle 77 No. 7 - 44 Office 701
Web page:www.gse.com.co
Responsible: Customer Service
Once a case is presented, it is forwarded along with the relevant information to the Customer Service process, following the established internal procedure for investigating and managing such cases. Similarly, the department responsible for taking corrective or preventive actions is identified, in which case the corresponding action procedure must be followed.
Once the investigation is generated, the response is evaluated in order to subsequently make the decision that resolves the PQRS and its final communication to the subscriber, responsible party or interested party.

1.4 Use of the certificate.
1.4.1 Proper use of certificates
The appropriate uses of certificates issued by ECD GSE are specified in the Certificate Policies for Digital Certificates. Certificates issued under these policies may be used for the following purposes:
° Subscriber Identification: The Digital Certificate Subscriber can authenticate their identity to another party by demonstrating the association of their private key with the respective public key contained in the Digital Certificate.
° Integrity: The use of a Digital Certificate to apply digital signatures guarantees that the signed document is complete, meaning it guarantees that the document was not altered or modified after being signed by the Subscriber. It certifies that the message received by the trusting Recipient is the same one that was sent by the Subscriber.
° Non-repudiation: The use of this Digital Certificate also guarantees that the person who digitally signs the document cannot repudiate it, that is, the Subscriber who has signed cannot deny the authorship or integrity of it.

The public key contained in a Digital Certificate can be used to encrypt data messages, such that only the holder of the private key can decrypt the message and access the information. If the private key used for decryption is lost or destroyed, the encrypted information cannot be decrypted. The subscriber, responsible parties, and third parties acting in good faith acknowledge and accept the risks involved in using digital certificates for encryption processes, and specifically, the use of keys to encrypt data messages is the sole responsibility of the subscriber or responsible party in the event of the key's loss or destruction.
The ECD GSE assumes no responsibility for the use of digital certificates for encryption processes.
Each certification policy is identified by a unique object identifier (OID) that also includes the version number.
Any use other than that described in this DPC will be considered a violation of this DPC and will constitute grounds for immediate revocation of the digital certification service and termination of the contract with the subscriber and/or responsible party, without prejudice to any criminal or civil actions that may be taken by the ECD GSE.
1.4.2 Prohibited use of certificates
Certificates may only be used for the purposes for which they were issued and specified in this DPC and specifically in the Certificate Policies for Digital Certificates.
Improper uses are those not defined in this DPC and, consequently, for legal purposes, ECD GSE is exempt from all liability for the use of certificates in operations that are outside the limits and conditions established for the use of Digital Certificates according to this DPC, which include, but are not limited to, the following prohibited uses:
Illicit purposes or operations under any legal regime in the world.
Any practice contrary to Colombian law.
Any practice contrary to the international agreements signed by the Colombian state.
Any practice contrary to supranational norms.
Any practice contrary to good business practices and customs.

Any use in systems whose failure could cause:
or Death
or Injuries to persons
or Environmental damage
As a control system for high-risk activities such as:
o Maritime navigation systems
o Land transportation navigation systems
o Air navigation systems
o Air traffic control systems
or Weapons control systems

1.5 Policy administration.
1.5.1 Organization that manages the document.
The DPC and certification policies are the responsibility and property of GSE and therefore it acts as its administrator.
1.5.2 Contact (ECD Manager):
Name: Álvaro de Borja Carreras Amorós Position: President
Address: Calle 77 # 7-44 Office 701 Home: Bogotá DC, Colombia.
Telephone: +57 (601) 4050082
Email: info@gse,com,co
1.5.3 Person who determines the suitability of the DPC for the policy.
Area in charge: Operations Coordinator Address: Calle 77 # 7-44 Office 701 Address: Bogotá DC, Colombia.
Telephone: +57 (601) 4050082
Email: info@gse.com.co

1.5.4 DPC approval procedures.
The Management Committee is the internal body of GSE responsible for reviewing, approving and authorizing the publication of the DPC on the websitehttp://www.gse.com.co
1.6 Definitions and acronyms.
Definitions.
The following terms are in common use and required for the understanding of this DPC:
Certification Authority (CA): In English "Certification Authority" (CA): Certification Authority, root entity and public key infrastructure certification service provider.
Registration Authority (RA): In English "Registration Authority" (RA): It is the entity responsible for certifying the validity of the information provided by the applicant for a digital certificate, through the verification of their identity and registration.
Time Stamping Authority (TSA): Acronym for "Time Stamping Authority": Certification entity providing time stamping services
Secure Data Archiving: This is the service GSE offers its clients through a technological platform. Essentially, it consists of a secure and encrypted storage space accessed with credentials or a digital certificate. Documentation stored on this platform will have evidentiary value as long as it is digitally signed.
Digital certificate: A document electronically signed by a certification service provider that links signature verification data to a signatory and confirms their identity. This is the definition in Law 527/1999, which in this document is extended to cases where the signature verification data is linked to a computer component.
Specific Accreditation Criteria (CEA): Requirements that must be met to obtain Accreditation as a Digital Certification Entity - ECD, before the National Accreditation Body of Colombia - ONAC; that is, to provide digital certification services in accordance with the provisions of Law 527 of 1999, Decree Law 019 of 2012, chapters 47 and 48 of title 2 of part 2 of book 2 of the Single Decree of the Commerce, Industry and Tourism Sector - DURSCIT and the regulations that modify or complement them.
Personal Access Key (PIN): Acronym for "Personal Identification Number": Sequence of characters that allow access to the digital certificate.
Private key compromise: compromise is understood as the theft, loss, destruction or disclosure of the private key that may put at risk the use of the certificate by unauthorized third parties or the certification system.
Certified email: A service that ensures the sending, receiving, and verification of electronic communications, guaranteeing at all times the characteristics of fidelity, authorship, traceability, and non-repudiation.
Certification Practice Statement (CPS): A statement by the certification body regarding the policies and procedures it applies to the provision of its services.
Chronological stamping: According to numeral 7 of Article 3 of Decree 333 of 2014, it is defined as: Data message with a specific moment or period of time, which allows establishing with proof that this data existed at a moment or period of time and that it did not undergo any modification from the moment the stamping was made.
Certification Entity: It is that legal person, accredited in accordance with Law 527 of 1999 and Decree 333 of 2014, authorized by the Colombian government (National Accreditation Body in Colombia) to issue certificates in relation to the digital signatures of the clients who acquire them, offer or facilitate the services of registration and time stamping of the transmission and reception of data messages, as well as fulfill other functions related to communications based on digital signatures.
Open Certification Authority: This is a Certification Authority that offers services typical of certification authorities, such as:

1. Its use is not limited to the exchange of messages between the entity and the subscriber, or
2. He receives remuneration for these.

Closed certification authority: An entity that offers services typical of certification authorities only for the exchange of messages between the entity and the subscriber, without requiring remuneration for it.
Public Key Infrastructure (PKI): A PKI is a combination of hardware and software, security policies and procedures that allows users of a basically insecure public network such as the Internet to exchange data messages securely using a pair of cryptographic keys (one private and one public) that are obtained and shared through a trusted authority.
Initiator: Person who, acting on their own behalf, or on whose behalf someone has acted, sends or generates a data message.
Trust hierarchy: A set of certification authorities that maintain trust relationships whereby a higher-level CDA guarantees the reliability of one or more lower-level CDAs.
Certificate Revocation List (CRL): English acronym for "Certificate Revocation List": A list that includes only revoked certificates that have not yet expired.
Public and Private Keys: The asymmetric cryptography on which PKI is based. It uses a pair of keys where encryption is done with one key and decryption is only possible with the other, and vice versa. One of these keys is called the public key and is included in the digital certificate, while the other is called the private key and is known only to the subscriber or certificate holder.
Private Key (Private Key): Numerical value or values that, used together with a known mathematical procedure, serve to generate the digital signature of a data message.
Public key (Public Key): Numerical value or values that are used to verify that a digital signature was generated with the private key of the person acting as the initiator.
Cryptographic Hardware Security Module: Acronym for "Hardware Security Module", hardware module used to perform cryptographic functions and store keys in secure mode.
Certification Policy (CP): It is a set of rules that define the characteristics of the different types of certificates and their use.
Certification Service Provider (CSP): A natural or legal person who issues digital certificates and provides other services related to digital signatures.
Online Certificate Status Protocol (OCSP): A protocol that allows you to verify the status of a digital certificate online.
Repository: an information system used to store and retrieve certificates and other related information.
Pseudonym: Hiding one's real name with a false name.
Pseudo-anonymous: Intentionally uses a false name
Revocation: Process by which a digital certificate is disabled and loses validity.
Applicant: Any natural or legal person who requests the issuance or renewal of a digital certificate.
Subscriber and/or responsible party: Natural or legal person to whom digital certification services are issued or activated and therefore acts as subscriber or responsible party thereof
Third party acting in good faith: A person or entity other than the subscriber and/or responsible party who decides to accept and rely on a digital certificate issued by ECD GSE. TSA GSE: This refers to the term used by ECD GSE, in the provision of its Time Stamping service, as a Time Stamping Authority.

Acronyms.
CA: Certification Authority
CA Sub: Subordinate Certification Authority CP: Certification Policy DPC: Certification Practice Statement CRL: Certificate Revocation List
CSP: Certification Service Provider
DNS: Domain Name System
FIPS: Federal Information Processing Standard
HTTP: The Hypertext Transfer Protocol (HTTP) is the protocol used in every transaction on the World Wide Web (WWW). HTTP defines the syntax and semantics used by the software elements of the web architecture (clients, servers, proxies) to communicate. It is a transaction-oriented protocol and follows a request-response pattern between a client and a server.
HTTPS: Hypertext Transfer Protocol Secure (in Spanish: Protocolo seguro de transferencia de hipertexto), better known by its acronym HTTPS, is a network protocol based on the HTTP protocol, intended for the secure transfer of hypertext data; that is, it is the secure version of HTTP.
HSM: Cryptographic Security Module (Hardware Security Module) IEC: International Electrotechnical Commission
IETF: Internet Engineering Task Force (Internet Standards Organization)
IP: Internet Protocol
ISO: International Organization for Standardization
LDAP: Lightweight Directory Access Protocol
OCSP: Online Certificate Status Protocol.
OID: Object identifier (Unique object identifier)
PIN: Personal Identification Number
PUK: Personal Unlocking Key
PKCS: Public Key Cryptography Standards. PKI standards developed by RSA Laboratories and accepted internationally.
PKI: Public Key Infrastructure
PKIX: Public Key Infrastructure (X.509)
RA: Registration Authority
RNEC: National Civil Registry
RFC: Request For Comments (Standard issued by the IETF)
URL: Uniform Resource Locator
VA: Validation Authority

Standards and Standardization Bodies.
CEN: European Committee for Standardization
CWA: CEN Workshop Agreement
ETSI: European Telecommunications Standard Inst
FIPS: Federal Information Processing Standard
IETF: Internet Engineer Task Force

PKIX: IETF Working Group on PKI
PKCS: Public Key Cryptography Standards
RFC: Request For Comments

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES.
Repositories.
2.1 ECD GSE Root Certificates
https://certs2.gse.com.co/CA ROOT.crthttps://certs2.gse.com.co/CA ECROOT.crthttps://certs2.gse.com.co/CA FEROOT.crt
ECD GSE Root Certificate Revocation List (CRL)https://crl2.gse.com.co/CA_ROOT.crl
https://crl2.gse.com.co/CA ECROOT.crlhttps://crl2.gse.com.co/CA FEROOT.crl
ECD GSE Subordinate Certificateshttps://certs2.gse.com.co/CA_SUB01.crt
https://certs2.gse.com.co/CA ECSUB01.crthttps://certs2.gse.com.co/CA FESUB01.crt
List of Revoked Certificates ECD GSE Subordinates (CRL)https://crl2.gse.com.co/CA_SUB01.crlhttps://crl2.gse.com.co/CA_ECSUB01.crlhttps://crl2.gse.com.co/CA FESUB01.crl
Online validation of digital certificateshttps://ocsp2.gse.com.co
Note: Online validation of digital certificates using OCSP must be performed with a tool that implements the OCSP protocol and is capable of understanding the responses generated by the service, such as OPENSSL.
This ECD GSE repository does not contain any confidential or private information.
The ECD GSE repositories are referenced by URL. Any changes to these URLs will be notified to all potentially affected entities. The IP addresses associated with each URL may be multiple and dynamic, and may be modified by ECD GSE without prior notice.
2.2 Publication of information on certification.
The Certificate Revoked List published on the GSE website is digitally signed by the ECD GSE.
Information on the status of valid digital certificates is available for consultation on the website and with the OCSP protocol.
2.3 Publication schedule or frequency.
Root Certificate
The root certificate will be published and will remain on the ECD GSE website for as long as digital certification services are being provided.
Subordinate Certificate
The Subordinate's certificate will be published and will remain on the ECD GSE website for as long as digital certification services are being provided.
Certificate Revoked List (CRL)
ECD GSE will publish on the website the list of revoked certificates at the events and with the periodicity defined in the CRLs Issuance Frequency section.
Certification Practice Statement (CPS) - Global Certification Authority Root GSE
With authorization from the Management Committee, validation by the auditing firm, issuance of the audit compliance report, and finally, express accreditation from ONAC, the final approved version for providing the digital certification service will be published. Subsequent publications will be subject to any necessary modifications, with the approval of the Management Committee. Changes made in each new version will be reported to ONAC and published on the ECD GSE website along with the new version. The annual audit will validate these changes and issue the compliance report.
Online validation of digital certificates
ECD GSE will publish the issued certificates in a repository in X.509 format, which can be consulted at the following address:https://ocsp2.gse.com.co
Online validation of digital certificates using OCSP must be done with a tool that implements the OCSP protocol and is able to understand the responses generated by the service, such as OPENSSL.
2.4 Access controls to repositories.
Access to the repositories available on the aforementioned GSE website is free and open to the general public. The integrity and availability of the published information is the responsibility of ECD GSE, which has the necessary resources and procedures to restrict access to the repositories for purposes other than consultation.

3. IDENTIFICATION AND AUTHENTICATION.

3.1 Names.

3.1.1 Types of names.
The guide document that ECD GSE uses for the unique identification of subscribers or those responsible for issued certificates is defined in the structure of the Distinguished Name (DN) of the ISO/IEC 9595 (X.500) standard.
Certificates issued by ECD GSE contain the X.500 distinguished name (DN) of the issuer and the recipient of the certificate in the issuer name and subject name fields respectively.

ECD GSE root certificates.
The DN of the 'issuer name' of the root certificate has the following fields and fixed values: C = CO O = GSE
C = CO
O = GSE
OU = PKI
CN = Root Authority GSE
E =info@gse.com.co
The following fields are included in the DN of the 'subject name': C = CO O = GSE
C = CO
O = GSE
OU = PKI
CN = Root Authority GSE E =info@gse.com.co
Elliptical Curve (ECDSA).
The DN of the 'issuer name' of the root certificate has the following fields and fixed values: C = CO
C = CO
S = Capital District
L = Bogota DC
O = ELECTRONIC SECURITY MANAGEMENT SA
OU = GSE CA ROOT R2
SERIALNUMBER = 900204278
CN = GSE ECDSA RAIZ
E =info@gse.com.co
STREET =www.gse.com.co
The following fields are included in the DN of the 'subject name':
C = CO
S = Capital District
L = Bogota DC
O = ELECTRONIC SECURITY MANAGEMENT SA
OU = GSE CA ROOT R2
SERIALNUMBER = 900204278
CN = GSE ECDSA ROOT
E =info@gse.com.co
STREET =www.gse.com.co
Certificates of Subsidiaries.
The DN of the 'issuer name' of the certificates of ECD GSE subsidiaries has the following characteristics:
C = CO
O = GSE
OU = PKI
CN = Root Authority GSE
E =info@gse.com.co
The following fields are included in the DN of the 'subject name':
C = CO
L = Bogota DC
O = GSE
OU = PKI
CN = Subordinate Authority 01 GSE
E =info@gse.com.co
Elliptical Curve (ECDSA).
The DN of the 'issuer name' of the certificates of ECD GSE subsidiaries has the following characteristics:
C = CO
S = Capital District
L = Bogota DC
O = ELECTRONIC SECURITY MANAGEMENT SA
OU = GSE CA ROOT R2 SERIALNUMBER = 900204278
CN = GSE ECDSA ROOT
E =info@gse.com.co
STREET =www.gse.com.co
The following fields are included in the DN of the 'subject name':
C = CO
S = Capital District
L = Bogota DC

O = ELECTRONIC SECURITY MANAGEMENT SA
OU = GSE ECDSA R2 SUB1
SERIALNUMBER = 900204278
CN = GSE ECDSA SUBORDINATE
E =info@gse.com.co
STREET =www.gse.com.co

ECD GSE Subscriber Certificates (Technical Certificate Profile Matrix).
The DN of the 'issuer name' of ECD GSE subscriber certificates has the following general characteristics:
C = CO
L = Bogota DC
O = GSE
OU = PKI
CN = Subordinate Authority 01 GSE
E =info@gse.com.co
The DN of the 'subject name' is determined by ANNEX 1 DPC TECHNICAL PROFILE MATRIX DIGITAL CERTIFICATES
ECD GSE subscriber certificates (Technical Profile Matrix of Electronic Signature Certificates).
STREET=www.gse.com.co,
E: info@gse,com,co,
CN = GSE INTERMEDIATE ELECTRONIC SIGNATURE,
SN=900204272,
OU = GSE ELECTRONIC SIGNATURE R1,
O = ELECTRONIC SECURITY MANAGEMENT SA,
L = BOGOTA DC,
ST=CAPITAL DISTRICT,
C=CO
3.12The need for names to make sense.
The Distinguished Names (DNs) of certificates issued by ECD GSE are unique and establish a link between the public key and the subscriber's identification number. Because the same person or entity can request multiple certificates in their name, these will be differentiated by the use of a unique value in the DN field.
Anonymity or pseudonymization of subscribers.
Aliases, nicknames, epithets, diminutives, and/or similar terms may not be used in the subscriber or responsible party fields, as the certificate must include the real name, company name, acronym, or designation of the certificate applicant.
Rules for interpreting the different forms of the name.
The rule used to interpret the distinctive names of the issuer and of the subscribers or those responsible for digital certificates issued by ECD GSE is the ISO/IEC 9595 (X.500) Distinguished Name (DN) standard.
3.1.3 Uniqueness of Names.
The DN of the issued digital certificates is unique for each subscriber.
3.1.4Recognition, authentication and role of trademarks.
3.16Recognition, Authentication, and Role of Recognized Trademarks: ECD GSE is not required to collect or request evidence regarding the ownership, subscription, or liability of trademarks or other distinctive signs prior to issuing digital certificates. This policy extends to the use and employment of domain names.

3.2 Initial identity validation.
The ECD GSE will receive requests to certify the unequivocal identification of the subscriber's identity (natural or legal person), the veracity and authenticity of the information through any identification system of its own, or if it belongs to a third party as long as a contract, agreement, accord, alliance, and/or any means of contractual and/or commercial relationship, direct and/or indirect, among others, exists, with which the verification of the information is carried out in a manner analogous to face-to-face validation by consuming one or more of the widely used services according to the digital certificate service requested, for this purpose listed below:
National Identification Archive - National Civil Registry.
Muisca -Unique Model of Income, Service and Automated Control - and/or databases of the DIAN (National Directorate of Taxes and Customs).
Confront.
Single Business and Social Registry and/or databases of the Chambers of Commerce (For Legal Entities).
Migration Colombia (for foreigners).
Databases maintained by the National Civil Registry that allow for the unequivocal identification of the applicant, in accordance with current regulations issued by the Registry.
Selfie versus identification document (hologram, digital, physical and foreigner's identity cards)
The ECD GSE reserves the right to decline the acceptance of an application or the maintenance of a contract for certification when, in its judgment, there are reasons that may jeopardize the credibility, commercial value, legal or moral suitability of the ECD; likewise, the demonstrated participation of the applicant in illegal activities, or similar issues related to the same, will be sufficient reason to reject the application.
The applicant's data: type of identification, identification number, names, surnames, NIT (applies to companies), company name (applies to companies) and email address are reviewed and/or validated together with the application form, the information and/or documentation provided for each type of digital certificate.
The Single Taxpayer Registry (RUT) document must be requested in the updated DIAN format, which includes a QR code (if applicable). These services are detailed in the Digital Certificate Issuance Procedure.

For digital certification services: Time Stamping, Certified Email, Generation of Certified Electronic Signatures, Archiving and Preservation of Transferable Electronic Documents and Data Messages, the identity verification service will not be consumed, but the verification mechanisms that apply to confirm the veracity and authenticity of the information will be used, such as:
National Identification Archive - National Civil Registry.
Muisca - Unique Model of Income, Service and Automated Control - and/or databases of the DIAN (National Directorate of Taxes and Customs).
Single Business and Social Registry and/or databases of the Chambers of Commerce (For Legal Entities).
Migration Colombia (for foreigners).
The ECD GSE reserves the right to request additional documents, in original or copy, in order to verify the applicant's identity. It may also waive the requirement to submit any document when the applicant's identity has been sufficiently verified by the ECD GSE through other means, if the application for a digital certificate for a natural person is made directly and/or indirectly from the platforms of the National Civil Registry - RNEC, after prior verification by said entity and its functions described in Decree 1010 of 2000.
(...)
ARTICLE 2. Purpose. The purpose of the National Civil Registry is to register civil life and identify Colombians and to organize electoral processes and mechanisms for citizen participation, in order to support the administration of justice and the democratic strengthening of the country.
(.)
ARTICLE 5. Functions. The functions of the National Civil Registry are the following:
To issue and produce Colombian citizenship cards, under optimal conditions of security, presentation and quality, and to adopt a single identification system for first-time applications, duplicates and corrections.
To handle everything related to the management of information, databases, the National Identification Archive and the documents necessary for the technical process of citizen identification, as well as to inform and issue certifications for the procedures that may be necessary.
24. To attend to requests for the issuance of the citizenship card at Colombian consulates abroad so that those who are enabled can exercise their political rights as Colombian citizens and provide information about their procedure.
This means that if a digital certificate request for an applicant (citizen) is made from the RNEC as the main source of information in Colombia, it ensures that the applicant had a prior validation of their identity and address data to carry out the process of issuing the citizenship card, the ECD GSE will receive the information from said source, the veracity and authenticity is ensured by making the unequivocal identification of the subscriber, the ECD GSE will maintain the records of the request ensuring the Digital Certification Lifecycle process.
In the case of electronic signature certificates, the identity of the applicant is not validated, but rather the data registered at the time of the signature request is verified by sending an OTP code to the registered email address.
3.2.1Method to prove possession of the private key.
To guarantee the issuance, possession and control of the private key by the subscriber and/or responsible party, a secure cryptographic token device is delivered directly to the subscriber and/or responsible party, in which the subscriber and/or responsible party generates the key pair and transmits the file in PKCS#10 format through a secure channel, demonstrating that they are in possession of the private key.
In the case of a centralized certificate, the generation of the key pair is carried out on an HSM device owned by the ECD GSE and the subscriber and/or responsible party is given a set of credentials (username and password) for their exclusive use.
Since electronic signature certificates are ephemeral and are used only for generating the signature, the credentials for using these certificates are not delivered to the subscriber and are instead generated automatically and randomly by the platform and discarded once the electronic signature is generated.
Pursuant to the provisions of ONAC in CEA 3.0-07, in the case where the key pair is generated by the applicant in its own infrastructure, for example, for the use of the certificate on unattended platforms, the applicant must accept and comply with the requirements set forth in Annex 1 of Terms and Conditions, numeral 6, literal m), if these were generated by software and through devices that comply with Annex F of the CEA, if they were generated by hardware.
3.2.2 Authentication of the organization's identity.
To verify the identity of a legal entity, the RA GSE requires the submission of the legal entity's information and/or the presentation of an official document proving its legal existence and that of its legal representative or authorized agents, who will be the only individuals authorized to request the digital certificate on behalf of said organization.
If the request is made by a third party, a scanned copy of the power of attorney authorizing the process for the representative must be submitted. Documents will be accepted as scanned copies, ensuring legibility for the purposes of data collection.
Notwithstanding the foregoing, ECD GSE reserves the right to withhold certificates when, in its judgment, the credibility, commercial value, or legal or moral suitability of the Digital Certification Entity may be jeopardized.
3.2.3 Authentication of individual identity.
To ensure the identity of an individual, the RA GSE requires the registration of information proving the applicant's identity and/or the presentation of the applicant's digital identity document. It then verifies the existence and correspondence of this information against its own and/or third-party databases, whether official or private, through contracts, agreements, partnerships, and/or any type of contractual and/or commercial relationship, whether direct or indirect. When the service is requested by a minor, their identity will be verified with an authenticated identity document (identity card) and a document supporting the relationship between the applicant and the minor. If the request is made by a third party, a scanned copy of the power of attorney authorizing the process must be submitted. Documents will be received as scans, ensuring legibility for the use of the information.
Notwithstanding the foregoing, ECD GSE reserves the right to withhold certificates when, in its judgment, the credibility, commercial value, or legal or moral suitability of the Digital Certification Entity may be jeopardized.
3.2.4Unverified subscriber information.
Under no circumstances will ECD GSE omit the verification work that leads to the identification of the applicant and that translates into the request and demand of the information and/or documents mentioned for organizations and individuals.
In the specific case of address data, the RA presumes the veracity of the information provided by the applicant in application of the principle of good faith in accordance with our Political Constitution, which is why an additional validation process is not necessary.
3.2.5 Authority validation.
GSE uses a reliable method of communication with the Applicant or their representative.
The Applicant's authority to request Certificates on behalf of an organization is verified during the Applicant identity validation.
GSE may allow Applicants to specify in writing the individuals authorized to apply for Certificates on their behalf. Once such a specification has been made, GSE will not accept certificate applications that fall outside this specification but, upon written request, will provide the Applicant company with a list of its authorized certificate applicants.
3.2.6 Interoperability criteria.

ECD GSE will only issue digital certificates to Subordinate ECDs, where the decision to issue or activate the digital certification service is made by the ECD GSE through a recommendation based on a review of the GSE RA's request.

3.3 Identification and Authentication for key renewal.
3.3.1 Identification and authentication for the key reuse routine.
The ECD GSE does not consider the process of reusing the public and private keys of the certificate for the renewal of digital certificates.
If a renewal of an issued certificate is requested, the issuance request process must be followed in the same way as for a new certificate, which will be generated from a new key pair.
ECD GSE performs the applicant authentication process for all events, including renewals, and issues digital certificates based on this authentication. This process is carried out using any identification system, provided that a contract, agreement, partnership, or any other type of direct or indirect contractual and/or commercial relationship exists with the National Civil Registry, credit bureau databases, or government data sources. Only applications digitally signed by the subscriber will have their digital certificate renewed without undergoing a new identification and authentication process, thus guaranteeing document validation.
Identification and authentication for the key reuse routine after revocation.
GSE does not consider the process of reusing the public and private keys of the certificate for the renewal of digital certificates, when their revocation has been requested.
If a revocation of an issued certificate is requested and then it is intended to request the certificate again with the same data as the revoked one, the issuance request process must be followed in the same way as a new certificate, which will be generated from a new key pair.
The process of replacing a digital signature certificate as a consequence of revocation for the different reasons defined in this DPC, requires a verification process for that request (Replacement).

3.4 Identification and authentication for the revocation request.
ECD GSE processes revocation requests in accordance with the grounds for revocation specified in the section "Circumstances for Revoking a Certificate" of this DPC and authenticates the identity of the person requesting the certificate revocation, in accordance with the established revocation procedure.

4. OPERATIONAL REQUIREMENTS OF THE CERTIFICATE LIFECYCLE.

4.1 Certificate application.
Anyone requiring digital certification services may do so using the channels, means, or mechanisms provided by ECD GSE. These channels will provide the necessary information to process the application for the required digital certification service. Once the terms and conditions are accepted and the application is submitted, the information is sent to the Registration Authority, which will review the application to ensure the unambiguous identification of the subscriber (natural or legal person), the veracity and authenticity of the information, and to provide a recommendation for decision-making in compliance with the requirements of the Certification Policies.
The applicant provides the necessary information and/or documents, as applicable, by submitting them as scanned copies or in electronic format, ensuring legibility for the intended use of the information. Alternatively, the information may be obtained from fully trusted databases, as previously mentioned, thus fulfilling the procedures established by the ECD GSE for obtaining the digital certificate.
The ECD GSE reserves the right to request additional information and/or documents beyond those required, in original or copy, to verify the applicant's identity. It may also waive the requirement to submit any document when the applicant's identity has been sufficiently verified by the ECD GSE through other available means or mechanisms.
The information and/or documentation provided will be reviewed according to the Application Evaluation Criteria and Methods established by GSE.
The applicant accepts that the ECD GSE has the discretionary right to reject a digital certificate application when, in its judgment, the credibility, commercial value, good name of GSE, legal or moral suitability of the entire digital certification system may be jeopardized, notifying the applicant of the non-approval.
The procedure for obtaining an electronic signature certificate is the ELECTRONIC SIGNATURE ACQUISITION PROCEDURE (PCO-PD-17).
Who can request a certificate?
Any legally authorized and duly identified natural or legal person may process the application for issuance of a digital certificate.
Application, registration and liability process.
Once the applicant's authentication and data verification requirements have been met, the GSE RA will approve and digitally sign the certificate of issuance. All related information will be recorded in the GSE RA system.

4.2 Certificate application processing.
4.2.1 Procedure for processing the application/ identification and authentication.
The authentication and identity verification functions of the applicant are performed by the GSE RA, responsible for making the recommendation for the decision on the digital certification based on the review of the application, who checks if the information provided is authentic and meets the requirements defined for each type of certificate in accordance with this DPC.
The information and/or documentation that the GSE RA must review to make the recommendation for decision-making for the correct issuance of each type of certificate is defined in the Certificate Policies for Digital Certificates.
Criteria for acceptance or rejection of the application.
Once the applicant's identity has been verified, if the information provided meets the requirements established by this DPC, the application is approved. If full identification of the applicant's identity is not possible, or if the information provided is not fully authentic, the application is denied and the certificate is not issued. ECD GSE assumes no responsibility for any consequences that may arise from the denial of a digital certificate, and this is accepted and acknowledged by the applicant whose certificate is denied.
Similarly, ECD GSE reserves the right not to issue certificates even if the applicant's identification or the information provided by the applicant has been fully authenticated, when the issuance of a particular certificate for reasons of legal order or commercial convenience, good name or reputation of GSE could endanger the digital certification system.
If after filing an application and the process does not approve the review of the application or the applicant does not carry out the identity validation, after fifteen (15) days without the issue being resolved, the RA of the ECD GSE will have the alternative of rejecting the application and the applicant will be notified to process a new application.
ECD GSE will notify the applicant of the approval or rejection of the application.
Deadline for processing certificate applications

The processing time for an application by the GSE RA is one (1) to five (5) business days from the moment the requested information and/or documentation is received and the applicant has passed the initial identity validation.
The delivery time of the digital certificate issued on a cryptographic device depends on the destination location, without exceeding eight (8) business days for delivery.

4.3 Issuance of the Certificate.
4.3.1 ECD GSE actions during certificate issuance.
The final step in the digital certificate issuance process is the issuance of the certificate by ECD GSE and its secure delivery to the subscriber and/or responsible party.
The GSE RA generates the formal documentation for the digital certificate once the decision to grant it has been made. The digital certificate issuance process securely links the registration information and the generated public key.
Notification mechanisms authorized by subscribers.
4.3.2 The subscriber will be notified of the issuance of their digital certificate via email or another previously defined and authorized method. The subscriber accepts and acknowledges that, upon receiving this notification, the certificate will be considered issued. The notification will be considered received when there are no issues with the delivery, that is, when the system confirms that the communication was successfully sent to the authorized channel. If the subscriber requested that the digital certificate be issued on a cryptographic device, it will be considered delivered once the shipping record is received: delivery note and/or shipping label from the logistics operator or courier, and/or the subscriber confirms in the issuance notification that they have received the cryptographic device.
Publishing a certificate in the certificate repository constitutes proof and public notification of its issuance.

4.4 Acceptance of the Certificate.

4.4.1 Mechanism for acceptance of the certificate by the subscriber.
No confirmation from the subscriber or responsible party is required as acceptance of the received certificate. A certificate is considered accepted by the subscriber or responsible party from the moment its issuance is requested. Therefore, if the information contained in the issued certificate does not correspond to its current status or was not provided correctly, it is the subscriber's responsibility to report this and/or request its revocation.

4.4.2 Publication of the certificate by the CA
GSE publishes all root and subordinate CA certificates in its repository and provides a mechanism for subscribers, as the digital certificate holder, to query end-entity certificates. On the website:https://ase.com.co/consultas-en-linea/

4.4.3 Notification of the issuance of certificates by the ECD GSE to other entities.
See section 4.4.2 above.

4.5 Use of key pairs and certificates.
4.5.1 Subscriber Responsibilities Regarding the Use of the Private Key and Certificate.
The subscriber or owner of the digital certificate and its associated private key accepts the terms of use established in this Terms of Use by the mere fact of having requested the issuance of the certificate and may only use them for the purposes explicitly mentioned and authorized in this Terms of Use and in accordance with the "Key Usage" fields of the certificates. Therefore, the issued certificates and the private key must not be used for any activities outside of the aforementioned uses. Once the certificate's validity period has expired, the subscriber or owner is obligated to cease using the associated private key. Based on the foregoing, the subscriber hereby accepts and acknowledges that they will be solely responsible for any loss, damage, or harm caused to third parties by the use of the private key after the certificate's validity period has expired. ECD GSE assumes no responsibility for unauthorized uses.
4.5.2 Responsibilities of the trusted third party related to the use of the subscriber's private key and certificate.
The subscriber to whom a certificate has been issued is obliged to inform third parties each time they use the certificate that they need to check the certificate's status on the certificate revocation list, as well as on the issued certificates list, to verify its validity and that it is being used within its permitted uses established in this DPC.
In this regard, it should:
Verify that the associated certificate does not violate the start and end validity dates.
Verify that the certificate associated with the private key is not revoked.
Verify that the fingerprint of the root ECD certificate and the ECD GSE subsidiary certificate match the one published by GSE on its website.
Fingerprint of the root ECD certificate:
SHA 256 Fingerprint=7C:iC:A5:5i:3i:2E:A0:2E:Fi:D6:3A:4F:56:54:D0:3F:D0:4F:6F:32:7C:8E:2E:03:52:iA:22:69:7A:B7:98:43 SHA256
Fingerprint=9F:BF:5F:Ei:A3:34:49:35:44:6A:95:EB:45:D3:DD:F3:49:36:i8:4i:2i:7i:7i:65:F0:B8:42:ii:85:0D:E6:F3 SHA256
Fingerprint=3F:CE:D4:24:F2:D5:70:53:6E:DA:65:2D:D7:C9:D3:6D:58:5A:i0:ED:BB:58:85:iC:F8:2C:9i:i2:03:4i:5C:0C Fingerprint of the certificate of the ECD subordinate GSE Subordinate Certificate 001: SHA 256
Fingerprint=70:99:0i:C9:iD:8F:B2:92:DB:8i:B7:04:8B:0B:06:E5:A2:AA:i4:59:7D:CA:C4:DF:BE:6B:DD:90:49:D8:E2:01 SHA256
Fingerprint=8C:8B:i7:8E:AA:D2:E9:AD:BF:2D:28:iE:9i:53:3F:96:BF:7C:BE:iB:2D:8A:89:A0:D8:AE:FD:i9:40:D0:35:88 SHA256
Fingerprint=6C:9i:FA:BA:42:7F:0D:93:CB:B4:EB:09:4A:3F:5E:4A:64:D8:F2:5F:B8:7B:AA:75:D8:26:8D:BF:79:8E:CC:95
4.6 Certificate renewal
The ECD GSE does not process certificate renewal requests without a change of keys.
4.6.1 Circumstances for certificate renewal.
This does not apply because certificates are not issued without a change of keys.
4.6.2 Who can request a renewal without changing the keys?
This does not apply because certificates are not issued without a change of keys.
4.6.3 Procedures for requesting renewal of certificates.

This does not apply because certificates are not issued without a change of keys.
4.6.4 Notification to the subscriber or person responsible for issuing a new certificate without changing the keys.
This does not apply because certificates are not issued without a change of keys.
4.6.5 How a certificate renewal is accepted.
This does not apply because certificates are not issued without a change of keys.
4.6.6 Publication of the certificate renewed by the ECD.
This does not apply because certificates are not issued without a change of keys.
4.6.7 Notification of the issuance of a renewed certificate by the ECD to other entities.
This does not apply because certificates are not issued without a change of keys.

4.7 Re-use of certificate key

For the ECD GSE, a certificate renewal request with key change is a normal procedure for requesting a digital certificate as if it were a new one and therefore involves the generation of new keys, which the applicant recognizes and accepts.
In conclusion, GSE treats all requests for re-issuance and/or renewal of certificates as requests for issuance of a new certificate, taking into account that it does not reuse keys in any case.
4.7.1 Circumstance for the reuse of certificate keys.
A new digital certificate can be generated at the request of the subscriber and/or responsible party due to the expiration or revocation of the current certificate in accordance with the grounds mentioned in this DPC or when required by the subscriber.
Not applicable. See section 4.7
Who can request certification of a new public key?
4.7.2 For certificates for individuals, the subscriber can request the renewal of the certificate. For legal entities, the legal representative, responsible alternates, or duly authorized appointees or agents can request the renewal of the digital certificate.
Not applicable. See section 4.7
4.7.3 Processing of certificate key reuse requests.
The procedure for renewing digital certificates is the same as the procedure for requesting a new certificate. The subscriber must access the designated system to submit the request to the ECD GSE and initiate the process for requesting a new digital certificate, just as they did when submitting the initial digital certificate request. Their request will be validated again to update the information if necessary.
Not applicable. See section 4.7
4.7.4 Notification to the subscriber of the issuance of a new certificate.
The subscriber will be notified of the issuance of their digital certificate via email or other suitable means. The subscriber acknowledges and accepts that upon receiving this notification, they agree to the terms and conditions of the ECD GSE for which the certificate was issued. If the subscriber requested that the digital certificate be issued on a cryptographic device, delivery will be considered complete upon receipt of proof of shipment: delivery note and/or shipping receipt from the logistics operator or courier, and/or confirmation in the issuance notification that the subscriber has received the cryptographic device.
Not applicable. See section 4.7
4.7.5Conduct that constitutes acceptance of a certificate with key reuse.
No confirmation from the subscriber or responsible party is required to accept the renewal of a received certificate. A renewed certificate is considered accepted by the subscriber or responsible party from the moment its issuance is requested. Therefore, if the information contained in the issued certificate does not correspond to its current status or was not provided correctly, the applicant or responsible party must request its revocation, and the applicant or responsible party must accept this.
Not applicable. See section 4.7
4.7.6 Publication of the certificate with key reuse by the CA
Not applicable because ECD GSE does not reuse certificate keys. Therefore, it is not appropriate. See section 4.7
4.7.7 Notification of the issuance of certificates by the CA to other entities
There are no external entities that need to be notified of the issuance of a renewed certificate. This is not applicable. See section 4.7

4.8 Certificate Modification.

Digital certificates issued by ECD GSE cannot be modified; amendments are not permitted. Therefore, the subscriber must request the issuance of a new digital certificate. In this case, a new certificate will be issued to the subscriber; the cost of this modification will be borne entirely by the subscriber according to the fees provided by ECD GSE or as defined in the contract.
4.8.1 Circumstance for the modification of the certificate.
This does not apply because digital certificates issued by ECD GSE cannot be modified.
4.8.2 Who can request a change to the certificate?
This does not apply because digital certificates issued by ECD GSE cannot be modified.
4.8.3 Processing of requests for modification of certificates.
This does not apply because digital certificates issued by ECD GSE cannot be modified.
4.8.4Notification to the subscriber of the issuance of a new certificate
This does not apply because digital certificates issued by ECD GSE cannot be modified.
4.8.5Conduct that constitutes acceptance of a modified certificate.
This does not apply because digital certificates issued by ECD GSE cannot be modified.
4.8.6 Publication of the certificate modified by the CA.

This does not apply because digital certificates issued by ECD GSE cannot be modified.

4.8.7 Notification of the issuance of certificates by the CA to other entities.
This does not apply because digital certificates issued by ECD GSE cannot be modified.

4.9 Revocation and Suspension of the Certificate.

4.9.1 Circumstances for revocation.
The subscriber or responsible party may voluntarily request the revocation of their digital certificate at any time in accordance with the provisions of Article 37 of Law 527 of 1999, but is obliged to request the revocation of their digital certificate under the following situations:
Due to loss or invalidation of the private key or digital certificate.
The private key has been exposed or is at risk of being misused.
Changes in the circumstances under which ECD GSE authorized the issuance of the digital certificate.
If during the validity period part or all of the information contained in the digital certificate becomes outdated or invalid.
If the subscriber or responsible party does not request the revocation of the certificate in the event of the above situations, they will be liable for the losses or damages incurred by third parties in good faith and without fault who relied on the content of the certificate.
The subscriber or responsible party acknowledges and accepts that certificates must be revoked when GSE knows or has indications or confirmation of the occurrence of any of the following circumstances:
At the request of the subscriber, responsible party or a third party on their behalf.
Due to the death of the subscriber or responsible party.
For the confirmation or evidence that some information or fact contained in the digital certificate is false.
The private key of the certification authority or its security system has been materially compromised in a way that affects the reliability of the certificate.
By court order or by a competent administrative body.
Due to a commitment to safety for any reason, in any way, situation or circumstance.
Due to the supervening incapacity of the subscriber or responsible party.
Due to the liquidation of the represented legal entity as stated in the digital certificate.
Due to the occurrence of new events that cause the original data to no longer correspond to reality.

Due to loss or disablement of the cryptographic device that has been delivered by ECD GSE.
Due to the termination of the subscription contract, in accordance with the grounds established in the contract.
For any reason that reasonably suggests that the certification service has been compromised to the point that the reliability of the digital certificate is called into question.
Due to the improper handling of the digital certificate by the subscriber.
Due to non-compliance by the subscriber or the legal entity he/she represents or is linked to through the terms and conditions document or the person responsible for digital certificates of the ECD GSE.
Knowledge of events that modify the initial state of the data provided, including: termination of Legal Representation, termination of the employment relationship, liquidation or extinction of the legal entity, cessation in public service or change to a different one.
At any time that falsehood is evident in the data provided by the applicant, subscriber or responsible party.
Due to non-compliance by the ECD GSE, the subscriber or responsible party with the obligations established in the DPC.
Due to non-payment of the fees for certification services, agreed between the applicant and ECD GSE.
Notwithstanding the above grounds, ECD GSE may also revoke certificates when, in its judgment, the credibility, reliability, commercial value, good name of ECD GSE, legal or moral suitability of the entire certification system may be jeopardized.
Who can request the revocation of a certificate
The subscriber or responsible party, a third party in good faith or any interested person when they have demonstrable proof of knowledge of facts and grounds for revocation mentioned in the section Circumstances for the revocation of a certificate of this DPC and that compromise the private key.
A third party acting in good faith or any interested person who has demonstrable evidence that a digital certificate has been used for purposes other than those set out in the section "Appropriate Uses of the Certificate" of this DPC.
Any interested person who has demonstrable proof that the certificate is not in the possession of the subscriber or responsible party.
The CA Technology team, as the highest control body responsible for managing the security of the ECD GSE's technological infrastructure, is able to request the revocation of a certificate if it has knowledge or suspicion of the compromise of the subscriber's private key, responsible party, or any other fact according to the circumstances for the revocation of a certificate.
Procedure for requesting revocation of a certificate.
The subscriber and/or responsible party, a third party in good faith or any person will have the opportunity to request the revocation of a digital certificate whose causes are specified in this DPC and can do so under the following procedures:
At the GSE offices.
During public service hours, written requests for revocation of digital certificates signed by subscribers and/or responsible parties are received, providing the original identification document.
Online revocation request:
The subscriber and/or responsible party may carry out the process of revoking the digital certificate through the GSE SA web portal.
https://gse.com.co/consultas-en-linea/- Request your revocation. When filling out the request, the current digital certificates will be displayed. You must select the certificate to be revoked and enter your registered email address. You will receive a notification with the security code to complete the online revocation request. The subscriber and/or responsible party must select the reason for the revocation, enter the security code, and submit the revocation request for their digital certificate. Once the request is complete, your digital certificate will be revoked, and a revocation notification will be sent to your registered email address.
Other means available to revoke the digital certificate by the subscriber and/or responsible party and/or third party in good faith may be through the tool(s) and/or application(s) from where the request for the issuance of the digital certificate of authorized third parties was filed.
Email Revocation Service
Through our emailrevocations@gse.com.co, subscribers and/or responsible parties may request the revocation of digital certificates in accordance with the grounds for revocation mentioned in the section Circumstances for the revocation of a certificate of this DPC, by sending a signed digital revocation request letter or email with the subscriber's data and grounds for revocation, Digital Certification Service Revocation Form.

Note: The ECD-GSE provides a template guide for writing the revocation request letter, which is available on the website.https://ase.com.co/auias-v-manuales, option Revocations and Root and Subordinate Certificates
The ECD, through the Technology area and the personnel designated to carry out the certification activities in accordance with the procedure for the revocation of digital certificates, will verify the revocation request.
4.9.4 Grace period to request revocation of a certificate.
Upon review of a revocation request, the ECD GSE will proceed immediately with the requested revocation during its regular business hours. Therefore, there is no grace period that allows the applicant to cancel the request. If the request was made in error, the subscriber or responsible party must request a new certificate, as the revoked certificate lost its validity immediately upon validation of the revocation request, and the ECD GSE will not be able to reactivate it.
The procedure used by the ECD GSE to verify a revocation request made by a specific person is to review the request in accordance with the previous section.
Once the revocation of the certificate has been requested, if it is evident that said certificate is used linked to the private key, the subscriber or responsible party releases ECD GSE from all legal responsibility, since he recognizes and accepts that the control, custody and confidentiality of the private key is his or her sole responsibility.
Time within which the CA must process the revocation request.
The request for revocation of a digital certificate must be handled with the highest priority, and its revocation should not take more than three (3) business days once the request has been reviewed.
Once the formalities for revocation have been fulfilled, and if for any reason the revocation of a certificate is not carried out in accordance with the terms established by this DPC, ECD GSE, as the certification service provider and responsible for the CA, will be liable for any damages caused to subscribers or third parties acting in good faith arising from errors and omissions, or from bad faith, by the administrators, legal representatives, or employees of ECD GSE in the performance of the activities for which it is authorized and for which it has civil liability insurance in accordance with Article 9, Guarantees, of Decree 333 of 2014. ECD GSE does not assume any other commitment or provide any other guarantee, nor does it assume any other responsibility to the subscriber and/or those responsible for the certificate or trusted third parties, except as established by the provisions of this DPC.
Revocation verification requirement for relying parties.
It is the responsibility of the subscriber and/or holder of a digital certificate, and they hereby accept and acknowledge this, to inform third parties acting in good faith of the need to verify the validity of the digital certificates they are using at any given time. The subscriber and/or holder shall also inform the third party acting in good faith that, for this purpose, they can consult the Certificate Revocation List (CRL), published periodically by the ECD GSE.
Relying parties must confirm the validity of each certificate in the certification chain by checking the relevant CRL or OCSP responder before relying on a certificate issued by the ECD GSE CA.
CRL emission frequency.
The ECD GSE will generate and publish a new CRL every twenty-four (24) hours in its repository with an online query availability 7x24x365, 99.8% uptime per year.
Maximum latency of the CRLs.
The time between the generation and publication of the CRL is minimal because the publication is automatic.
Availability of online revocation/status verification
The ECD GSE will publish both the CRL and the status of revoked certificates in freely accessible and easily searchable repositories, available 24/7, 365 days a year. The ECD GSE offers an online query service based on the OCSP protocol at the following address:https://ocsp2.ase.com.co.
Online validation of digital certificates using OCSP must be done with a tool that implements the OCSP protocol and is able to understand the responses generated by the service, such as OPENSSL.
Online revocation verification requirements.
To obtain information on the revocation status of a certificate at any given time, you can make an online query at the following addresshttps://ocsp2.ase.com.coThis requires software capable of operating with the RFC6960 protocol. Most browsers offer this service.
Online validation of digital certificates using OCSP must be done with a tool that implements the OCSP protocol and is able to understand the responses generated by the service, such as OPENSSL.
Other forms of revocation notices are available.
Within 24 hours of revoking a certificate, ECD GSE will inform the subscriber and/or responsible party via email or other means that their digital certificate has been revoked. The applicant acknowledges and accepts that upon receiving this notification, their request will be considered fulfilled. Receipt of the certificate revocation notification will be deemed to have occurred when said notification is entered into the information system designated by the applicant.
The publication of a revoked certificate in the CRL constitutes proof and public notification of its revocation.
The ECD GSE will maintain a historical archive of up to three (3) years of the generated CRLs and will be available to subscribers through a written request addressed to the ECD GSE.
Special requirements for renewal of compromised keys.
If a digital certificate was revoked due to compromise (loss, destruction, theft, disclosure) of the private key, the subscriber may request a new digital certificate for a period equal to or longer than the one initially requested by submitting a renewal request for the compromised digital certificate. The subscriber or responsible party is responsible for the safekeeping of the key and acknowledges and accepts this responsibility; therefore, they assume the cost of the renewal in accordance with the current fees established for digital certificate renewals.
In the event that a subscriber's private key is compromised, the subscriber must immediately notify the ECD GSE of the compromise. The ECD GSE will revoke the certificate in question, and this will be reflected in the next Certificate List (CRL) published in the following update to inform users that the certificate is no longer trusted. The subscriber is responsible for investigating the circumstances of the compromise.
Circumstances for suspension
ECD GSE does not offer the service of suspending digital certificates, only revocation.

4.9.74 Who can request the suspension
This does not apply because ECD GSE does not offer the service of suspending digital certificates, only revocation.

4.9.15 Suspension application procedure
This does not apply because ECD GSE does not offer the service of suspending digital certificates, only revocation.

4.9.16 Limits of the suspension period
This does not apply because ECD GSE does not offer the service of suspending digital certificates, only revocation.

4.10 Certificate Status Services.
Operational characteristics
To check the status of certificates issued by ECD GSE, an online query service based on the OCSP protocol is available at the following address:https://ocsp2.ase.com.coThe subscriber or person responsible for sending a request to check the status of the certificate through the OCSP protocol, which, once the database has been consulted, is handled by means of a response via http or the query via CRL.
The CRLs issued by the ECD GSE comply with RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile V2" and contain the following basic elements:
Revocation entries for a CRL or OCSP response are not removed until after the expiration date of the revoked certificate.
Service availability
The GSE ECD operates and maintains its CRL and OCSP capabilities with sufficient resources to provide a response time of ten seconds or less under normal operating conditions.
Certificate status services are available 24 hours a day, 7 days a week, unless temporarily unavailable due to maintenance, but always guaranteeing 24/7/365 online query availability, 99.8% uptime per year
Version number.
CRLs issued by ECD GSE comply with the current X.509 standard. CRL and CRL extensions.
Information about the reason for revoking a certificate will be included in the CRL, using CRL extensions and more specifically in the revocation reason field (reasonCode).
CRL Availability.
As indicated in section 4.9.9 Availability of online verification of revocation/status OCSP Profile.
The OCSP service complies with the provisions of RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP". Version number.
Compliant with OCSP Version 1 of RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP". OCSP Extensions. Not applicable
OCSP service availability
As indicated in section 4.9.9 Availability of online revocation/status verification
4.10.3 Optional features.
To obtain information on the certificate status at any given time, you can make an online query at the following addresshttps://ocsp2.ase.com.coThis requires software capable of operating with the OCSP protocol. Most browsers offer this service or allow you to query the CRL published on the portal.https://crl2.ase.com.co.
Online validation of digital certificates using OCSP must be done with a tool that implements the OCSP protocol and is able to understand the responses generated by the service, such as OPENSSL.
4.11 End of Subscription.
The ECD GSE terminates the validity of a digital certificate issued under the following circumstances:
Loss of validity due to revocation of the digital certificate.
Expiration of the period for which a subscriber contracted the validity of the certificate.
4.12 Key Custody and Recovery

4.12.1 Policy and practices regarding key custody and recovery.
The subscriber's private key can only be stored on a cryptographic hardware device (token or HSM).
The cryptographic hardware devices used by the ECD GSE comply with the following certifications as cryptographic chips: security level CC EAL5+ PP 9806, BSI-PP-002-2001, FIPS 140-2 LEVEL 3 or higher and the following OS certifications of the cryptographic chip: security level CC EAL4+ BSI-PP-0006-2002 (CWA 14169 SSCD Type-3) - BSI -DSZ-CC-0422-2008 and support the standards PKCS#11, Microsoft CAPI, PC/SC, X.509 current certificate storage, SSL v3, IPsec/IKE.
The ECD GSE publishes in the Digital Certificate Policies for Digital Certificates the characteristics of the cryptographic devices it offers to subscribers who request them for the creation and storage of their private keys.
Key custody and recovery policies.
The generated private key is stored on a secure device (hardware) from which it cannot be exported. Consequently, it is not possible to retrieve the subscriber's private 4.12.2 key. The subscriber is responsible for the safekeeping of the private key, and the subscriber accepts and acknowledges this.
Session key encapsulation and recovery policies and practices.
Recovering the subscriber's session key or PIN is not possible, as the subscriber is solely responsible for assigning it, and this is declared and accepted by the subscriber. The subscriber is responsible for safeguarding the session key or PIN and agrees not to maintain digital, written, or any other type of record. The subscriber is also obligated to protect access to the PIN. Therefore, if the PIN is forgotten, a case will be filed with the ECD-GSE service desk to verify the request. If necessary, the subscriber may submit a request to revoke the digital certificate through the designated channels and will process the request for a new digital certificate.

5. FACILITIES, MANAGEMENT AND OPERATIONAL CONTROLS.

5.1 Physical Security Controls.
The ECD GSE's AC infrastructure is located and managed in secure facilities. Detailed security procedures are in place and followed, prohibiting unauthorized access and entry to the areas of the facility where the AC systems reside.

5.1.1 Physical location of the ECD construction.

5.2 The ECD GSE has security measures in place to control access to the building housing its infrastructure. The regulated digital certification services provided through this DPC are delivered by a service provider. Access to the rack housing the servers that manage the ECD GSE's communication services is restricted to previously identified and authorized personnel who visibly display their visitor badge.
The ECD GSE guarantees that the PKI servers are in continuous operation virtually in the Amazon cloud.
This provider has procedures in place for managing the ECD GSE communications infrastructure, where only authorized personnel have access.
The restricted area of the communications center meets the following requirements:
Only authorized personnel are allowed entry.
Critical communication equipment is properly protected in racks.
It does not have windows facing the exterior of the building.
It is monitored 24 hours a day through a closed-circuit television system, with cameras both inside and outside the computer center.
It has physical access control.
Fire protection and prevention systems: smoke detectors, fire extinguishing system.
It has trained personnel to act in the event of catastrophic events.
It has a physical intruder detection system.
The cabling is properly protected against damage, sabotage attempts or interception by means of cable trays.

Physical access control mechanisms.
There are several levels of security that restrict access to the communications infrastructure through which ECD GSE provides its services, and each level has physical access control systems. The facilities are equipped with closed-circuit television and security personnel. Within the facilities, there are restricted areas where, due to the critical communications equipment and sensitive operations handled, access is permitted only to certain individuals.
Energy and air conditioning.
The communications center is equipped with an air conditioning system and a reliable power supply with protection against voltage drops and other electrical fluctuations that could potentially damage equipment. Additionally, a backup system ensures uninterrupted service with sufficient autonomy to guarantee continuity. In the event of a backup system failure, there is ample time to perform a controlled shutdown.
Exposure to water.
The data centers where the PKI services are hosted have isolation from possible sources of water and have flood detection sensors connected to the general alarm system.
Fire prevention and protection.
The communications center is equipped with a fire detection system and a fire suppression system. A cabling system protects the internal networks.
Backup copy system - Media storage.
There are procedures in place for taking backups, restoring, and testing databases for accredited services.
Mission-critical servers are located in cloud environments; however, on-premises servers are backed up and stored on a local NAS server with their respective contingency plan.
Waste disposal
All paper documents containing sensitive information belonging to the organization that have reached the end of their useful life must be physically destroyed to ensure that the information cannot be recovered. If the document or information is stored on magnetic media, the device must be formatted, permanently erased, or physically destroyed in extreme cases such as damage to storage devices or non-reusable devices, always ensuring that the information cannot be recovered by any means, whether currently known or unknown.
Off-site backup.
ECD GSE will maintain a backup copy of the databases on Amazon, which will be replicated if needed for restoration. Physical controls are in place for the technological infrastructure through which ECD GSE provides its services.
The technological infrastructure services through which ECD GSE provides its services.
5.2 Procedural Controls.
ECD Trust Roles.
The RA has defined the following roles, which cannot be performed by the same person within the area:
RA Agents: Individuals responsible for daily operations such as: reviewing and approving applications, attending to all activities related to the digital certification services provided by the ECD GSE through the RA. The roles and responsibilities of RA agents are defined in accordance with the ECD GSE Profiles and Functions.
AR Administrator: The person responsible for administering and configuring AR.
RA Auditor: A trained and impartial person responsible for evaluating compliance with RA requirements, auditing RA information systems, clarifying that their role is different from that of the internal auditor of management systems.
Number of people required in each role.
For each of the aforementioned roles, the ECD will guarantee collaborators to perform the tasks that affect the management of cryptographic keys of the ECD itself.
Identification and authentication of each role.
RA Agents and RA Administrators are authenticated using digital certificates issued by ECD GSE.
Each person only controls the assets necessary for their role, ensuring that no one accesses unassigned resources. Access to resources is granted based on the asset, using a login/password or digital certificates.
Roles that require segregation of duties.
The roles of RA Administrator, RA Agents, and RA Auditor are independent.

5.3 Personnel controls.

Requirements regarding qualification, experience and licensing requirements.

A personnel selection process has been defined based on the profile of each position involved in the digital certificate issuance process and digital certification service procedures. Candidates for each position must possess the training, experience, knowledge, and skills defined in the Job Profile and Functions document.

Background check procedure.

Candidates for positions in the certification cycle must present their current background certificate, as established in the ECD GSE's internal human talent processes.

Training requirements.

The training requirements for each of the aforementioned positions are detailed in the Job Profile and Functions, which is provided to the selected candidate as part of their onboarding process. Key aspects of the training include:

Knowledge of the Certification Practice Statement.

Knowledge of current regulations related to open certification entities and the services they provide.

Knowledge of Security Policies and acceptance of a confidentiality agreement regarding the information handled by virtue of the position.

Knowledge of the operation of the software and hardware for each specific role.

Knowledge of security procedures for each specific role.

Knowledge of the operating and administrative procedures for each specific role.

Training requirements and frequency of updates.

The annual training program includes an update on Information Security for members of the Digital Certificate Issuance Cycle.

Frequency and sequence of task rotation.

There is no job rotation in the aforementioned positions.

Penalties for unauthorized actions.

It is classified as a serious offense to carry out unauthorized actions and the individuals will be sanctioned in accordance with a reprimand and/or disciplinary process.

Controls for contracting third parties.

Among the requirements for hiring third parties is knowledge of the Security Policies and a confidentiality clause regarding information that is supplied or known for reasons of the contractual relationship with GSE.

Documentation provided to staff.

The documentation mentioned in the Training Requirements section is published for easy reference and is part of the staff induction.

5.4 Audit Recording Procedures.

Security audit procedures are performed internally or by third-party audit providers.

Type of events recorded.

The most critical activities in the certification cycle require monitoring and tracking of events that may occur during their operation. Based on their level of criticality, events are classified as follows:

News report: An operation was successful

Type of brand: Start and end of a session

Warning: Presence of an abnormal event but not a failure

Error: An operation resulted in a predictable failure

Fatal error: An operation generated an unpredictable failure

Log processing frequency.

Audit records are reviewed using manual and/or automated procedures.

Log reviews are performed once a week or when a security alert is detected or there are indications of unusual system operation.

Audit record retention period.

Audit records are kept for three (3) years after the last file modification, ensuring that any issues encountered can be compared with those recorded in the historical data. After three years, and with authorization from the GSE Management Committee, the records may be destroyed. However, if the records are being used in legal proceedings, they will be retained indefinitely.

Protection of audit records.

The information system audit logs are preserved in the same way, keeping one copy on-site and another copy off-site.

Procedure for backing up audit logs.

Backups of audit logs are replicated to a centralized log site

Audit record collection system (internal or external)

The audit information collection system relies on automatic logs from applications that support the certification cycle, including application logs, security logs, and system logs. These are stored in CloudWatch and databases for monitoring.

Notification to the person responsible for the security incident.

In the opinion of the Information Security Officer, the subject responsible for a security incident detected through the audit logs will be notified in order to obtain a formal response regarding what happened.

Vulnerability analysis.

In addition to regular log reviews, ECD GSE also conducts sporadic log reviews or reviews of suspicious activity in accordance with established internal procedures. Similarly, it reviews the results of Ethical Hacking and the actions taken to address any findings.

5.5 Records Archive.
The file logging and event logging is performed by the ECD GSE NOC SOC.
Types of archive records.
A record file is kept of the most relevant events regarding the operations carried out during the process of issuing digital certificates.
Retention period for archiving
The retention period for this type of documentation is 3 years and/or indefinite if there are open legal proceedings.
File protection
The generated files are kept under strict security measures to preserve their condition and integrity.
File backup copy procedures
Backup copies of the Log Files are performed according to the established procedures for backup copies and recovery of backups of the rest of the information systems.
Requirements for time-stamping records.
The servers are kept up-to-date with UTC Time (Coordinated Universal Time). They are synchronized using the Network Time Protocol (NTP). Since, according to section 14 of article 6 of Decree number 4175 of 2011, the National Institute of Metrology (INM) is the official body that maintains, coordinates, and disseminates the legal time of the Republic of Colombia, adopted by Decree 2707 of 1982, synchronization will be carried out with the INM's NTP server.
File collection system (internal or external).
Both external and internal audit information is stored and secured off-site, separate from ECD GSE's facilities, once it has been digitized. Digitized audit files are accessed only by authorized personnel using viewing tools. Databases are maintained on Amazon's CloudWatch service.
Procedures for obtaining and verifying file information.
Log files are accessed only by authorized personnel using event viewing and management tools for the purpose of verifying their integrity or for audits in the event of security incidents.
Key Change.
ECD GSE root key change.
The procedure for changing the ECD GSE Root key is equivalent to generating a new digital certificate. Certificates issued by subsidiaries with the old key must be revoked, or the infrastructure must be maintained until the expiration of the last issued certificate. If the certificates are revoked and new ones issued, there will be no cost to the subscriber or responsible party.
Before the ECD GSE private key expires, a key exchange will be performed. The previous root CA and its private key will only be used for CRL signing while active certificates issued by the previous CA's sub-CAs exist. A new root CA will be generated with a new private key and a new DN. The public key will be published in the same repository with a new name to distinguish it from the previous one.
Changing the keys of the ECD GSE Subordinate.
The procedure for changing the keys of an ECD GSE subsidiary is equivalent to generating a new digital certificate. Certificates issued with the subsidiary's previous key must be revoked, or the infrastructure must be maintained until the expiration of the last issued certificate. If the option is chosen to revoke the certificates and issue new ones, there will be no cost to the subscriber or responsible party.
Before the private key of the ECD GSE sub-member expires, a key swap will be performed. The previous ECD sub-member and its private key will only be used for CRL signing while active certificates issued by the previous ECD sub-member exist. A new ECD GSE sub-member will be generated with a new private key and a new DN. The public key will be published in the same repository with a new name to distinguish it from the previous one.
Commitment and Disaster Recovery.

Incident and engagement management procedures
The ECD GSE has established and tested an Information Security Incident Procedure that outlines the actions to be taken in the event of a vulnerability or security incident. Once the system restoration procedures have been successfully completed, service will be restored to the public.
Procedure in case of damage to computer resources, software and/or data.
In the event of suspected tampering with hardware, software, or data resources, the ECD GSE will shut down until the environment's security is restored. To prevent a recurrence of the incident, the cause of the tampering must be identified. Upon such an event, the ECD GSE will inform ONAC, providing an explanation and justification.
Recovery procedure in the event of a compromise of the ECD private key.
The ECD GSE has established and tested a Business Continuity Plan that defines the actions to be taken in the event of a vulnerability in the private key of the ECD GSE root or one of its sub-keys. In these cases, the compromised private keys of the ECD GSE and the certificates signed under its hierarchy must be revoked immediately. A new private key must be generated, and at the request of the subscribers and/or responsible parties, new certificates must be issued. Additionally, this plan will be executed under the following scenarios:
When the security system of the certification authority has been compromised.
When failures occur in the certification entity's system that compromise the provision of the service.
When encryption systems become obsolete because they do not offer the level of security contracted by the subscriber.
4. When any other information security event or incident occurs.
In the event of an ECD GSE commitment:
Implement incident containment measures to prevent recurrence
It will inform all Subscribers, Responsible Parties, Third Parties that it relies on and other CAs with whom it has agreements or other types of relationships of the commitment.
It will indicate that certificates and information relating to the status of revocation signed using this key are not valid.
ONAC will inform customers now.
5.7.4 Disaster recovery capacity.

In the event of a natural disaster or other catastrophe, ECD GSE is capable of recovering the most critical business services, as described in the Business Continuity Plan, within forty-eight (48) hours of the event or within the Recovery Time Objective (RTO) of the process. The restoration of other services, such as the issuance of digital certificates, will take place within five (5) days of the event or according to the Recovery Point Objective (RPO) specified in the Business Continuity Plan.

5.8 Termination of the CA or the RA.
Procedure in case of termination of the CA and the RA
In accordance with the provisions of Article 34 of Law 527 of 1999, modified by Article 163 of Decree Law 019 of 2012, External Circular No. 30-2021 and in accordance with Decree 333 of 2014 and DURSCIT Article 2.2.2.48.3.8, open digital certification entities must inform ONAC of the cessation of activities at least 30 days in advance.
The ECD - GSE will inform all subscribers and/or responsible parties through two notices published in newspapers or media of wide national circulation, with an interval of 15 days, about:
The termination of the activity or activities and the precise date of cessation.
The legal consequences of the cessation with respect to the accredited services
The possibility that a subscriber may obtain a refund equivalent to the value of the remaining validity period of the contracted service.
The authorization issued by the Superintendency of Industry and Commerce for the ECD to cease the service, and if applicable, the CRL operator responsible for publishing the certificates issued by the ECD - GSE until the last one expires.
The ECD GSE will inform the name of the entity that will guarantee the continuity of the service for those who have contracted, directly or through third parties, services of the ECD GSE, at no additional costs. If the subscriber and/or responsible party does not accept the continuation of the service through the third party, they may request the revocation and the refund equivalent to the value of the remaining validity time of the digital certification service, if they request it within two (2) months following the second publication on the website and notices.
The ECD GSE has a safety plan in case of cessation of activities which includes the guidelines and activities for its execution.

6. TECHNICAL SAFETY CONTROLS.

6.1 Generation and Installation of Key Pairs.
Key pair generation
From the ECD Raíz.
The generation of the ECD Root key pair was carried out at the platform service provider's facilities under the strictest security measures and following the established key generation ceremony protocol for this type of event, and in the presence of an ECD representative. A FIPS 140-2 Level 3 or higher certified cryptographic device was used to store the private key.
From the subordinates of ECD GSE.
The generation of the ECD GSE subordinate key pair was performed at the ECD GSE service provider's facilities under the key generation ceremony protocol. A FIPS 140-2 Level 3 or higher certified cryptographic device was used to store the subordinate private key.
From the subscribers or those responsible for ECD GSE.
The generation of the ECD GSE subscriber key pair is performed at the ECD GSE service provider's facilities. A FIPS 140-2 Level 3 or higher certified cryptographic device is used to store the subscriber's private key.
Delivery of the private key to subscribers.
The private key is delivered to the subscriber and/or responsible party on their cryptographic device and cannot be extracted. Therefore, no copy of the subscriber's private key exists.
Delivery of the public key to the certificate issuer.
The public key is sent to the ECD GSE as part of the digital certificate application request in PKCS#10 format.
Delivery of the public key of the CA to the trusting parties.
The public key of the Root ECD and the Subordinate ECD is included in your digital certificate.
The ECD Root certificates can be consulted by trusted third parties in the repositories listed in section 4.1 Repositories, ECD GSE Root Certificates.
The ECD Subordinate certificates can be consulted by trusted third parties in the repositories listed in section 4.1 Repositories, ECD Subordinate Certificates GSE.
Key Size.
The following key sizes are defined for RSA:
ECD Root of ECD GSE is 4096 bits.
Subordinate ECD GSE is 4096 bits.
Certificates issued by ECD GSE to end users are 2048 bits.
When attempting to derive the private key from the 2048-bit public key contained in end-user certificates, the problem lies in finding the prime factors of two large numbers, as there would be 22,047 possibilities for each number. It is estimated that decrypting a 2048-bit public key would require processing power on the order of 3 x 10^{20} MIPS-years.
MIPS-year: a unit used to measure the processing capacity of a computer running for one year. It is equivalent to the number of millions of instructions a computer is capable of processing per second for one year.
The following key sizes are defined for ECDSA:
ECD Root of ECD GSE is 384 bits.
Subordinate ECD GSE is 384 bits.
Certificates issued by ECD GSE to end users are 256 bits.
For elliptic curves, a specific and published base point G is chosen for use with the curve E(q), and then a random integer k is chosen as the private key. The corresponding public key would be P = k*G and is made public. The discrete algorithm problem states that obtaining k from P is a problem of exponential complexity. It is estimated that 2.4 x 10^26 MIPS-years are required to derive a 256-bit elliptic curve public key.
Public key generation parameters and quality control.

The root ECD public key is encoded according to the RFC 5280 and PKCS#11 standards. The signature algorithm used in key generation is RSA or EC.
The public key of the ECD GSE subordinates is encoded according to the RFC 5280 and PKCS#11 standards. The signature algorithm used in key generation is RSA or EC.
The public key of the end-user certificates is encoded according to the RFC 5280 and PKCS#11 standards. The signature algorithm used in key generation is RSA or EC.

6.1.7 Key usage purposes (according to the use field of key X.509 v3).
The permitted uses of the key for each type of certificate are established by the Certificate Policies for digital certificates and in the policies defined for each type of certificate issued by ECD GSE.
All digital certificates issued by ECD GSE contain the 'Key Usage' extension defined by the X.509 v3 standard, which is considered critical. CERTIFICATE TYPE KEY USAGE Digital Signature Certificate Signature Authentication Certificate Non-Repudiation
6.2 Private key protection and engineering controls of cryptographic modules.
Standards and controls for the use of cryptographic modules.
The cryptographic modules used in the creation of keys used by ECD Root Certification Authority ECD GSE meet the requirements established in accordance with ITSEC, Common Criteria or FIPS 140-2 Level 3 or higher security level.
Multi-person control (n of m) of the private key.
The private keys of the ECD GSE Root and the private keys of the ECD GSE sub-keys are under multi-person control. The private keys are activated by initializing the ECD GSE software using a combination of keys held by multiple people.
Custody of the ECD private key.
ECD GSE private keys are stored on cryptographic devices that meet the requirements set in accordance with ITSEC, Common Criteria or FIPS 140-2 Level 3 or higher security level.
The technical specifications of the device are as follows:
• SafeNet Luna SA
The private key of end-user digital certificates is under the exclusive control and custody of the subscriber or administrator. Under no circumstances does ECD GSE store a copy of the subscriber's private key or the certificate managed by the administrator, as this key is generated by the subscriber or administrator and ECD GSE cannot access it.
Backup copy of the private key.
The ECD GSE private keys are stored on cryptographic devices that meet the requirements set in accordance with ITSEC, Common Criteria or FIPS 140-2 Level 3 or higher security level, (see 8.2.3 Private Key Custody).
The backup copies of the ECD GSE private keys are stored on external devices cryptographically protected by dual control and are only recoverable within a device identical to the one on which they were generated.
Private key file.
ECD GSE private keys are stored on cryptographic devices that meet the requirements set in accordance with ITSEC, Common Criteria or FIPS 140-2 Level 3 or higher security level, (see 8.2.3 Private Key Custody).
They are located in a cryptographic backup box in a different location from where the HSMs are located.
Transfer of private keys to or from a cryptographic module.
ECD GSE private keys are stored on cryptographic devices that meet the requirements established in accordance with ITSEC, Common Criteria, or FIPS 140-2 Level 3 or higher security level. (See 8.2.3 Private Key Custody).
The private key download process is performed according to the cryptographic device's procedure and they are securely stored protected by cryptographic keys.
Storing the private key in the cryptographic module.
The ECD GSE private keys are generated and stored on cryptographic devices that meet the requirements established in accordance with ITSEC, Common Criteria, or FIPS 140-2 Level 3 or higher security level. (See 8.2.3 Private Key Custody).
Cryptographic keys can be loaded onto a peer-to-peer cryptographic device from backup copies through a process that requires the participation of at least two operators.
Private key activation method.
The private keys, both for the Root ECD GSE and the Subordinate ECDs, are under multi-person control. The private key is activated by initializing the ECD GSE software using a combination of keys held by multiple operators.
Multi-person access is required to activate the ECD GSE private key. At least two people are needed to activate the keys.
Method for deactivating the private key.
The private key is deactivated by disabling the software or shutting down the ECD server. It is reactivated using multi-user access control, following the procedures specified by the cryptographic module manufacturer.
Method to destroy the private key.
The method used in the event that the destruction of the private key is required is by erasing the keys stored in the cryptographic devices as described in the device manufacturer's manual and by physically destroying the access cards held by the operators if required.
Cryptographic module classification.
The cryptographic devices used by ECD GSE comply with what is indicated in Annex F: Cryptographic Devices, of the CEA. Evaluation of the cryptographic module.
The cryptographic device is monitored using its own software to anticipate potential failures. Evaluation of the encryption system.

ECD GSE adheres to the recommendations for the use of cryptographic algorithms and key lengths published by NIST (National Institute of Standards and Technology) and ONAC. If any circumstance arises where the algorithms used for signing and encryption by ECD GSE are compromised at all levels, ECD GSE will immediately take the measures and recommendations issued by this entity or by ONAC to maintain the security of the signature for the remainder of its life cycle.

6.3 Other Aspects of Key Pair Management.
Public key file.
ECD GSE will maintain controls for archiving its own public key.
Operating periods of the certificates and period of use of the key pair.
The usage period of the key pair is determined by the following validity of each certificate: RSA Algorithm:
The validity period of the RSA digital certificate and root key pair is thirty (30) years.
The validity period of the RSA digital certificate and the subordinate key pair is ten (10) years.
ECDSA Algorithm:
The validity period of the ECDSA digital certificate and the Root key pair is twenty-five (25) years. The validity period of the ECDSA digital certificate and the Subordinate key pair is ten (10) years.
6.4 Activation Data.
Generation and installation of activation data.
For the operation of the ECD GSE, passwords are created for the operators of the cryptographic device and will serve together with a PIN for the activation of the private keys.
The private key activation data is divided into passwords guarded by a multi-person system where 4 people share the access code of said cards.
Protection of activation data.
Knowledge of activation data is personal and non-transferable. Each participant is responsible for its safekeeping and must treat it as confidential information.
Other aspects of activation data.
The activation key is confidential, personal and non-transferable, and therefore security rules must be observed for its safekeeping and use.

6.5 Information Security Controls.
The equipment used is initially configured with the appropriate security profiles by the systems personnel, in the following aspects:
Operating system security settings.
Application security settings.
Device access control.
Closing system vulnerabilities.
Hardening of systems according to best practices.
Network configuration at the security level (Internal Network, Administrative Network, among others)
User and permission settings.
Log event configuration.
Backup and recovery plan.
Antivirus settings.
Network traffic requirements configured in the firewall.

Specific technical requirements for computer security.
ECD GSE has a technological infrastructure that is properly monitored and equipped with the security elements required to guarantee the availability established in the CEA and confidence in the services offered to its subscribers, entities and trusted third parties.
Information related to Information Security is considered confidential and therefore can only be provided to those control entities that require knowledge of it.
Classification of computer security.
The security of end-user equipment is managed from ECD GSE and supported by a risk analysis so that the security measures implemented are responses to the probability and impact produced by a group of defined threats that may take advantage of security gaps.
Additionally, periodic security tests (ethical hacking) are carried out to identify potential system vulnerabilities and help to close them.
Actions in case of an information security event or incident.
The Information Security Management System implemented by ECD GSE has an established incident management procedure that specifies the actions to be taken, components or resources to be used, and how staff should react in the event of an intentional or accidental event that disables or degrades ECD GSE's digital certification resources and services.
1. Incident Detection and Reporting: Security incidents must be reported via email to seguridad.informacion(5)ase.com.co, which is managed by the ECD GSE Information Security Officer.
Incidents may be detected through monitoring systems, intrusion detection systems, system logs, notification by staff or by subscribers and/or managers.
Incident Analysis and Evaluation: Once an incident is detected, the response procedure is determined, and the responsible parties are contacted to assess and document the actions to be taken based on the severity of the incident. An investigation is conducted to determine the scope of the incident, that is, to ascertain the extent of the attack and gather as much information as possible about the incident.
Incident damage control: React quickly to contain the incident and prevent it from spreading by taking measures such as blocking access to the system.
Investigation and evidence gathering: Review audit records to track what happened.

Recovery and incident prevention measures: Restore the system to its correct functioning and document the procedure and ways to prevent the incident from recurring.
Post-incident analysis for procedure improvement: Conduct an analysis of everything that happened, identify the cause of the incident, correct the cause for the future, analyze the response, and correct errors in the response.

6.6 Technical Lifecycle Controls.
Systems development controls.
The ECD GSE complies with the established change control procedures for new software developments and updates.
Security management controls.
ECD GSE maintains control over the inventories of assets used in its certification process. These assets are classified according to their level of risk.
ECD GSE periodically monitors its technical capacity in order to guarantee an infrastructure with the minimum availability required by the CEA.
Lifecycle safety controls.
ECD GSE has the appropriate security controls throughout the entire lifecycle of systems that have any impact on the security of the digital certificates issued.
Network Security Controls.
ECD GSE has a properly monitored network infrastructure equipped with the security elements required to guarantee the availability and reliability of the services offered to its subscribers, entities and third parties acting in good faith.
Information related to Information Security is considered confidential and therefore can only be provided to those control entities that require knowledge of it.
Chronological Stamp.
ECD GSE offers a timestamping service, which is described in the corresponding Certificate Policies for Timestamping Service, published on the portal.http://www.ase.com.co.

7. CERTIFICATE, CRL AND OCSP PROFILES.

7.1 Certificate Profile.
The certificates comply with the current X.509 standard and the authentication infrastructure is based on RFC5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
Certificate Content. A certificate issued by ECD GSE, in addition to being digitally signed by it, will contain at least the following:
Name, address and domicile of the subscriber.
A unique identifier of the subscriber named in the certificate.
The name and location where the CA carries out its activities
Public key of the certificate.
The methodology for verifying the subscriber's digital signature imposed on the data message.
The (unique) serial number of the certificate.
Certificate issue and expiry date.
Additionally, the Accreditation Code assigned by ONAC is included according to the certificate extension defined in numeral 4.2 of RFC 5280 identified in the field: Alternative name of the subject

Field	RSA value or restrictions	ECDSA Value or Restrictions
Version	3 (0x2)	3 (0x2)
Serial Number	Unique identifier issued by ECD GSE	Unique identifier issued by ECD GSE
Signature Algorithm	SHA256withRSAEncryption	SHA384withECDSA
Transmitter	See section "Rules for the interpretation of various forms of name". For ECD GSE as the issuer, the following is specified: E=info@gse.com.co, CN=Subordinate Authority 01 GSE, OU = PKI, 0=GSE, L=Bogota DC, C=CO	See section "Rules for the interpretation of various forms of name". For ECD GSE as the issuer, the following is specified: STREET=www.gse.com.co, E=info@gse.com.co, CN = GSE ECDSA SUBORDINADA, SN=900204278, OU=GSE ECDSA R2 SUB1, 0=GESTION DE SEGURIDAD ELECTRONICA SA, L=Bogota DC, S= Distrito Capital, C=CO
Valid from	Specify the date and time from which the certificate is valid.	Specify the date and time from which the certificate is valid.
Valid until	Specify the date and time from which the certificate ceases to be valid.	Specify the date and time from which the certificate ceases to be valid.
Subject	In accordance with the policy of Annex 1 and the "Rules for the interpretation of various forms of name".	In accordance with the policy of Annex 1 and the "Rules for the interpretation of various forms of name".
Subject's Public Key	Encoded according to RFC 5280. Certificates issued by ECD GSE have a length of 2048 bits and RSA algorithm.	Encoded according to RFC 5280. Certificates issued by ECD GSE have a length of 256 bits and use the EC algorithm.
Authority Key Identifier	It is used to identify the root certificate in the certification hierarchy. It typically references the "Subject Key Identifier" field of ECD GSE as the digital certification authority.	It is used to identify the root certificate in the certification hierarchy. It typically references the "Subject Key Identifier" field of ECD GSE as the digital certification authority.
Subject Key Identifier	It is used to identify a certificate that contains a specific public key.	It is used to identify a certificate that contains a specific public key.

Certificate Directives	Describe the policies applicable to the certificate, specify the OID and the URL where the certification policies are available.	Describe the policies applicable to the certificate, specify the OID and the URL where the certification policies are available.
Using the key	Specify the permitted uses of the key. It is a CRITICAL FIELD.	Specify the permitted uses of the key. It is a CRITICAL FIELD.
CRL Distribution Point	It is used to indicate the addresses where the ECD GSE CRL is published. This attribute is not specified in the ECD Root certificate.	It is used to indicate the addresses where the ECD GSE CRL is published. This attribute is not specified in the ECD Root certificate.
Access to Authority Information	It is used to indicate the addresses where the ECD GSE root certificate is located. Additionally, it indicates the address for accessing the OCSP service. This attribute is not specified in the ECD GSE root certificate.	It is used to indicate the addresses where the ECD GSE root certificate is located. Additionally, it indicates the address for accessing the OCSP service. This attribute is not specified in the ECD GSE root certificate.
Alternative subject name	It is used to indicate the email address and additionally to indicate the accreditation code assigned by ONAC. Name RFC822=email@company.com URL= https://ase.com.co/documentos/certificaciones/acreditacion/16-ECD-001.Ddf	It is used to indicate the email address and additionally to indicate the accreditation code assigned by ONAC. Name RFC822=email@company.com URL= https://ase.com.co/documentos/certificaciones/acreditacion/16-ECD-001.Ddf
Extended uses of the key	Other purposes beyond the use of the key are specified.	Other purposes beyond the use of the key are specified.
Basic restrictions	The "PathLenConstraint" extension indicates the number of sub-levels allowed in the certificate path. There is no restriction for ECD GSE, therefore it is zero.	The "PathLenConstraint" extension indicates the number of sub-levels allowed in the certificate path. There is no restriction for ECD GSE, therefore it is zero.

Version numbers.
Certificates issued by ECD GSE comply with the current X.509 standard.
Certificate extensions.
Annex 1 of this DPC describes in detail the certificates issued by GSE. Key Usage.
The "key usage" is a critical extension that indicates the use of the certificate in accordance with RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".
Certificate policy extension.
The current X.509 "certificatepolicies" extension is the object identifier for this DPC, in accordance with the Object Identifier section of this DPC's Certification Policy. The extension is not considered critical.
Alternative name of the subject.
The "subjectAltName" extension is optional and its use is "non-critical". Basic restrictions.
In the case of ECD GSE, the "PathLenConstraint" field of the subordinate certificate has a value of 0, indicating that the ECD GSE does not allow any further sub-levels in the certificate path. This is a critical field.
Extended use of the key.
This extension allows you to define additional purposes for the key. It is considered non-critical. The most common purposes are:

OID	Description	Types of Certificates
1.3.6.1.5.5.7.3.4	Email protection	Digital Signature of a natural person and Electronic Agent
1.3.6.1.5.5.7.3.8	Timestamping	Timestamping
1.3.6.1.5.5.7.3.34	TLS web server authentication	All types of certificate

Algorithmic object identifiers.
The object identifier of the signature algorithm is:
1.2.840.113549.1.1.11 SHA256 with RSA Encryption
The object identifier of the public key algorithm is:
1.2.840.113549.1.1.1 rsaEncryption
The object identifier of the signature algorithm is:
1.2.840.10045.4.3.3 SHA384WITHECDSA.
The object identifier of the public key algorithm is:
1.2.840.10045.2.1 ecPublicKey-id
Forms of names.
In accordance with the provisions of the Name Types section of this DPC.
Name restrictions.
Names should be written in capital letters and without accents.
The country code is assigned according to the ISO 3166-1 standard "Codes for the representation of the names of countries and their subdivisions. Part V Country codes".
In the case of Colombia, it is "CO".
Certification Policy Object Identifier.
The Certificate Policy object identifier corresponding to each type of certificate is a subclass of the class defined in the section Document Name and Identification of this DPC, as established in the Certificate Policies for digital certificates.
Using the Policy Constraints extension.
It is not stipulated.
Syntax and semantics of Policy Qualifiers
The policy qualifier is defined in the "Certificate Policies" extension and contains a reference to the URL where the DPC is published.
Semantic treatment for the Certificate Policies extension.

It is not stipulated.

7.2 CRL profile.
CRLs issued by ECD GSE comply with RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile V2" and contain the following basic elements.
Version number(s)
The CRLs issued by ECD GSE comply with RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile V2" and contain the following basic elements:
CRL and CRL input extensions
Information about the reason for revoking a certificate will be included in the CRL, using CRL extensions and more specifically in the revocation reason field (reasonCode).

7.3 OCSP profile.
The OCSP service complies with the provisions of RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".
Version number(s)
Complies with OCSP Version 1 of RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP" and RFC6019 "The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments".
OCSP Extensions
The singleExtensions of an OCSP response DO NOT CONTAIN the CRL reasonCode input extension (OID 2.5.29.21).

8. COMPLIANCE AUDIT AND OTHER EVALUATIONS.
Frequency or Circumstances of the Evaluation.
Compliance with controls that ensure security in the issuance of digital certificates will be assessed through an annual audit conducted by an external auditing firm.
Evaluator identity and qualifications.
In accordance with Decree 333 of 2014 and specifically in Article 14. Audits. Certification entities must comply with the third-party audit under the terms provided in the Specific Accreditation Criteria established by ONAC.
Assurance Requirements: A legally established auditing firm in Colombia whose corporate purpose includes: systems auditing services, information security, and public key infrastructure (PKI). The audit team's competence must be demonstrated with respect to the specific accreditation criteria, the requirements of the international standard ISO/IEC 27001 regarding information security, and in relation to ISO 9001 or ISO/IEC 20000-1. If the auditor lacks PKI competence, they must be accompanied by a technical expert knowledgeable in the management of public key infrastructure (PKI). Audit personnel must hold a valid professional engineering license.
Relationship of the evaluator with the entity being evaluated.
The only relationship established between the auditor and the audited entity is that of auditor and auditee. The audit firm exercises absolute independence in carrying out its audit activities, and there is no conflict of interest because the relationship is purely contractual.
Topics subject to evaluation.
The aspects covered by the audit control frame the scope accredited by ONAC for the ECD, in accordance with the provisions of the section MANAGEMENT SYSTEM REQUIREMENTS - Third Party Audit of the CEA document established by ONAC, the deliverable is the conformity report, no exceptions or reasonableness are allowed.
Actions taken as a result of the deficiency.
The deficiencies detected during the audit process must be remedied through corrective or improvement actions, procedures and implementation of the controls required to address the findings.
Communication of Results.
Once the audit is completed, the auditing firm must submit the audit report to ECD GSE, and if necessary, ECD GSE must establish corrective and improvement actions. The final report must be submitted to ONAC.

9. OTHER COMMERCIAL AND LEGAL MATTERS.

9.1 Fees.
Not Applicable.
Certificate issuance or renewal fees
GSE charges fees for issuing and renewing certificates. GSE may modify its fees in accordance with the applicable customer agreement. See the fee schedule in section 9.17.
Certificate access fees
Unless otherwise specified in the relevant legal agreements or CP of a third-party partner, GSE may charge a reasonable fee for access to its certificate databases.
Rates for access to information on revocation or status
GSE does not charge fees for certificate revocation or for checking the validity status of a certificate issued using a CRL. GSE may charge a fee for providing certificate status information through OCSP.
Fees for other services
Without stipulation.
Refund policy

As established in the relevant customer agreement with GSE.

9.2 Financial Responsibility.

Insurance or guarantee of coverage for subscribers, responsible parties and bona fide third parties.

In compliance with Article 9, Guarantees, of Decree 333 of 2014, ECD GSE has acquired insurance issued by an insurance entity authorized to operate in Colombia, which covers all contractual and extra-contractual damages of subscribers, responsible parties and third parties in good faith without fault derived from errors and omissions, or from acts of bad faith of the administrators, legal representatives or employees of ECD GSE in the development of the activities for which it is authorized.

Other assets.

ECD GSE has sufficient economic and financial capacity to provide the authorized services and fulfill its obligations as a certification authority. As a certification service provider, ECD GSE will be liable for any damages caused to subscribers, entities, or third parties acting in good faith resulting from errors or omissions, or from bad faith actions by ECD GSE's administrators, legal representatives, or employees in the performance of its authorized activities. To this end, ECD GSE maintains civil liability insurance in accordance with Article 9, Guarantees, of Decree 333 of 2014. ECD GSE assumes no other commitments or provides any other guarantees, nor does it assume any other liability to subscribers and/or certificate holders or trusted third parties, except as established by the provisions of this DPC (Diagram of Certification and Certification).

Insurance coverage or guarantee for end entities

Without stipulation.

9.3 Confidentiality of Commercial Information.

9.3.1 Scope of confidential information.

ECD GSE is committed to protecting all data to which it has access as a result of its activity as an ECD.

All non-public information is considered confidential and therefore restricted access, except in those cases provided for by law such as courts or competent administrative bodies or imposed by law; confidential information is not disseminated without the express written consent of the subscriber or the entity that has granted it the character of confidentiality.

However, it reserves the right to disclose to employees and consultants, external or internal, the confidential data necessary to carry out its activities as an ECD, requiring all personnel to sign a confidentiality agreement within the framework of the contractual obligations undertaken with ECD GSE.

Confidential information.

1.The following information is considered confidential:

2.Private key of the Certification Authority and/or ECD

3.Private key of the subscriber or entity

4.information provided by the subscriber or entity that is not necessary to validate the subscriber's or entity's trustworthiness

5.Information about the applicant, subscriber and/or responsible party obtained from different sources (for example, from a complainant or from regulators)

6.Transaction records

7.Audit records

8.Security policies

9.Business Continuity Plan All information that is classified as "Confidential" in the documents delivered by ECD GSE

9.3.2 Non-confidential information.

All non-confidential information is considered public and therefore freely accessible to third parties:

The one contained in this Certification Practice Statement and its annexes.

The information contained in the repository regarding the status of the certificates.

The list of revoked certificates.

All information that is classified as "PUBLIC" in the documents delivered by ECD GSE.

9.3.3 Duty to protect confidential information.

ECD GSE maintains security measures to protect all confidential information provided to ECD GSE directly or through established channels, from receipt to storage and safekeeping, where it will be kept in accordance with the Records Retention Schedule (TRD). ECD GSE has an Integrated Management System that includes an Information Security System. This allows us to ensure that our subscribers' information will not be compromised or disclosed to third parties unless formally requested by a competent authority.

9.4 Privacy of Personal Information.

Privacy Plan - Personal Data Processing Policy.

ECD GSE has a Personal Data Processing Policy in accordance with the provisions of Law 1581 of 2012, Decree 1377 of 2013, and other regulations that add to, modify, complement, or replace it, which can be consulted on our website.https://ase.com.co/PoliticasIn the Personal Data Processing Policy section, you can also consult the authorization for the processing of personal data.

9.4.1Information treated as private.

Personal information provided by the subscriber or responsible party and required for the approval of the digital certificate is considered private information.

Information that is not considered private.

These are personal data that the rules and the Constitution have expressly determined as public, for whose collection and processing the authorization of the data subject is not necessary.

Responsibility to protect private information.

ECD GSE is responsible and has the appropriate technological resources to help guarantee the proper custody and preservation of personal data collected through the channels used by the company, complying with Law 527 of 1999 "Article 32. Duties of certification entities. Certification entities shall have, among others, the following duties: Guarantee the protection, confidentiality and proper use of the information provided by the subscriber, responsible party and entity."

GSE ECD uses technological mechanisms such as Active Directory, where access control policies are implemented, and a centralized repository where information is protected by a firewall that prevents intrusions within the network for office equipment, and by digital certificates for access to ECD's production servers.
Notice and consent to use private information.
Personal data may not be communicated to third parties without the proper notification and consent of the data subject, in accordance with applicable regulations on the protection of personal data.
Disclosure pursuant to a judicial or administrative proceeding.
Personal data may be disclosed when required by one of the public or administrative entities in the exercise of their legal functions or by court order without due notification and consent of its owner, in accordance with current personal data protection regulations.
Other circumstances of information disclosure.
ECD GSE's privacy policy strictly adheres to the provisions of data protection law: "Private information is that which, whether personal or not, and which is in a private sphere, can only be obtained or offered to third parties authorized by the Subscriber or responsible party or by law."
Security system to protect information.
Regarding the system that houses the information provided by the subscriber or the person responsible for the certification service, the following validations are performed:
The infrastructure provider must adhere to the best practices outlined in the following Standards:

A.ISO 27001
B.ISO 9001

2.Penetration testing and vulnerability scanning of the network, performed by a company specializing in Ethical Hacking.

9.5 Intellectual Property Rights.
In Colombia, copyright protection includes all literary, artistic, or scientific works that can be reproduced or disseminated through any medium. Therefore, ECD GSE reserves all rights related to intellectual property and prohibits, without its express authorization, the reproduction, dissemination, public communication, and transformation of the information, techniques, models, internal policies, processes, procedures, or any of the elements contained in this Privacy Policy, in accordance with national and international regulations related to intellectual property.
Representations and Guarantees.
The ECD GSE will at all times have civil liability insurance in accordance with the provisions of Decree 333 of 2014 with coverage of 7500 legal monthly minimum wages per event.
The ECD GSE will act in covering its responsibilities either on its own or through the insurance entity, satisfying the requirements of the applicants for the certificates, the subscribers/responsible parties and the third parties who rely on the certificates.
The responsibilities of the ECD GSE include those established by this DPC, as well as those that may apply as a result of Colombian and International Regulations.
ECD GSE will be liable for damages caused to the Subscriber, Entity or any person who in good faith relies on the certificate, provided there is intent or gross negligence, with respect to:
The accuracy of all information contained in the certificate on the date of its issue.
The guarantee that, at the time of delivery of the certificate, the Subscriber has in his possession the private key corresponding to the public key given or identified in the certificate.
The guarantee that the public and private keys work together and complementarily.
The correspondence between the requested certificate and the certificate delivered.
Any liability established by current legislation.

CA Declarations and Guarantees
Unless expressly stated otherwise in this DPC or in a separate agreement with a Subscriber, GSE makes no representations regarding its products or services. GSE represents, to the extent specified in this DPC, that: GSE complies, in all material respects, with the PC, this DPC and all applicable laws; GSE regularly publishes and updates the CRL and the database for generating OCSP responses.
RA Declarations and Guarantees
The RA declares that:
The RA's certificate issuance and management services are aligned with the GSE PC and are already part of the DPC.
The information provided by the RA does not contain any false or misleading information.
The translations performed by the RA are an exact translation of the original information, and
4. All certificates requested by the RA comply with the requirements of this DPC.
The GSE agreement with the RA may contain additional statements.
Subscriber Agreements may include additional representations and warranties.
9.6.3 Subscriber Representations and Warranties
Before a Certificate is issued and received, the subscriber will be solely responsible for any false statements made to third parties and for all transactions in which the Subscriber's Private Key is used, regardless of whether such use was authorized. Subscribers are required to notify GSE of any change that may affect the status of the Certificate or the application.
Subscribers agree to comply with the commitments and guarantees of this DPC and the following points:
If generating requests in PKCS#10 format, you must securely generate your private keys and protect them from any compromise.
Provide accurate and complete information when communicating with GSE,
Confirm the accuracy of the certificate data before using it.
Immediately if applicable:

request the revocation of a Certificate, cease using it and its associated Private Key, and notify GSE if misuse or compromise of the Private Key associated with the Public Key included in the certificate occurs or is suspected, and request the revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate,

Ensure that individuals using certificates on behalf of an organization have received appropriate security training related to the certificate.
Use the certificate only for authorized and lawful purposes, in accordance with the purpose of the certificate, this DPC, any applicable PC and the corresponding subscriber agreement.
Use the certificate only for authorized and lawful purposes, in accordance with the purpose of the certificate, this DPC, any applicable PC and the corresponding subscriber agreement, including installing certificates only on authorized servers with the subscriber's consent, and
Immediately cease using the certificate and its associated private key upon certificate expiration. Subscription agreements may include additional representations and warranties.

9.6.4 Representations and warranties of the partyconfident

Each Relying Party declares that, before relying on a Certificate issued by GSE:

1. He gained sufficient knowledge about the use of digital certificates and PKI,
2. You have studied the limitations applicable to the use of Certificates and accept GSE's limitations of liability related to the use of Certificates,
3. You have read, understand and accept the GSE Trusted Party Agreement and this DPC,
4. It has verified both the subscriber certificates issued by GSE and the certificates in the certification chain using the corresponding CRL or OCSP,
5. You will not use a certificate issued by GSE if the certificate has expired or been revoked, and
6. It will take all reasonable steps to minimize the risk associated with relying on a digital signature, including relying solely on a certificate issued by GSE after considering:

a) the applicable legislation and legal requirements for the identification of the parties, the protection of the confidentiality or privacy of the information, and the applicability of the transaction;
b) the intended use of the Certificate as listed in the certificate or in this DPC,
c) the data listed in the Certificate
d) the economic value of the transaction or communication
e) the potential loss or damage that would result from misidentification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
f) the prior track record of the Party Relying on the subscriber,
g) the relying party's business knowledge, including experience with computerized business methods, and
h) any other indication of reliability or unreliability in relation to the subscriber and/or the application, communication or transaction.

Any unauthorized reliance on a Certificate is at the reliance party's own risk.
Relying Party Agreements may include additional representations and warranties.

9.6.5 Representations and warranties of other participants

Not Applicable
Warranty Disclaimers.
Not Applicable
Limitations of Liability.
Responsibility for the veracity of the Subscriber's information.
The Subscriber assumes all risks for damages that may arise from conduct such as providing false information, impersonating third parties, validating incomplete or outdated documents or information.
Responsibility for service availability.
The Subscriber agrees to act diligently to minimize the possibility of failures or interruptions that may occur within their organization. Failures caused by the Subscriber's equipment being inadequate or incapable, or by their lack of knowledge regarding the use of the service, will in no case be attributable to ECD GSE, and ECD GSE will not be liable for any damages.
Responsibility for the functionality of the service on the Subscriber's infrastructure.
The Subscriber will be solely responsible for the provision and payment of the costs necessary to ensure the compatibility of the service (digital signature certificate), with their equipment, including all hardware, software, electrical components and other physical or logical components required to access and use it, including but not limited to telecommunications services, Internet access and connection, links, browsers, or other programs, equipment and services required to access and use the service.
Liability for cybercrimes.
In the event that the Subscriber is a victim of any of the conduct classified as a crime by Law 1273 of 2009 (Computer Crimes Law), in its information systems, in its applications and technological infrastructure, in the execution of electronic transactions or in the access and use of the service, phishing attacks, identity theft, due to negligence in the handling and confidentiality of the digital certificate, the Subscriber will be solely responsible and will remedy any damages that may arise, since it is their obligation to adopt the security measures, policies, cultural campaigns, legal instruments and other mechanisms to safeguard the confidentiality and proper use of their digital certificate.
Warranty disclaimers.
ECD GSE will not be liable under any circumstances when faced with any of these situations:
State of War, natural disasters, terrorism, strikes or any other case of Force Majeure.
For the use of certificates whenever it exceeds the provisions of current regulations and this DPC and its Annexes.
For the improper or fraudulent use of certificates or CRLs issued by the Certification Authority.
For the use of the information contained in the Certificate or in the CRL.
For failure to comply with the obligations established for the Subscriber, Entities, Responsible Parties or Third Parties who rely on the current regulations, this DPC and its Annexes.
For the damage caused during the verification period of the causes of revocation/suspension.
Due to the content of the messages or documents that are digitally signed or encrypted.
Due to the failure to recover documents encrypted with the public key of the Subscriber or Entity.
Fraud in the documentation submitted by the applicant.

9.9 Compensation.
Not Applicable.
9.10 Duration and Termination.

9.10.1 Duration.
The DPC and PC come into effect from the moment they are published on the ECD GSE website, from that moment the previous version of the document is repealed and the new version completely replaces the previous version.
ECD GSE retains previous versions of the DPC and PC in the repository.
Termination.
For digital certificates that have been issued under an older version of the DPC or PC, the new version of the DPC or PC applies in all aspects that do not conflict with the statements of the previous version.
Termination effect, notification and communication.
ECD GSE notifies changes to this certification practice statement by publishing the new version on the website once it has been authorized by the Management Committee, and the respective change control will be recorded therein.
Procedure for Change in the DPC and PC.
Changes that affect DPC and PC.
Any change affecting the DPC and PC of the ECD GSE will follow the following procedure:
1. The Management Committee will approve any changes it deems appropriate regarding the DPC and the PC.
2. The updated DPC and PC is published on the ECD GSE website once it has been authorized by the Management Committee. Circumstances under which the OID must be changed.
In the following cases, the ECD GSE will make adjustments to the OID identification:
1. The authorization of a new certification hierarchy, an event in which the OIDs must be defined according to the structure.
2. In the event that changes to the DPC and PC affect the acceptability of digital certification services, the OID will be adjusted. This type of modification will be communicated to the users of the certificates corresponding to the PC or DPC.
9.11 Individual notifications and communications to participants.
9.11.1 ECD GSE Obligations.
ECD GSE, as a certification service provider, is obliged according to current regulations and the provisions of the Certification Policies and this DPC to:

1. Respect the provisions of current regulations, this DPC and the PC Certification Policies.
2. Publish this DPC and each of the Certification Policies on the GSE website.
3. Inform ONAC about the modifications to the DPC and the Certification Policies.
4. Keep the DPC with its latest version published on the GSE website.
5. Protect and safeguard your private key securely and responsibly.
6. Issue certificates in accordance with the Certification Policies and the standards defined in this DPC.
7. Generate certificates consistent with the information provided by the applicant or subscriber.
8. Retain information on digital certificates issued in accordance with current regulations.
9. Issue certificates whose minimum content is in accordance with current regulations for the different types of certificates.

10. Publish the status of issued digital certificates in an open access repository.
11. Do not keep a copy of the applicant's or subscriber's private key.
12. Revoke digital certificates as provided in the Digital Certificate Revocation Policy.
13. Update and publish the CRL revoked digital certificate list with the latest revoked certificates.
14. Notify the Applicant, Subscriber or Entity of the revocation of the digital certificate within 24 hours of the revocation of the certificate in accordance with the digital certificate revocation policy.
15. Inform subscribers of the approaching expiration of their digital certificate.
16. Having qualified personnel with the knowledge and experience necessary to provide the certification service offered by the ECD GSE.
17. Provide the applicant with the following information on the ECD GSE website free of charge and with open access, complying with the parameters and characteristics of current regulations without inducing error:

- The Certification Practice Statement, its Annexes, the Certificate Policies, and all updates to the aforementioned documents.
- Subscriber obligations and how the data must be kept safe.
- Procedure for requesting the issuance of a certificate.
- The procedure for revoking your certificate.
- The conditions and limits of the use of the certificate

18. To verify, either personally or through a different person acting on their behalf, the identity and any other circumstances of the applicants or data of the certificates, which are relevant for the purposes of the verification procedure prior to their issuance.
19. Report to the Superintendency of Industry and Commerce and to ONAC, immediately, the occurrence of any event that compromises or may compromise the provision of the service.
20. Report promptly any modification or update of services included in the scope of accreditation, in accordance with the procedures, rules and requirements of the ONAC accreditation service.
21. Update contact information whenever there is a change or modification to the data provided.
22. To train and warn users about the safety measures they must observe and about the logistics required for the use of the service delivery mechanisms.
23. To guarantee the protection, integrity, confidentiality and security of the information provided by the subscriber by keeping the documentation that supports the certificates issued.

24. To guarantee the conditions of integrity, availability, confidentiality and security, in accordance with current national and international technical standards and with the specific accreditation criteria established for this purpose by ONAC.
25. List the accredited services on the ECD GSE website.

9.11.2 Obligations of the RA.

The RA of the ECD GSE is responsible for carrying out the identification and registration work; therefore, the RA is obligated, under the terms defined in this Certification Practice Statement, to:

1. To know and comply with the provisions of this DPC and the Certification Policies corresponding to each type of certificate.
2. Safeguard and protect your private key.
3. Review and/or verify the initial validation records of the identity of Applicants, Responsible Parties or Subscribers of digital certificates.
4. Verify the accuracy and authenticity of the information provided by the Applicant.
5. To archive and safeguard the information and/or documentation provided by the applicant or subscriber for the issuance of the digital certificate, for the time established by current legislation.
6. Respect the provisions of the contracts signed between ECD GSE and the subscriber.
7. Identify and inform the ECD GSE of the reasons for revocation provided by applicants regarding current digital certificates.

9.11.3 Obligations (Duties and Rights) of the Subscriber and/or Responsible Party.

The Subscriber, as subscriber or responsible party for a digital certificate, is obliged to comply with the provisions of current regulations and the provisions of this DPC, which are:

1. Use your digital certificate or electronic signature certificate according to the terms of this DPC.
2. Verify within the next business day that the digital certificate information is correct. If any inconsistencies are found, notify the ECD.
3. Refrain from: lending, transferring, writing, publishing the password for using your digital certificate and take all necessary, reasonable and timely measures to prevent it from being used by third parties.
4. Do not transfer, share, or lend the cryptographic device to third parties.
5. Provide all the information required in the application form or using the channels, means or mechanisms provided by GSE for the application of digital certificates to facilitate your timely and full identification.
6. Request the revocation of the digital certificate upon change of name and/or surnames.
7. Request the revocation of the digital certificate when the Subscriber has changed their nationality.
8. Comply with what has been accepted and/or signed in the terms and conditions document.
9. Provide the required information accurately and truthfully.
10. Report any changes to the data initially provided for the issuance of the digital certificate during its validity period.
11. Safeguard and protect your private key responsibly.
12. Use the certificate of conformity with the PCs established in this DPC for each of the certificate types.
13. As a subscriber and/or responsible party, you may immediately request the revocation of your digital certificate when you become aware of a cause defined in the section "Circumstances for the revocation of a certificate" of this DPC.
14. Do not use the private key or the digital certificate once it has expired or has been revoked.
15. Inform trusted third parties of the need to verify the validity of the digital certificates they are using at any given time.
16. Inform the third party acting in good faith of the status of a revoked digital certificate, for which purpose the Certificate Revocation List (CRL) is available, published periodically by ECD GSE.
17. Do not use your digital certificate in a way that violates the law or causes a bad reputation for the ECD.
18. Do not make any statements related to your digital certification in the ECD GSE that may be considered misleading or unauthorized, in accordance with this DPC and PC.
19. Once the digital certification service has expired or been revoked, the subscriber must immediately stop using it in all advertising material that contains any reference to the service.
20. When referring to the digital certification service provided by ECD GSE in media such as documents, brochures or advertising, the subscriber must state that it complies with the requirements specified in the PCs of this DPC, indicating the version.
21. The subscriber may use the conformity marks and information related to the digital certification service provided by ECD GSE in media, such as documents, brochures or advertising, as long as they comply with the requirements in the preceding paragraph.

On the other hand, it has the following rights:

1. Receive the digital certificate within the timeframes established in the DPC.
2. Request information regarding applications in process.
3. Request revocation of the digital certificate by providing the necessary documentation.
4. Receive the digital certificate in accordance with the scope granted by ONAC to GSE.

9.11.4 Obligations of Third Parties in Good Faith.

Third parties acting in good faith, as parties relying on digital certificates issued by ECD GSE, are obliged to:

1. To know the provisions regarding Digital Certification in the current regulations.
2. Know the provisions of the DPC.
3. Verify the status of digital certificates before performing operations with digital certificates.
4. Verify the Certificate Revocation List (CRL) before performing operations with digital certificates.
5. To know and accept the conditions regarding guarantees, uses and responsibilities when carrying out operations with digital certificates.

9.11.5 Obligations of the Entity (Client).

As established in the PCs related in this document, in the case of certificates where the link of the subscriber and/or responsible party with the same is accredited, it will be the obligation of the Entity to:

1. Request the RA of the ECD GSE to suspend/revoke the digital certificate when said link ceases or is modified.
2. All those obligations related to the person responsible for the digital certification service.

3. When referring to the digital certification service provided by ECD GSE in media such as documents, brochures or advertising, the entity must state that it complies with the requirements specified in the PCs related to this DPC.
4. The entity may use the conformity marks and information related to the digital certification service provided by ECD GSE in media, such as documents, brochures or advertising, as long as it complies with the requirements in the preceding paragraph.

9.11.6 Obligations of other participants in the ECD.
The Management Committee and the Integrated Management System, as internal bodies of ECD GSE, are obliged to:

1. Review the consistency of the DPC with current regulations.
2. Approve and decide on changes to certification services, due to regulatory decisions or requests from subscribers or managers.
3. Approve the notification of any changes to subscribers and/or responsible parties, analyzing their legal, technical, or commercial impact.
4. Review and take action on any comments made by subscribers or managers when a change to the certification service is made.
5. Report action plans to ONAC on any changes that have an impact on the PKI infrastructure and that affect digital certification services, in accordance with the current RAC-3.0-01.
6. Authorize the required changes or modifications to the DPC.
7. Authorize the publication of the DPC on the ECD GSE website.
8. Approve changes or modifications to the ECD GSE Security Policies.
9. Ensure the integrity and availability of the information published on the ECD GSE website.
10. Ensure the existence of controls over the technological infrastructure of the ECD GSE.
11. Request the revocation of a digital certificate if you have knowledge or suspicion of the compromise of the subscriber's private key, entity or any other fact that tends to the improper use of the subscriber's private key, entity or the ECD itself.
12. To recognize and take appropriate action when security incidents occur.
13. Perform a review of the DPC at a maximum frequency of one year to verify that the lengths of the keys and periods of the certificates being used are adequate.
14. Review, approve and authorize changes to certification services accredited by the competent body.
15. Review, approve and authorize the ownership and use of symbols, certificates and any other mechanism that ECD GSE requires to indicate that the digital certification service is accredited.
16. To ensure that the accreditation conditions granted by the competent body are maintained.
17. Ensure the proper use in documents or any other advertising of the symbols, certificates, and any other mechanism that indicates that ECD GSE has an accredited certification service and complies with the provisions of the ONAC Accreditation Rules.
18. Ensure that critical suppliers and reciprocal ECDs, if any, are kept informed of the obligation to comply with the CEA requirements, in the relevant sections.
19. The Integrated Management System will execute corrective action plans and improvement actions to respond to any risk that compromises the impartiality of the ECD, whether it arises from the actions of any person, body, organization, activities, their relationships or the relationships of its staff or itself, for which it uses the ISO 31000 standard for the identification of risks that compromise the impartiality and non-discrimination of the ECD, delivering to the Management Committee the mechanism that eliminates or minimizes such risk, on a continuous basis.
20. Ensure that all ECD staff and committees (internal or external) that may have influence on certification activities act with impartiality and non-discrimination, especially those arising from commercial, financial or other pressures that compromise their impartiality.
21. Document and demonstrate the commitment to impartiality and non-discrimination.
22. Ensure that the administrative, management, and technical staff of the PKI and the ECD associated with consulting activities maintain complete independence and autonomy from the staff involved in the review and decision-making process regarding the certification of this ECD.
23. Ensure that critical suppliers such as reciprocal ECD and data centers that meet ECD accreditation requirements are kept informed as support for their contracting and compliance with the requested administrative and technical requirements.

9.12 Amendments.
Digital certificates issued by ECD GSE cannot be modified; amendments are not permitted. Therefore, the subscriber must request the issuance of a new digital certificate. In this case, a new certificate will be issued to the subscriber; the cost of this modification will be borne entirely by the subscriber according to the fees provided by ECD GSE or as defined in the contract.
9.12.1 Amendment procedure.
This does not apply because digital certificates issued by ECD GSE cannot be modified.
9.12.2 Notification mechanism and deadline.
This does not apply because digital certificates issued by ECD GSE cannot be modified.
9.12.3 Circumstances in which an OID must be modified.
This does not apply because digital certificates issued by ECD GSE cannot be modified.
9.12.4 Notification to the subscriber or person responsible for issuing a new certificate.
This does not apply because digital certificates issued by ECD GSE cannot be modified.
9.12.5 How a certificate modification is accepted.
This does not apply because digital certificates issued by ECD GSE cannot be modified.
9.12.6 Publication of the certificate modified by the ECD.
This does not apply because digital certificates issued by ECD GSE cannot be modified.
9.12.7 Notification of the issuance of a certificate by the ECD to other entities.
This does not apply because digital certificates issued by ECD GSE cannot be modified.
9.13 Provisions on dispute resolution.
If for any reason a difference arises between the Parties (subscriber/responsible and ECD GSE) on the occasion of: 1. The provision of the digital certification services described in this DPC.

During the execution of the contracted services.
For the interpretation of the contract, DPC and any other document delivered by ECD GSE.
The interested party will notify the other party via certified email of the existence of said difference, with the complete and duly supported information of the difference, so that within fifteen (15) business days following said notification, the Parties seek to reach a direct settlement between them as a first instance.
If, after this period, the difference(s) persist, the Parties will be free to resort to the ordinary Colombian justice system to assert their rights or demands, which will be subject to the current regulations on the matter; the costs incurred in connection with the summons will be entirely borne by the losing Party.
In accordance with the provisions of Annex 2 - Terms and Conditions of the DPC.

9.14 Applicable legislation.
The operation and activities carried out by the ECD GSE, as well as this Certification Practice Statement and the Certification Policies applicable to each type of certificate, are subject to the regulations that apply to them and in particular to:

1. Law 527 of 1999, By means of which the access and use of data messages, electronic commerce and digital signatures are defined and regulated, and certification entities are established and other provisions are issued.
2. Decree 333 of 2014, which regulates article 160 of Decree-Law 019 of 2012 regarding the characteristics and requirements of certification entities, and related to digital certificates.
3. Chapters 47 and 48 of Title 2 of Part 2 of Book 2 of the Single Decree of the Trade, Industry and Tourism Sector - DURSCIT.

Compliance with applicable legislation.
The ECD GSE states compliance with Law 527 of 1999 and its associated decrees, and furthermore, that the Certification Practice Statement is satisfactory in accordance with the requirements established by the National Accreditation Body of Colombia.
Various provisions.

Full agreement
The ECD GSE contractually obligates each RA to comply with this DPC and applicable industry guidelines. Furthermore, the ECD GSE requires each party using its products and services to enter into an agreement defining the terms and conditions associated with the product or service. If an agreement contains provisions that differ from this DPC, this DPC shall prevail. Third parties may not rely on or take action to enforce such an agreement if it conflicts with this DPC.
Assignment
Entities operating under this DPC may not assign their rights or obligations without the prior written consent of the ECD GSE.
Divisibility
If any provision of this DPC is declared invalid or unenforceable by a competent court or tribunal, the remainder of the DPC will remain valid and enforceable.
Enforcement (attorney fees and waiver of rights)
ECD GSE may seek compensation and attorney's fees from either party for damages, losses, and expenses related to that party's conduct.
The fact that ECD GSE does not enforce a provision of this DPC does not imply that it waives its right to enforce the same provision later or its right to enforce any other provision of this DPC.
To be effective, the resignations must be in writing and signed by the ECD GSE.
Force Majeure
ECD GSE shall not be liable for any delay or failure to perform an obligation under this DPC to the extent that the delay or failure is due to an event beyond ECD GSE's reasonable control.
The functioning of the Internet is beyond the reasonable control of the ECD GSE.
To the extent permitted by applicable law, the Subscriber Agreements and Relying Party Agreements will include a force majeure clause that protects the ECD GSE.
9.17 Other Provisions.
CHANGES THAT AFFECT DIGITAL CERTIFICATION SERVICES.
ECD GSE may make adjustments or changes to digital certification services in the following events:

1. Due to regulatory changes in legislation for ECD.
2. At the request of ONAC.
3. At the request of the Superintendency of Industry and Commerce of Colombia - SIC.
4. Technological changes that affect digital certification services.
5. At the request of subscribers or those responsible, with prior approval from the Management Committee.

For this purpose, the Subscriber or responsible party must send a communication addressed to the ECD GSE Management Committee regarding the requested change; acceptance or rejection will be at the discretion of the Management Committee.
Procedure for Changes.
Changes that do not require notification.

1. When the changes made do not affect the operation of the services provided to current subscribers or responsible parties, it will be the responsibility of the Management Committee to define the level of impact of the changes.
2. When the changes involve typographical or editing corrections in the content of the services provided.

Changes that require notification
1. When the changes made affect the operation of the services provided to current subscribers or responsible parties, it will be the responsibility of the committee to
Management define the level of impact of the changes.
2. When the changes involve updating contact details with the ECD GSE.
Notification mechanism and period

ECD GSE will notify subscribers, responsible parties, ONAC and SIC via email and/or web portal with detailed technical information and contract modifications regarding changes made to digital certification services when:

1. The Management Committee and the Integrated Management System process of the ECD GSE consider that changes to digital certification services affect their operation and acceptability.
2. The changes introduce new requirements for the provision of digital certification services due to technological updates or regulatory changes that affect the services.

Subscribers and/or those responsible for the digital certification services affected by the changes made may submit their comments or rejection to the provision of the ECD GSE service in a communication addressed to the Management Committee within thirty (30) days following the notification; after thirty (30) days, the conditions will be understood as accepted by the subscribers or those responsible.

DESCRIPTION OF PRODUCTS AND SERVICES

TYPE OF DIGITAL CERTIFICATE	OBJECT
Company Membership	This certificate guarantees the identity of the individual holder and their affiliation with a specific legal entity by virtue of their position within that entity. This certificate does not, in itself, grant the holder any greater powers than those they possess through their regular duties.
Company Representation	It is issued to a natural person representing a specific legal entity. The certificate holder is identified not only as a natural person belonging to a company, but also as its legal representative.
Public Service	This certificate guarantees the identity of the individual holder and their affiliation with a Public Administration by virtue of their position as a public official. This certificate does not, in itself, grant the holder any greater powers than those they possess through the performance of their regular duties.
Qualified Professional	This certificate guarantees the identity of the individual holder and their status as a qualified professional. This certificate does not, in itself, grant the holder any greater powers than those they possess by virtue of their regular professional activities.
Natural person	It only guarantees the identity of the natural person.
Electronic Invoice for natural person	Exclusive certificate for electronic invoicing, addressing the needs of individuals seeking the security of the certificate for issuing electronic invoices. Exclusive certificate for the digital signature of electronic invoices, credit notes, debit notes, electronic payroll payment receipts, adjustment notes of the electronic payroll payment receipt document and other documents resulting from the processes of the unattended platforms of the technology providers approved by the DIAN, the DIAN's free invoicing system and the RADIAN platform, in compliance with the technical annexes issued by said entity.
Electronic Invoice for legal entities	Exclusive certificate for electronic invoicing, addressing the needs of companies seeking secure certificates for issuing electronic invoices. Exclusive certificate for the digital signature of electronic invoices, credit notes, debit notes, electronic payroll payment receipts, adjustment notes of the electronic payroll payment receipt document and other documents resulting from the processes of the unattended platforms of the technology providers approved by the DIAN, the DIAN's free invoicing system and the RADIAN platform, in compliance with the technical annexes issued by said entity.
Artificial person	Performing business procedures by an application running on a machine in automated and unattended signing processes on behalf of a legal entity of public or private law that require guaranteeing the authenticity and integrity of the data sent or stored digitally together with the establishment of secure communication channels between clients, and which will be represented by a natural person (Controller), holder of the certificate issued under this policy and called Controller.
Generation of Certified Electronic Signatures	Exclusive certificate for generating certified electronic signatures.
Certified Email Service	Certified email service ensures the sending, receiving, and verification of electronic communications, guaranteeing at all times the characteristics of fidelity, authorship, traceability, and non-repudiation.
Chronological Stamping Service (TSA)	Data message that links another data message to a specific moment or period of time, which allows proof to be established that this data existed at that moment or period of time and that it did not undergo any modification from the moment the stamp was made.
Electronic Document and Data Message Archiving and Preservation Service	The service consists of a secure, encrypted storage space accessed with credentials or a digital certificate. Documents stored on this platform will have evidentiary value provided they are digitally signed.

Note: For verification of the generation process for each service, refer to the corresponding procedures.

RATES.

Fees for issuing or renewing certificates.

Product details	Delivery time	Validity	Price excluding VAT	VAT	Total
Natural Person Certificate	Normal	1	$192,794	$36,631	$229,425
Natural Person Certificate	Normal	2	$313,399	$59,546	$372,945
Certificate Belonging to company	Normal	1	$192,794	$36,631	$229,425
Certificate Belonging to company	Normal	2	$313,399	$59,546	$372,945
Professional Certificate	Normal	1	$192,794	$36,631	$229,425
Professional Certificate	Normal	2	$313,399	$59,546	$372,945
Company Representative Certificate	Normal	1	$192,794	$36,631	$229,425

Company Representative Certificate	Normal	2	$313,399	$59,546	$372,945
Public Service Certificate	Normal	1	$192,794	$36,631	$229,425
Public Service Certificate	Normal	2	$313,399	$59,546	$372,945
Legal Entity Certificate	Normal	1	$600,000	$114,000	$714,000
Legal Entity Certificate	Normal	2	$1,120,000	$212,800	$1,332,800
Electronic Billing	Normal	1	$233,286	44,324	$277,610
Electronic Billing	Normal	2	$313,399	$59,546	$372,945

These prices are calculated based on a one- and two-year validity period. The figures shown here for each type of certificate may vary depending on special commercial agreements reached with subscribers, entities, or applicants, as part of promotional campaigns conducted by GSE.
In the case of the electronic signature certificate, there is no cost because it is included in the packages for generating certified electronic signatures.
ECD GSE offers the issuance of digital certificates valid for days or months, not exceeding 24 months. The sale prices of these certificates will be agreed upon with the client after prior negotiation.
The same prices defined in the fee schedule will apply to the issuance of digital certificates using the elliptic curve algorithm.

Certificate access fees.
Access to the status of issued certificates is free and therefore does not require a fee.

Fees for revocation or access to status information.
There is no charge for requesting the revocation of a certificate. Access to the status information of issued certificates is free of charge and therefore no fee applies.

Rates for other services.
Once other services are offered by GSE, they are published on the service PCs on the GSE website.

Return policy.
Please refer to the Returns Policy published on the GSE website:https://ase.com.co/politicas

IMPARTIALITY AND NON-DISCRIMINATION
ECD GSE, led by the Management Committee and its collaborators, is committed to safeguarding impartiality and independence in digital certification processes and services, in order to prevent conflicts of interest within the company, with relevant internal and external stakeholders, acting within the legal framework of Law 527 of 1999, Decrees 019 of 2012, 333 of 2014 and 1471 of 2014, and the specific accreditation criteria of the National Accreditation Body of Colombia (ONAC), for which the following compliance mechanisms are established:

- The Management Committee and GSE employees declare that they do not participate directly or indirectly in services or activities that may endanger free competition, responsibility, or transparency.
- Employees will use the development of preventive and corrective actions to respond to any risk that compromises the company's impartiality.
- Employees who are part of accredited digital certification services may not provide consulting services, nor involve the development team in providing technical support services to the subscriber or client.
- GSE is responsible for impartiality in the development of its activities and does not allow commercial, financial or other pressures to compromise its impartiality.
- GSE may decline to accept an application or maintain a contract for certification when there are substantiated and proven reasons, for example, the applicant's and/or subscriber's involvement in illegal activities, or similar issues related to the subscriber.
- GSE may decline to accept an application or maintain a contract for certification when there are well-founded, proven, or undue reasons on the part of the applicant and/or subscriber.
- GSE offers access to a digital certification service that is not dependent on the size of the applicant or subscriber, nor on membership in any association or group, nor should it depend on the number of certifications already issued.

Note: Any case that puts at risk the impartiality of the ECD GSE as an ECD or of its staff, body or organization, will be brought to the attention of the Integrated Management System Process.
In accordance with the provisions of the ECD GSE's Fairness and Non-Discrimination Policy, which can be found at the following link:https://gse.com.co/politicas.

CERTIFICATION POLICIES.
The interrelationship between this DPC and the certification policies of the various certificates is fundamental. This is because:
The DPC is the set of practices adopted by ECD GSE for the provision of services accredited by ONAC and contains detailed information about its security system, support, administration and issuance of certificates, as well as about the relationship of trust between Applicant, Subscriber, Responsible, Entity, Third Party in good faith and the ECD.
Certification policies constitute the set of rules that define the characteristics of the different ECD GSE certificates and the applicability of these certificates to certain applications that require the same security requirements and forms of use.
In short, the policy defines "what" requirements are necessary for the issuance of the various ECD GSE certificates, while the DPC tells us "how" the security requirements imposed by the policy are met.
Certificate Policies for Digital Certificates:
For this reason, the following Certificate Policies are related:

OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.4.18
LocationeitherPC number	https://ase.com.co/documentos/calidad/Doliticas/Politica de certificado cara certificados digitales V18.Ddf

•PolYoCronol Stamping Service Certificate codeseitherlogical:

OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.2.15
LocationeitherPC number	https://ase.com.co/documentos/calidad/politicas/PoliticaCertificate for Chronological Stamping Service V15.pdf

• Certificate Policies for Archiving and Preservation Service of Transferable Electronic Documents and Data Messages:

OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.3.14
PC Location	https://gse.com.co/documentos/calidad/politicas/Politica_de_Certificado_para_Servicio_de_Archivo_Confiable_de_Datos_V14.pdf

• Certificate Policies for Certified Email Service:

OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.5.15
PC Location	https://ase.com.co/documentos/calidad/rJoliticas/Politica Certified Email Service V15.Ddf

• Policies for Generating Certified Electronic Signatures:

OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.6.5
PC Location	https://ase.com.co/documentos/calidad/Doliticas/Politica de Generación de Firmas Electrónicas Certificadas V5.Ddf

ANNEX 1 DPC TECHNICAL PROFILE MATRIX DIGITAL CERTIFICATES.
ANNEX 2 DPC MODELS AND MINUTES OF TERMS AND CONDITIONS DOCUMENTS.
ANNEX 3 DPC TECHNICAL PROFILE MATRIX ELECTRONIC SIGNATURE CERTIFICATES.