

DPC-001-ING
Certification Practices Statement
Version No. 16

CONTENTS

1. REVISION HISTORY 9

2. INTRODUCTION 17

2.1. GENERAL DESCRIPTION 17

2.2. DEFINITIONS AND ABBREVIATIONS 18

2.3. NAME AND IDENTIFICATION OF THE DOCUMENT 23

2.4. INFORMATION ON THE INFORMATION SECURITY SYSTEM FOR THE PURPOSE OF ISSUING CERTIFICATES 26

2.5. MANAGEMENT SYSTEM REQUIREMENTS 26

2.7. PERMITTED USES FOR DIGITAL CERTIFICATES 33

2.8. MANAGEMENT POLICIES 38

3. INFORMATION REPOSITORIES OF THE DIGITAL CERTIFICATION ENTITY 39

3.1. REPOSITORIES 39

3.2. INFORMATION PUBLICATION 39

3.3. UPDATE FREQUENCY OF THE INFORMATION CONTAINED IN THE DIGITAL CERTIFICATES 41

3.4. ACCESS CONTROL TO STORED INFORMATION 42

4. AUTHENTICATION AND IDENTIFICATION OF INFORMATION 42

4.1. DENOMINATION IN THE NAMES 43

4.2. SUBSCRIBER IDENTIFICATION PROCEDURES (IDENTITY VALIDATION) 43

5. LIFE CYCLE OPERATION OF DIGITAL CERTIFICATES 49

5.1. APPLICATION FOR ISSUANCE OF DIGITAL CERTIFICATES 49

5.2. CERTIFICATE REQUEST PROCESSING 54

5.3. PROCEDURE FOR THE ISSUANCE OF DIGITAL CERTIFICATE 55
5.4. ACCEPTANCE OF THE DIGITAL CERTIFICATE 61
5.6. DIGITAL CERTIFICATE RENOVATION 62
5.7. CERTIFICATES MODIFICATION 62
5.8. REVOCATION OF DIGITAL CERTIFICATES AND GROUNDS FOR REVOCATION 62
5.9. CERTIFICATES' STATUS 67
5.10. SERVICE TERMINATION 67
5.11. TYPES OF HSM OFFERED 67
5.12. RISKS AND COMMITMENTS OF THE CRYPTOGRAPHIC DEVICES OFFERED BY OLIMPIA IT 68
5.13. PAIR OF KEYS CUSTODY 68
6. SECURITY CONTROLS 69
6.1. PHYSICAL SECURITY CONTROLS 69
6.2. PROCEDURAL CONTROLS 71
6.3. PERSONNEL SECURITY CONTROLS 72
6.4. SECURITY EVENTS CONTROLS 74
6.5. AUDIT EVENTS RECORD 76
6.6. RE-CREATION OF THE ROOT CA KEY 78
6.7. CONTINUITY AND CONTINGENCY 78
6.8. COMPLETION OF ACTIVITIES AS A DIGITAL CERTIFICATION ENTITY 80
7. TECHNICALL SECURITY CONTROLS 81
7.1. CREATION AND INSTALLATION 81

7.2. PRIVATE KEY SECURITY 83
7.3. ADDITIONAL INFORMATION REGARDING KEY PAIR MANAGEMENT 86
7.4. ACTIVATION DATA 86
7.5. COMPUTER SECURITY CONTROLS 87
7.6. LIFE CYCLE SAFETY CONTROLS 87
7.7. WEB SECURITY CONTROLS 88
8. TECHNICAL STANDARDS OF THE CERTIFICATES 88
8.1. CERTIFICATE PROFILE 88
8.2. CRL PROFILE 90
8.3. VALIDITY OF CERTIFICATES BY OCSP 90
8.4. CURRENT TECHNICAL STANDARDS 91
9. COMPLIANCE AUDIT 91
9.1. AUDIT FREQUENCY 91
9.2. AUDIT TEAM 91
9.3. RELATIONSHIP BETWEEN THE AUDITED ENTITY AND THE AUDITOR 92
9.4. CONFORMITY CONTROL 92
9.5. PREVENTIVE OR IMPROVEMENT ACTIONS AS A RESULT OF NON-CONFORMITIES 92
9.6. RESULTS REPORT 92
9.7. AUDIT EVENTS RECORD 93
10. CHRONOLOGICAL STAMPING 93
10.1. TIME STAMP AUTHORITY (TSA) 93

10.2. OPERATION OF THE CHRONOLOGICAL STAMP 94
10.3. MEANS FOR THE SERVICE REQUEST 95
10.4. CHRONOLOGICAL STAMPING FOR A DATA MESSAGE 95
10.5. POLICIES FOR THE TIME STAMPING SERVICE PROVISION 96
10.6. NUMBER OF TIME STAMPS 96
10.7. PROCEDURE FOR ENABLING THE SERVICE FOR THE SUBSCRIBER 97
10.8. TIME STAMPING SERVICE REQUIREMENTS (DOCUMENT AND INFORMATION REQUESTED) 97
10.9. PROCEDURE FOR ENABLING THE CHRONOLOGICAL STAMPING SERVICE FOR THE APPLICANT / SUBSCRIBER 99
10.10. SERVICE ACTIVATION PERIOD 102
10.11. OPERATION OF THE TIME STAMPING SERVICE 102
10.13. TIME SOURCE 103
11. COMMERCIAL TERMS 104
11.1. FEE POLICY FOR ISSUANCE AND REVOCATION OF CERTI FICATES 104
11.2. FEES FOR DIGITAL SERVICES IN PROJECTS 104
11.3. PAYMENT METHOD 104
11.4. POLICIES FOR MONEY REFUND 105
11.5. FINANCIAL RESPONSIBILITY 105
12. INFORMATION CONFIDENTIALITY 106
12.1. SCOPE OF CONFIDENTIAL INFORMATION 108
12.2. INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION 108
12.3. RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION 109

13. INTELLECTUAL PROPERTY RIGHTS 110

14. OBLIGATIONS AND GUARANTEES 110

14.2. CONDITIONS AND OBLIGATIONS OF SUBSCRIBERS 118

14.3. APPLICANT'S OBLIGATIONS 122

14.4. OBLIGATIONS AND PRECAUTIONS OF THE RELYING PARTIES 124

14.5. RIGHTS ASSOCIATED WITH EACH OF THE SERVICES PROVIDED AS ECD 127

15. LIABILITY DISCLAIMER 128

15.1. LIABILITY LIMITS FOR THE EXERCISE OF THE ACTIVITY 128

15.2. RESPONSIBILITIES OF APPLICANTS AND SUBSCRIBERS 130

15.3. LIABILITY OF RELYING PARTIES 131

15.4. COMPLIANCE WITH OLIMPIA IT'S OBLIGATIONS 132

16. DISPUTE RESOLUTION AND CONTRACTUAL MINUTES FOR THE PROVISION OF SERVICES AS ECD 133

16.1. CONTRACT ENTERED INTO BETWEEN THE ECD AND THE APPLICANTS AND/OR SUBSCRIBERS 135

16.2. APPLICABLE LAW 135

17. CERTIFICATE MANAGEMENT POLICY 135

17.2. COMPLIANCE WITH APPLICABLE LAW 136

17.3. COMPLIANCE WITH LEGAL REQUIREMENTS 136

18. TERMS AND CONDITIONS AGREEMENT 136

19. CERTIFICATES' TERM 136

19.1. ROOT CERTIFICATE TERM 136

19.2. SUBORDINATE CERTIFICATES' TERM 137

19.3. TERM OF CERTIFICATES ISSUED TO SUBSCRIBERS 137

20. DELIVERY OF DIGITAL CERTIFICATE 137

20.1. DELIVERY OF THE PHYSICAL TOKEN 137

20.2. MAXIMUM DELIVERY TIMES 138

20.3. OBTAINING THE CERTIFICATE FROM THE WEB PORTAL 138

21. IMPARTIALITY, NON-DISCRIMINATION, AND INDEPENDENCE IN SERVICES 138

21.1. NON-DISCRIMINATION FACTORS 139

22. CERTIFICATE DIRECTIVES 139

23. TYPE OF CERTIFICATES 142

24. SERVICE'S DESCRIPTION 142

24.1. DESCRIPTION OF THE DIGITAL CERTIFICATE SERVICE - NATURAL PERSON 142

24.2. DESCRIPTION OF THE DIGITAL CERTIFICATE SERVICE - LEGAL PERSON 143

24.3. DESCRIPTION OF THE DIGITAL CERTIFICATE SERVICE - CERTIFIED PROFESSIONAL 144

24.4. DESCRIPTION OF THE DIGITAL CERTIFICATE SERVICE - COMPANY BELONGING 145

24.5. DESCRIPTION OF THE DIGITAL CERTIFICATE SERVICE - PUBLIC FUNCTION 145

24.6. DESCRIPTION OF THE DIGITAL CERTIFICATE SERVICE – LEGAL REPRESENTATIVE 146

24.7. DESCRIPTION OF THE TIME STAMPING SERVICE 146

24.8. DESCRIPTION OF THE CENTRLIZED SIGNATURE SERVICE 147

24.9. DESCRIPTION OF THE CERTIFIED EMAIL SERVICE 148

25. CRYPTOGRAPHIC DEVICES 149

26. SERVICES AND APPLICATIONS FOR THE SERVICES USAGE 149

26.1. SIGNATURE VALIDITY 150

26.2. OLYMPIA SIGN 150

26.3. DRIVER TOKEN 150

26.4. CSR GENERATOR 150

26.5. ISSUANCE OF DIGITAL CERTIFICATES FOR PKCS#10 REQUEST 150

27. LOCATION 151

28. POLICY TO RESOLVE PETITIONS, COMPLAINTS, CLAIMS AND SUGGESTIONS 151

28.1. PROCEDURE FOR THE RESOLUTION OF PETITIONS, COMPLAINTS, CLAIMS AND SUGGESTIONS - PQRS- 152

29. PROPERTY OF OLYMPIA 152

1. REVISION HISTORY

VERSIÓN	FECHA	DESCRIPCIÓN
DPC ING # 1 DPC ESP # 15	01/24/2023	Creation of the document, version No. 15 is translated from Spanish to English.
DPC ING # 2 DPC ESP # 16	30/03/2023	Update of the fees for 2023 in chapters 11.1.1.1. Issuance of Digital Certificate with Physical Token, 11.1.1.2. Issuance of Digital Certificate for PKCS#10 Certification Request (Unlimited for 1 year), 11.1.1.3. Issuance of Digital Certificate for PKCS#10 Certificate Request (on demand), 11.1.2. Chronological Stamp Fees, 11.1.3. Centralized Signature Service Fees, 11.1.4. Fees Certified Email Service and 11.1.5. Fees Certified SMS Service Modification of the telephone number of the company .
DPC ING # 3 DPC ESP # 17	29/05/2023	Modifies the name of the data center (from Centurylink Colombia S.A.S., to Cirion Technologies Colombia S.A.S.) in numeral 2.3.3.1 Changes the way to update the certificates, from "automatic" to "Manual" in section 3.3.3. Includes the possibility of presenting a signature by mandate in front of a notary in numeral 4.2.2 Includes disability as a factor that can generate discrimination in numeral 21.1 Changes the name "OlimpiaIT" to "Olimpia IT" and other formal adjustments
DPC ING # 4 DPC ESP # 18	21/07/2023	Modifies the name of the CEO in numeral 2.8.2. Includes a note in numeral 5.3.6 clarifying that the services through Tokens operate in the same way as centralized signatures.

VERSIÓN	FECHA	DESCRIPCIÓN
		In numeral 5.3.8, it is made clear that, for both physical and virtual tokens, the subscriber is notified via email of the generation of a random pin that can be modified via the "Driver token" published on the website. Also, a note is included indicating that the formal documentation of the digital certification services must comply with the provisions of the *Reglamento de uso de los símbolos de Acreditado y/o Asociado* of ONAC. Includes the technical description of the HSM and Tokens in numeral 5.11.
DPC ING # 5 DPC ESP # 19	14/09/2023	Includes guidelines on updating the Certificate of Incorporation of Olimpia IT (Certificado de Existencia y Representación Legal) on the website, within numeral 2.3.3.1 Includes the situations in which the ECD will notify ONAC for organizational changes, in numeral 3.3.4. Deletes the reference to restrictive lists in numeral 5.2.2. Updates the number reference for identity validation in section 5.3.1.1. Modifies the wording of section 11.4.1. to indicate that the fees are annual rates Clarifies that the certified email services use Olimpia IT's certificate, in numeral 24.9 Includes statment of the prevalence of the Spanish version over the English of this documento, in section 29

VERSIÓN	FECHA	DESCRIPCIÓN
		Includes form corrections
DPC ING # 6 DPC ESP # 20	31/01/2024	Adds definition of “electronic signature” in section 2.2.1. Adds the Certified Electronic Signature service for a natural person or legal entity or person and explanatory note in section 2.3.2. Adds the term “electronic signature”, “electronic” or “electronically” in the following paragraphs: • Section 2.6.2.2, literal v • Section 2.6.4.5 • Section 2.7.1, literal b • Section 3.2 • Section 5.2.2 • Section 5.3 • Section 5.3.1.1 • Section 14.2, literals j, t, aa and cc • Section 14.4, literal a • Section 14.4.1 • Section 14.4.2 • Section 14.4.3 • Section 14.5 • Section 15.1, letters h and j • Section 15.2 • Section 15.3 Modifies the charge of “Digital Identity & E-Signature Business Director” to “Product Director”. Add clarification to the “Certificate Status Verification” (OCSP) in Section 3.3.3. Clarifies that Section 4.2.2. does not apply to Certified Electronic Signature, and adds section

VERSIÓN	FECHA	DESCRIPCIÓN
		4.2.3 on identity authentication for Certified Electronic Signature. Adds the following text to the online application in section 5.1: "or through any other portal than Olimpia IT, or through an API duly integrated into the portal of the Digital Certification Entity." Likewise, it adds the possibility of validating through a delegate. Adds the text "or any document that allows the quality and identification of the subscriber to be reliably validated" in Section 5.3.1.1, literals a, b, d, e and f. Adds the form of use of certified electronic signature, through web portal, API and other mechanisms in Section 5.3.5. Delete texts "The applicant may embed a time stamp in a digital signature with a digital certificate service from Olimpia IT" in Section 10.8.3. Adjusts the service rates for the year 2024 (section 11) and adds the certified electronic signature rates in Section 11.1.5. Adjusts text of Section 14.1, paragraphs z and bb, Section 14.4 and Section 14.4.1, clarifying that it applies to digital certification services in general. Adjusts the form of Section 14.5, eliminating redundant text "the rights are detailed" Adds OID of Certified Electronic Signature of a natural person and a legal entity in Section 22

VERSIÓN	FECHA	DESCRIPCIÓN
		Adds Certified Electronic Signature service for a natural person or legal entity and explanatory note in Section 23. Adds section 24.1 with the description of the certified electronic signature service of a natural person or legal entity.
DPC ING # 7 DPC ESP # 21	31/01/2024	Adjusts the type of certified electronic signature in sections 2.3.2, 23 and 24.10. Adds the option of delegated identity validation through a third party in section 4.2.2. Modifies the forms of identity validation of the certified electronic signature in section 4.2.3. Adds the possibility of amending errors in section 14.3, literal c. Adjust the OID of the certified electronic signature in section 22. Includes the description of the requirements and procedures for the issuance of the certified electronic signature in section 24.10.1.
DPC ING # 8 DPC ESP # 22	04/04/2024	Adds section 4.2.3 and 4.2.3.1, which includes delegated identity validation carried out by entities in the Public Service Sector through an agreement. Adds section 5.8.3.2 on the revocation of certificates in compliance with an agreement.
DPC ING # 9 DPC ESP # 23	20/05/2024	The fees for digital certification services from section 11.1 of the DPC have been eliminated, with a reference that the fees will be published on the Mi

VERSIÓN	FECHA	DESCRIPCIÓN
		Certificado portal, complying with ONAC NC 1, ID 241 of the Kawak tool and correcton 268.
DPC ING # 10 DPC ESP # 24	27/06/2024	Adjust numeral 4.2.2. indicating the cases in which there are specific authentication processes. Adds the texts "and following" and "or the regulations that modify or add them" in section 4.2.3.1.
DPC ING # 11 DPC ESP # 25	28/03/2025	The wording of numerals 5.1.2, 5.2.2, and 5.3.1.1 is simplified to enhance the review process of the RA request, supported by technological advancements. The email address of the Product Director is updated in numeral 2.8.3. Formatting, wording, and cross-references are adjusted. Numerals 4.2.3.1 and 5.1 are modified to allow the issuance of digital certificates with an identity card for the DIAN system, clarifying that a representative will not be required in certain cases. The template and logo are updated.
DPC ING # 12 DPC ESP # 26	10/06/2025	The review path for documents is adjusted in Sections 2.1, 3.3.4, 5.1, and 10.9. The access links of documents are adjusted in Sections 2.3, 14.4.3, 15.2, 16.1, and 18. The request process for the certificate of existence and legal representation, as well as the data center information, is adjusted in Section 2.3.3.1. The CRL update period is adjusted to 24 hours in

VERSIÓN	FECHA	DESCRIPCIÓN
		Section 3.3.2. Remove the references to the Certified Electronic Signature service.
DPC ING # 13 DPC ESP # 27	17/10/2025	Sections 5.3.8 and 20.1 are adjusted to clarify that the "Descargas" ("Downloads") option has been moved to the "Documentación" section of the website. The sections (2.1, 2.3.3.1, 3.2, 3.3.4) that reference the "Marco Legal" button on the website are adjusted to refer to "Documentación" instead.
DPC ING # 14 DPC ESP # 28	20/01/2026	Modify Olimpias business address in sections 2.3.3, 2.8, and 27. Adjust section 2.8 regarding the role of ECD management and the contact email address. Remove any information that is not required. Adjust the OID of the certified email and include an explanatory note in section 22.
DPC ING # 15 DPC ESP # 29	11/06/2026	Adjust section 2.3.2.1 to reflect the changes made to the website www.olimpiait.com. Update the URL address in the "Acceso de la información de la entidad emisora" section (2.6.2.2).
DPC ING # 16 DPC ESP # 30	29/10/2026	In response to NC identified by ONAC, the following adjustments are made: Section 5.3.8 includes a clarification stating that, if the subscriber does not receive the notification of approval together with the formal documentation for the digital certificate by email, they may request that this information be sent through the

VERSIÓN	FECHA	DESCRIPCIÓN
		communication channels made available by Olimpia IT. Section 24.7 clarifies that the Time Stamping service requires the purchase of any of the accredited digital certificates offered by the ECD.

2. INTRODUCTION

2.1. GENERAL DESCRIPTION

Olimpia IT makes clear to all interested parties, with free access on its website, that the purpose of this Certification Practices Statement -DPC, is to establish the general guidelines for certification services.

This Certification Practices Statement will be fully valid for subscribers, third parties and other parties throughout the life cycle of the digital certificate, and the provision of services that Olimpia IT provides as an Open Digital Certification Entity The content of this Certification Practices Statement is based on Decree 333 of 2014, the RFC standard 3647, RFC 3628 standard, the requirements of CEA 3.0-07, the requirements of the National Accreditation Agency of Colombia (ONAC), and Colombian regulations that apply and Webtrust program controls in effect; Its application is accepted by the laws of the Colombian territory.

Any modification, clarification, deletion, addition, or supplementation that Olimpia IT makes of this Certification Practices Statement will be performed in accordance with the procedure that Olimpia IT has established for this.

Notwithstanding the foregoing, each of the changes made in this DPC will go through version control, each version must be approved by the Policies Committee of Olimpia IT.

The applicant for the modification must comply with what is described in Numeral 3.2 of this CPS, and if the requested modification is approved, it will require that the new version be published and informed to consumers and the general public on the website https:// micertificado.olimpiait.com, "Documentación" section, "Certification Practices Statement" link.

This Certification Practices Statement is published for consultation by consumers and the general public on the website https://micertificado.olimpiait.com, "Documentación" section, "Certification Practices Statement" link.

2.2. DEFINITIONS AND ABBREVIATIONS

2.2.1. DEFINITIONS

i. Algorithm: It is a prescribed set of well-defined, ordered, and finite instructions or rules that allows an activity to be performed through successive steps that do not generate doubts for the person who must perform said activity. Given an initial state and following the successive steps, a final state is reached, and a solution is obtained.

ii. Registration Authority (RA): It is in charge of receiving the requests related to digital certification, to register the requests made by the applicants to obtain a certificate, verify the veracity and correctness of the data provided by the users in the requests, and send the requests that meet the requirements to a CA for processing.

iii. Time Stamping Authority (TSA): Trusted entity that issues time stamps.

iv. Root CA: First level certification authority, trust base.

v. Subordinate CA: Certification authority of second level or more levels.

vi. Characterization of processes and services: Documented description of the general characteristics of the process or service that establishes the relationship with the other internal or external processes of the organization, the inputs and outputs of the process, the suppliers and subscribers, the risks and controls, and their interaction.

vii. Digital certificate: electronic data message signed by the digital certification entity, which identifies both the issuing certification entity and the subscriber and contains the latter's public key.

viii. Signature Creation Data (Private Key): are unique numerical values

that, used together with a known mathematical procedure, are used to generate the digital signature of a data message.

ix. Signature Verification Data (Public Key): is the data, such as codes or public cryptographic keys, which are used to verify that a digital signature was generated with the subscriber's private key.

x. Certification Practice Statement (CPS): It is the document that contains in detail the procedures applied by the ECD for the provision of its services. A statement of the practices that an ECD employs to issue, manage, revoke, and renew certificates with and without key changes.

xi. Certification Entity: In accordance with what is indicated in Law 527 of 1999, Article 2, Literal d, it is that natural or legal person that is empowered to issue digital certificates in relation to the digital signatures of people, offer or facilitate registration services and chronological stamping of the transmission and reception of data messages, as well as fulfilling other functions related to communications based on digital signatures.

xii. Open Certification Entity: Entity that offers the general public, ECD-specific services, its use is not limited to the exchange of messages between the entity and the subscriber, and it receives remuneration.

xiii. Digital signature: It will be understood as a numerical value that is attached to a data message and that, using a known mathematical procedure, linked to the subscriber's key and the text of the message, makes it possible to determine that this value has been obtained exclusively with the subscriber's key and that the initial message has not been modified after the transformation.

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

xv. Certificate Revocation List (CRL): It is that relationship that must include all the certificates revoked by the digital certification authority.

xvi. Log: Event registration service of the information system,

maintaining the previous and current information, identifies who and when the event took place.

xvii. Technological Neutrality: principle contemplated in Law 1341 of 2009 and Article 2.2.2.47.2. of the DURSCIT, according to which there should be no preference or restriction of any kind of the various techniques or technologies that can be used to electronically sign, generate, communicate, store or file information. According to Judgment C-403/10 of the Constitutional Court, “it is the freedom that network, and service providers have to use technologies for the provision of all services without restriction other than possible harmful interference, and efficient use of scarce resources. This principle is applicable to the activity performed by the Digital Certification Entities, as long as the criteria established in CEA 3.0-07 are complied.

xviii. Security Levels: These are the various security levels offered by electronic signature variables whose benefits and risks must be evaluated by the person, company or institution that intends to opt for an electronic signature modality to send or receive data messages or electronic documents.

xix. OID: Unique object identifier. Term acronym in English language "Object Identifier", which consists of a unique identification number assigned which is based on international standards and commonly used to identify documents, systems, equipment, etc., with the purpose, among others, of knowing the origin, ownership, and age of the identified object.

xx. PKI: Public Key Infrastructure: is the set of hardware, software, policies, procedures, and technological elements that, through the use of a pair of cryptographic keys, a private one that only the service subscriber has and a public one, which is included in the digital certificate, achieve:

- Identify the sender of an electronic data message.
- Prevent third parties from observing the messages that are sent through electronic means.

- Prevent a third party from altering the information that is sent through

  electronic media.

- Prevent the subscriber of the digital certification service that sent an

  electronic message may later deny said delivery.

xxi. Certificate Policy (CP): It is the set of rules that indicates the requirements of a certificate in a particular community and/or class, within the framework of legal and regulatory requirements, and with common security requirements.

xxii. Supplier: The term "supplier" includes organizations, individuals, manufacturers, distributors, technology assemblers, and others who supply products, goods, and services. ECD providers include Reciprocal entities, technology companies that provide services in their different modalities such as: hosting, colocation, document repository (electronic or physical), device provider, telecommunications provider, etc.

xxiii. Complain: Dissatisfaction expression, other than the appeal, submitted by a person or organization to an ECD or an accreditation body, related to the activities of one of the two, for which a response is expected.

xxiv. Certification Requirements: It is the set of obligations established in Colombian law, which the applicant for the digital certification service must demonstrate to the ECD, in order to be a subscriber of the requested certificate.

xxv. Revocation: For the purposes of this document, it is the process by which the issued Digital Certificate is disabled, and its validity period of use is terminated as of the date of revocation when any of the causes established in the Statement of Practices of Certification are present.

xxvi. OCSP Online certificate status protocol: Real-time query activity to the ECD system, on the status of a digital certificate through the

OCSP protocol.

xxvii. Digital Certification Service: Set of certification activities offered by the ECD to certify the origin and integrity of data messages, based on digital or electronic signatures, time stamping, as well as the applicability of accepted and current technical standards in public key infrastructure – PKI.

xxviii. Digital signature generation service: For all purposes of the Olimpia IT digital certification entity, the centralized signature service will be understood.

xxix. Applicant: Natural or legal person who requests the digital certification service from the ECD in order to obtain digital certification services.

xxx. Subscriber: In digital certification services, the term subscriber identifies the natural or legal person who contracts the digital certification service from the ECD. In the case of issuing digital certificates activity, it will also be the natural or legal person in whose name a certificate is issued.

xxxi. Relying third party: Natural or legal person who decides to accept and trust a digital certificate issued by Olimpia IT.

2.2.2. ABBREVIATIONS

CA: Certification Authority

CPD: Certification Practice Statement
CPS: Certificate Revocation List
CP: Certificate Policy

OCSP: Offensive Security Certified Professional RA: Registration Authority
PKI: Public Key Infrastructure ECD: Digital Certification Entity
ONAC: National Accreditation Body of Colombia OID: Object Identifier
TSA: Time Stamp Authority

2.3. NAME AND IDENTIFICATION OF THE DOCUMENT

Name:	CERTIFICATION PRACTICES STATEMENT
Code:	DPC – 001
Approval date:	February 23, 2022
VERSION:	**09**
Description:	This document contains the Certification Practices Statement for certificates, services, and TSA for Olimpia IT associated with the issuance of digital certificates, which are approved by the Olimpia IT Policy Committee and are available to the public.
Link	https://micertificado.olimpiait.com/Publica/Politica

2.3.1. SCOPE

The scope of this Certification Practices Statement (CPS) and Certificate Policies (CP) is limited to the certification activities for which the National Accreditation Body of Colombia has given viability in their realization, as well as for the provision of services also feasible to provide by Olimpia IT as an Open Digital Certification Entity.

Each of the accredited activities or services to be developed by Olimpia IT as an Open Digital Certification Entity, have a detail on the limit of obligations, responsibilities, rights, and security that each one can provide, which are developed extensively in each point of the services dealt with in this CPS.

2.3.2. SERVICES OFFERED BY THE ECD

Natural person digital certificate, Legal person digital certificate, Certified professional digital certificate, Company belonging digital certificate, public function digital certificate, Legal representative digital certificate, Certified email service, Chronological stamping service, Centralized signature service, Certified Electronic Signature Service.

Note: It is clarified that the Certified Electronic Signature service is not accredited.

2.3.2.1. INFORMATION FOR CONSUMERS AND GENERAL PUBLIC

Consumers and the public are informed of the ECD activities and the accredited scope on the website https://micertificado.olimpiait.com.

From the website https://micertificado.olimpiait.com, "Productos" button in the link "Certificados Digitales", information is provided regarding the different types of certificates offered, and in the link "Servicios Digitales", information is provided about the services offered in accordance with the provisions of ONAC document RAC-3.0-03.

On the website www.olimpiait.com, under the “Términos y Condiciones” link, users can find information such as the type of company, the guidelines governing the use of the platforms, products, and services offered by the company, among other relevant aspects.

All services provided and the issuance of certificates accredited by Olimpia IT before ONAC, are provided independently and impartially, likewise, each of the certificate policies contained in this Certification Practices Statement are subject to compliance with the provision of services with independence and impartiality, and its conditions are treated and developed in the impartiality mechanism established by Olimpia IT called the Impartiality Committee, and associated with the risks that this committee identifies and mitigates or accepts.

2.3.3. ABOUT OLYMPIAIT

Olympia IT SAS is a commercial company constituted entirely by private capital through public deed # 1513 of Notary 32 of the Circle of Bogotá on July 1, 2005, registered on July 12, 2005, under # 01000696 of Book IX whose NIT is 900,032.774-4, Olimpia IT, is a company registered with the Chamber of Commerce of Bogotá and whose status is active.

The registered office and correspondence of Olimpia IT, is located in the

city of Bogotá DC, at Cra. 7 #24-89, Torre Colpatria, Piso 46, which correspond to the one registered in the certificate of existence and representation issued by the Chamber of Commerce of Bogotá, whose main telephone number is (+57 601) 742 7878, and email is notificaciones.gerencia@olimpiait.com , a company to which corresponds the mercantile registration Nº 01505286 of July 12, 2005 and whose activity as Digital Certification Entity was granted by the National Accreditation Agency of Colombia (ONAC) through an accreditation certificate issued by ONAC, accreditation that can be consulted in the official directory of accreditations for digital certification entities: www.onac.org.co/modulos/contenudo/defuaul.asp?idmodulo=599

2.3.3.1. CERTIFICATE OF EXISTENTE AND LEGAL REPRESENTATION OF OLIMPIA IT

Olimpia IT hereby declares and informs the general public that the certificate of existence and legal representation of Olimpia IT S.A.S., issued by the Bogotá Chamber of Commerce, can be requested via the email address notificaciones.gerencia@olimpiait.com, as detailed on the website https://micertificado.olimpiait.com, under the "Documentación" section. Olimpia IT will update this document whenever there is a change in relevant information (such as company name, corporate purpose, or legal representation), and in any case, at least once a year and before December 31 of each year.

Other subcontracted entities are listed below:

Data Center Provider: SENCINET Latam Colombia S.A., with Tax Identification Number (NIT) 800255754-1 and Commercial Registration No. 637298, currently active in the Bogotá Chamber of Commerce, with its registered and mailing address at Cl. 113 #743 a 7-53, Bogotá, Colombia. Contact email: contact@sencinet.com; phone number: +57 320 8734576. The certificate of existence and legal representation may be requested via the email address notificaciones.gerencia@olimpiait.com, as detailed on the website https://micertificado.olimpiait.com, under the "Documentación"

section.

Data Center Provider: Cirion Technologies Colombia SAS, with NIT 800.136.835-1, commercial registration No. 00464163, whose status is active in the Chamber of Commerce of Bogotá, with registered office and correspondence is Calle 185 No. 45-03 Centro Comercial Santafé, Torre Empresarial P, in the city of Bogotá, with email german.garcia@centurylink.com and telephone: (57 601) 6119000, whose certificate of existence and legal representation can be requested via the email address notificaciones.gerencia@olimpiait.com, as detailed on the website https://micertificado.olimpiait.com, under the "Documentación" section.

2.4. INFORMATION ON THE INFORMATION SECURITY SYSTEM FOR THE PURPOSE OF ISSUING CERTIFICATES

Olimpia IT has implemented the information security system based on the international standard NTC-ISO/IEC 27001 in its current version.

2.5. MANAGEMENT SYSTEM REQUIREMENTS

Olimpia IT has implemented the management system based on the international standard ISO/IEC 9001 in its current version.

2.6. PARTICIPANTS AND STRUCTURE IN THE DIGITAL CERTIFICATION PROCESS

The following shows how the Olimpia IT Digital Certification System is organized. For these purposes, it will be understood that the system is made up of a structure and some participants, among others, by the root CA, the subordinate CA, an impartiality committee, the RA, subscribers and relying parties.

2.6.1. ROOT CA:

First level certification authority, trust base.

2.6.1.1. THE CONTENT OF THE GERENATED CERTIFICATE IS:

Certificate field		Worth
version		v3
serialNumber		Unique positive integer with respect to the CA issuing the certificate
signature		Signature Algorithm Parameters
signature algorithm		SHA 256 RSA
issuer		DN of the CA issuing the certificate
validity	**notBefore**	Certificate validity start date and time, UTC time
	notAfter	Date and time of end of validity of the certificate, UTC time
subject		DN of the certificate holder
subjectPublicKeyInfo		algorithm parameters and public key value
Identificador de la clave en la entidad emisora		Identifier of the key in the issuing entity
Identificador de clave del titular		Holder key identifier
Puntos de distribución CRL		La url de la CRL
Acceso a la información de la entidad emisora		[1]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=https://ocsp.olimpiait.com/api/ocsp [2]Acceso a información de autoridad Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://crt.olimpiait.com/olimpiaitroot.crt
Restricciones básicas		Tipo de asunto=Entidad de certificación (CA) Restricción de longitud de ruta=Ninguno
Uso de la clave		Sin repudio, Firma de certificados, Firma CRL sin conexión, Firma de lista de revocación de certificados (CRL) (46 00)
Huella digital		Línea alfanumérica 89ebb74b4b2c

Note: The digital Certificate is generated in CRT format.

2.6.2. SUBORDINATE CA:

Certification authority of second level, or more levels.

2.6.2.1. THE CONTENT OF THE SUBODINATE CA CERTIFICATE IS:

Certificate field		Worth
version		v3
serialNumber		Unique positive integer with respect to the CA issuing the certificate
signature		Signature Algorithm Parameters
signature algorithm		SHA 256 RSA
issuer		DN of the CA issuing the certificate
validity	**notBefore**	Certificate validity start date and time, UTC tim
	notAfter	Date and time of end of validity of the certificate, UTC time
subject		DN del titular del certificado
subjectPublicKeyInfo		parámetros del algoritmo y valor de la clave pública
Identificador de la clave en la entidad emisora		Identificador de la clave en la entidad emisora
Identificador de clave del titular		Identificador de clave del titular
Puntos de distribución CRL		La url de la CRL
Acceso a la información de la entidad emisora		[1]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=https://ocsp.olimpiait.com/api/ocsp [2]Acceso a información de autoridad Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://crt.olimpiait.com/olimpiaitroot.crt

Certificate field	Worth
Restricciones básicas	Tipo de asunto=Entidad de certificación (CA) Restricción de longitud de ruta=Ninguno
Uso de la clave	Sin repudio, Firma de certificados, Firma CRL sin conexión, Firma de lista de revocación de certificados (CRL) (46 00)
Huella digital	Línea alfanumérica 89ebb74b4b2c

2.6.2.2. THE CONTENT OF THE SUBSCRIBER´S CERTIFICATE IS:

Certificate field		Worth	Certificate field
version		Nº de versión	v3
serialNumber		Nº de serie	Unique positive integer with respect to the CA issuing the certificate
signature		signature algorithm	OID and signature algorithm parameters
signature algorithm		signature algorithm	cryptographic hash functions
issuer		Issuer (DN)	DN of the CA issuing the certificate
validity	**notBefore**	Valid from	Certificate validity start date and time, UTC time
	notAfter	valid until	Date and time of end of validity of the certificate, UTC time
subjectPublicKeyInfo		public key	algorithm parameters and public key value
Parámetros de clave pública			05 00
Key identifier at the issuing		**Key identifier at the issuing**	Id. de clave=eeb5ba8bc455b5b7b1f773f32079f3feab67a85e
holder key identifier		holder key identifier	holder key identifier
Basic Constraints		End entity - none	Tipo de asunto=Entidad final Restricción de longitud de ruta=Ninguno
certificate policies		certificate policies	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.50890.2.1.7.3 [1,1]Información de certificador de directiva:

Certificate field	Worth	Certificate field
		Id. de certificador de directiva=CPS Certificador: https://micertificado.olimpiait.com/recursos/archivos/declaraciondepracticasdecertificacion.pdf
Alternative name of the issuer	ONAC accreditation code	Nombre DNS=21-ECD-001
CRL distribution points Validation	points of revoked certificates	La url de la CRL
Access to the information of the issuing	Entity data	[1]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=https://ocspecd.olimpiait.com:8372 [2]Acceso a información de autoridad Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://crt.olimpiait.com/olimpiaitroot.crt
Basic Constraints	Certification Authority (CA)	Tipo de asunto= Entidad de certificación (CA) Restricción de longitud de ruta=Ninguno
Key Usage Purposes	for which the certificate should be used.	Sin repudio, Firma de certificados, Firma CRL sin conexión, Firma de lista de revocación de certificados (CRL) (46 00)
Fingerprint	The synthesis or fingerprint of the certificate data	Línea alfanumérica 89ebb74b4b2c

Note: Olimpia IT declares that the subscriber's digital certificates contain the information required by article 35 of Law 527 of 1999 and that it is described below:

i. Name, address, and domicile of the subscriber.

ii. Identification of the subscriber named in the certificate.

iii. The name, address, and place where the certification body performs activities.

iv. The user's public key.

v. The methodology to verify the subscriber's digital signature imposed on the data message.

vi. The serial number of the certificate.

vii. Date of issue and expiration of the certificate.

2.6.3. TIME STAMP AUTHORITY

It guarantees the integrity of a moment (date and time), with the imposition of a digital signature on said data message, by which Olimpia IT gives certainty that said time stamp is a reliable data message, which has not been altered since its creation. The date and time are taken from the National Institute of Metrology (INM).

2.6.3.1. THE DATA STRUCTURE OF THE SUBORDINATE TSA IS:

- Signature algorithm
- Hash signature algorithm
- Issuer
- Valid since
- Valid until

- Subject
- Public key
- Public key parameters
- Holder's Key Identifier
- Certificate directives
- Basic restrictions
- Key Usage
- Improved key usage
- Identification algorithm
- Fingerprint

2.6.4. PARTICIPANTS

2.6.4.1. SUBSCRIBER:

It is that person, natural or legal, which appears as the owner of the digital certificate issued by Olimpia IT, as established in the PC established for each certificate.

2.6.4.2. RELYING PARTIES

Person or organization that receives, makes use, or trusts in any way the digital certificates issued by Olimpia IT and that is therefore legally bound by virtue of the terms of this CPS.

2.6.4.3. REGISTRATION AUTHORITY (RA)

The registration authority designated by Olimpia IT is in charge of receiving applications, identity validation, approval, rejection of emission requests, and communication with the subscriber as established by current

Colombian regulations.

2.6.4.4. CERTIFICATION AUTHORITY

The certification authority designated by Olimpia IT is responsible for making the decision regarding the issuance of digital certificates and/or associated services, as well as the generation of digital certificates, both for Olimpia IT and for subscribers.

2.6.4.5. PKI STUCTURE

Combination of hardware, software, security policies and procedures, which allow the execution with guarantees of cryptographic operations such as encryption, digital signature, and non-rejection of electronic transactions.

PKI components:

i. Certification authority (CA)
ii. Registration Authority (RA)
iii. Time Stamping Authority (TSA)
iv. Applicants and subscribers
v. Relying Parties
vi. Information repositories

2.7. PERMITTED USES FOR DIGITAL CERTIFICATES

The certificates may be used as stipulated in this CPS and the respective PC. The Key Usage and Extended Key Usage extensions may be used to establish technical limits to the use of the private key of the corresponding certificate. The root digital certificate can only be used for the identification of the root certification authority itself and for the distribution of its public key in a secure manner. The use of the certificates issued by the root CA will be limited to the signing of digital certificates and the signing of the

corresponding certificate revocation lists.

2.7.1. OLIMPIA IT RULES FOR DIGITAL CERTIFICATES ISSUED

a) The permitted uses for the Digital Certificate issued by Olimpia IT will be those stipulated in this CPS. Any different use given to the Digital Certificate will be considered a fair revocation of it and the termination of the business relationship with the subscriber.

b) The use of the digital certificate and the data messages that are digitally signed are the responsibility of the subscriber, therefore, Olimpia IT, in its capacity as ECD, is exempt from any responsibility regarding the verification or certifying function that the data messages digitally signed by the subscriber may contain.

c) In their condition of accepting the digital certificate, the relying parties must:

- Verify the suitability of the digital certificate that is in use by the subscriber through the means exposed by Olimpia IT, likewise Olimpia IT in its capacity as Digital Certification Entity (ECD) will review the other information that is subject to validation and that may be arranged by Olimpia IT.

- Relying parties should consult the lists of revoked certificates provided by Olimpia IT on its website.

Subscribers and relying parties accept and acknowledge that the use of the subscriber's public key is understood as an appropriate technological resource to encrypt or encipher data messages, with the purpose that only the holder of a private key is responsible for its custody. In the same way, the subscriber declares to know that in case of loss of the same, it will cause the impossibility to recover the encrypted or enciphered data

message. Due to the foregoing, Olimpia IT assumes no responsibility for this fact, and the parties involved (subscriber and relying parties) acknowledge this situation. Once the subscriber verifies that part of the information in the digital certificate has lost its validity or effectiveness, they must request the renewal of their certificate.

d) The storage of the certificates regardless of the state in which it is found will be performed by Olimpia IT indefinitely.

e) The use of digital certificates will be predetermined to fulfill the following purposes:

- Non-rejection: It is that virtue emanated from the law and deposited in a Digital Certification Entity to determine the impossibility for a subscriber to subtract from the recognition of the acts that he has digitally signed with his digital certificate.

- Integrity: is that virtue emanating from the law and deposited in a Digital Certification Entity so that a relying third party in the digital certificate has the legal certainty that the data message digitally signed by the subscriber at the time of receipt has not been altered or modified in such a way that its content corresponds to that initially sent.

- Identification: Procedure by means of which it is recognized that a natural or legal person is who they really claim to be, through an authentication process before a computerized process and that this person acts in their capacity as signatory with respect to the digital certificate issued.

- Confidentiality: In order to avoid unauthorized intervention or intrusion of the data message, the subscriber's public key may be used to

encrypt the data messages and guarantee their sending in a confidential manner, as long as the encryption or information encryption techniques correspond to those endorsed for a digital certification system adopted by Colombia or by international agreementspublic or private signed by Colombia or the Digital Certification Entity.

By virtue of the foregoing, the public or private agreement that has been signed between digital certification entities exempts Olimpia IT from liability for this encryption or ciphering activity. For this, Olimpia IT ensures that the security of the subscriber's private key complies with the parameters required by ONAC. Olimpia IT is not responsible, has no interference, nor the ability to recover the encrypted data that, due to the loss of the private key by the subscriber, cannot be decrypted or deciphered.

f) The additional obligations between Olimpia IT and the subscriber and/or the relying parties will be the subscriber's exclusive responsibility, however, said obligations must be previously informed to the parties involved or affected by said obligations.

2.7.2. PERMITTED USES AND RESTRICTIONS

2.7.2.1. REQUEST FOR MULTIPLE CERTIFICATES

The subscriber can make a new request for a certificate (with a physical token), even when they already have a type of certificate of the same nature as the one, they are requesting.

2.7.2.2. ISSUANCE OF CERTIFICATES TO DIFFERENT SERVICES

For services that use a centralized signature and digital certificate Natural Person, Legal Person, or Public Function: Olimpia IT will issue a maximum of one type of certificate per service.

2.7.2.3. MULTIPLICITY OF POSITIONS OR FUNCTIONS

For services that use a centralized signature and type of Professional degree certificate and Belonging to a company: When the subscriber has multiple positions, professions and/or legal representations, may have a maximum of one certificate for each function, profession or legal representation exercised.

2.7.3. IMPROPER USE OF DIGITAL CERTIFICATES

a) The use of digital certificates by the subscriber, the third parties involved or whoever holds the quality of digital holder for the realization, planning, agreement, or other type of activities aimed at the execution of any activity considered as illicit is prohibited by Colombian legislation, by the international agreements that Colombia signs, by supranational standards, or by the standards of third countries where the digital certificate issued by Olimpia IT can be verified or used, or that contravenes good customs, healthy practices and all standards contained in this Certification Practices Statement.

b) Likewise, the use of the digital certification system and the use of digital certificates is prohibited in activities related to control systems for high-risk activities or for error-proof systems, not limited to the following:

- Land, air, or sea transport navigation systems.
- Air traffic control systems.
- Weapons control systems.

Olimpia IT, may at any time define mechanisms, policies, processes, or procedures aimed at establishing new high-risk activities and inform them in accordance with what is required by law and regulations to the general public.

c) The use of digital certificates is limited to the execution of activities that

are not directly or indirectly related to computer systems that may cause, by action or omission, the death or injury of persons or cause harm to the environment.

d) When it has been agreed with the subscriber that the subscriber's private key will be stored on a physical medium guarded by the subscriber, this device may only be used in activities with direct reference to the Digital Certification Computer System. Information other than that expressly authorized by Olimpia IT may not be incorporated into the physical support provided by Olimpia IT, nor used outside the Digital Certification Computer System.

2.7.4. RESTRICTION TO SIGN DOCUMENTS

The signing of document types *.pdf, protected by a modification password, can only be done from the application in a web environment and in *.p7z format.
Clarify that the installers or drivers required for the physical token usage are not compatible with macOS operating systems, within numbers 2.7.4, 20.1 and 26.1.

2.8. MANAGEMENT POLICIES

2.8.1. OLIMPIA IT ADMINSITRATIVE ORGANIZATION

Name: Olimpia IT SAS

Email:servicioalcliente@olimpiait.com/ notificaciones.gerencia@olimpiait.com

Commercial and judicial notifications address: Cra. 7 #24-89, Torre Colpatria, Piso 46.

2.8.2. CONTACT PERSON

Role of ECD management: July Alexandra Medina Zoa

Email: notificaciones.gerencia@olimpiait.com

Address: Cra. 7 #24-89, Torre Colpatria, Piso 46, Bogotá (Colombia).

Phone number: (+57 601) 742 7878

3. INFORMATION REPOSITORIES OF THE DIGITAL CERTIFICATION ENTITY

3.1. REPOSITORIES

Olimpia IT guarantees the availability of the information in its repository in accordance with the availability levels required by ONAC and contained in the legal and technical regulations applied to this item, this repository contains information on the Root CA Certificates, Subordinate CA and list of certificates revoked CRL, in case of interruption due to force majeure, the service will be restored in the times established by Olimpia IT.

3.1.1. INFORMATION ON ECD CERTIFICATES AND REVOKED CERTIFICATES

On the web page https://micertificado.olimpiait.com , the status of the certificate can be consulted through OCSP, in the "Validations" link, " Validate signature" button, attaching the p7z type file, from the location where it is saved and by clicking on the "validate signature" button at the bottom; and the consultation list of revoked certificates through CRL, in the link "Validations" button. Status of the certificate (OCSP)" attaching the certificate and clicking on the "search" button at the bottom

3.2. INFORMATION PUBLICATION

- The "Chief Legal Officer" is responsible for reviewing the CPS together with the work team that may require it.
- The Policy Committee has the authority to approve this document.

- The Senior Management of the ECD is responsible for publishing this document to the public.
- The following information will be available on the website https://micertificado.olimpiait.com

In the Validations menu

- The Certificate Revoked List (CRL) on the button
- olimpiaitroot.crl
- olimpiaitecdsub.crl
- Certificate Status (OCSP)
- Validate Signature "In this module you can validate and detail the Digital Signature of files in p7z format"
- Subscriber Certificates "In this module you can consult and download the current certificates of the subscribers."
- CA certificates
- Root certificates olimpiaitroot
- OlimpiaIT ECD Sub Subordinate Certificates
- Olimpiaitecdtsa TSA certificates
- In the Legal Framework menu
- Certification Practice Statement
- Certificate Policies
- Data protection policy
- Integrated Management System Policy
- Impartiality, Non-Discrimination and Independence Policy
- ECD Liability Consent
- Olimpia IT civil liability policy
- Certificate of existence and legal representation DataCenter
- Certificate of existence and legal representation Olimpia IT
- Authorization for the processing of personal data”

The Policy Committee has the authority to approve this document through

the format designated for it.

3.3. UPDATE FREQUENCY OF THE INFORMATION CONTAINED IN THE DIGITAL CERTIFICATES

3.3.1. CERTIFICATES ISSUED BY THE ROOT CA OF OLIMPIA IT

The certificate will be published prior to its entry into force through the Olimpia IT website and will be updated whenever required.

3.3.1.1. PROCEDURE FOR UPDATING THE INFORMATION CONTAINDED IN THE CERTIFICATES

To update the information on the certificates, Olimpia IT will issue a new certificate, following the issuance rules for a new digital certificate described both in this DPC and in the PC and in compliance with the Personal Data Protection Policy.

The validity of the new certificate will be subject to those described in numeral 19 of this CPS.

3.3.2. CRL – CERTIFICATE REVOCATION LIST

The CRL must be updated automatically before the "next update" date informed in the CRL without revocation or when a revocation is made, as follows:

- The effective date of the CRL is updated once the review is made for the date and time of the next update and no revocations have been made.

- The effective date is updated when generating the CRL after any revocation.

- The next CRL update date is always 24 hours after the effective date.

3.3.3. CERTIFICATE STATUS CKECK PROTOCOL (OCSP)

Certificates are updated on the Olimpia IT website.

3.3.4. CPS (Certification Practices Statement):

The CPS is published on the website https://micertificado.olimpiait.com , in the "Docuentación" section, “Certification Practices Statement” link, it is updated as established by Olimpia IT with due approval of the Policy Committee.

The updating processes will be informed to ONAC, when necessary. ONAC will be informed of all changes in the platform of digital certification services related to the scope of accreditation, in particular ONAC will be informed of the changes in relation to: 1. the legal status in relation ownership; 2. organization and management (e.g. key personnel); 3. Olimpia IT facilities and other resources, where relevant; 4. regulatory documents specified in the scope of accreditation, when these are not technical regulations or national or international technical standards; 5. any other fundamental change that occurs in the initial conditions under which accreditation is granted.

3.4. ACCESS CONTROL TO STORED INFORMATION

The access control to the information contained in the repositories is limited to any natural or legal person who wishes to consult the information which Olimpia IT establishes as Public.

4. AUTHENTICATION AND IDENTIFICATION OF INFORMATION

4.1. DENOMINATION IN THE NAMES

4.1.1. NAMING STANDARD

Olimpia IT establishes in this document an Identifier Object (OID) and a Distinguished Name (DN) defined for each of the generated certificates and the one supplied by IANA, signed according to the X-509 v3 standard.

4.1.2. NAMES DISTINCTION

Olimpia IT guarantees its subscribers the total identification of it and its generated certificate by assigning a distinctive name (DN).

4.1.3. INTERPRETATION OF NAME FORMATS

The standards used for the interpretation of the nomenclature in the issued certificates are based on the regulation given by the ISO/IEC 9595 (X.500) standard Distinguished Name (DN).

4.1.4. NAMES SINGULARITY

Olimpia IT guarantees through the applicability of its policies and procedures the uniqueness in the names of each certificate generated using the Distinguished Name (DN) system.

4.1.5. NAMING DISPUTE RESOLUTION

Olimpia IT establishes in this Certification Practices Statement the abstinence in conflict resolution regarding the ownership of legal or natural persons.

4.2. SUBSCRIBER IDENTIFICATION PROCEDURES (IDENTITY VALIDATION)

4.2.1. PROOF OF PRIVATE KEY POSSESSION METHOD

When a certificate is issued in the Centralized HSM, the private key is generated in the HSM at the moment prior to the issuance of the certificate, through a procedure that guarantees its confidentiality and its link with the Applicant. When a certificate is issued in Other Devices, the proof method

of possession of the private key will be the delivery to the RA of a certificate request in PKCS #10 format that contains the corresponding public key.

4.2.2. IDENTITY AUTHENTICATION

With the exception of the authentication or validation contemplated in Section 4.2.3 and 4.2.4 of this DPC, Olimpia IT declares that it validates the identity of the people who make the requests for digital certificates against the biographical database managed and produced by the National Registry of Civil Status or the Colombia Migration Administrative Department.

To validate the validity status of the applicant's identity document, Olimpia IT establishes two alternative methods, which are implemented independently depending on the type of service or product requested:

a) The applicant must attach a certificate of citizenship or immigration status, for the services that require it, with which the validity of their identity document will be validated.
b) When the certificate of citizenship card status is not required from the applicant, the validity of their identity document will be validated by consulting the National Identification File of the National Registry of Civil Status (ANI).

The identity authentication methods of the applicants may be complemented with other additional information, either as a result of an agreement or as part of an application; considering the above, Olimpia IT may request information that contains biometric or sociodemographic data of the applicant to authenticate the identity; Said validation will consider the result of the biometric comparison and the authenticity of the biometric or sociodemographic information provided, at the end of this process the RA team makes the recommendation for the issuance or rejection of the request.

Olimpia IT will validate the identity of the applicants, in accordance with the internal digital certificate life cycle document, which consists, in

summary, of applying one of the following methods:

i. Validation by facial recognition: The applicant will be able to capture a face photograph and upload the image of the identity document on both sides.

ii. RA operator call: Demographic questions will be asked to the applicant over the phone to confirm their identity.

iii. Validation of identity by means of a fingerprint document: The applicant may attach a notarized document (which can be a document with a signature by mandate in front of a notary, in the case of not being able or not knowing how to sign) or liability consent available in the certificate application process.

iv. Delegated identity validation through a third party: Validation through a third party delegated by the applicant and who previously carried out the identity authentication of the applicant. The delegate will make the request for the certificate through the website.

Olimpia IT will verify and guarantee that the delegate is carrying out adequate identity validation of the applicants, for which it will execute the following controls with the delegates:

- ECD contract with the third-party delegate: Olimpia IT will sign a contract with the third-party delegate, through which the delegate's obligations will be included regarding: a) carrying out a validation of the applicant's identity, which includes requesting and storing a copy of the ID document (*Cédula de Ciudadanía*), and for legal entities, Certificate of Existence and Legal Representation and RUT; Depending on the type of certificate and its purpose or use, and according to the risk analysis, additional identity validation controls may also be added; b) possibility of the delegate of being audited by Olimpia IT or by any public or certification authority including

ONAC to verify their identity validation obligations, information security, among others; and c) possibility of terminating the contract in case of non-compliance with the identity validation or audit obligations of the delegated third party.

- Audit of the third-party delegate: An annual analysis will be carried out on the third delegate in order to verify that this delegate has the following: a) the documentation that allows verifying the identity of the applicants (ID document - *Cédula de Ciudadanía*, and in the case of legal entities, Certificate of Existence and Legal Representation and RUT) and the additional controls established according to the risk analysis; b) mandate contract or similar concluded with the applicant that contemplates an express authorization of the applicant to submit an application for a digital certificate to a Digital Certification Entity; c) compliance with accepted information security standards; and d) others that are required by the audit.

- Digital certificate of the delegated third party: The delegated third party must acquire a digital certificate from Olimpia IT which will allow them to prove their identity for the delegated request to the ECD.

Olimpia IT reserves the right to request additional documents to those required in the application form when it deems necessary to verify the identity or any applicant quality. Olimpia IT may waive the presentation of any additional document when the applicant's identity has been sufficiently verified by other means.

Olimpia IT may additionally require one, some or more of the following documents when it deems necessary:

- Business references or Personal references or Employment certificates
- Bank certifications

- Valid driver's license
- Certificate of judicial record or valid passport
- Military card
- Document of affiliation to the Social Security System in Health
- Document of affiliation to the Professional Risk Management company or Certificate of appointment and/or possession of a position
- Certifications from inspection, surveillance, and control authorities.
- Other documents that allow verifying the identity or faculties of the subscriber or the entity for the issuance of any of the certificate types issued by Olimpia IT

4.2.3. DELEGATED IDENTITY VALIDATION CARRIED OUT BY ENTITTIES IN THE PUBLIC SERVICE SECTOR THROUGH AN AGREEMENT

This method will be admitted, provided that an entity of the Public Service Sector (according to article 2.1.1.1 of Decreto 1083 de 2015, *Decreto Único Reglamentario del Sector de Función Pública*) has previously carried out an identity authentication process of the applicant and Olimpia IT had signed an agreement, contract or alliance with the entity of the Public Service Sector.

The Public Service Sector entity must have authorization for identity validation, which may include the following:

- Is legally or regulatory authorized to carry out the applicant's identity validation process.
- It has a contractual or other type of authorization that allows it to validate the applicant's identity.

Olimpia IT may request certification, written procedures and other documentation that proves the identity authentication carried out by the Public Service Sector entity, if it is considered necessary.

4.2.3.1. IDENTITY VALIDATION CARRIED OUT BY THE DIAN FOR THE FREE ELECTRONIC INVOICING PLATFORM

Olimpia IT will admit the identity validation carried out by DIAN, for the issuance of digital certificates of a natural person or legal entity, intended for signing of documents in the free solution of the DIAN Electronic Billing System. Identity validation will be accepted for registration or updating of the Registro Único Tributario – RUT, according to the legal requirements established in the Estatuto Tributario (Articulo 555-2 and the following) and Decreto 1625 de 2016 or the regulations that modify or add them.

Olimpia IT will accept the identity validation for the issuance of digital certificates in the free platform of the DIAN Electronic Billing System, once the authentication of the applicants is carried out by sending a token to the email registered in the RUT, or through similar or equivalent methodology.

For this identity validation process, and the issuance of digital certificates, Olimpia IT will store one(s) of the following identification numbers of the applicant:

- *Cédula de Ciudadanía*
- *Cédula de Extranjería*
- *NIT*
- *Permiso por Protección Temporal - PPT*
- *Pasaporte*
- *Tarjeta de Identidad (provided that it is allowed by the DIAN in its* free platform of the DIAN Electronic Billing System*)*

4.2.4. PROOF OF PRIVATE KEY POSSESSION METHOD

Through the application of the implemented digital certification system, Olimpia IT performs the control, possession, and issuance of the private key through the use of cryptographic devices certified in FIPS 140 -2 level

3, this is achieved through the PKCS # 11 format.

5.LIFE CYCLE OPERATION OF DIGITAL CERTIFICATES

Olimpia IT defines the states for the issuance of digital certificates, which cannot be valid for more than 2 years and cannot be activated after being expired or revoked.

5.1. APPLICATION FOR ISSUANCE OF DIGITAL CERTIFICATES

Olimpia IT establishes in this document the way to request a digital certificate, through the following means:

- Internet: Through the website of the Digital Certification Entity https://micertificado.olimpiait.com , or through any other web portal that Olimpia IT defines as a sales channel for its digital certification services, provided that said portals are duly integrated to the portal of the Digital Certification Entity.
- The applicant must register on the web portal using the "registrarse" button or through any other portal than Olimpia IT, or through an API duly integrated into the portal of the Digital Certification Entity and enter the information required there:
    - Type of identification
    - Document number
    - Document issue date
- A validation of the information entered will be performed against the Biographical Database of the National Registry of Civil Status, against its own or third-party databases, whether official or private.
- If the information is not valid, the application will report that the information is invalid.

- If the information is valid, the applicant or his delegate, will need to enter the following information:

    - Email address
    - Cell phone number and its confirmation.
    - Read and accept the terms and conditions of use

- The subscriber or who his delegate will receive a message to his email, in which the activation of his account will be requested through a link contained in the same email.
- The subscriber must log in to the web portal https://micertificado.olimpiait.com, on the “ingresar” button and submitting the information:

    - Type of identity document
    - Number of identity document

- An OTP (One Time Password) consisting of a 4-digit single-use code will be sent to the cell phone number registered by the applicant, so that the applicant can enter it in the space provided for it, at the bottom of the login window in order to generate an authentication before the portal.

- Once the authentication is effective, the web portal will inform the applicant who is already in his private account, the applicant may request digital certificates from the "Certificates" or "Services" link from the "Services" link.

- When the service is requested by a minor, their identity will be ensured with the authenticated identity document (tarjeta de identidad) and a document that supports the link between the applicant and the

minor (when this link is required according to the regulations)..

- Olimpia IT reserves the right to issue certificates when, in its opinion, the credibility, commercial value or legal or moral suitability of the Digital Certification Entity may be put at risk.

Note: The website of the Digital Certification Entity may be displayed in Chrome browsers in its version 71.0.3578.98 and Microsoft EDGE version 38.14393.2068.0. The use of any other browser may cause problems with the portal use, the request for certificates or services.

- By phone: By contacting the customer service line (+57 601) 742 7878, where the operator will send the applicant to register on the website https://micertificado.olimpiait.com, described in the previous item.

a) The applicant may check the status of his application on the website https://micertificado.olimpiait.com. If the user complies with the requested documentation and with the established requirements, Olimpia IT will proceed to issue the certificate within a maximum period of 2 business days, counted from the certification decision to accept the request, and without counting the time that the applicant delays in responding to requests for correction of information, if applicable.

Note: When the certificate is issued in Token, the time it takes for delivery must be added to the 2 days of issuance, which will depend on the place where the subscriber resides.

b) Applications are registered from the website https://micertificado.olimpiait.com .

c) Olimpia IT has the power to request clarification of the information or documentation provided in the event that the information or

documentation cannot be clarified, the certification decision by the CA will be to reject the request.

d) All documentation provided by the applicant must be stored safely following the standards established by Olimpia IT under the certifications of NTC-ISO/IEC ISO 9001 and NTC-ISO/IEC 27001 in its current version.

5.1.1. MAKING THE REQUEST

The applicant satisfactorily registers on the website https://micertificado.olimpiait.com and makes a request for a certificate or service.

The applicant selects a certificate or service option on the website https://micertificado.olimpiait.com, in one of the two tabs that contain the certificates or services that Olimpia IT issues or provides.

The following is a representative list of the steps that the applicant must follow. According to each type of product or service requested, a different order can be established in the steps described here:

a) The applicant clicks on the purchase button of the certificate or service they wish to purchase.
b) The applicant accepts the terms and conditions in order to continue with the application.
c) The applicant fills out the information requested by the web portal
d) The applicant attaches the documentation requested by the web portal
e) The applicant fills out the information if he requires the service with a physical token

f) Select the validity of the certificate you want (maximum 2 years)
g) Select the start date of the validity (Optional)
h) The applicant indicates the package he wishes to acquire
i) The applicant generates the payment indicating the package he wishes to acquire
j) The applicant attaches the proof of payment in a file, in the formats allowed for uploading documents
    - If the applicant made the payment online, the application would take the payment made and continue with the certificate activation step.
k) Olimpia IT performs an automatic or manual validation of the payment, contrasting the request reference with the bank record, and stores the record or evidence of the validation performed.

Note: The effective date of the certificate may not be less than the current date, if the effective date is not selected, by default the effective date will be the date of issuance of the certificate, the effective date may not be greater than 30 days.

5.1.2. APPLICATION REVIEW AND CERTIFIFCATION DECISION

5.1.2.1. APPLICATION REVIEW

The RA will review the certificate request submitted in accordance with the procedure established for this within the ECD.

The RA will send the review of the request to the CA Operator, who will review it and decide on the certification.

5.1.2.2. CERTIFICATION DECISION

The CA operator, once the RA has reviewed the application, will make the

certification decision, in accordance with the procedure established for it within the ECD.

If the certification decision is to reject the application, the applicant will be informed of this decision by email.

The RA only processes applications that are within the scope of the accreditation granted by ONAC.

5.1.3. PEOPLE WHO CAN APPLY FOR A CERTIFICATE

The people who can request a digital certificate are those natural persons or legal representatives of national or foreign legal entities who are of legal age under Colombian law (Applies to natural persons) who reside in Colombian territory and have an activated email.

5.1.4. REGISTRATION PROCESS

The registration process for requesting a digital certificate is performed through the Digital Certification Entity website, the responsibilities are accepted by the applicant when they accept the agreement of terms and conditions and the acceptance of the DPC.

5.2. CERTIFICATE REQUEST PROCESSING

5.2.1. PERFORM IDENTIFICATION AND AUTHENTICATION FUNCTIONS

The request processing is done from the application, separating the RA (Registration Authority) and CA (Certificate Authority) by means of permissions and responsibilities, authenticating the requesters by means of the demographic data requested, and supports the restrictions implemented by Olimpia IT for identity validation.

5.2.2. APPROVAL OR REJECTION OF CERTIFICATE REQUEST

Once the corresponding validations have been performed as specified in the ECD management system operating procedures, the Operator of the CA with the review performed by the RA and its complementary reviews approves or rejects requests made by the applicants. If Olimpia IT decides to reject the request to issue the digital signature certificate, it will notify the applicant by email indicating the reasons that justify this decision.

The reasons for rejection can be, among others, the following:

- Documentation not corresponding to the certificate applicant
- False information and/or documentation
- Incomplete documentation
- Reputational danger for the company
- Incomplete documentation
- Others

Before the requests are rejected, the RA, through the digital channel of Olimpia, or the area acting in its place, will inform the applicant about the documentary or registry inconsistency, as well as the impossibility of providing the service, if the requested service is found outside the scope of the accreditation granted.

5.2.3. TIME TO PROCESS CERTIFIFCATE REQUEST

The times established by Olimpia IT to generate the certificate is a maximum of two (2) business days from the completion of the request, without counting the time that the applicant takes to respond to requests for information correction, if applicable.

5.3. PROCEDURE FOR THE ISSUANCE OF DIGITAL CERTIFICATE

Request by the applicant for a digital certificate or service offered by the ECD. It begins with the registration of the applicant in the web portal https://micertificado.olimpiait.com, described in number 5.1 of this CPS and

ends with the generation of the certificate, and delivery of the digital signature to the subscriber or provision of the requested service.

5.3.1. REGISTRATION AUTHORITY ACTIVITIES (RA)

The security control of the RA (in the physical and logical environment) is performed through the process where the RA identifies itself to the CA through the use of a digital certificate.

The RA has the role of ensuring that:

a) The review of the request must ensure the unequivocal identification of the subscriber's identity (natural or legal person), the veracity and authenticity of the information, which allows giving a recommendation for decision making.
b) The ECD must maintain records of the identity validation processes to demonstrate effective compliance with the subscriber's unambiguous identification and allow an evaluation of said records.
c) Any known differences in understanding between the ECD and the applicant are resolved, including the agreement regarding the DPC, normative documents, or other regulatory documents.
d) The scope of the requested digital certification service is defined.
e) The means to perform all verification activities are available.
f) The ECD has the competence and capacity to perform digital certification activities and services.
g) The ECD must decline a request for a digital certification service, if it is not within the scope of the accreditation granted by ONAC.
h) The ECD must document the processes and outcomes related to the application review, including the recommendation for the certification decision based on the review.
i) The RA carries out the documentary and identity validations of the different requests and issues a recommendation where the issuance or non-issuance of the certificate is defined. This request is

digitally signed so that the CA generates the certificate.

5.3.1.1. APPLICATION REVIEW

The procedure for the issuance of digital certificates involves the validation of the identity and the quality in which the applicant acts by the RA.

The RA will validate the applicant's identity in accordance with the provisions of this CPS in Numeral 4.2.

The RA will validate the quality in which the applicant requests the service to be granted in the following way:

a) If it is a Natural person with what is established in Numeral 4.2 of this DPC, and when applicable, with the information that rests in the Single Tax Registry (RUT) and the documents and procedures established in the Certificate Policy or any document that allows the quality and identification of the subscriber to be reliably validated.
b) If it is a legal person, with the information that rests in the certificate of existence and legal representation of the Chamber of Commerce (of the domicile of the legal person), or with the information that rests on the Tax Registry (RUT), and the other documents and internal procedures determined by Olimpia IT in the Certificate Policy, or any document that allows the quality and identification of the subscriber to be reliably validated.
c) If he is a certified professional, with the entity that issued the title that accredits the applicant, or the official database that has been determined for it and by the internal procedures that Olimpia IT determines for it.
d) If he belongs to a company, with the entity that certifies that the applicant has the quality requested in the employee or contractor certificate and by the internal procedures determined by Olimpia IT for it, or any document that allows the quality and identification of

the subscriber to be reliably validated.

e) If it is a public function, with the entity's information that granted the public function or administrative act of its appointment and by the internal procedures that Olimpia IT determines for it, or any document that allows the quality and identification of the subscriber to be reliably validated.

f) If he is a legal representative, with the information that rests on the company in the Chamber of Commerce of the company's domicile and by the internal procedures determined by Olimpia IT for it, or any document that allows the quality and identification of the subscriber to be reliably validated.

Whenever it deems appropriate, the RA operator may request the correction of the information initially provided by the applicant in his application, necessary for the correct validation and approval of the product or service. The time that the applicant takes to respond to the rectification requests will not be counted within the maximum delivery period, which Olimpia IT has established for its services.

The RA communicates with the CA based on annotations made at each review of each request that the RA sends to the CA, along with the recommendation to issue a digital certificate.

5.3.2. CERTIFICATION DECISION

Once the review described above has been received, the CA Operator will make the certification decision to accept or reject the request.

The decision will be notified in accordance with the provisions of Numeral 5.1.2 . of this CPD.

5.3.3. CERTIFIFCATE ISSUANCE REQUEST

The internal portal will notify the CA of the request for the Digital Certificate

issuance, which will proceed in accordance with the procedure established for it.

5.3.4. CERTIFIFCATE ISSUANCE

The subordinate CA of Olimpia IT will generate the Digital Certificate.

5.3.5. WAY OF USE

The subscriber's digital signature must be used from a FIPS 140-2 level 3 certified HSM (Hardware Secure Module) device.

5.3.6. TOKEN DELIVERY TO SUBSCRIBER

In the event that the request requires the delivery of the digital signature in a physical token, the CA operator will store the digital signature of the requested certificate in a FIPS 140 -2 level 3 certified HSM (Hardware Secure Module) device, which will be stored in a security bag and delivered by a contracted courier company.

Note: For services through virtual tokens, these have the same operation as the centralized signature.

5.3.7. ACTIVITIES OF THE CERTIFIFCATION AUTHORITY FOR THE CERTIFIFCATE ISSUANCE

The actions of the CA (Certification Authority) are performed after realizing the corresponding validations by the RA (Registration Authority) and are limited to:

- Generation of certificates in a secure way (in a physical and logical environment), authenticating administrators and operators with a double biometric authentication factor such as physical access control and username and password for logical access control.
- Safe storage of the private key.

5.3.8. NOTICE TO APPLICANT

Olimpia IT notifies applicants regarding the granting of the digital certification service, by sending an email to the email address specified in the registration

Once the Digital Certification Service is approved, the subscriber will receive an approval notification with a formal Document containing the following information:
a) The name and address of the ECD;
b) The date on which the digital certification is granted (this date must not be earlier than the date on which the decision on digital certification was made);
c) The name and address of the subscriber;
d) The scope of digital certification;
e) The term or expiration date of the digital certification;
f) All other information required for the certification service.

For certificates issued by means of a physical or virtual token, the subscriber is notified via email of the generation of a 4-digit pin randomly and indicating that he must generate the change by using the "Driver token" published on the web page of my certificate in the “Documentación” section.

If the subscriber does not receive the notification of approval together with the formal document by email, the suscriber may request that this information be sent by contacting Olimpia IT through its designated communication channels (see Section 2.3.3).

Note: The formal documentation of the digital certification services must comply with the provisions of the “Regulations for the use of symbols of the Associate” (*Reglamento de uso de los símbolos de Acreditado y/o Asociado*) issued by ONAC, that is currently in force.

5.4. ACCEPTANCE OF THE DIGITAL CERTIFICATE

5.4.1. CONDUCT CONSTITUTING ACCEPTANCE OF THE DIGITAL CERTIFIFCATE

Olimpia IT, in its capacity as Digital Certification Entity, establishes that the digital certificate generated by the trust hierarchy established in Olimpia IT is considered accepted, at two levels from the Root CA to the Sub CA, when the applicant or subscriber receives the generation notification of his certificate via email.

Unless agreed between the parties, it is understood that a subscriber has accepted a certificate when the certification entity, at the request of the subscriber or of a person on his behalf, has saved said certificate in a repository.

5.4.2. PUBLICATION OF THE DIGITAL CERTIFIFCATE´S STATUS

Olimpia IT publishes the digital certificates status issued on the website of the Digital Certification Entity https://micertificado.olimpiait.com, which can be consulted by anyone.

5.5. CONDITIONS OF USE OF THE DIGITAL CERTIFICATE AND THE GENERATED KEY

The responsibility of Olimpia IT for the use of the certificate is established in the provisions of the corresponding Colombian regulations.

5.5.1. PRIVATE KEY USAGE

Olimpia IT establishes in this Certification Practices Statement the use of private keys by subscribers who own the key, as long as an effective use is made of any of the services or certificates exposed by the Digital Certification Entity.

5.5.2. PUBLIC KEY USAGE

The use of the digital certificates public key issued by Olimpia IT is of public reliability, in which the user must previously validate the certificate status in the service portal of the Digital Certification Entity in which the validity of

the exposed public key is obtained.

5.6. DIGITAL CERTIFICATE RENOVATION

It is established in this Certification Practices Statement that under no circumstances will the renewal of a digital certificate be performed, it is understood that a subscriber requests the renewal of a certificate when it has expired or is about to expire, for this reason it is necessary to make a new request meeting the requirements established by the ECD at the new requested time.
Likewise, the suspension of certificates that do not lead to an immediate revocation status is not allowed. In this sense, Olimpia IT does not suspend certificates.

5.7. CERTIFICATES MODIFICATION

Olimpia IT establishes in this Certification Practices Statement that no modifications can be made to the digital certificates generated, if any modification is required, it is necessary to revoke the certificate and issue a new one.

5.8. REVOCATION OF DIGITAL CERTIFICATES AND GROUNDS FOR REVOCATION

5.8.1. REVOCATION

Olimpia IT will perform the revocation of digital certificates for one of the following reasons:

5.8.2. REVOCATION CAUSES

i. Security compromise in any reason, mode, situation, or circumstance.
ii. Death or disability of the subscriber.
iii. Liquidation of the represented legal entity that appears in the digital certificate
iv. Confirmation that some information in the digital certificate is false.

v. Due to the occurrence of new facts that cause the original data not to correspond to reality.
vi. Court order or competent administrative entity.
vii. Loss, disablement of the digital certificate that has been reported to the ECD.
viii. Termination of the subscription contract, in accordance with the grounds established in the contract.
ix. For any reason that reasonably calls into question the reliability of the digital certificate.
x. Due to breach of the Digital Certification Service Contract provided by the ECD to the subscriber or the legal person.
xi. Due to loss of key assigned by the subscriber.
xii. Due to improper handling by the subscriber of the digital certificate.
xiii. Misuse (blocking) the certificate.
xiv. Others

5.8.3. REVOCATION REQUEST (PERSONS WHO INVOKE THE GROUNDS FOR REVOCATION OF THE CERTIFIFCATES)

The request for revocation of a certificate can be requested by:

a) The Subscriber and/or Applicant, who must request the revocation of the certificate in case of becoming aware of any of the established circumstances or causes for revocation.
b) Any person or entity may request the revocation of a certificate or certificates in case of becoming aware of any of the established circumstances or causes for revocation.
c) Collaborators authorized by Olimpia IT

The subscriber must consider that he will not be able to request the revocation of a digital certificate, when said certificate has not entered into force.

5.8.3.1. PURSUANT TO A COURT OR ADMINISTRATIVE ORDER

In compliance with a judicial or administrative order issued by a competent official, any digital certificate may be revoked.

5.8.3.2. PURSUANT TO AN AGREEMENT

Entities in the Public Service Sector with agreements can request the revocation of certificates processed under the agreement by using web services or by sending a request email indicating the causes or reasons for the revocation.

5.8.4. REVOCATION PROCESS OF DIGITAL CERTIFIFCATES AND VERIFICATIONS OF THE REVOCATION REQUEST

The revocation process of a digital certificate may be initiated informally by Olimpia IT, provided that said revocation precedes a just legal, contractual cause, or that is found in this Certification Practices Statement.

The procedure for revoking certificates is called "Certificate Revocation" and lists the following activities to be deployed:

a) Request for revocation

b) Subscriber Identity Validation

c) Application Validation

d) Revoke certificate

e) Records

In the revocation of the certificate, a communication will be sent by email to the Subscriber.

This procedure details the identity and certificate status verifications that must be performed in order to execute the revocation request.

5.8.4.1. MEANS FOR RECEIVING REVOCATION REQUEST

Olimpia IT enables the revocation of digital Certificates easily and safely like this:

- On the website https://micertificado.olimpiait.com, the subscriber registers with a username and password and indicates which certificate to revoke, he must use the revocation button, select and describe the reason in the comments, once confirmed the request the CA immediately revokes the certificate.

- By telephone (+57 601) 742 7878, the opening hours will be from 8AM to 5PM.

Note: The note is included in Numeral 5.8.4.1. that in the event that a certificate is revoked in relation to digital signatures, it cannot subsequently be rehabilitated by Olimpia IT.

5.8.5. OPPORTUNITY TO INVOKE THE GROUNDS FOR REVOCATION OF CERTIFICATES

The request to revoke a certificate may be made at any time, provided that the certificate is in active status.

5.8.6. CONSEQUECES OR CERTIFIFCATE REVOCATION

Olimpia IT, in order to guarantee the reliability and other legal and technical attributes granted to digital certificates, prior to the revocation or cancellation of a service granted, must verify compliance with any of the grounds for revocation or cancellation called prosper from which are contractually agreed or described in this Certification Practices Statement.

The successful completion of the digital certificate revocation process, giving rise to the digital certificate revocation, does not imply the denial of new services to the subscriber or the revoked or canceled services/certificates, and the subscriber may again request any of the services/ certificates to Olimpia IT under the same technical and legal conditions and for the purposes for which the new service/certificate is required.

Once the digital certificate has been revoked from that moment on, said certificate will not enjoy the reliability attribute granted by law, making it impossible to use this revoked digital certificate for any legal use, including the services for which it was obtained.
As a consequence of the digital certificate revocation, the use of this or its physical or logical components that are provided to the subscriber for the use of said certificate is prohibited.

If the certificate has been revoked by a decision attributable to the Digital Certification Entity, it will have the obligation to issue a new digital certificate with the same conditions and parties involved in the revoked digital certificate, excluding the validity period, which will be for the lack of validity time established for the digital certificate that is revoked.

5.8.7. PUBLICATION OF CERTIFICATE REVOCATION

Olimpia IT undertakes to inform subscribers about the revocation of digital certificates through the communication means agreed and published in the CRL, which can be found on page https://micertificado.olimpiait.com .

The certificate revocation validity will begin when the certificate is published in the CRL, and the private key is destroyed. Olimpia IT must update its CRL
(List of revoked certificates) and publish it according to the times established in this CPS (Declaration of Certification Practices).

Olimpia IT guarantees the retention of digital certificates while Olimpia IT provides services as ECD, after the loss of certificate validity, or its revocation, If necessary.

5.8.8. CRL PUBLICATION FREQUENCY

The CRL publication frequency is determined according to Numeral 3.3.2 of this Certification Practices Statement.

5.8.9. STATUS CHEK AVAILABILITY

The status of the certificates can be consulted online through the CRL use, or the OCSP protocol whose characteristics are specified in Numeral 3.3.2 and 3.3.3 of this Certification Practices Statement, available on page https://micertificado.olimpiait .com

5.9. CERTIFICATES' STATUS

5.9.1. CHARACTERISTICS

The digital certificates' status is found online and the validation of each of the certificates is performed through the implementation of the OCSP protocol (Online Certificate Status Protocol) which allows the subscriber, trusting parties and interested third parties, to know the certificate current status.

5.9.2. AVAILABILITY

The availability of the updating service list of Olimpia IT revoked certificates is aligned with what is required by ONAC, which specifies 99.8% availability per year.

5.10. SERVICE TERMINATION

The termination of the digital certification service occurs in the following cases:

- Revocation of the certificate for any revocation cause.
- End of certificate validity.
- For total consumption of the purchased package.

Once the service has ended, for any of its causes, the preservation of the digital certificates issued will be for a minimum of ten (10) years, counted from the day following the service completion.

5.11. TYPES OF HSM OFFERED

Olimpia IT, offers the subscriber that the use of the private key can be done

from the HSMs housed in the Olimpia IT data centers or in a portable cryptographic device HSM "token" that is delivered to the subscriber and that contains the subscriber's private key, in both cases the cryptographic device is FIPS 140-2 level 3 certified.

The technical characteristics of the device delivered to the subscriber are detailed in the following link: https://csrc.nist.gov/Projects/Cryptographic-Module ValidationProgram/Certificate/2434

- HSM

Protectserver Internal Express 2 (PSI-E2) – Safe net – Inc – Hadware versión VDB – 05 Versión Code 0200 Fimware versión 5.00.02

- Token

ePass2003 Cryptographic Module Feitian Technologies Co., Ltd. Hardware Version: ePass2003-A3 and ePass2003-X15; Firmware Version: 1.0.11

5.12. RISKS AND COMMITMENTS OF THE CRYPTOGRAPHIC DEVICES OFFERED BY OLIMPIA IT

The risks and technical commitments of the cryptographic devices offered by Olimpia IT are listed below, based on the information provided by the manufacturer, and found at the following link: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation- Program/Certificate/2434

The associated risks are:

- Technological obsolescence
- Lack of technical support from the manufacturer or supplier
- Risks outside the manufacturer's security policy

5.13. PAIR OF KEYS CUSTODY

The pair of keys custody generated in the Root CA and the subordinate CA

are stored in the technological infrastructure of Olimpia IT, which contains HSM cryptographic devices, and which can only be accessed through the combination of the keys assigned to custodians of Olympia IT.

The password for the generation of the pair of keys is divided into two parts, each one in charge of a management within Olimpia IT.

The characters of the passwords are in sealed envelopes, which in turn are under the physical security of each management in charge of the password parts custody for generating the Root CA and the CA Subordinate certificates.

6. SECURITY CONTROLS

6.1. PHYSICAL SECURITY CONTROLS

6.1.1. LOCATION AND CONSTRUCTION

All operations related to the Digital Certification Entity are physically protected with a biometric access system which has a 24X7X365 functionality which allows identifying the people who require access to the facilities where the information assets are contained in such a way that guarantees that only authorized personnel can access them. In addition, it has equipment located in the data center equipped with the necessary protections determined by the contractual agreement between the data center and Olimpia IT.

6.1.2. ACCESS CONTROL

The control for physical access to the company's facilities is defined by the internal policies in which security perimeters are established corresponding to the level of confidentiality of the information required, additionally the personnel who enter have access permissions predefined according to the access requirements by profile or position, additionally

the facilities are monitored through CCTV.
Access to the data centers is controlled and performed considering the access control policies and protocols defined by the company.

6.1.3. INFRASTRUCTURE SECURITY

Meeting the ONAC requirements, 99.8% uptime for the PKI and for the CRL, Olimpia IT has the PKI infrastructure implementation in high availability by safeguarding its critical equipment in two data centers which have the controls of physical and logical access security, a continuity plan in the event of an emergency, and periodic maintenance of the internal infrastructure improves the safety of the equipment.

6.1.4. STORAGE SYSTEM

The physical information related to the issuance of digital certificates is securely stored in safes and drawers protected with a key according to the evaluation of the level of importance determined by the owner or asset custodian.

6.1.5. INFORMATION DELETION

Olimpia IT guarantees the optimal elimination of sensitive information through the application of an internal procedure which is based on the recommendations provided by international standards with the generation of evidence of the total destruction of information.

6.1.6. BACKUP STORAGE

The backup copies are stored after generating the private and public keys of the ROOT CA and the SUBORDINATED CA. Once the keys have been generated, the entire cryptographic device is backed up in the "SmartCards" which remain in custody of Olimpia IT.

6.1.7. EXCLUSIVE USE OF CERTIFICATION SYSTEMS

It is established as a security control that the systems that fulfill the certification functions are and will only be used for that purpose and, therefore, do not perform any other function.

6.1.8. DATA CENTER PROTECTION

The data center facilities are built with concrete materials that guarantee protection against brute force attacks, and are located in a low-risk disaster area that allows quick access, has raised floors, detection systems, and fire extinguishing, anti-moisture systems, cooling system and power supply system, the data center has protection against electromagnetic waves.

6.2. PROCEDURAL CONTROLS

6.2.1. TRUST ROLES

Olimpia IT currently has roles and responsibilities related to the processes of issuing digital certificates, which are defined as follows:

The CA Administrator must perform the functions according to his role in the ECD. The CA Operator must perform the functions according to his role in the ECD. The RA Administrator must perform the functions according to his role in the ECD. The RA Operator must perform the functions according to his role in the ECD.
The ECD Senior Management must perform the functions according to their role in the ECD. The PKI Administrator must perform the following functions according to his role in the ECD.

6.2.2. NUMBER OF PEOPLE REQUIRED PER ACTIVITY

It is guaranteed that at least 1 person is available to perform the required task.

6.2.2.1. CONTINUITY

In the event of total or partial absenteeism from the role defined above, it will be taken over by a worker who holds a parallel role and who has a similar profile.

6.2.3. IIDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

The users in charge of each role described in the previous Numerals are authenticated through the Olimpia IT active directory, which has a unique authentication user and a solid key generated under the best industry practices, in addition, the Sensitive information security is limited only to authorized personnel, denying access permissions to the login account.

6.3. PERSONNEL SECURITY CONTROLS

6.3.1. REQUIREMENTS, QUALIFICATIONS AND EXPERIENCE

Olimpia IT guarantees that its employees designated to work in the issuance of digital certificates must possess:

- Minimum development level of soft skills according to the position level.
- Approval of technical tests of performance and knowledge.
- Knowledge in ISMS and GIS.
- Academic title according to the position to be held in the company.
- Selection interview.

6.3.2. BAKGROUND VERIFIFCATION

Olimpia IT establishes in its hiring process the validation of criminal, civil and judicial records of each of its workers, which are validated and accepted.

6.3.3. STAFF TRAINING REQUIREMENTS

Olimpia IT contemplates within its training plan, the training of personnel involved in the process of issuing digital certificates for the correct function development within the company, which includes at least:

- Security of physical and logical information.

- Services provided by the ECD.
- General Concepts of the DPC.
- Basic concepts on incident monitoring and management.
- Legal and disciplinary framework to take into consideration.

6.3.4. FREQUENCY WITH WHICH STAFF TRAINING IS PERFOMED

Olimpia IT annually validates individual or corporate motivational training actions on the previously defined topics in:

- Security aspects of the company including the issuance of digital certificates, Virtual course on information security
- Virtual Course of Customer Service
- Virtual and face-to-face induction

6.3.5. ROTATION FREQUENCY OF RESPONSIBILITIES IN OLIMPIA IT

Olimpia IT currently does not perform rotation in the roles defined for activities execution since these are inherent to the position, although each qualified person, in the training and induction activities associated with a role, has a backup resource in case of absence of the principal associated to the role.

6.3.6. WORKER SANCTIONS

Olimpia IT defines within its Internal Work Regulations the actions to be taken due to suspicion or evidence of unauthorized actions in the tasks implementation for which the employee was hired, these sanctions can range from a call for attention, the resource relocation until the dismissal of the worker involved

6.3.7. DOCUMENTATION PROVIDED TO OLIMPIA IT WORKERS

Olimpia IT has a Quality Management System NTC-ISO/IEC ISO 9001 and Information Security NTC-ISO/IEC 27001 in its current version, which

provides its employees with all the documentation and good practices necessary for the correct performance of their duties. Documentation provided includes the following:

- Certification Practices Statement
- Information Security Policy
- Safety and Health Policy at Work
- Quality Management Policy
- Institutional Organization Chart
- Procedures and characterizations

6.4. SECURITY EVENTS CONTROLS

6.4.1. AUDIT RECORDS (LOGS)

Olimpia IT has technological platforms in order to guarantee the monitoring of transactional and security events according to the service need; In the event of a security incident, the internal procedure will be followed, it includes the review of each event log and the following relative data:

- Date and time of the security incident
- Incident identification by means of an identification number
- Identification of the security incident causes.
- Monitoring and events generation on the critical system components
- Identification of the security incident criticality.
- Reactive and initiative-taking incident response

The logs are reviewed within Olimpia IT, at least once a year.

6.4.2. STORAGE FREQUENCY FOR LOGS

Olimpia IT guarantees the frequency of log storage and the monitoring of information in real time through the use of technological tools for monitoring and recording logs

6.4.3. AUDIT LOGS STORAGE

The audit trail collection system is executed automatically in the application, which complies with what is defined by the surveillance and control entity, the regulatory entity, or a minimum of 3 years.

6.4.4. WARNING OF SECURITY EVENTS

The Olimpia IT monitoring service alerts the CA Administrator regarding the generation of unauthorized activities or records of potentially dangerous events in the infrastructure of the Digital Certification Entity; the CA Administrator must perform the escalation to the corresponding units and execute the internal procedure of Olimpia IT when:

- The private key security has been compromised
- When the security system has been compromised
- When failures occur in the system that compromise the service provision
- When the encryption systems become invalid because they do not offer the security level contracted by the subscriber
- When any other information security event or incident occurs.

6.4.5. VULNERABILITY ANALYSIS

Olimpia IT's cybersecurity team periodically performs a vulnerability analysis of the Digital Certification Entity's critical infrastructure, making the corresponding report regarding the vulnerabilities found during the analysis.

6.5. AUDIT EVENTS RECORD

6.5.1. TYPES OF RECORD STORED

The following parameters are monitored within the cycle of digital certificates:

- Application form
- Record review by the RA
- Decision record by the CA
- Digital certificate generation
- Private key storage
- Notifications to applicants
- Use of the digital certificate or services purchased
- Revocation record
- Destruction of cryptographic keys
- OCSP:
- CRL

For the ROOT CA and Subordinate CA:

- Key generation
- Cryptographic device management (HSM)
- Cryptographic keys storage
- Destruction of cryptographic keys

Monitoring public information:

- Update or modification of the Certification Practices Statement

- Updating or modifying the terms and conditions agreements
- Update or modification of the management system documentation
- Access authorization to information systems.

6.5.2. INFORMATION STORAGE TIME

The information required in the life cycle of the certificates will be kept for the period established by current legislation when applicable.
The storage of transactional and security audit records complies with what is defined by the surveillance and control entity, the regulatory entity or a minimum of 3 years.

6.5.3. INFORMATION PROTECTION

The information security protected by Olimpia IT has restricted access and both physical and logical storage is performed safely following the policies of the Digital Certification Entity in information security.

6.5.4. INFORMATION BACKUP PROCEDURE

The information backup copies are made on the Digital Certification Entity's servers through an automatic synchronization process with servers located in the alternate Datacenter.

6.5.5. AUDIT LOG PROTECTION

The audit records generated by Olimpia IT for the activity's execution as a Digital Certification Entity are protected by physical and logical access through the implementation of biometric devices for physical access to confidential information, the assignment of permissions by the person in charge of the Digital Certification Entity, and monitoring access to audit records.

The verification of the implemented security is performed through the internal and external audit action by competent personnel for this activity

and validated by the Security Officer in order to have the necessary controls to safeguard the audit trails.

6.6. RE-CREATION OF THE ROOT CA KEY

The re-creation of the CA ROOT key is performed through a self-signed process as long as the pair of previously generated keys expires or there is a revocation process for them, Olimpia IT undertakes to perform the Timely alert to the Conformity Assessment Body (ONAC) in order to comply with the provisions of the legal and technical standards and comply with all the security parameters established by the Digital Certification Entity.

6.7. CONTINUITY AND CONTINGENCY

Olimpia IT has established the business continuity plan of the digital certification entity and contingency documents aimed at guaranteeing the certification service continuity.

Where compliance with 95% availability of the PKI and 99.8% of the CRL is established.

6.7.1. SECURITY PROCEDURES FOR HANDLING EVENTS AND INCIDENTS

An internal procedure is established for managing incidents in compliance with Annex A of the NTC-ISO/IEC 27001 standard in its current version, transversal to the organization for the alerting and solution of possible information security incidents in the Digital Certification Entity together with the business continuity plan, if necessary, in which priority is given to the solution of incident alerts; among others there may be:

- Affectation of services availability
- Information alteration of the Digital Certification Entity

- Disclosure of restricted or private information of the Digital Certification Entity

Olimpia IT maintains its commitment to information security in accordance with the General Policy of its Integrated Management System.

6.7.1.1. SECURITY EVENTS TO BE LOGGED

The following events will be considered, among others:

a) When the private key security of the certification entity has been compromised.
b) When the security system of the certification entity has been compromised.
c) When failures occur in the certification entity system that compromise the service provision.
d) When the encryption systems become invalid because they do not offer the security level contracted by the subscriber.
e) When any other information security event or incident occurs.

6.7.2. UNAUTHORIZED CHANGES IN RESORUCES

Olimpia IT has in its business continuity plan the necessary times to recover the integrity of the information altered in its critical infrastructure, which is reviewed and evaluated periodically (at least once a year) in order to validate its effectiveness in possible incidents. In addition, the priority is established for the information of the digital certificates issued, revoked, or expired, as established by the auditing entity.

6.7.3. PROCEDURE BEFORE THE PRIVATE KEY COMPROMISE

When the commitment to the security of the private key is presented, be it from the ROOT CA, Subordinate CA or from the subscribers, Olimpia IT must execute the revocation procedure for the affected certificates, in the case where it is from the ROOT CA or subordinate CA the new key pair must be

issued as specified in this Certification Practice Statement.

Olimpia IT will notify subscribers of the revocation when the private key is compromised

6.7.4. BUSINESS CONTINUITY IN THE EVENT OF A NATURAL DISASTER

Olimpia IT's business continuity plan contemplates safeguarding information in different locations, having a redundancy in the services, provided that the event occurs, in addition, periodic monitoring of the provided services status will be performed.

6.8. COMPLETION OF ACTIVITIES AS A DIGITAL CERTIFICATION ENTITY

In accordance with article 17 of Decree 333 of 2014, the certification entities accredited by the ONAC may cease to perform their activities under the conditions established in article 34 of Law 527 of 1999, modified by article 163 of the Decree-law 19 of 2012 and must inform ONAC.

In the event that Olimpia IT for any reason cease its activities, it must:

- Inform all subscribers through two notices published in newspapers or media with wide national circulation, with an interval of 15 days, about:

  i. The termination of its activity or activities and the precise date of cessation.
  ii. The legal consequences of the cessation with respect to the issued certificates.
  iii. The possibility that a subscriber obtains the reimbursement equivalent to the value of the certificate's remaining term.
  iv. The communication sent to the Superintendence of Industry and Commerce, and if applicable, the operator of the CRL responsible for the

publication of the certificates issued by the ECD, until the last one expires.

In any case, subscribers may request the revocation and reimbursement equivalent to the value of the certificate's remaining term, if they request it within two (2) months following the second publication.

The activity or activities termination will be done following the schedule presented by the ECD to the surveillance and control entity and approved by it.

7. TECHNICALL SECURITY CONTROLS

7.1. CREATION AND INSTALLATION

7.1.1. PAIR OF KEYS GENERATION

The generation of the keys of the Root CA and the Subordinate CA is carried out with authenticity and integrity in accordance with the key ceremony procedure, in a FIPS 140-2 level 3 certified hardware cryptographic device (HSM), and with the participation of different stakeholders that includes the audit role.
The key pair of each of the above CAs has been generated in accordance with the Key Generation Ceremonies procedure
The key pair generation algorithm is RSA (Rivest, Shamir and Adlemar) a signature algorithm SHA (Secure Hash Algortim).

7.1.2. DELIVERY OF THE PROVATE KEY TO THE SUBSCRIBER

Olimpia IT has a private key delivery method to the subscriber, which consists in that through an HSM with FIPS 140 – 2 Level 3 security, the private key is stored, which is delivered to the subscriber as established in this Declaration of Certification Practices.

7.1.3. DELIVERY OF THE PUBLIC KEY TO THE CERTIFICATE ISSUER

The public key will be stored and published by Olimpia IT when its request

form is different from PKCS#10, when the request for the service is made using the PKCS#10 form, Olimpia IT will not store or publish the public key, since it is the applicant's responsibility who supplies it through a CSR (Certificate *Signing Request*).

Olimpia IT may issue digital certificates based on a request for digital certification filed by the subscriber or by an authorized third party. Therefore, the third party must guarantee that the parameters used for the public key are the SHA 256 + RSA cryptographic algorithm, and that these keys have a 2048 bits size.

7.1.4. DELIVERY THE CA PUBLIC KEY TO TRUSTED PARTIES

Olimpia IT allows the download of the public key from its web portal of the Digital Certification Entity through access to download the self-signed digital certificate that contains the public key.

7.1.5. KEY SIZE

Olimpia IT uses a length of 4096 bits based on the RSA algorithm as the size of the ROOT CA and of the subordinate CA keys.

Olimpia IT uses as a key size for subscribers 2048 bits based on the RSA algorithm.

7.1.6. PUBLIC KEY PARAMETERS AND QUALITY VERIFICATION

The parameters used for the public key are the SHA256 + RSA cryptographic algorithm.

7.1.7. KEY USAGE

The use of the ROOT CA key will be to sign the Subordinate CA certificate, guaranteeing authenticity, non-rejection, integrity, the Root CA will remain in the off state.

The use of the subordinate CA key is to sign subscriber's digital certificates, CRL signing, guaranteeing authenticity and non-rejection.

The use of subscribers' digital certificates will be as permitted by law, this CPS, the accredited scope and what has been agreed with the subscriber.

7.2. PRIVATE KEY SECURITY

Olimpia IT establishes the protection of the private key of the subordinate CA and the root CA through the cryptographic module (Hardware Secure Module) located in the technological infrastructure of Olimpia IT, with its respective backup stored in the smart cards which are in custody of Olimpia IT.

7.2.1. STANDARDS FOR HSMs

Olimpia IT establishes in its cryptographic modules the applicability of the FIPS 140-2 level 3 standard described by the NIST (National Institute of Standards and Technology) for cryptographic devices reference "Luna PCI - e cryptographic module safenet.inc".

7.2.2. ACCESS CONTROL TO PRIVATE KEY

The access control to the private key of ROOT CA and Subordinate CA is performed through a multi-person control of the roles involved defined by Olimpia IT for the execution of this process.

7.2.3. KEY CUSTODY

The private key custody of ROOT CA and subordinate CA is performed through the use of the methodology established by Olimpia IT for the management of Cryptographies keys and stored securely on the designated infrastructure or device.

The private keys custody which are delivered directly to the subscribers through the authorized delivery service and are the responsibility of the subscriber through their custody.

7.2.4. PRIVATE KEY BACKUP

The subscribers' private keys backup copies of the ROOT CA and subordinate CA are duly stored in the Olimpia IT SmartCards which are guarded and safeguarded in the Olimpia IT offices.

7.2.5. PRIVATE KEY FILE

The private key file is protected in Olimpia IT's technology infrastructure located in two different data centers and is stored in FIPS 140-2 level 3 cryptographic devices, which comply with the physical security requirements established by Olimpia IT.

7.2.6. PRIVATE KEY STORAGE IN THE HSMs

The cryptographic key of the Root CA, Subordinate CA and TSA is created and stored in the HSM module, backup copies and recovery are described in the internal procedure of Olimpia IT

7.2.7. PRIVATE KEY ACTIVATION PROCEDURE

The private key activation is performed in a multi-person procedure executed in the HSMs, in which those involved (workers and observers) validate and leave evidence of the process performed for the private key activation.

Note: The responsibility for the private key custody will remain in Olimpia IT, or in case of delivering the HSM (token) to the applicant, he will be responsible for his private key.

7.2.7.1. PROCEDURE FOR GENERATING THE PRIVATE KEY OF THE ROOT CA AND SUBORDINATES

For the generation of the new private key in case of expiration of the root CA and the subordinates' private keys, it is necessary to:

- Perform the destruction of the private keys of cryptographic devices
- Elimination of backups

- Perform the key ceremony again
- Assign new access passwords
- Secure custody of the new private key
- Private key backup execution

Additionally, the system must reject any attempt to generate or sign a certificate if the key is in an expired state.

7.2.8. PRIVATE KEY DESACTIVATION PROCEDURE

The private key deactivation is performed once the service has ended for any legal or contractual reason, and the certificate status will become revoked.

7.2.9. PRIVATE KEY ELIMINATION PROCEDURE

The CA's private key is not destroyed until the business purpose has ceased to have any value or the legal obligations have expired.

There are 3 mechanisms to perform the deletion of the HSM, the person in charge of the ECD approves the deletion mechanism to be implemented according to what is required by the managed change control

i. Delete from the app
ii. Delete from the tools that come with the HSM
iii. You can force the jumper for the secure deletion of the information (According to the HSM configuration)

The devices that have stored any part of the private key for signing certificates of the Root CA and the Subordinate CA, or their activation data, will be physically destroyed or reinitialized at a low level, also including devices that contain copies of these keys or your activation data.

7.2.9.1. SUBSCRIBER´S PRIVATE KEY ELIMINATION PROCEDURE

The subscriber's private key elimination is performed through the use of secure erasure of information by software from the database where the

subscriber's private key is stored.

This is associated with the certificate revocation, at the digital certificate expiration or any other cause that prevents the certificate use.

7.2.10. ENCRYPTION SYSTEMS VULNERABILITIES

Olimpia IT establishes an RSA size of 2048 to mitigate the loss of validity of the encryption key by intrusion method, which is currently one of the safest encryption methods known.

7.2.11. CRYPTOGRAPHIC MODULE CERTIFICATION

The cryptographic modules acquired by Olimpia IT (HSM) for the ROOT CA and the subordinate CA comply with the FIPS140-2 LEVEL 3 standard or higher.

7.3. ADDITIONAL INFORMATION REGARDING KEY PAIR MANAGEMENT

7.3.1. PUBLIC KEY FILE

The private key file is protected in Olimpia IT's technology infrastructure located in two different data centers and is stored in FIPS 140-2 level 3 cryptographic devices, which comply with the physical security requirements established by Olimpia IT.

7.3.2. CERTIFICATES OPERATIONAL TIME

The validity time of the certificates is determined by the validity granted by Olimpia IT and can be reduced in case the certificate revocation process is performed, which can be evidenced by consulting the list of revoked certificates (CRL) on the entity's web page.

7.4. ACTIVATION DATA

7.4.1. GENERATION AND INSTALLATION OF ACTIVATION DATA

The activation data of the ROOT CA and Subordinate CA must be generated and stored in the HSMs and whose protection is headed by 2 or

more Olimpia IT workers.

7.4.2. ACTIVATION DATA PROTECTION

Only authorized personnel have access keys to cryptographic devices. For this, you need the presence of 2 people who guard part of the key to be able to access the device.

The access key is confidential, personal, and non-transferable and it is the parameter that protects the private keys allowing the use of the ROOT CA and Subordinate CA certificates; therefore, security standards for custody defined by Olimpia IT must be considered.

7.5. COMPUTER SECURITY CONTROLS

7.5.1. COMPUTER SECURITY REQUIREMENTS

Olimpia IT has defined the following as technical requirements applicable to its infrastructure:

- Physical and logical access control
- Actions monitoring
- Deleting user accounts by default
- Secure cryptography
- Periodic audits of systems
- Risk analysis on the operation

7.5.2. OLIMPIA IT'S COMPUTER SECURITY LEVELS

Olimpia IT has a security level based on ITSEC, NIST, CIS, among others.

7.6. LIFE CYCLE SAFETY CONTROLS

7.6.1. CONTROLS IN SYSTEM DEVELOPMENT

Olimpia IT establishes a security system for the ROOT CA, subordinate CA, and RA portal systems in physical and logical terms according to what is

established by the best practices of the industry and continuously improving according to business needs. In turn, the security system is based on the NTC-ISO/IEC 27001 standard in its current version, complying with the established requirements.

7.6.2. SECURITY MANAGEMENT CONTROLS

Olimpia IT maintains an information security system which includes controls such as training for all personnel in security, maintenance of updated information, active monitoring system for the service, a risk analysis is performed in accordance with the management procedure risks of the organization and the corresponding action plans are performed.

7.6.3. SECURITY EVALUATION DURING THE LIFE CYCLE

Olimpia IT implements and maintains the security controls established in this certification practices statement, in the policies and procedures established in its Integrated Management System.

7.7. WEB SECURITY CONTROLS

Olimpia IT's network security is determined by the implementation of secure data transmission, high availability infrastructure, ethical hacking analysis and regular internal and external audits, infrastructure security updates (firewall, switch, databases) among other controls, giving a high reliability on the service provided.

8. TECHNICAL STANDARDS OF THE CERTIFICATES

8.1. CERTIFICATE PROFILE

8.1.1. VERSION NUMBER

Olimpia IT digital certificates support and issue certificates under the RFC 5280 standard - Internet X.509 Public Key Infrastructure Certificate and CRL Profile, for certificate and CRL profiles.

8.1.2. CERTIFICATE EXTENSIONS

Olimpia IT establishes in this Certification Practices Statement, the use of at least the following certificate extensions:

- Key Identifier of the issuing entity
- Holder's Key Identifier
- Basic restrictions
- Certificate directives
- CRL Distribution Points
- Access to issuing entity information
- Key Usage
- Improved key usage

8.1.3. CRYPTOGRAPHIC ALGORITHM USED IN CERTIFICATES

The cryptographic algorithm used by Olimpia IT in the key pair generation is:

- SHA256 with RSA encryption.

8.1.4. NAMES FORMATS

Olimpia IT is aligned with the provisions of the X.500 standard for the generation of distinguished names (DN) identifying the holder of the digital certificate.

8.1.5. NAME RESTRICTIONS

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

8.1.6. IDENTIFIER OBJECT OF THE CERTIFICATION POLICY

The root CA has an OID assignment policy defined within its private numbering tree.

The OIDs are indicated in Numeral 22 of this DPC.

8.2. CRL PROFILE

8.2.1. VERSION NUMBER

The ECD issues the revoked certificates (CRL) in reference to the X. 509 v.3 format.

8.2.2. CRL AND ITS EXTENSIONS

It is established that the list of revoked certificates (CRL) is based on the standard RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
Olimpia keeps the CRL updated automatically

8.3. VALIDITY OF CERTIFICATES BY OCSP

This protocol allows the status of digital certificates to be validated online. Olimpia IT delivers a general response on the certificate status at the request of a third party, confining party or information holder through a general response and public consultation exposed and unsigned on the ECD service portal.

8.3.1. REFERENCE STANDARD FOR THE OCSP

Olimpia IT implements as standard version reference for the OCSP RFC 6960 -

X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

8.3.2. CERTIFICATE EXTENSIONS USED IN THE OCSP PROTOCOL

SIGNING

- Key Identifier of the issuing entity
- Holder's Key Identifier
- Basic restrictions
- Certificate directives
- CRL Distribution Points
- Access to issuing entity information
- Key Usage
- Improved key usage

8.4. CURRENT TECHNICAL STANDARDS

Olimpia IT establishes in the document POL-030 CERTIFICATE POLICY the current applicable technical standards defined in the Specific Accreditation Criteria in accordance with the activities of article 161 that refer to Decree Law 019 of 2012 for digital certification services.

9. COMPLIANCE AUDIT

9.1. AUDIT FREQUENCY

The accreditation system of the Digital Certification Entity will be subject to a third-party audit in accordance with current legal and technical regulations. In this way, it is ensured the proper functioning and operability with the

stipulations included in this DPC and in accordance with the accreditation granted by ONAC.

9.2. AUDIT TEAM

Olimpia IT will select the team of auditors to execute the activities, which must meet the following requirements:

- Proven experience in Information Security audits, PKI Security, with

knowledge in Risk Management Systems.

9.3. RELATIONSHIP BETWEEN THE AUDITED ENTITY AND THE AUDITOR

The relationship between the auditor and the audited entity will be strictly limited to the processes and information required for the audit, thereby guaranteeing the absence of conflicts of interest, and leaving evidence of the relationship specified in the contractual agreement between Olimpia IT and the auditing company.

9.4. CONFORMITY CONTROL

The audit scope is established for the operation and maintenance of the services mentioned in this declaration of certification practices in which the following aspects are verified:

- Documentation of the integrated management system
- Physical and logical security control
- Life cycle compliance of digital certificates
- Business Continuity Plan
- Staff roles and functions

9.5. PREVENTIVE OR IMPROVEMENT ACTIONS AS A RESULT OF NON-CONFORMITIES

Olimpia IT upon identification of any non-compliance in the audit will implement corrective actions performed in the shortest possible time together with a continuous action plan which will serve as a control to prevent the non-compliance from occurring again.

9.6. RESULTS REPORT

The Auditor will communicate the audit results to the General Management of Olimpia IT and to the process owners in which nonconformities are detected.

9.7. AUDIT EVENTS RECORD

In compliance with what is stated in the article of Decree 333 of 2014, Olimpia IT as an open Digital Certification Entity, must comply with the third-party audit in the terms provided in the specific accreditation criteria established by ONAC.

10. CHRONOLOGICAL STAMPING

The chronological stamping service gives certainty on the date and time integrity of a document by taking the Colombian legal time of the National Institute of Metrology, or whoever acts on its behalf, affixing a digital signature of the TSA.

This service will be provided for the following types of certificates:

- Digital Certificate - Natural Person
- Digital Certificate - Legal Person
- Digital Certificate - Certified Professional
- Digital Certificate - Belonging to a Company
- Digital Certificate - Public Function
- Digital Certificate - Legal Representative

The service may be used in other certificates; however, this does not imply reciprocity of certificates, nor is it guaranteed that its display can be executed in the same way that it is executed with the certificates issued by Olimpia IT.

The chronological stamps may be used in documents without a signature, but their visualization cannot be detected with the naked eye, so the subscriber must have the appropriate tools for it.

10.1. TIME STAMP AUTHORITY (TSA)

The time stamping service is generated by the TSA, and its administration is headed by Olimpia IT.

The information obtained from the National Metrology Institute is digitally signed by Olimpia IT in its capacity as TSA, based on the certificate issued by the sub-CA that has been issued to Olimpia IT for this purpose. This service allows to impose a time stamp on a digitally signed document through one of the certificates issued by Olimpia IT as ECD, with the certainty of its integrity and authenticity.
The information contained in a time stamp allows two essential characteristics to be established:

i. The time expressed in hours, minutes, and seconds, according to the time issued by the National Institute of Metrology, according to Decree 4175 of 2011.

ii. Date expressed in day, month, and year, according to the Gregorian calendar, which is the one officially accepted by the Republic of Colombia.

10.2. OPERATION OF THE CHRONOLOGICAL STAMP

A Registration Authority (RA) is responsible for the management of requests, identification, and registration of applicants for the time stamping service, and any specific responsibility established in this CPS and the Certification Policies. The RAs are authorities delegated by the ECD for the time stamping service, although the ECD is ultimately responsible for the service. The ECD can perform the duties of RA at any time.

The CA is responsible for making the decision to issue, revoke, or cancel a chronological stamping service.

The requirements for the service are:

- Identification document: Citizenship ID, Immigration ID, or valid Passport
- Chamber of Commerce certificate no older than 30 days
- Single tax registry – RUT of the current year

10.3. MEANS FOR THE SERVICE REQUEST

Olimpia IT establishes in this document the way to access the chronological stamping service which can be requested through the following means:

- Olimpia IT website https://micertificado.olimpiait.com in which the time stamp service must be selected.

Olimpia IT, undertakes with subscribers to enable within a period not exceeding two

(2) business days for the chronological stamping service, unless there is a different legal agreement with the applicant, and without considering the time that the applicant takes to respond to the requests for correction of information, if applicable.

The certificate with which a time stamp is digitally signed corresponds to one of the certificates issued by Olimpia IT as ECD.

10.4. CHRONOLOGICAL STAMPING FOR A DATA MESSAGE

The chronological stamping service establishes the custody of the subscriber's private key on the Olimpia IT servers in a secure way, and once the subscriber has the chronological stamping service, a user will be assigned, which will be linked to a 4-digit password that will be created by the subscriber and with which they can access the Olimpia IT portal and use the chronological stamping service.

10.5. POLICIES FOR THE TIME STAMPING SERVICE PROVISION

Olimpia IT establishes the following necessary policies for the service:

a) All managed requests must be documented and stored in the system logs.
b) The applicant must be kept informed of his application status.
c) Compliance with the provisions of CPS "Certification Practices Statement".
d) The corporate support team validates the service status, and the applicant's documentation when the review is performed automatically
e) All the activities performed by the role of "service portal" correspond to activities automatically executed by the application.
f) The applicant's identity validation is performed in the digital certificate issuance process.
g) To make the service request, the user must be authenticated in the service portal.
h) The time stamp is applied before the end of the signer's certificate validity period.
i) All time stamps are issued with a time precision of less than one second.
j) The expected lifetime of the signature used to sign the time stamp token (depends on the hash algorithm being used, the signing algorithm used, and the length of the private key).
k) If an NTP server is not found to generate the time stamp, the system will not generate any time stamps.

10.6. NUMBER OF TIME STAMPS

For the chronological stamping service, Olimpia IT has a limited or unlimited number of stamps available depending on the service package purchased.

10.7. PROCEDURE FOR ENABLING THE SERVICE FOR THE SUBSCRIBER

The procedure for the service authorization for the applicant, in the chronological stamping service, will be the one established in the internal procedure that Olimpia IT has established for it, and that lists the following activities:

a) Process request

b) Validate consignment

c) Validate collection

d) Proof of payment

e) Sending email to applicant

f) Validate request

g) Issue decision

h) Records

10.8. TIME STAMPING SERVICE REQUIREMENTS (DOCUMENT AND INFORMATION REQUESTED)

- The applicant must accept the terms and conditions.
- The applicant must answer the validation questions.

For the chronological stamping service provision, the following documentation is established:

10.8.1. DOCUMENTATION TO REQUEST

- Certificate of citizenship/immigration status identity card/Certificate of existence and representation issued by the Chamber of Commerce (Issued by the National Registry of Civil Status/Administrative Department of Migration Colombia)

- Legible image of the identity document

10.8.2. INFORMATION TO FILL IN THE APPLICATION

- Names and surnames
- Type of identity document
- Number of identity document
- Department of residence
- City of residence
- Residence address
- Cell phone
- Email:
- Another phone (not mandatory field)

The applicant must select one of the packages offered for this service and pay by the means established in this CPS, the value of the selected package.

If a payment was made online, the application will take the payment and allow the applicant to continue with the activation process.

If the payment was made by consignment, the applicant must attach proof of the consignment and may validate the application status on the website https://micertificado.olimpiait.com

In order for the applicant to associate a digital certificate with this service, he may acquire it through the centralized signature service and pay the package cost in accordance with the forms established for this purpose in this CPS.

If the certificate generation is successful, the applicant must activate the same according to what is specified in the application for the centralized signature service.

10.8.3. TIME STAMPING SERVICE REQUIREMENTS

The applicant must have attached the information required by the application and filled out the information requested, likewise must have selected one of the packages offered for this service and if it has a cost, have paid the selected package value.

If the applicant requires that the chronological stamping service be used with a digital certificate from another certification entity, Olimpia IT does not supply the technological components for this type of integration.

If the applicant requires the chronological stamp for an unsigned document, he must have the appropriate technology for its visualization, because, although the time stamp is embedded in the document, its visualization is not guaranteed without a digital signature that accompanies the time stamp.

10.9. PROCEDURE FOR ENABLING THE CHRONOLOGICAL STAMPING SERVICE FOR THE APPLICANT / SUBSCRIBER

Olimpia IT establishes below, the way to request the chronological stamping service, through the following means:

- Internet: Through the website of the Digital Certification Entity https://micertificado.olimpiait.com , or through any other web portal that Olimpia IT defines as a sales channel for its digital certification services, provided that said portals are duly integrated to the portal of the Digital Certification Entity.
- The applicant must register on the web portal using the "registration" button and enter the required information there:
    - Type of identification
    - Document number

- Document issue date

- A validation of the information entered will be performed against the Biographical Database of the National Registry of Civil Status.
- If the information is not valid, the application will report that the information is invalid.
- If the information is valid, the applicant will need to enter the following information:
    - Email address
    - Phone number:

- Read and accept the terms and conditions of useThe subscriber will receive a message to his email, in which the activation of his account will be requested through a link contained in the same email.
- The subscriber must log in to the web portal https://micertificado.olimpiait.com, on the “Ingresar” button and submitting the following information:

    - Type of identity document
    - Number of identity document

- An OTP (One Time Password) consisting of a 4-digit single-use code will be sent to the cell phone number registered by the applicant, so that the applicant can enter it in the space provided for it, at the bottom of the window of login in order to generate an authentication before the portal.
- Once the authentication is effective, the web portal will inform the applicant who is already in his private account, the applicant may request digital certificates from the "Certificates" link, or "Services" from the "Services" link.

Note: The website of the Digital Certification Entity may be displayed in Chrome browsers in its version 71.0.3578.98 and Microsoft EDGE version 38.14393.2068.0. The use of any other browser may cause problems with the portal use, the request for certificates or services.

- By phone: By contacting the customer service line (+57 601) 742 7878, where the operator will send the applicant to register on the website https://micertificado.olimpiait.com, described in the previous item.

The subscriber accepts compliance with the following policies and procedures established by Olimpia IT:

a) The applicant may check the status of his application on the website https://micertificado.olimpiait.com. If the user complies with the requested documentation and with the established requirements, Olimpia IT will proceed to issue the certificate within a maximum period of 2 business days, counted from the certification decision to accept the request, and without counting the time that the applicant delays in responding to requests for correction of information, if applicable.

b) Applications are registered from the website https://micertificado.olimpiait.com .

c) Olimpia IT has the power to request clarification of the information provided or documentation; In the event that the information or documentation cannot be clarified, the certification decision by the CA will be to reject the request.

d) All documentation provided by the applicant must be stored safely following the standards established by Olimpia IT under the certifications of NTC-ISO/IEC ISO 9001 and NTC-ISO/IEC 27001 in its

current version.

10.10. SERVICE ACTIVATION PERIOD

Olimpia IT below establishes the times for the service provision and the validity period when the service is associated with digital signatures:

- If the subscriber's digital certificate is revoked for reasons of certificate improper use, the chronological stamping service is immediately canceled
- due to expiration of time stamping service
- Due to non-compliance with Olimpia IT's security policies, the chronological stamping service may be canceled for legal reasons related to Colombian laws and regulations
- When the cancellation of the digital certificate associated with this service is generated, due to expiration of the term, the chronological stamping service will continue to be active, but to access it the subscriber must associate a new digital certificate to the chronological stamping service.

In the event of generating a new certificate to replace one that was revoked, the contracted chronological stamping service may continue to be used.

10.11. OPERATION OF THE TIME STAMPING SERVICE

The data message that is made up of the time information expressed in the Julian calendar and in hours, minutes, and seconds, is digitally signed by the TSA digital certificate.

This data message, which contains a digitally signed time stamp, may be used by the subscriber in an electronic document in order to be certain of when said document was signed.

10.12. RESPONSIBILITIES FOR EACH DOCUMENT THAT OLIMPIA IT STAMPS

Each document stamped by Olimpia IT, is limited to testifying by technical, suitable, and safe means that the date and time in which a document has been stamped corresponds to the legal date and time for the Republic of Colombia, and that said time stamp

corresponds to the moment in which a document has been digitally signed, when the time stamp is used with a digital certificate issued by Olimpia IT.

Olimpia IT is responsible for the veracity, integrity, authenticity, and non-rejection of the stamp that is supplied and that is certified by the Olimpia IT TSA, as evidenced in the information of the digital certificate supplied of the time stamp imposed on the digitally signed document.

The risks derived from the service will be the responsibility of Olimpia IT, provided that the time stamps are in the possession of Olimpia IT and have not been delivered to the subscriber, once the time stamps are made available to the subscriber for consumption, the subscriber will be the person responsible for its use and proper management in accordance with this CPS.

The subscribers and relying parties of this service accept the regime of responsibilities that correspond to them with respect to this service and that are contained in this CPS.

10.13. TIME SOURCE

Olimpia IT performs an Identification process for the required infrastructure for which the proper time synchronization must be performed (Central Time Server), said connection is made through a Master Domain Controller Server that synchronizes its time with the Colombian legal time: horalegal.inm.gov.co, finally the client machines and servers synchronize

their time against the Master Domain Controller server through GPO.

The TSA will not synchronize its clocks with the Colombian legal time since the Colombian legal time will be taken from the official website of the National Institute of Metrology.

11. COMMERCIAL TERMS

11.1. FEE POLICY FOR ISSUANCE AND REVOCATION OF CERTI FICATES

The fees defined by the digital certification entity for each of the services within the accredited framework can be consulted on the certification entity's website, under the 'Productos' subsection, within the "ver planes y precios" option for each type of certificate.

Olimpia IT establishes that it does not have a fee for the revocation of certificates.

11.2. FEES FOR DIGITAL SERVICES IN PROJECTS

Olimpia IT may establish special conditions for the issuance of digital certificates or services accredited by ONAC which must previously be agreed with the subscriber and in which specific conditions required by the subscriber may be established provided that it adheres to this Certification Practices Statement and current Colombian regulations.

11.3. PAYMENT METHOD

Cash payment: It is made through Bancolombia' Collection to Agreement 76321 in the name of OLIMPIA IT SAS. indicating as reference number the number of the applicant's identification document and if applicable, the unique reference number of the application.

Online payment: the payment process will be performed with the applicant's bank through the payment gateway provided by Olimpia IT

within the website https://micertificado.olimpiait.com

11.4. POLICIES FOR MONEY REFUND

Subscribers and/or applicants for digital certificates may request reimbursement of money in the following cases:

11.4.1. EVENTS FOR MONEY REFUND

- When a subscriber requests a service and his request is rejected: The RA operator will inform Customer Service so that it executes the refund to the user or applicant.
- When Olimpia IT considers it necessary due to an applicant affectation during the application process or of the subscriber in the services usage: The RA operator may determine a reimbursement, informing Customer Service the causes, so that it executes the refund to the user or applicant.
- When Olimpia IT ceases activities as a Digital Certification Entity: in this case, the subscriber can request a money refund, which will be proportional to the digital certificate validity period until the end of activities.

11.4.2. VALUE TO BE REIMBURSED

Subscribers and/or applicants will be entitled to reimbursement of fifty percent (50%) of the value paid for the certificate request, or service they have performed. When the issuance of a digital certificate or the provision of a service cannot be performed for reasons attributable to Olimpia IT, the Customer Service area will evaluate in accordance with the internal procedure, the reimbursement of a value greater than 50%.

11.5. FINANCIAL RESPONSIBILITY

Olimpia IT has financial stability and the necessary resources for its operation as established in Decree 333 of 2014, which is evidenced by compliance with the financial statements validated by the statutory auditor and the civil liability insurance acquired since July 2018 this in order

to be able

to compensate for damages or losses that may be caused in the operation of Olimpia IT as a Digital Certification Entity.

12. INFORMATION CONFIDENTIALITY

Olimpia IT catalogs within its integrated management system all non-public information as confidential information (labeling according to its publicity level in public, internal, restricted, or reserved) according to the information security policies established by the company.

The treatment given to confidential information, as well as the authorized uses of the same, are determined by the labeling that is given to it.

CONFIDENTIALITY LEVEL	AUTHORIZED USE
PUBLIC	Transportation: By any means used by Olimpia. Storage: Usually this information is transitory, and when it corresponds to information from the Integrated Management System, it is performed in accordance with internal procedures.
INTERNAL	Transportation: It can be transported by any means that is part of Olimpia's internal technological infrastructure.Storage: It will stay within the boundaries of

	Olympia, physically or logically.
RESTRICTED Transportation:	This information must be managed within the means designated by the process owner, Storage: It will be stored in the means or places designated by the process owner
RESERVED	Transportation: It is mandatory to transport this information using secure, encrypted means and should always be considered an acknowledgment confirmation. Storage: It will be kept encrypted in a protected medium with access controls or locked (access only to the Owner).

Access to confidential information (internal, restricted, or reserved use) will only be allowed to persons authorized by the owner of the corresponding information asset, this information is listed in the asset inventory of Olimpia IT.

The information that is of a confidential nature and inherent to the activities of the Digital Certification Entity, will be disclosed in accordance with the previous paragraph and when there is a judicial or administrative order issued by a competent public official that requires the disclosure of said information. When a request is submitted by a judicial or administrative authority, said request must be submitted to the legal area, which will respond to the request for disclosure of confidential information.

When Olimpia IT is required, by law or authorization in the contractual provisions, to disclose confidential information, the subscriber or the person involved must, unless prohibited by law, be notified of the information provided.

Olimpia IT guarantees subscribers that in accordance with this DPC and its personal data protection policy, the personal data of applicants and subscribers are treated properly and under the limits of the authorization that applicants and subscribers have given for it.

The information provided by applicants and subscribers is classified as restricted and will be treated accordingly within Olimpia IT.

The information collected in order to provide the acquisition services of any certificate type, the certified email services, centralized signature, the certificate, and chronological stamping are subject to the information protection declared in this CPS.

12.1. SCOPE OF CONFIDENTIAL INFORMATION

Confidential information is considered:

- Registration information, all data related to the registration of certificates.
- The business information provided by its suppliers and other people with whom Olimpia IT has a legally or conventionally established duty of secrecy.
- Information on the certificate's life, all the data related to the issuance and revocation (except its publication in the CRL) of ECD certificates.
- All information classified as "Confidential"

12.2. INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL

INFORMATION

Olympia defines the following as non-confidential information:

- Certificate Revocation List (CRL)
- The public key of the digital certificates issued by Olimpia IT
- The CPD versions
- The PQRS procedure for the subscriber
- Information of the company that rests on the certificate of existence and representation issued by the corresponding Chamber of Commerce in the company's domicile.
- Personal data, except those of a public nature

12.3. RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

The workers and allies of Olimpia IT are responsible for protecting confidential information, and accept the contractual regulations acquired and the current Colombian regulations.

12.4. MINFORMATION MANAGEMENT PROVIDED BY SUBSCRIBERS

Olimpia IT, in its capacity as a Digital Certification Entity, complies with the provisions of Colombian regulations for the protection of applicant or subscriber information through the implementation and compliance with the Personal Data Protection Policy, which specifies the guidelines to which Olimpia IT adheres, which is available to the public on the Digital Certification Entity portal.

Information about the subscriber obtained from sources other than the subscriber (for example, from a complainant or from regulators) must be treated as confidential.

13. INTELLECTUAL PROPERTY RIGHTS

This document is protected by copyright regulations, any reproduction, distribution, or total or partial modification to unauthorized users, or any improper use of confidential information will be considered a crime in accordance with the provisions of the Penal Code and current Laws of the Colombian state.

14. OBLIGATIONS AND GUARANTEES

Olimpia IT establishes below the obligations and duties of each party involved, framed within the requirements made by Decree 333 of 2014, the regulations that modify it, clarify, or replace it, as well as CEA 3.0-07.

14.1. OBLIGATIONS AND DUTIES OF THE DIGITAL CERTIFICATION ENTITY

Olimpia IT ensures that all subscribers and clients have met the requirements defined in Colombian laws and the provisions issued by the regulatory entities to obtain the requested digital certification service.

Olimpia IT declares that it is subject to compliance with the following obligations and duties for the provision of services that as ECD, the following obligations are stipulated:

a) As for the security systems necessary for the proper functioning of the service, it will be Olimpia IT's obligation to ensure its optimal functionality at all times and take the contingent and technical measures to achieve said operation.

b) As for the necessary infrastructure for the correct operation as ECD, they must be implemented and in operation, and it will be necessary to perform the maintenance required for their adequate performance.

c) Accept, respect, and apply the Certification Practices Statement (DPC) in its entirety and honor the agreements with the users of the ECD services.

d) Make known and/or make available to users the content of the terms and conditions, as well as the policies in an adequate and sufficient manner, on the service to be provided, as well as its general and particular characteristics, the contract to be provided, subscribe and/or the acceptance given by the user of the services to be provided, informing clearly and truthfully the ECD status that Olimpia IT enjoys and the services for which it is authorized to provide.

e) Make known and/or make available to users the responsibilities or obligations of their competence, as the acquirer of the services made available or contracted for the execution of Olimpia IT in its capacity as ECD.

f) Through the Policy Committee, approve the content of this Certification Practices Statement (CPS), which contains the rules for the TSA and the Certificate Policies.

g) Refrain from storing and/or accessing the subscriber's private key.

h) Maintain the custody and protection of the physical support of the digital certificate until the delivery of it to the subscriber is verified by any means (if applicable).

i) Help, collaborate and facilitate access both to the facilities and to the other spaces in which Olimpia IT has control, to the National Accreditation Body of Colombia for the development of audits, whether face-to-face or remote.

j) Issue digital certificates in accordance with the provisions of this Certification Practices Statement and that agreed with the subscriber, setting the legality and authorization required for the event as a limit.

k) Keep a record of the certificates issued and publish them in accordance with what is defined in this Certification Practices Statement.

l) When there is knowledge of an event that may compromise the provision of the service, inform the National Accreditation Agency of Colombia by the most effective and appropriate means of said eventuality.

m) When modifying, supplementary, introductory, or suppressing changes are generated in the PKI, which may affect the service provision, inform the National Accreditation Body of Colombia by the most effective and suitable means of such change.

n) When changes in the status of the subscriber's certificate occur for any reason, inform the subscriber of said change effectively, informing the reasons for the change and its legal basis sufficiently and thoroughly.

o) Take all reasonable and sufficient security and control measures that do not compromise the disclosure of his private key.

p) Make all the necessary efforts for the permanent and uninterrupted provision of digital certification services.

q) Keep the database of revoked digital certificates updated in accordance with what is instructed in this Certification Practices

Statement and make the notices and publications required by law to satisfy the notification of the given updates.

r) Perform the revocation of the digital certificates in accordance with the provisions of section 5.8 of this Certification Practices Statement.

s) Once the revocation of a digital certificate is performed by Olimpia IT, the subscriber must be informed the following business day of said eventuality.

t) Ensure that the administrators are not involved in the causes established in literal c of article 29 of Law 527 of 1999, and once an administrator is found involved, perform their immediate removal.

u) Make available to subscribers a permanent communication mechanism that allows them to promptly resolve queries and concerns that arise regarding digital certificates and their revocation.

v) Collaborate timely and effectively with the judicial or administrative authorities when required in all aspects related to the digital signatures and certificates issued and in general on any data message that is in their custody and administration.

w) Preserve in any suitable and legally permitted medium the supporting documentation of the digital certificates issued, for the term provided by law for the papers of the merchants and take the necessary measures to guarantee the integrity and confidentiality that are proper to it.

x) At the request of the subscriber, of a person authorized by him or of any judicial or administrative authority that has the competence to do so,

supply, transfer or transmit the information delivered by the subscriber and report said operation no later than the next business day on which the operation of the required information is executed or starts its execution in case of being a successive transaction operation.

y) Comply with the CEA-3.0-07 Accreditation Criteria issued by the National Accreditation Agency of Colombia.

z) Inform the subscriber the obligations in the care, custody and responsibility that corresponds to him, in terms of the proper legal use, and in accordance with good commercial customs of the digital certificate.

aa) Provided that an applicant for the services offered by Olimpia IT as a Digital Certification Entity, complies with the legal requirements and those established both in this Certification Practices Statement and in the general policies of Olimpia IT, the latter may not refuse to provide the service. The subscriber's exercise of illicit activities, or the public or judicial link of the subscriber as an active subject to illicit activities may be cause for rejection of the applicant's request for the services offered by Olimpia IT.

bb) Comply with the provisions of Statutory Law 1581 of 2012, its regulatory decrees, other regulations that modify, add, replace, or complement it, with respect to all data of those involved in the process of digital certification or related, especially the subscriber's personal data.

cc) The providers of the Datacenter service, which are considered critical for the Digital Certification Entity operation, are subject to compliance with the requirements established for them as providers of this service in the CEA-3.0-07 Accreditation Criteria document, issued by the National Accreditation Agency of Colombia (ONAC).

cc) The providers of the Datacenter service, which are considered critical for the Digital Certification Entity operation, are subject to compliance with the requirements established for them as providers of this service in the CEA-3.0-07 Accreditation Criteria document, issued by the National Accreditation Agency of Colombia (ONAC).

ee) Olimpia IT has established a personal data protection protocol and a personal data processing manual as a security system to protect the information that is collected in order to provide the time stamping service, issuance of digital certificates and signature services, centralized, certified electronic mail, file, conservation, registration, custody, and annotation.

ff) Olimpia IT has a documented procedure to receive, evaluate and make decisions about complaints and claims. It must record and track complaints and grievances, as well as the actions that have been taken to resolve them.

gg) Olimpia IT registers and confirms if a claim is related to the digital certification activities for which it is responsible and, if so, it must treat and respond to them.

hh) Olimpia IT is responsible for gathering and verifying all the information necessary to reach a decision on the complaint and claim.

ii) The decision that resolves the complaint or claim must be made, reviewed, and approved by persons who are not involved in the digital certification activities related to the claim.

jj) Olimpia IT must provide the claimant with a formal notification of the outcome and completion of the claim process.

kk) Olimpia IT must undertake the subsequent actions necessary to resolve the claim.

ll) Olimpia IT must deal with the claims made by the subscribers regarding the issued certificates, the services provided and the chronological stamping service.

mm) The senior management of the ECD must ensure that this CPS is properly implemented.

nn) Olimpia IT exercises control over the accredited digital certification services, regarding the ownership and use of symbols, certificates, any other mechanism to indicate that the digital certification service is accredited.

oo) Have sufficient economic and financial capacity to provide the authorized services as a certification entity.

pp) Have the capacity and technical elements necessary for the generation of digital signatures, the issuance of certificates on the authenticity of the same and the conservation of data messages in the terms established in Article 29 of Law 527 of 1999.

qq) a) Issue certificates as requested or agreed with the subscriber.

rr) Implement security systems to guarantee the issuance and creation of digital signatures, the conservation and filing of certificates and documents in support of data messages.

ss) Guarantee the protection, confidentiality and proper use of the information provided by the subscriber.

tt) Guarantee the permanent provision of the certification entity service.

uu) Respond in a timely manner to requests and claims made by subscribers.

vv) Make notices and publications in accordance with the provisions of the law.

ww) Provide the information required by the competent administrative or judicial entities in relation to the digital signatures and certificates issued and in general about any data message that is in its custody and administration.

xx) Allow and facilitate the performance of audits by the National Accreditation Body of Colombia. It is responsibility of the certification entity to pay the accreditation costs and those of the surveillance audits, in accordance with the rates of the National Accreditation Body of Colombia.

yy) Prepare the regulations that define the relations with the subscriber and the service provision form.

zz) Keep a record of certificates.

aaa) Unless otherwise agreed between the parties, the certifying entity may terminate the relationship agreement with the subscriber by giving notice of no less than ninety (90) days. After this term, the certification entity will revoke the certificates that are pending expiration.

bbb) Be responsible for their decisions related to digital certification, retaining the power to decide when granting, maintaining, canceling, or

withdrawing (revoking) the certification, obligations that are not delegated or contracted with third parties.

14.2. CONDITIONS AND OBLIGATIONS OF SUBSCRIBERS

The obligations described below will be the subscriber's responsibility

a) Comply with the requirements of the respective digital certification service, including the implementation of changes when communicated by Olimpia IT.

b) That the information provided for the certificate is consistent with the requested service and provide the RA with the real, true, and necessary information to make a correct identification.

c) Not to use your digital certification in a way that violates the law, or causes bad reputation or damage to the ECD, and not making any statement related to your digital certification that the ECD could consider misleading or unauthorized.

d) That immediately after the cancellation or termination of the digital certification, the subscriber stops using it in all advertising material that contains any reference to it, and undertakes the actions required by the digital certification service (for example, the return of the certification documents) and any other measures required.

e) That, when referring to the digital certification service in communication media, such as documents, brochures or advertising, the subscriber informs that it meets the requirements specified in the Certificate Policies.

f) Inform the ECD about the changes that may affect the certificate

information that was granted or that is in the process of being issued.

g) Perform an adequate, legal, and consistent use of the private key, as well as use it only for the established purposes and in accordance with what is agreed in the contract entered into and with what is stipulated in this Certification Practices Statement.

h) Inform the third parties involved and who have an interest in the process, the quality in which the data messages are signed in accordance with the classification given to the subscriber contractually. When the data message or electronic document

signed by the subscriber with his digital certificate. The quality in which the subscriber signs will be determined by the contractual and customary context of use between the parties and in accordance with the signed document.

i) Once any of the assumptions required to perform the revocation of the digital certificate that has been delivered to you have been fulfilled, request the inclusion of said digital certificate in the lists of revoked certificates that Olimpia IT manages and maintains.

j) Give an adequate use and in accordance with what is contractually agreed and with what is established in this Certification Practices Statement, accepting that the private key is personal and non-transferable, for which the use by third parties other than the subscriber, without this being contractually agreed, implies an acceptance of the subscriber in the use that the third party gives to the private key. This infringement will not affect the legal qualities of the digital signature.

k) The subscriber declares that all the information contained in the digital

certificate is true and truthful, and in the event that said recorded information does not correspond to reality, it is the subscriber's obligation to immediately inform Olimpia IT of the correction, modification, addition, or deletion to take place.

l) If the subscriber knows of any condition of any nature that may affect the reliability or any other of the legal virtues of the digital certificate, he must immediately inform Olimpia IT. When the signature or the digital certificate are stored or addressed by a physical medium, any damage, substantial deterioration, loss, or theft that prevents the use of the services offered by Olimpia IT must be notified.

m) When the digital signature or certificate is stored on a physical medium, destroy the physical medium when required by Olimpia IT, either by substitution

by another or when the period of the purchased service ends, following the instructions of Olimpia IT.

n) When the digital certificate and its private key are stored in the physical infrastructure of a third party, destroy the certificate together with its public and private keys when required by Olimpia IT, either by substitution for another, or when the period of the purchased service ends.

o) Return the physical support of the digital certificate when required by Olimpia IT.

p) Refrain from violating in any way the industrial and intellectual property rights of Olimpia IT in the use of digital certificates. The subscriber guarantees that the information included in the digital certificate by his

instruction does not constitute any violation of the intellectual or industrial property rights of Olimpia IT or any third party and undertakes to keep Olimpia IT harmless from any appeal for the occurrence of this type of facts. In turn, the inappropriate use that the subscriber makes of the digital signature or certificate will be understood to be his or her entire responsibility.

q) Any other derived from the law or from the content of this Certification Practices Statement.

r) Refrain from making copies, modifying, altering, reproducing, adapting, translating, using reverse engineering techniques, decompiling, or disassembling, altering, or interfering in any other way with the provision of the service provided by Olimpia IT.

s) The subscriber may not use the name and/or trademark of Olimpia IT, as well as the Olimpia IT brand or the company's accredited services, in advertising or Marketing programs, nor may they refer to Olimpia IT directly or indirectly before third parties without the prior written consent of Olimpia IT, The use of the brand

and the intellectual property of Olimpia IT without prior authorization, license, or assignment, may lead to the initiation of legal actions and the collection of damages caused to Olimpia IT.

t) When the subscriber uses the services of Olimpia IT and requires or wishes to communicate the use of the service provided by Olimpia IT, he must inform in the media in which the service is cited, that it complies with all the legal parameters required both for the digital certificate and for the digital signature.

u) Comply with the obligations that are agreed regarding the use of

trademarks in the provision of services and consequently respect the trademark rights that belong to Olimpia IT.

v) Any voluntary technological change made by the subscriber that may affect the provision of the service must be reported to Olimpia IT.

w) The subscriber must consult, know, and accept this DPC, as well as its scope both for digital certificates, the services provided and the chronological stamping service.

x) When obtaining a time stamp, the subscriber must verify that it has been signed correctly and that the certificate is not revoked.

y) The subscriber and clients ensure to have met the requirements defined in Colombian laws and the provisions issued by the regulatory entities to obtain the requested digital certification service.

z) The subscriber may terminate the relationship agreement with the certifying entity by giving notice of not less than thirty (30) days.

aa) Receive the digital signature from the certification entity or generate it, using a method authorized by it.

bb) Supply the information required by the certification entity.

cc) Maintain control of the digital signature.

dd) Timely request the revocation of the certificates.

14.3. APPLICANT'S OBLIGATIONS

a) The applicant is obliged to Olimpia IT to read the "Terms and

Conditions", accept them in their entirety and fully comply with them during the term of the commercial relationship object of this document and after the termination of the commercial relationship, regarding the aspects that by law the parties are obliged, such as, but not limited to the care and custody of information, etc.

b) The applicant adheres to the provisions of the Personal Data Protection Policy of Olimpia IT, exposed to the public on the ECD page

c) Guarantees that all the information provided before, during and after the process of issuing digital certificates and/or providing services accredited by ONAC is true and that any falsity in the information provided will be grounds for indefinite suspension of the services and certificates issued. Likewise, the applicant accepts that in the event that errors, or obvious typos occur in the writing or presentation of the application information, the ECD may adjust or correct this information in order to effectively provide the service, provided that situations do not arise that reasonably allow one to conclude that there is an intention to present false information, or bad faith on the part of the applicant.

d) It is the applicant's commitment to use the authentication mechanism established by Olimpia IT as the only method of entering the portal, in case of difficulties with the entry, the applicant can contact the Olimpia IT customer service line.

e) Applicants are prohibited from entering harmful software or another similar to the web portal of the digital certification entity which may cause any damage or harm to Olimpia IT, or third parties involved in the provision of the service, or parties relying on the service.

f) Applicants are required to have an active email account and active cell

phone number, if they do not have one of these two services, the applicant will be instructed that they must acquire one of them to provide the service.

The terms and conditions of use of the electronic mail that the applicant acquires will be of exclusive compliance of the applicant.

g) Olimpia prevents the use of its internal portal for activities considered illegal according to current Colombian regulations.

h) The applicant's account will be suspended for prolonged inactivity for more than 2 years, counted from its creation date.

14.4. OBLIGATIONS AND PRECAUTIONS OF THE RELYING PARTIES

The digital certification service integrates the use of a set of elements for the effective provision of a service for subscribers and which in turn affects the legal and contractual trust that third parties have regarding the digital certificates issued by Olimpia IT.

The reliability based on the non-rejection of the operation is a factor of trust in the third party recipients of the digital certificate issued by Olimpia IT and under the presumptive protection of the law, the third party understands and accepts that the act held provides functional equivalence to that of a handwritten signed document, that third person becomes a participant in the Digital Certification System, as a relying party, and therefore assumes the obligations set forth below:

a) Verify that both the digital certificate and the digital signature are not listed in the certificate revocation lists managed and administered by Olimpia IT available on the OlimpiaIT website

b) Accept and recognize digital certificates only for the use that is allowed in accordance with the provisions of the Use of digital certificates section.

c) Comply with the special chapter of this Certification Practices Statement addressed to the relying party.

d) Inform Olimpia IT of any event that may affect the use of the Digital Certification System.

e) Refrain from making copies, modifying, altering, reproducing, adapting, translating, using reverse engineering techniques, decompiling, or disassembling, altering, or interfering in any other way with the provision of the service provided by Olimpia IT.

f) The relying party must consult, know, and accept this DPC, as well as its scope both for digital certificates, the services provided and the chronological stamping service.

g) When obtaining a time stamp, the subscriber must verify that it has been signed correctly and that the certificate is not revoked.

14.4.1. TRUST STATUS OF CERTIFICATES OF DIGITAL SIGNATURES

Olimpia IT's Digital Certification System complies and continues to fully comply with all legal, technical and technological requirements that give certainty of the attributes granted by law to offer reliable digital certificates and signatures that share non-rejection and other characteristics that the law grants so that these services offered by Olimpia IT, comply to the full satisfaction of both the enabling authorities, as well as the subscribers and trusting parties, with the principle of functional equivalence that allows

affixing the digital signature to a text message and electronic documents, as well as the issuance of their digital certificates comparable to physical documents, in order to obtain the deprecated legal certainty of this type of procedure.

14.4.2. TRUST STATUS OF DIGITAL SIGNATURES

In order to guarantee the reliability acquired by the relying party regarding the digital signature, this party must, after a reliability vote, be familiar with this Certification Practices Statement, especially the part that corresponds to the relying party, having completed the reliability process of the digital certificate described below and that its creation corresponds to an act prior to the act to sign and verify the root certificate of the Olimpia IT digital signature that contains the public key.

14.4.3. TRUST STATUS OF DIGITAL CERTIFICATES

To guarantee the reliability acquired by the trusting party regarding the digital certificate, this party, after a reliability vote, must verify that the certificate is not included in the revocation lists administered by Olimpia IT, that the digital certificate is found at the time of the act to be performed with an expiration date later than the act to be executed and having exhausted the digital signature reliability process.

It is understood that a digital certificate will be valid as long as it is not found in the revocation lists managed by Olimpia IT, its creation is prior to the moment of its use, and it is associated with the root certificate of the digital signature of Olimpia IT.

The use of a digital certificate by any participant is subject to strict compliance with the following parameters:

- The contractual agreement entered into with the subscriber of the

digital certification service, and whose content can be found at the following link that is part of the official website of Olimpia IT, https://micertificado.olimpiait.com/Publica/Politica

- Certification Practices Statement.

14.5. RIGHTS ASSOCIATED WITH EACH OF THE SERVICES PROVIDED AS ECD

The certificate policies will host the following rights for each of the services:

- The subscriber has the right to use the digital signature associated with the certificate issued by Olimpia IT as ECD in all the documents required.
- The subscriber and the applicant have the right to inform the relying on third parties in the digital signature that Olimpia IT is the ECD that provides the service.
- The subscriber has the right to use the time stamp that Olimpia IT has granted him, in any document that he has signed or legally used.
- The subscriber has the right to access the certificated email services and centralized signature through the channels that Olimpia IT has for this, such as ECD.
- The applicant and the subscriber have the right to receive clear information regarding the values or prices, certificates or services issued by Olimpia IT.
- The applicant and the subscriber have the right to have their personal data processed in accordance with current regulations, in particular Law 1581 of 2012 and Decree 1377 of 2013.

The subscriber, the relying parties and others involved, have the right to submit requests, complaints or claims in a respectful manner to Olimpia IT, and to obtain a response to them.

15. LIABILITY DISCLAIMER

15.1. LIABILITY LIMITS FOR THE EXERCISE OF THE ACTIVITY

a) The service offered by Olimpia IT as a Digital Certification Entity, reflects an obligation of means and not of result. Therefore, Olimpia IT will make available to the service, the subscriber and other third parties involved or with legitimate interest, due diligence with their professionalism, and experience in providing the digital certification service, and will be responsible only for slight fault in their actions as Digital Certification Entity. Olimpia IT cannot ensure or guarantee that the certification activity will have a certain result, Olimpia IT will only be responsible for those errors that could have been avoided due to its professional diligence.

b) The breach of any of the obligations by the subscriber or the relying on third party, its consequences of all kinds will be borne by them, this including the damages that even due to circumstances beyond their control have occurred, in the same application for the loss of the physical device when applicable.

c) When the breach of any of the obligations by the subscriber or the relying on third party is the cause of a defective provision of the service, Olimpia IT will not be responsible for the defective provision of this service, nor for the consequences of the loss of the legal qualities granted by law to the digital signature.

d) Olimpia IT will not be responsible for the damages caused by the breach of its obligations due to force majeure, fortuitous event and in general, any circumstance over which Olimpia IT cannot have reasonable control, including but not limited to the following: electrical and/or telephone suspension.

computer systems viruses, deficiencies in telecommunications services (Internet, communication channels, etc.) or the compromise of asymmetric keys derived from unforeseeable technological risk.

e) The limit of patrimonial responsibility for contractual or extra-contractual civil liability regardless of the cause or origin of its responsibility, on the side of Olimpia IT is set as the maximum amount for damages compensation for damages caused by digital certificate issued, the protection or coverage granted in the professional civil liability policy taken by Olimpia IT. Consequently, Olimpia IT will only compensate the people harmed by a digital certificate issued by it, regardless of the number of times it has been used or the number of harmed by said uses. In the event that there are several affected parties, the maximum amount that can be compensated will be distributed proportionally among them. If, having distributed the compensation, new injured parties arise, these should be directed against the persons already compensated for the purpose of obtaining their compensation on a proportional basis.

f) Olimpia IT will only be liable for damages caused by the use of digital certification services within the year following the expiration or revocation of the digital certificate. Olimpia IT does not offer any type of guarantee that is not expressly stipulated, nor will it be liable for events that are not expressly contemplated in this Certification Practices Statement.

g) When the laws concerning the digital certification service establish the ineffectiveness of any clause that implies limiting the amount of damages derived from contractual or non-contractual civil liability, the nullity of the clauses will not affect the other clauses of this Certification Practices statement.

h) Digital signature certificates issued by foreign certification entities may be recognized under the same terms and conditions required in the law for the issuance of certificates by Olimpia IT as long as such certificates are recognized by an authorized certification entity that guarantees in the same way that it does with its own certificates the regularity of the details of the certificate as well as its validity and term.

i) With the purpose of making possible the impartiality that, as a Digital Certification Entity, Olimpia IT requires, it has designed, implemented, and accepted a policy of impartiality - non-discrimination and independence, in order to identify the risks that may affect it, as well as the necessary controls to safeguard impartiality within the digital certification entity.

j) Olimpia IT as ECD limits its responsibility for each signed document as follows: the content of each of the signed documents, their commitment and legality are the sole and exclusive responsibility of the subscriber so Olimpia IT is limited to supplying a digital certificate for the use of a digital signature by the subscriber and that said certificate can be verified by the means arranged for it by Olimpia IT.

15.2. RESPONSIBILITIES OF APPLICANTS AND SUBSCRIBERS

In accordance with the provisions of article 40 of Ley 527 of 1999, the subscriber will be responsible for the falsehood, error or omission in the information provided to the certification entity and for the breach of their duties as subscriber.

The subscriber who has caused any damage to Olimpia IT must compensate it, as well as if his actions have caused damage to other parties involved or recipients.

The subscriber will also be responsible for the indemnification of damages

that may arise due to the violation of this Certification Practices Statement, the breach of the terms and conditions of the page https://micertificado.olimpiait.com/Publica/Politica and other documents that are established for the fulfillment of the commercial relationship that arises from the provision of Olimpia IT services as ECD, assuming the legal expenses incurred by Olimpia IT for this cause, including the attorney costs.

Regardless of the cause for which the subscriber has delivered said false, inaccurate, or insufficient information. The subscriber will assume the damages suffered as a result of acts of God or force majeure.

The custody and care of the physical support (smart card, token, hard disk, USB or other supplied or not by Olimpia IT) of the digital certificate will be the sole responsibility of the subscriber.

Regardless of whether or not the means used by the relying party validate the term conditions of the digital certificate and the digital signature as well as the quality in which it acts, the subscriber is obliged to inform the relying party about the condition or quality in which the digital certificate is being used, this duty of information will be assumed exclusively by the subscriber and there will be no solidarity of the duty of this information with respect to Olimpia IT with the relying parties.

The acts executed by the subscriber under the protection of the digital certificate granted, under the concluded contractual framework, will be his entire and exclusive responsibility, as well as his capacity to be bound is excluding the obligational capacity of the Olimpia IT Digital Certification Entity, for what the effects of the legal acts or businesses will correspond exclusively to the subscriber.

15.3. LIABILITY OF RELYING PARTIES

Relying parties are responsible for verifying the certificate status in order to ensure that the digital signature on the document they have received is valid.

The certificate status can be validated at the following link https://micertificado.olimpiait.com

15.4. COMPLIANCE WITH OLIMPIA IT'S OBLIGATIONS

a) Olimpia IT has signed an insurance policy with an insurance company authorized to operate in Colombian territory and under Colombian law, which covers all contractual and non-contractual damages of subscribers and third parties in good faith exempt from fault arising from errors and omissions, or of acts of bad faith of the administrators, legal representatives, or employees of Olimpia IT in the development of the activities for which it requests or has accreditation.

b) The accredited activities and services are published on the website https://micertificado.olimpiait.com in accordance with the regulations for the use of ONAC accredited and/or associated symbols.

c) Conditions of the insurance policy:

Olimpia IT has signed an insurance policy with an insurance company authorized to operate in Colombian territory and under Colombian law, which covers all contractual and non-contractual damages of subscribers and third parties in good faith exempt from fault arising from errors and omissions, or of acts of bad faith of the administrators, legal representatives, or employees of Olimpia IT in the development of the activities for which it has accreditation.

The insurance policy acquired by Olimpia IT complies with the following

paragraphs of article 9 of Decree 333 of 2014.

> *"c) Covers the aforementioned risks for an insured amount per event of 7.500 legal monthly minimum wages per event.*
>
> *d) Includes automatic restitution clause of the insured value.*
>
> *e) It includes a clause that obliges the insurance company, the policyholder, and the insured to inform ONAC in advance the termination of the insurance contract, or the modifications that reduce the scope or coverage amount."*

The policy is professional civil liability, the policyholder is Olimpia IT SAS, the insurer is SBS Seguros de Colombia SAS, the beneficiaries are affected third parties and its validity is available to the public for consultation on the digital certification entity portal https://micertificado.olimpiait.com

d) Olimpia IT has the financial stability and the necessary resources for its operation as established in Decree 333 of 2014, which can be evidenced through its Financial Statements.

16. DISPUTE RESOLUTION AND CONTRACTUAL MINUTES FOR THE PROVISION OF SERVICES AS ECD

Any controversy that arises between the parties as a result of the contract entered into and/or the application of this certification practice statement (DPC) or the certificate policies (PC), as well as other agreements and/or rules for the provision of services, their interpretation, their execution, domicile and in general their construction, the city of Bogotá DC is indicated as domicile, and will be governed by the laws that regulate the matter in the Republic of Colombia . Therefore, the disputes that arise will be governed in what is not provided for by the regulations of the

Colombian Commercial Code, and in the absence of these, by analogous regulations of the Colombian legal system, as well as by the general principles of law, so that, in In any case, any situation resulting from the execution can be legally resolved. If necessary, local commercial custom will also apply

The differences or controversies that arise between the parties, on the occasion of the signing, execution, interpretation, extension or termination of the contract and other rules or regulations that regulate the provision of the service will be resolved in the following manner, and based on the following parameters:

a) Any conflict arising due to or regarding the contract and other rules or regulations that regulate the service provision will be resolved as a first step according to the procedure indicated below.

b) The Parties shall attempt in good faith to promptly resolve any conflict arising from or with respect to the contract and other rules or regulations that regulate the provision of the service through negotiation between the Legal Representatives and/or those they designate so that they can resolve the dispute.

PROCEDURE:

a) Either Party may give written notice to the other of any conflict or difference that has not been resolved in the normal course of their business dealings.

b) Within a period of no more than ten (10) calendar days from the notification delivery of the conflict and/or difference, the party receiving the notice will deliver a written response to the other. The notice and response will include a) the arguments that support your response; and b) The name and position of the representative of the interests, to this

party and of any other person who will accompany him.

c) Once the response is received, within the following ten (10) calendar days, the representatives of both parties must meet at a mutually agreed time and place, in the city of Bogotá DC, in order to seek a solution to the conflict.

Any controversy or difference related to this contract that the parties cannot resolve in direct negotiation will be submitted to ordinary justice.

16.1. CONTRACT ENTERED INTO BETWEEN THE ECD AND THE APPLICANTS AND/OR SUBSCRIBERS

At https://micertificado.olimpiait.com/Publica/Politica applicants and/or subscribers will find the contract to be concluded with the ECD, which is in the form of acceptance or rejection of terms and conditions, in order to provide the services and/or issue of digital certificates that they require.

If the applicant and/or subscriber rejects the terms and conditions, the application process will end.

16.2. APPLICABLE LAW

Olimpia IT accepts all applicable Colombian laws, evidencing its compliance in the documents of the Digital Certification Entity.

17. CERTIFICATE MANAGEMENT POLICY

Olimpia IT declares that it has an independent document to this Certification Practices Statement, which contains the Certificates Policy.

17.1. ISSUANCE OF DIGITAL CERTIFICATES – REQUIREMENTS AND PROCEDURES

Olimpia IT establishes in its Certificates Policy, Numeral 2, the requirements and procedures for the issuance of digital certificates.

17.2. COMPLIANCE WITH APPLICABLE LAW

Olimpia IT establishes in the document called Certificates Policy, in Numeral 2, compliance with the applicable law.

17.3. COMPLIANCE WITH LEGAL REQUIREMENTS

Olimpia IT establishes that in the document called Certificate Policy in Numeral 2, compliance with the applicable law.

18. TERMS AND CONDITIONS AGREEMENT

Olimpia declares that the applicant prior to acquiring a digital certificate reads and accepts the terms and conditions that must be fulfilled by all those people who wish to interact with Olimpia IT SAS, as an open Digital Certification Entity, for registration on the Olimpia IT website, https://micertificado.olimpiait.com in which the applicant and/or subscriber is obliged to read and accept them.

Once the subscriber and/or applicant has accepted the terms and conditions set forth on the website https://micertificado.olimpiait.com/Publica/Politica. it will be understood that the subscriber and/or applicant is bound by the conditions and obligations established therein.

This agreement may be subject to modifications and its content is in accordance with Colombian legislation in force at the time of its publication.

19. CERTIFICATES' TERM

19.1. ROOT CERTIFICATE TERM

The root certificate term is 20 years from the generation of the self-signed certificate.

19.2. SUBORDINATE CERTIFICATES' TERM

The term of the subordinate certificates of the subordinate CA and TSA are 15 years from the generation of the certificate signed by the Root CA.

19.3. TERM OF CERTIFICATES ISSUED TO SUBSCRIBERS

The term of the certificates issued to subscribers for the certificates of natural persons, legal persons, belonging to a company, legal representative, certified professional and public function is a maximum of 2 years from the issuance of the certificate issued by Olimpia IT.

20. DELIVERY OF DIGITAL CERTIFICATE

20.1. DELIVERY OF THE PHYSICAL TOKEN

Olimpia IT, in its capacity as an Open Digital Certification Entity, is willing to deliver the requested digital certificates in a physical medium by contracting a courier service whose activity is that of courier in Colombian territory, to whom will be delivered the information duly stored in compliance with the security and confidentiality requirements of the information sent.

Additionally, the scope of sending the physical token is restricted only to capital cities, main cities, municipalities surrounding said cities, and municipalities with secondary access roads, Olimpia IT will be able to evaluate special cases where shipments to municipalities outside the established scope are required.

The subscriber will be able to download the manual for the installation and use of the token from the website https://micertificado.olimpiait.com, in section "Documentación", clicking the option " Manual de uso e Instalación

Olimpia Sign, Token Físico y Token Virtual".

Clarify that the installers or drivers required for the physical token usage are not compatible with macOS operating systems.

20.2. MAXIMUM DELIVERY TIMES

Olimpia IT establishes in this Certification Practices Statement a delivery time for the certificate in a maximum of 2 business days from the date of the certification decision, without considering the time that the applicant takes to respond to the requests for rectification of information (if applicable), confirming that the certificate has already been issued and the cryptographic token is ready to be sent.

20.3. OBTAINING THE CERTIFICATE FROM THE WEB PORTAL

In services other than the delivery of the cryptographic token to the subscriber, the subscriber may request Olimpia IT to generate the secure storage of the digital certificate and thus be able to use it from any IP address, through authentication on portal: HTTPs; or through web services, APIs or other forms of software integration, as provided in number 26.6.

21. IMPARTIALITY, NON-DISCRIMINATION, AND INDEPENDENCE IN SERVICES

Olimpia IT establishes in all the activities performed in the operation of the Digital Certification Entity the fulfillment of the impartiality, non-discrimination and independence policy established, and the mitigation of impartiality risks through the sessions of the Impartiality Committee, as a control mechanism.

Olimpia IT, guarantees that the services provided are executed under a framework of independence of functions, objective segregation of the same that allows the roles and functions involved in the provision of the service, not to be affected or biased by external factors.

21.1. NON-DISCRIMINATION FACTORS

For each of the activities performed, the Digital Certification Entity acts in such a way that it allows the presentation of a service request by any person without distinction of sex, race, nationality or family origin, language, religion, political or philosophical opinion or disability.

The technological or cost limitations of the service, as well as the objective causes of rejection of the service, are not factors of discrimination and are due to the technological limitations, financial estimates, and characteristics of the services that Olimpia IT has defined for the provision of its services.

22. CERTIFICATE DIRECTIVES

Olimpia IT then presents the OIDs for the root CA, as well as for the sub-CA certificate and each of the certificates and services provided by Olimpia IT as ECD.

OID
ECD
IANA
1.3.6.1.4.1.50890
Olimpia IT SAS

The structure of the certificate directive will be based on the following specification:

OID
ECD
IANA
1.3.6.1.4.1.50890

Olimpia IT SAS

The structure of the certificate directive will be based on the following specification:

1.3.6.1.4.1 (Standard code – Not modifiable)

50890 (IANA Code – Modifiable only if a new one is acquired)

50890.X (Olimpia Root Certificate – Modify according to partition)

50890.2.X (Partitions in the HSM – Subordinate - It is modified according to the partition) 50890.2.XX (Identification of services – It is modified according to the services offered)
50890.2.XXX (Identification of Sub-services – It is modified to the scope of each service)

CERTIFICATES ISSUED BY THE ROOT
CA OF OLIMPIAIT
1.3.6.1.4.1.50890.2

SUB-CA TO SIGN SUBSCRIBERS
1.3.6.1.4.1.50890.2.1
Natural Person
1.3.6.1.4.1.50890.2.1.1
Legal Person

1.3.6.1.4.1.50890.2.1.2
Certified Professional
1.3.6.1.4.1.50890.2.1.3
Belonging to Company
1.3.6.1.4.1.50890.2.1.4
Public Function
1.3.6.1.4.1.50890.2.1.5
Legal Representative
1.3.6.1.4.1.50890.2.1.6
SERVICES PROVIDED BY OLIMPIAIT
Centralized Signature
1.3.6.1.4.1.50890.2.1.7
Centralized Signature Natural Person 1.3.6.1.4.1.50890.2.1.7.1
Centralized Signature Legal Person 1.3.6.1.4.1.50890.2.1.7.1
Centralized Firm Certified Professional
1.3.6.1.4.1.50890.2.1.7.3
Centralized Signature Belonging to Company 1.3.6.1.4.1.50890.2.1.7.4
Centralized Signature Public Function
1.3.6.1.4.1.50890.2.1.7.5
Centralized Signature Legal Representative
1.3.6.1.4.1.50890.2.1.7.6
Reserved for OlimpiaIT
1.3.6.1.4.1.50890.2.1.8
Certified Email
1.3.6.1.4.1.50890.2.1.9

OIDs ending in 2.1.10 and 2.1.11 are reserved for internal testing by Olimpia

TSA
1.3.6.1.4.1.50890.2.1.12

Certificate for encryption of subscribers' private keys 1.3.6.1.4.1.50890.2.2

TSA Time Stamp
1.3.6.1.4.1.50890.2.3

Note: The certified email service is provided through a third party.

23. TYPE OF CERTIFICATES

Olimpia IT offers the following certificates and services:

- Digital Certificate Natural Person
- Digital Certificate Legal Person
- Digital Certificate Legal Representative
- Digital Certificate Public Function
- Digital Certificate Certified Professional
- Digital Certificate Belonging to a Company
- CHRONOLOGICAL STAMPING
- Centralized Signature
- Certified Email

24. SERVICE'S DESCRIPTION

24.1. DESCRIPTION OF THE DIGITAL CERTIFICATE SERVICE - NATURAL PERSON

The Natural Person certificate accredits the identity of the holder in the signing of electronic documents, guaranteeing the authenticity of the sender of the communication, the non-rejection of the origin and the integrity of the content. The holder of a natural person certificate acts in his own name and interest.

Olimpia IT performs its digital certificate – Natural Person in accordance with the provisions of the asymmetric encryption methodology to guarantee its incorruptibility, which is valid throughout the Colombian territory with a maximum expiration date established in this document.

If the subscriber wants to use this certificate with the centralized signing service, they will need to take one of the centralized signing service packages.

If the subscriber wishes to have the certificate to be used through their own technological platform, or through an authorized third party, and with a specific use, they must file a request with the ECD that complies with the *PKCS#10* certification request standard, - *Format of the messages sent to a Certification Authority to request the certification of a public key*. Therefore, the third party must guarantee that the parameters used for the public key are the SHA256 + RSA cryptographic algorithm, and that these keys have a 2048 bits size.

24.2. DESCRIPTION OF THE DIGITAL CERTIFICATE SERVICE - LEGAL PERSON

The Legal Entity certificate accredits the identity of the subscriber and their status as a company or legal person and allows the subscriber to digitally sign documents in the quality that their certificate accredits.

Olimpia IT performs its digital certificate – Legal Entity in accordance with

the provisions of the asymmetric encryption methodology to guarantee its incorruptibility, which

is valid throughout the Colombian territory with a maximum maturity established in this document.

If the subscriber wants to use this certificate with the centralized signing service, they will need to take one of the centralized signing service packages.

If the subscriber wishes to have the certificate to be used through their own technological platform, or through an authorized third party, and with a specific use, they must file a request with the ECD that complies with the *PKCS#10* certification request standard, - *Format of the messages sent to a Certification Authority to request the certification of a public key*. Therefore, the third party must guarantee that the parameters used for the public key are the SHA256 + RSA cryptographic algorithm, and that these keys have 2048 bits

24.3. DESCRIPTION OF THE DIGITAL CERTIFICATE SERVICE - CERTIFIED PROFESSIONAL

The Certified Professional certificate accredits the identity of the subscriber and his status as a Professional and allows the subscriber to digitally sign documents in his own name and interest.

Olimpia IT performs its digital certificate – Certified Professional in accordance with the provisions of the asymmetric encryption methodology to guarantee its incorruptibility, which is valid throughout the Colombian territory with a maximum expiration date established in this document.

If the subscriber wants to use this certificate with the centralized signing service, he will need to take one of the centralized signing service

packages.

24.4. DESCRIPTION OF THE DIGITAL CERTIFICATE SERVICE - COMPANY BELONGING

The Company Belonging certificate accredits the subscriber's identity and their status as a company or legal person and allows the subscriber to digitally sign documents in the quality that their certificate accredits.

Olimpia IT performs its digital certificate – Company Belonging in accordance with the provisions of the asymmetric encryption methodology to guarantee its incorruptibility, which is valid throughout the Colombian territory with a maximum expiration date established in this document.

If the subscriber wants to use this certificate with the centralized signing service, they will need to take one of the centralized signing service packages.

24.5. DESCRIPTION OF THE DIGITAL CERTIFICATE SERVICE - PUBLIC FUNCTION

The Public Function certificate is issued in the name of natural persons who prove the holder's identity and his character as a public official or individual in the exercise of a public function, either by appointment or as a result of the signing of a contract that enables him as such, in the signing of electronic documents guaranteeing the authenticity of the sender of the communication, the non-rejection of the origin and the integrity of the content. The holder of a Public Function certificate acts in the quality accredited in it.

Olimpia IT performs its digital certificate – Public Function in accordance

with the provisions of the asymmetric encryption methodology to guarantee its incorruptibility, which is valid throughout the Colombian territory with a maximum expiration date established in this document.

If the subscriber wants to use this certificate with the centralized signing service, he will need to take one of the centralized signing service packages.

24.6. DESCRIPTION OF THE DIGITAL CERTIFICATE SERVICE – LEGAL REPRESENTATIVE

The Legal Representative certificate accredits the identity of the subscriber and his status as legal representative of an entity or legal person, It allows the subscriber to digitally sign documents on behalf of the entity or legal person he represents.

Olimpia IT performs its digital certificate – Legal Representative in accordance with the provisions of the asymmetric encryption methodology to guarantee its incorruptibility, which is valid throughout the Colombian territory with a maximum expiration date established in this document.

If the subscriber wants to use this certificate with the centralized signing service, he will need to take one of the centralized signing service packages.

24.7. DESCRIPTION OF THE TIME STAMPING SERVICE

The chronological stamping service gives certainty on the date and time integrity of a document by taking the Colombian legal time of the National Institute of Metrology, or whoever acts on its behalf, affixing a digital signature of the TSA.

To use the Time Stamping service, the subscriber must purchase any one

of the accredited digital certificates offered by the ECD, whose commercial terms and fees are specified in this DPC (see Section 11.1).

24.8. DESCRIPTION OF THE CENTRLIZED SIGNATURE SERVICE

It is a centralized management of the digital certificates used in an organization, where the digital certificates operate from a single, controlled, and secure repository.

They are digital certificates generated and stored on the Olimpia IT server, which allows the subscriber to use them from any computer.

To do this, in the digital signature certificate the information that the subscriber has previously provided through the portal https://micertificado.olimpiait.com will be used, the subscriber will perform an authentication (entry code sent to his email or mobile number in SMS, registered at the time of registration of the applicant) in the portal https://micertificado.olimpiait.com the subscriber may request the service from any IP, with internet service.

Through the application of the digital certification system implemented, Olimpia IT performs the issuance and possession of the private key by generating the encrypted digital signature certificate and complemented with a 4-digit private key (PIN) that only the subscriber knows; is done using a FIPS 140-2 Level 3 certified HSM (Hardware Security Module). It is stored in an independent and isolated technological infrastructure, which complies with the PKCS#11 format and with the international information security standards established by the international standard NTC-ISO/IEC 27001 in its current version. The subscriber can use his certificate by accessing this technology (wrapping key), which consists of calling the service from his secure and isolated hosting, to be used from a FIPS 140-2 Level 3 certified HSM (Hardware Security Module).

To use the service, the subscriber must link a digital certificate issued by

Olimpia IT that contains the subscriber's information (the subscriber must select the digital certificate with which he will use this service at the time of service acquisition), this procedure will be done on the portal https://micertificado.olimpiait.com. The cost of this service, which includes the issuance of the respective digital certificate, is defined in the fee section.

In .pdf type files, the signature will be integrated into the file and when it is another type of file, the signature is not integrated, but it will be delivered together with the original document in a p7z type file, which contains the information of the original file and the digital signature.

The subscriber must purchase one of the commercial packages offered for this service.

24.8.1. THIS SERVICE HAS THE FOLLOWING LIMITATIONS:

- The service will work correctly using Chrome browsers version 71.0.3578.98 and Microsoft EDGE version 38.14393.2068.0.

24.8.2. THIS SERVICE INCLUDES, IN ADDITION TO THE ESTABLISHED REQUIREMENTS, THE FOLLOWING OPERATION:

- The subscriber must enter a 4-digit password (PIN), in order to generate an authentication on the page https://micertificado.olimpiait.com and after that, be able to use the service.

24.9. DESCRIPTION OF THE CERTIFIED EMAIL SERVICE

This service accredits the subscriber's identity and allows him to send digitally signed email-type data messages, guaranteeing the authenticity of the communication sender, the non-rejection of the origin and the integrity of the content.

The mail service will be provided through a provider that complies with the

provisions of current regulations, particularly articles 20 and 21 of Law 527 of 1999.

The accuse of receipt are admissible regarding the fact of shipment and delivery, as well as the legal date and time of shipment, and the authenticity of its content, in accordance with articles 12 and 20 of Law 527 of 1999.
Olimpia IT will be in charge of carrying out the complete life cycle to safeguard the Subscriber's information and comply with the Specific Accreditation Criteria. Likewise, through the platform of the service provider, it will be in charge of generating the credentials with their respective keys and will include the time stamp and Olimpia IT's digital signature, so that they give probative value to the email or its content, in accordance with article 10 of Law 527 of 1999. The certified email service does not require the issuance of a digital certificate for the subscriber.
By granting the service by the ECD, the Subscriber will receive emails with the approval of the service, where the scope and access to the documentation necessary for use of the service is specified, and email with the user credentials and password to activate the service, service and start using it.

The subscriber must purchase one of the commercial packages offered for this service as defined in the section on fees. The subscriber must keep the notification option of acknowledgment of receipt of their email account active during the provision of the certified email service.

25. CRYPTOGRAPHIC DEVICES

The cryptographic devices guidelines used for the issuance of each of the digital certificates issued by Olimpia IT are described in Numerals 7.2.1 and 7.2.11 of this Certification Practices Statement.

26. SERVICES AND APPLICATIONS FOR THE SERVICES USAGE

26.1. SIGNATURE VALIDITY

Olimpia IT's signature validity service is exposed on the website and allows applicants, subscribers, and relying parties, among others, to know the validity of a signature, as well as the time stamp made by the Digital Certification Entity, for which the user must load the signature in format *.p7z and the system responds if the signature is valid or not. Clarify that the installers or drivers required for the physical token usage are not compatible with macOS operating systems.

26.2. OLYMPIA SIGN

The "Olimpia SIGN" service is the signature application developed by Olimpia IT so that its subscribers can sign documents when they acquire a physical token. This application can be downloaded directly from the website of the Digital Certification Entity and only works on computers with the Windows 10 operating system.

26.3. DRIVER TOKEN

It allows the interaction of the operating system with the token cryptographic device, makes it easier for the user to import certificates, authenticate in signing processes and configure the access PIN.

26.4. CSR GENERATOR

CSR GENERATOR Software provided to applicants for certification services to facilitate the generation of a certificate request in PKCS#10 format.

26.5. ISSUANCE OF DIGITAL CERTIFICATES FOR PKCS#10 REQUEST

Olimpia IT may issue digital certificates based on a request for digital certification filed by the subscribers, or third parties authorized by the subscribers, by law, or by a competent public or private entity.

In these cases, the petitions filed must comply with the certification request standard *PKCS#10 - Format of messages sent to a Certification Authority to request the certification of a public key*. Therefore, the third party must guarantee that the parameters used for the public key are the SHA256 +

RSA cryptographic algorithm, and that these keys have a 2048 bits size.

26.6. WEB SERVICES, APIS AND OTHER FORMS OF SOFTWARE INTEGRATION

Depending on the needs and requirements of subscribers regarding the use of digital certificates, or the consumption of accredited services, Olimpia IT may make available to them APIs web services, and other forms of software integration, which may be integrated into the platforms or tools made available to subscribers or third parties authorized by subscribers, by law, or by a competent public or private entity for this purpose.

27. LOCATION

Commercial and judicial notifications address: Cra. 7 #24-89, Torre Colpatria, Piso 46, Bogotá
Telephone: (+57 601) 742 7878
Email: gerencia@olimpiait.com

28. POLICY TO RESOLVE PETITIONS, COMPLAINTS, CLAIMS AND SUGGESTIONS

Olimpia IT makes available to the general public and its related parties to address any request, complaint or claim, the following channels:

- Website https://micertificado.olimpiait.com where you will be given a timely solution according to the established times.
- PQRS hotline: (+57 601)742 7878

28.1. PROCEDURE FOR THE RESOLUTION OF PETITIONS, COMPLAINTS, CLAIMS AND SUGGESTIONS - PQRS-

Olimpia IT declares that the procedures to resolve requests, complaints, claims, and suggestions are available to the public on the website https://micertificado.olimpiait.com

29. PROPERTY OF OLYMPIA

This document is protected by copyright regulations, any reproduction, distribution, or total or partial modification to unauthorized users, or any improper use of confidential information will be considered a crime in accordance with the provisions of the Penal Code and current Laws of the Colombian state.

The Spanish version of this document (Declaración de Prácticas de Certificación – DPC), will take precedence over this English version and any difference or controversy between this document and the Spanish version must be resolved in accordance with the interpretation and reading of the DPC in Spanish.