

POL-030-ING Certificates Policy

Version Nro. 09

CONTENTS

1. REVISION HISTORY 3

2. CERTIFICATES MANAGING POLICIES 7

2.1. ABOUT COMPLIANCE WITH THE CONTENT OF CERTIFICATES MANAGEMENT POLICIES 7

2.2. CHARACTERISTICS OF CERTIFICATES 10

2.2.1 DIGITAL CERTIFICATE IN PHYSICAL TOKEN OR VIRTUAL TOKEN O TOKEN VIRTUAL OR VIRTUAL TOKEN O TOKEN VIRTUAL 10

2.2.2 CRYPTOGRAPHIC DEVICE CARE 10

2.2.3 CERTIFICATE IN VIRTUAL TOKEN O TOKEN VIRTUAL 11

2.2.4 CHARACTERISTICS 12

2.2.5 DEVICE CARE 12

2.2.6 ASSOCIATED RISKS 13

2.3. REQUIREMENTS AND REGULATORY SOURCE 13

2.3.1 THE CONTENT OF THE CERTIFICATE 13

2.3.2 INTERNAL REQUIREMENTS 15

2.3.3 REGULATORY SOURCE 15

2.4. RESTRICTIONS ON UPLOADING DOCUMENTS BY THE APPLICANT 18

2.4.1 DIGITAL CERTIFICATION SERVICES REQUIREMENTS 19

2.4.2 TYPES OF DATA MESSAGES THAT CAN BE SIGNED BY DIGITAL CERTIFICATES 21

2.4.3 RESTRICTIONS ON INSTALLERS 21

2.5. DESCRIPTION OF THE REQUIREMENTS AND PROCEDURES FOR THE ISSUANCE OF DIGITAL CERTIFICATES 21

2.5.1 DIGITAL CERTIFICATE - NATURAL PERSON 22

2.6. DESCRIPTION OF THE REQUIREMENTS AND PROCEDURES FOR THE ISSUANCE OF DIGITAL CERTIFICATES THROUGH CENTRALIZED SIGNATURE 37

2.7. CRYPTOGRAPHIC DEVICES OFFERED BY OLIMPIA 49

2.8. LIABILITY DISCLAIMER 49

2.9. CHANGES IN THE CERTIFICATE'S CONTENT 50

3. PROPERTY OF OLYMPIA 50

1. REVISION HISTORY

VERSION	DATE	DESCRIPTION
POL IN # 1 POL ES # 11	2023-01-23	Creation of the document, version No. 11 is translated from Spanish to English.
POL IN # 2 POL ES # 12	2023-04-04	In numeral 2.2.1 The content of the certificate, the matrix of the content of the certificate is included. In numeral 2.3 RESTRICTIONS ON UPLOADING DOCUMENTS BY THE APPLICANT, the capacity to sign a document is no longer 3 megabytes, but 40 megabytes.
POL IN # 3 POL ES # 13	2023-05-29	It is made clear in numeral 2.1. ABOUT COMPLIANCE WITH THE CONTENT OF THE CERTIFICATES MANAGEMENT POLICIES, that in number 11.1 of the Certification Practices Statement are the rates. In numeral 2.3 RESTRICTIONS ON UPLOADING DOCUMENTS BY THE APPLICANT, the capacity is no longer 30 megabytes if it is not 40 megabytes for centralized signature. In numeral 2.3 RESTRICTIONS ON UPLOADING DOCUMENTS BY THE APPLICANT, it is made clear that when signing from a Token o Token Virtual there is no limit on uploading documents. In numeral 2.4.7 Certified email This service is acquired in the same way as the other services found in the platform of my certificate.

POL IN # 4 POL ES # 14	2023-09-27	Numerals 2.2 are included. CHARACTERISTICS OF CERTIFICATES, 2.2.1. Digital certificate in Physical Token or Virtual Token o Token Virtual or virtual Token o Token Virtual, 2.2.2. Care of the cryptographic device, 2.2.3. Certificate in virtual Token o Token Virtual, 2.2.4. Characteristics, 2.2.5. Device care, and 2.2.6. Associated risks The name of the DIGITAL CERTIFICATION SERVICES is updated within the "technical source" box and the centralized signature scope is eliminated since it is found in the other scopes It makes it clear that to sign from a physical Token or Virtual Token there is no upload limit, in section 2.4. The Token or Virtual Token is included in all the policy that is related to the physical Token or Virtual Token. The lifecycle process is updated and the ID certificate is removed for all policies. It is included in section 2.5.7. For the mail service, it is not necessary to issue a digital certificate for a subscriber. • In this same section it is made clear that 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. For the mail service, the request for certificates of a qualified professional, public function, membership and legal entity is eliminated, since it is a service that is only used for a legal representative or natural person and is not a digital certificate but a service. In section 2.5.7.1.1, the following comment is left: "Information to be filled out in the application: (only works for digital certificates)", this functionality only works for digital signatures, not for the certified email service.

POL IN # 5 POL ES # 15	2024-02-06	It is included in section 2.3.3. Regulatory Source, Decree 2364 of 2012 and the scope of Generation of Certified Electronic Signatures with their respective standards is included. It is made clear in Section 2.4. RESTRICTIONS ON UPLOADING DOCUMENTS BY THE APPLICANT, that the uploading of documents is for signature services. Section 2.4.2 "Limitations for use of certified electronic signature services" is included. Section 2.7 DESCRIPTION OF THE REQUIREMENTS AND PROCEDURES FOR THE ISSUANCE OF THE CERTIFIED ELECTRONIC SIGNATURE is included. Section 2.8 PLATFORM SECURITY POLICIES is included. Section 2.12 POLICIES OF THE CERTIFIED ELECTRONIC SIGNATURE SERVICE is included.
POL IN # 6 POL ES # 16	2024-02-16	The technical standards are updated in section 2.3.3, the activities of Decree Law 019 of 2012- Article 161 are included. Add notes in section 2.4.1, section 1 and section 2. Eliminate numeral 2.4.2, 2.7

POL IN # 7 POL ES # 17	2025-06-10	Remove the references to Certified Electronic Signature. Template and logo updated
POL IN # 8 POL ES # 18	2026-06-11	Update the URL address in the “Access to the information of the issuing” section (2.3.1).
POL IN # 9 POL ES # 19	2026-06-26	As a result of the evaluation carried out, item 2.11. CERTIFIED ELECTRONIC SIGNATURE SERVICE POLICIES is removed. Likewise, in item 2.4 the reference to the certified electronic signature service is withdrawn, in order to provide formality.

2. CERTIFICATES MANAGING POLICIES

Below are the certificate policies applicable to ECD Olimpia IT, Olimpia declares that it has a public document called Certificate Policies, available on the page https://micertificado.olimpiait.com which contains the Policies for managing certificates.

2.1. ABOUT COMPLIANCE WITH THE CONTENT OF CERTIFICATES MANAGEMENT POLICIES

Olimpia IT establishes that the subscriber identification procedures are described in the Certification Practice Statement, in Numeral 4.2.

Olimpia IT establishes that the procedure for updating the information contained in the certificates is described in the Certification Practice Statement, Numeral 3.3.1.1.

Olimpia IT, establishes that the procedure, the verifications, the opportunity, and the people who may invoke the causes of revocation of the certificates, are described in numeral 5.8 of the Certification Practices Statement.

Olimpia IT, establishes that the Information on the security system to protect the information that is collected in order to issue the certificates, is described in Numeral 2.4 of the Certification Practices Statement.

Olimpia IT establishes that the duties and rights of the ECD applicants, subscribers and trusting third parties are detailed in Number 14 of the Certification Practices Statement.

{Olimpia IT establishes that the duties and rights of the ECD applicants, subscribers and trusting third parties are detailed in Number 14 of the Certification Practices Statement.

{Olimpia IT establishes that the commercial conditions of the ECD digital certificates are detailed in Number 11 of the Certification Practices Statement.

Olimpia IT establishes that the conditions of independence and impartiality of the ECD are detailed in the Impartiality, Independence, and Non-Discrimination Policy.

In addition to including the regulatory and legal provisions, Olimpia IT, accepts in this Certificate Policy, the recommendations of RFC 3647.

The applicable terms of RFC 3647, to this Certificate Policy, will be accepted from the referral made of this document to the Certification Practices Statement, and in what is not contained therein, in this Certificate Policy.

The obligations of the ECD and the subscribers of the digital certificate, and the precautions that third parties who trust the digital certificate must observe are published in Numeral 14 of the Certification Practices Statement.

The information that will be requested from subscribers is published in Numeral 2 of this Certificate Policy.

The ECD's liability limits for each of its services and for each signed document are published in number 15 of the Certification Practices Statement.

The validity of each type of digital certificates are published in Numeral 19 of the Certification Practices Statement.
The fees for issuing certificates and the services they include are published in number 11.1 of the Certification Practices Statement

The information that will be requested from subscribers for the chronological stamping service is published in Numeral 10 of the Certification Practices Statement.

The models and minutes of the subscription contracts that the ECD will use to provide its digital certification services are published in Numeral 16 of the Certification Practices Statement and on the website https://micertificado.olimpiait .com

Digital certification services requirements: According to the regulatory entities, the ECDs must publish the specific policies that establish the requirements and regulatory source to provide each of the digital certification services, established in Numeral 2 of this Certificate Policy.

Olimpia IT reports the supported cryptographic devices it offers, the associated risks, and the security commitments contained, in Numeral 2 of this Certificate Policy.

2.2. CHARACTERISTICS OF CERTIFICATES

2.2.1 Digital certificate in Physical Token or Virtual Token o Token Virtual or virtual Token o Token Virtual

It corresponds to a physical device that connects to the USB port of the computer equipment, which contains the digital certificate and the pair of public and private keys. It is also protected by a fixed key to execute its use. It is not required to have the device connected to the Internet to use the Token o Token Virtual.

It is the client's responsibility to safeguard the delivered device, as well as manage the respective password.

Olimpia IT, committed to managing the environmental impact of physical storage devices delivered to clients, will make the following available to users:

- A new Physical Token or Virtual Token o Token Virtual or virtual Token o Token Virtual delivery option which has gone through a high-standard physical and functional review reconditioning process.

- A secure deletion process has been carried out to eliminate the previous digital certificate, in accordance with the application functionalities provided by the provider.

This new process guarantees that the Token o Token Virtual or virtual Token o Token Virtual meets the appropriate usability and technological operation conditions.

2.2.2 Cryptographic device care

- Operating temperature 0°C to 70°C (32°F to 158°F)
- Storage temperature -40°C to 85°C (-40°F to 185°F)
- Humidity range 0- 100% without condensation

For the assignment of keys by the subscriber, the following recommendations and care must be taken into account for their protection:

- The password must be for personal use and must not be transferred to a third party.
- Store your password in safe places, it is recommended to memorize it to prevent other people from knowing it.
- Do not leave the device connected to the equipment when it is not in use.
- Correctly disconnect the device
- Avoid bumps and falls.
- Use the applications provided by Olimpia IT to use your certificate.

The risks to which the cryptographic devices used would be exposed are:

- Environmental fluctuations outside normal operating ranges, such as voltage and temperature.
- Attempts at unauthorized physical access, outside the manufacturer's technical sheet

To know the level of risks associated with cryptographic devices, you can consult the following link: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

2.2.3 CERTIFICATE IN VIRTUAL TOKEN O TOKEN VIRTUAL

It corresponds to an infrastructure arranged as a service in which the digital certificates issued are kept together with their pair of keys in the technological infrastructure of Olimpia IT, which are associated with a username and password given to the certificate holder. To use it you must

have an active Internet connection.

2.2.4 CHARACTERISTICS

- 2048-bit private key.
- Certificate signing algorithm with SHA256 hash.
- X.509 v3 certificates.
- Storage in infrastructure that complies with FIPS 140-2 Level 3.
- File signature with hash of the document (does not require sending the document to protect its confidentiality).
- Signature component that allows consumption by Olimpia sign
- Windows 10 or higher
- Framework 4.0 or higher
- Access to URLs
- https://micertificado.olimpiait.com/Publica/Descargas
- https://micertificado.olimpiait.com/Publica/ValidacionCRL

2.2.5 DEVICE CARE

There is physical and technological care of the data center where the HSM is located, to ensure its proper functioning, where you can find humidity, electricity, unauthorized access controls, fire detectors, biometric security for access to the rack and the data center area, among others.

For the assignment of keys by the subscriber, the following recommendations and care must be taken into account for their protection:

- The password must contain eight (8) numeric digits
- The password must be for personal use and must not be transferred to a third party.
- Store your password in safe places, it is recommended to memorize

it to prevent other people from knowing it.

2.2.6 ASSOCIATED RISKS

For the virtual Token o Token Virtual certificate, the risks to which it is exposed are those in which environmental aspects prevent the proper functioning of the data center where the HSM is installed.

In logical terms, the associated risks are defined by cyber attacks that prevent access and/or availability.

2.3. REQUIREMENTS AND REGULATORY SOURCE

2.3.1 THE CONTENT OF THE CERTIFICATE

The certificate generated by Olimpia IT will have the following content:

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: 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: The digital Certificate is generated in CRT format

2.3.2 INTERNAL REQUIREMENTS

OlimpiaIT declares that it meets all the internal requirements necessary to be accredited as an open ECD.

2.3.3 REGULATORY SOURCE

Legal source:

Decree Law 019 of 2012, (Its articles 160, 161, 162 and 163 modify the articles 29, 30, 32 and 34 of Law 527 of 1999), Law 527 of 1999, Decree 107 4 of 2015, "By means of which the Single Regulatory Decree of the Commerce, Industry and Tourism Sector is issued", Decree 333 of 2014 , Decree 2460 of 2013 "By which article 555-2 of the Tax Statute is regulated" and the RUT is established as the unique mechanism to identify, locate and classify the subjects bound by the DIAN, Specific Accreditation Criteria - CEA- 3.0-07 V2, Decree 2364 of 2012 and the other complementary technical and legal standards that support the correct and legal operation of the services and the certificates that are issued.

Technical source:

DIGITAL CERTIFICATION SERVICE		TECHNICAL REQUIREMENTS
Digital certificates for natural persons on local or centralized devices	1,2,3,4	RSA 2048 RSA 4096 SHA-256 minimum key size 2048 bits Aug 2002 RFC 3647 Nov 2003 RFC 4523 June 2006 RFC 5126 February 2008 RFC 5280 May 2008 RFC 6960 June 2013 ETSI EN 319 142-2 (2025-7) W3C XML (XAdES) FIPS 140-2 level 3 May 2001
Digital certificates for legal entities on local or centralized devices	1,2,3,4	RSA 2048 RSA 4096 SHA-256 minimum key size 2048 bits Aug 2002 RFC 3647 Nov 2003 RFC 4523 June 2006 RFC 5126 February 2008 RFC 5280 May 2008 RFC 6960 June 2013 ETSI EN 319 142-2 (2025-7) W3C XML (XAdES) FIPS 140-2 level 3 May 2001
Digital certificates for qualified professionals on local or centralized devices	1,2,3,4	RSA 2048 RSA 4096 SHA-256 minimum key size 2048 bits Aug 2002 RFC 3647 Nov 2003 RFC 4523 June 2006 RFC 5126 February 2008 RFC 5280 May 2008 RFC 6960 June 2013 ETSI EN 319 142-2 (2025-7) W3C XML (XAdES) FIPS 140-2 level 3 May 2001

DIGITAL CERTIFICATION		TECHNICAL REQUIREMENTS
Digital certificates for company membership on local or centralized devices	1,2,3,4	RSA 2048 RSA 4096 SHA-256 minimum key size 2048 bits Aug 2002 RFC 3647 Nov 2003 RFC 4523 June 2006 RFC 5126 February 2008 RFC 5280 May 2008 RFC 6960 June 2013 ETSI EN 319 142-2 (2025-7) W3C XML (XAdES) FIPS 140-2 level 3 May 2001
Digital certificates for public functions on local or centralized devices	1,2,3,4	RSA 2048 RSA 4096 SHA-256 minimum key size 2048 bits Aug 2002 RFC 3647 Nov 2003 RFC 4523 June 2006 RFC 5126 February 2008 RFC 5280 May 2008 RFC 6960 June 2013 ETSI EN 319 142-2 (2025-7) W3C XML (XAdES) FIPS 140-2 level 3 May 2001
Digital certificates for legal representative on local or centralized devices	1,2,3,4	RSA 2048 RSA 4096 SHA-256 minimum key size 2048 bits Aug 2002 RFC 3647 Nov 2003 RFC 4523 June 2006 RFC 5126 February 2008 RFC 5280 May 2008 RFC 6960 June 2013 ETSI EN 319 142-2 (2025-7) W3C XML (XAdES) FIPS 140-2 level 3 May 2001

CHRONOLOGICAL STAMPING	5	RSA 4096 SHA-256 minimum key size 2048 bits Aug 2002 RFC 3161 Aug 2001 RFC 3628 November 2003 RFC 5905 June 2010

DIGITAL CERTIFICATION		TECHNICAL REQUIREMENTS
Certified Email	2,5,9	RSA 2048 RSA 4096 SHA-256 minimum key size 2048 bits Aug 2002 RFC 3647 Nov 2003 RFC 4523 June 2006 RFC 5280 May 2008 RFC 5652 September 2009 RFC 6960 June 2013 FIPS 140-2 level 3 May 2001

2.4. RESTRICTIONS ON UPLOADING DOCUMENTS BY THE APPLICANT

OlimpiaIT informs applicants of the following restrictions when providing a digital certification service:

- Maximum size per document attached to the service request, 40 MB.
- Document format allowed in the Request for services: "Any file format is allowed."
- The size limitation required of applicants for the upload, which is 40 MB, applies to the Centralized Signature service.
- To sign from Token o Token Virtual there is no charge limit.
- The service will work correctly using Chrome browsers version

71.0.3578.98 and Microsoft EDGE version 38.14393.2068.0.

- The Windows Olimpia Sign application is supported on Windows 10 or higher operating system.

- The web application does not allow the use of the exposed services with certificates issued by other certification entities. If the subscriber makes use of the services with certificates issued by other Certification Entities, OLIMPIA IT does not supply the necessary technical complements for its proper functioning.
- The email service cannot exceed a maximum size of 15 MB
- For validation by Facial recognition, you must make the request with a device that has an integrated or connected camera or have a legible image of the identity document to be uploaded to the portal.

2.4.1 DIGITAL CERTIFICATION SERVICES REQUIREMENTS

1. Digital Certificate Natural Person: This certificate will allow a person to digitally sign under the condition that the signer is a natural person, accept the content of the signed data message and be bound with respect to its content as a natural person.

Note: When issuing a digital signature for a natural person, Olimpia IT may use a delegated identity validation mechanism through a third party, which has the sole purpose of issuing certificates for electronic billing, and which complies with the Specific Criteria of Accreditation, in section 10.3

2. Digital Certificate Legal Person: This certificate will allow a data message to be digitally signed, under the condition that the person who owns the digital signature is the legal representative of a legal person,

safeguarding the obligation of the trusting third party to verify by legal and appropriate means the scope and validity of the legal representation exercised by the signatory.

Note: When issuing a digital signature for a legal entity, Olimpia IT may use a delegated identity validation mechanism through a third party, which has the sole purpose of issuing certificates for electronic billing, and which complies with the Specific Criteria of Accreditation, in section 10.3

3. Digital Certificate Legal Representative: This certificate will allow a data message to be digitally signed, under the condition that the person who owns the digital signature is the legal representative of a legal person, safeguarding the obligation of the trusting third party to verify by legal and appropriate means the scope and validity of the legal representation exercised by the signatory.

4. Digital Certificate Qualified Professional: This certificate will allow a data message to be digitally signed, under the condition that the person who owns the digital signature acts as a professional of an accredited area under a Colombian legal framework, safeguarding the obligation of the trusting third party to verify by legal and appropriate means the scope and validity of the legal representation exercised by the professional.

5. Digital Certificate Belonging to a Company: This certificate will allow a data message to be digitally signed, under the condition that the person who owns the digital signature acts as an employee or under a personal service provision contract, safeguarding the obligation of the

trusting third party to verify by legal and appropriate means the scope and validity of the belonging to the company.

6. Digital Certificate Civil Service: This certificate will allow a data message to be digitally signed, under the condition that the person who owns the digital signature acts as a civil officer or under a personal service provision contract, safeguarding the obligation of the trusting third party to verify by legal and appropriate means the scope and validity of the civil service.

2.4.2 TYPES OF DATA MESSAGES THAT CAN BE SIGNED BY DIGITAL CERTIFICATES

Any of the digital certificates issued by Olimpia to subscribers can be used in data messages whose extension is pdf., doc., xml., cms., .zip.

2.4.3 RESTRICTIONS ON INSTALLERS

Clarify that the installers or drivers required for the Physical Token or Virtual Token o Token Virtual usage are not compatible with macOS operating systems.

2.5. DESCRIPTION OF THE REQUIREMENTS AND PROCEDURES FOR THE ISSUANCE OF DIGITAL CERTIFICATES

Olimpia IT establishes that the procedure for issuing the requested digital certificates is detailed and developed in Numeral 5 of the Certification Practice Statement, and is complemented by the development of this Numeral, which specifies the application process by the applicant.

It is clarified that the identity validation mechanisms described in Section 4.2 of the CPS apply to the issuance of these digital certification services. The same, it is clarified that the subscriber will receive the

documentation of the digital certification once OlimpiaIT grants the digital certification service.

2.5.1 DIGITAL CERTIFICATE - NATURAL PERSON

➢ The applicant must accept the terms and conditions.

➢ The applicant must answer the validation questions.

2.5.1.1 DOCUMENTS TO REQUEST:

- Legible image of the identity document
- Public service bill image.
- RUT in the cases of natural or legal persons who perform an economic activity for which they are obliged to register in a Single Tax Registry.

Note:

- OlimpiaIT may exclude the presentation of some of the previously indicated documents, for natural person digital certificates that will be used in the electronic billing process, and in accordance with the results of the risk analysis.
- Documentation containing the applicant's biometric or sociodemographic information may be additionally requested if Olimpia deems it necessary.
- Adds Explanatory note of "When validation of identity by facial recognition is selected, the applicant is not asked for a copy of the identity document or the state document of the citizenship/foreigner ID" for the issuance of all digital certificates.
- The subscriber will not be allowed to use the issued digital certificate until the effective date begins.

2.5.1.2 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
- The applicant must fill in the effective date on the application form.
    - If the field is not filled out, the effective date will be the date the digital certificate is issued.

If the applicant acquires the digital certificate with a Physical Token or Virtual Token o Token Virtual, he must purchase the single package and pay the cost of the Physical Token or Virtual Token o Token Virtual detailed in section 11 of the CPS.
If the applicant acquires the digital certificate with centralized signature, he must purchase one of the centralized signature service packages that are detailed in this CPS and pay the cost of the package according to the forms established for it in section 11 of the CPS.
If the certificate generation is successful, the applicant must activate the same according to what is specified in the application, whether through Physical Token or Virtual Token o Token Virtual or centralized signature.
OlimpiaIT may issue digital certificates from a *PKCS#10* certification request - *Format of messages sent to a Certification Authority to request the certification of a public key*. In these cases, the required documentation and the information requested in the form may be limited and will be the minimum necessary to validate the quality of

Natural Person of the applicant.

2.5.2 DIGITAL CERTIFICATE – LEGAL PERSON

➢ The applicant must accept the terms and conditions.

➢ The applicant must answer the validation questions.

2.5.2.1 DOCUMENTS TO REQUEST:

- Certificate of Existence and Legal Representation (validity no older than 30 days.)
- Legible image of the Legal Representative's identity document

Note: In the case of legal person digital certificates that are going to be used in the electronic billing process, Olimpia IT will request the legible image of the Legal Representative's identity document and the RUT of the legal person.

2.5.2.2 INFORMATION TO FILL IN THE APPLICATION:

- Name or business name of the company
- NIT:
- Company Address (Department)
- Company Address (City)
- Company Address (Address)
- Company Email
- Company's Telephone
- Names and surnames of the legal representative
- Type Identity document of the Legal Representative

- Identity document number of the Legal Representative
- Commercial registration number
- In the request for the digital certificate, the applicant must inform the effective date, if not completed, the effective date will be the issuance date of the digital certificate.

If the applicant acquires the digital certificate with a Physical Token or Virtual Token o Token Virtual, he must purchase the single package and pay the cost of the Physical Token or Virtual Token o Token Virtual detailed in section 11 of the CPS.

If the applicant acquires the digital certificate with centralized signature, he must purchase one of the centralized signature service packages that are detailed in this CPS and pay the cost of the package according to the forms established for it in section 11 of the CPS.

If the certificate generation is successful, the applicant must activate the same according to what is specified in the application, whether through Physical Token or Virtual Token o Token Virtual or centralized signature.

OlimpiaIT may issue digital certificates from a *PKCS#10* certification request - *Format of messages sent to a Certification Authority to request the certification of a public key*. In these cases, the required documentation and the information requested in the form may be limited and will be the minimum necessary to validate the quality of Legal Person of the applicant.

The subscriber will not be allowed to use the issued digital certificate until

the effective date begins.

2.5.3 DIGITAL CERTIFICATE - QUALIFIED PROFESSIONAL

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

2.5.3.1 DOCUMENTS TO REQUEST:

- Legible image of the identity document
- Public service bill image
- Degree certificate or professional card (legible)

Note:

- Documentation containing the applicant's biometric or sociodemographic information may be additionally requested if Olimpia deems it
- When identity validation by facial recognition is selected, the applicant will be asked for a copy of the identity document or the state document of the citizenship/foreigner identity card..
- The subscriber will not be allowed to use the issued digital certificate until the effective date begins.

2.5.3.2 INFORMATION TO FILL IN THE APPLICATION:

- Type of Certificate: Qualified Professional
- Names and surnames
- Type of identity document
- Number of identity document
- Department of residence

- City of residence
- Residence address
- Cell phone
- Another phone
- Email
- Obtained title
- Professional card number or degree certificate
- Name of Entity where the professional card or degree certificate was obtained
- In the request for the digital certificate, the applicant must inform the effective date, if not completed, the effective date will be the issuance date of the digital certificate.

If the applicant acquires the digital certificate with a Physical Token or Virtual Token o Token Virtual, he must purchase the single package and pay the cost of the Physical Token or Virtual Token o Token Virtual detailed in section 11 of the CPS.
If the applicant acquires the digital certificate with centralized signature, he must purchase one of the centralized signature service packages that are detailed in this CPS and pay the cost of the package according to the forms established for it in section 11 of the CPS.

If the certificate generation is successful, the applicant must activate the same according to what is specified in the application, whether through Physical Token or Virtual Token o Token Virtual or centralized signature.

2.5.4 DIGITAL CERTIFICATE - BELONGING TO A COMPANY

➢ The applicant must accept the terms and conditions.

➢ The applicant must answer the validation questions.

2.5.4.1 DOCUMENTS TO REQUEST:

- Legible image of the employee's identity document
- Labor Certificate (validity no older than 30)
- Certificate of Existence and Legal Representation (validity no older than 30 days.) Note:
    - Documentation containing the applicant's biometric or sociodemographic information may be additionally requested if Olimpia deems it
      Necessary
    - When validation of identity by facial recognition is selected, the applicant is not asked for a copy of the identity document, or the state document of the citizenship/foreigner ID.
    - The subscriber will not be allowed to use the issued digital certificate until the effective date begins.

2.5.4.2 INFORMATION TO FILL IN THE APPLICATION:

- Type of Certificate: Belonging to Company
- Name or business name of the company
- Company's NIT
- Company Address (Department)
- Company Address (City)
- Company Address (Address)

- Company Email
- Company's Telephone
- Names and surnames of the employee
- Type of the employee's identity document
- Number of the employee's identity document
- Area of the company to which the employee belongs
- Position held by the employee
- In the request for the digital certificate, the applicant must inform the effective date, if not completed, the effective date will be the issuance date of the digital certificate.

If the applicant acquires the digital certificate with a Physical Token or Virtual Token o Token Virtual, he must purchase the single package and pay the cost of the Physical Token or Virtual Token o Token Virtual detailed in section 11 of the CPS.

If the applicant acquires the digital certificate with centralized signature, he must purchase one of the centralized signature service packages that are detailed in this CPS and pay the cost of the package according to the forms established for it in section 11 of the CPS.

If the certificate generation is successful, the applicant must activate the same according to what is specified in the application, whether through Physical Token or Virtual Token o Token Virtual or centralized signature.

2.5.5 DIGITAL CERTIFICATE - PUBLIC FUNCTION

➢ The applicant must accept the terms and conditions.

➢ The applicant must answer the validation questions.

2.5.5.1 DOCUMENTS TO REQUEST:

- Legible image of the employee's or contractor's identity document
- Labor Certificate, administrative act of appointment or contract for the provision of services (Valid for no more than 30 days).

Note:

- Documentation containing the applicant's biometric or sociodemographic information may be additionally requested if Olimpia deems it necessary
- When validation of identity by facial recognition is selected, the applicant is not asked for a copy of the identity document, or the state document
  of the citizenship/foreigner identity card.
- The subscriber will not be allowed to use the issued digital certificate until the effective date begins.

2.5.5.2 INFORMATION TO FILL IN THE APPLICATION:

- Type of Certificate: Civil Service
- Company name
- Company Address (Department)
- Company Address (City)
- Company Address (Address)
- Company Email
- Company telephone
- Area of the company to which the employee or contractor belongs

- Position held by employee or contractor
- Names and surnames of the employee or contractor
- Type of the employee's or contractor's identity document
- Number of the employee's or contractor's identity document
- In the request for the digital certificate, the applicant must inform the effective date, if not completed, the effective date will be the issuance date of the digital certificate.

If the applicant acquires the digital certificate with a Physical Token or Virtual Token o Token Virtual, he must purchase the single package and pay the cost of the Physical Token or Virtual Token o Token Virtual detailed in section 11 of the CPS.
If the applicant acquires the digital certificate with centralized signature, he must purchase one of the centralized signature service packages that are detailed in this CPS and pay the cost of the package according to the forms established for it in section 11 of the CPS.

If the certificate generation is successful, the applicant must activate the same according to what is specified in the application, whether through Physical Token or Virtual Token o Token Virtual or centralized signature.

2.5.6 DIGITAL CERTIFICATE LEGAL REPRESENTATIVE

➢ The applicant must accept the terms and conditions.

➢ The applicant must answer the validation questions.

2.5.6.1 DOCUMENTS TO REQUEST:

- Legible image of the Legal Representative's identity document
- Certificate of Existence and Legal Representation (validity no older

than 30 days.) Note:

- Documentation containing the applicant's biometric or sociodemographic information may be additionally requested if Olimpia deems it necessary
- When validation of identity by facial recognition is selected, the applicant is not asked for a copy of the identity document, or the state document of the citizenship/foreigner ID.
- The subscriber will not be allowed to use the issued digital certificate until the effective date begins.

2.5.6.2 INFORMATION TO FILL IN THE APPLICATION:

- Type of Certificate: Legal Representative
- Name or business name of the company
- Company's NIT
- Company Address (Department)
- Company Address (City)
- Company Address (Address)
- Company Email
- Company's Telephone
- Names and surnames of the legal representative
- Type Identity document of the Legal Representative
- Identity document number of the Legal Representative
- Email of the legal representative
- Area of the company to which the employee belongs.
- In the request for the digital certificate, the applicant must inform the

effective date, if not completed, the effective date will be the issuance date of the digital certificate.

If the applicant acquires the digital certificate with a Physical Token or Virtual Token o Token Virtual, he must purchase the single package and pay the cost of the Physical Token or Virtual Token o Token Virtual detailed in section 11 of the CPS.

If the applicant acquires the digital certificate with centralized signature, he must purchase one of the centralized signature service packages that are detailed in this CPS and pay the cost of the package according to the forms established for it in section 11 of the CPS.

If the certificate generation is successful, the applicant must activate the same according to what is specified in the application, whether through Physical Token or Virtual Token o Token Virtual or centralized signature.

2.5.7 CERTIFIED EMAIL

- For mail service, it is not necessary to issue digital certificate to a subscriber; The certificate may be provided by the ECD or by a third-party platform, which will enable the mail service that includes a stamp and digital signature to give probative value of certified email.
- This service is acquired in the same way as the other services found on the my certificate platform.
- In all cases the applicant must accept the terms and conditions
- In all cases the applicant must answer the validation questions
- 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 service provider's platform, they will generate the credentials with their respective keys; This service includes a stamp and digital signature so that these give probative value to the messages sent by email, in accordance with article 10 of Law 527 of 1999; as defined in section 24.9 of the DPC.

- The mail service will be provided through a provider that complies with the provisions of current regulations, particularly in articles 20 and 21 of Law 527 of 1999.

2.5.7.1 WHEN THE SERVICE IS TAKEN WITH A DIGITAL CERTIFICATE AS A NATURAL PERSON, THE FOLLOWING DOCUMENTS WILL BE REQUIRED:

- Legible image of the identity document
- Public service bill image.

Note:

- Documentation containing the applicant's biometric or sociodemographic information may be additionally requested if Olimpia deems it necessary
- When validation of identity by facial recognition is selected, the applicant is not asked for a copy of the identity document, or the state document of the citizenship/foreigner ID.

2.5.7.1.1 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
- In the request for the digital certificate, the applicant must inform the effective date, if not completed, the effective date will be the issuance date of the digital certificate.

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

2.5.7.2 WHEN THE SERVICE IS TAKEN AS A NATURAL PERSON, THE FOLLOWING DOCUMENTS WILL BE REQUIRED:

- Certificate of Existence and Legal Representation (validity no older than 30 days.)
- Legible image of the Legal Representative's identity document

2.5.7.2.1 INFORMATION TO FILL IN THE APPLICATION:

- Name or business name of the company
- NIT:
- Company Address (Department)
- Company Address (City)
- Company Address (Address)

- Company Email
- Company's Telephone
- Names and surnames of the legal representative
- Type Identity document of the Legal Representative
- Identity document number of the Legal Representative
- Commercial registration number
- In the request for the digital certificate, the applicant must inform the effective date, if not completed, the effective date will be the issuance date of the digital certificate.
- The subscriber will not be allowed to use the issued digital certificate until the effective date begins.

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

2.5.7.3 WHEN THE SERVICE IS TAKEN WITH A LEGAL REPRESENTATIVE'S DIGITAL CERTIFICATE, THE FOLLOWING DOCUMENTS WILL BE REQUIRED:

- Legible image of the Legal Representative's identity document
- Certificate of Existence and Legal Representation (validity no older than 30 days.)

Note: Documentation containing the applicant's biometric or sociodemographic information may be additionally requested if Olimpia deems it necessary.
The subscriber will not be allowed to use the issued digital certificate until the effective date begins.

2.5.7.3.1 INFORMATION TO FILL IN THE APPLICATION:

- Type of Certificate: Legal Representative
- Name or business name of the company
- Company's NIT
- Company Address (Department)
- Company Address (City)
- Company Address (Address)
- Company Email
- Company's Telephone
- Names and surnames of the legal representative
- Type Identity document of the Legal Representative
- Identity document number of the Legal Representative
- Email of the legal representative
- Area of the company to which the employee belongs.
- In the request for the digital certificate, the applicant must inform the effective date, if not completed, the effective date will be the issuance date of the digital certificate.

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

2.6. DESCRIPTION OF THE REQUIREMENTS AND PROCEDURES FOR THE ISSUANCE OF DIGITAL CERTIFICATES THROUGH CENTRALIZED SIGNATURE

Olimpia IT establishes that the procedure for issuing the requested digital certificates through a centralized signature, is detailed, and developed in Numeral 5 of the Certification Practices Statement, and is complemented by the development of this Numeral, which specifies the application process by the applicant.

It is clarified that the identity validation mechanisms described in Numeral 4.2 of the DPC apply to the issuance of these digital certification services.
The same, it is clarified that the subscriber will receive the documentation of the digital certification once OlimpiaIT grants the digital certification service.

2.6.1 NATURAL PERSON

- The applicant must accept the terms and conditions.
- The applicant must answer the validation questions.
- Select the natural person digital certificate Note:
  - Documentation containing the applicant's biometric or sociodemographic information may be additionally requested if Olimpia deems it necessary
  - When identity validation by facial recognition is selected, the applicant will be asked for a copy of the identity document or the state document of the citizenship/foreigner identity card.
  - The subscriber will not be allowed to use the issued digital certificate until the effective date begins.
  - The RUT may be requested in cases of natural or legal persons who perform an economic activity for which they are obliged to register

in a Single Tax Registry.

2.6.1.1 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
- In the request for the digital certificate, the applicant must inform the effective date, if not completed, the effective date will be the issuance date of the digital certificate.

2.6.1.2 DOCUMENTS TO REQUEST:

- Legible image of the identity document
- Public service bill image.

2.6.1.3 PAYMENT AND ACTIVATION:

The applicant must follow the instructions described in the service portal to make the payment by the established means and enter their personal password to proceed to activate the service.

2.6.2 LEGAL PERSON

- The applicant must accept the terms and conditions.
- The applicant must answer the validation questions.
- Select Digital Certificate Legal Person

2.6.2.1 INFORMATION TO FILL IN THE APPLICATION:

- Name or business name of the company
- NIT (No check digit)
- Company Address (Department)
- Company Address (City)
- Company Address (Address)
- Company Email
- Company's Telephone
- Names and surnames of the legal representative
- Type Identity document of the Legal Representative
- Identity document number of the Legal Representative
- Commercial registration number
- In the request for the digital certificate, the applicant must inform the effective date, if not completed, the effective date will be the issuance date of the digital certificate.

2.6.2.2 DOCUMENTS TO REQUEST:

- Certificate of Existence and Legal Representation (validity no older than 30 days.)

- Legible image of the Legal Representative's identity document

2.6.2.3 PAYMENT AND ACTIVATION:

The applicant must follow the instructions described in the service portal to make the payment by the established means and enter their personal password to proceed to activate the service.

2.6.3 QUALIFIED PROFESSIONAL

- The applicant must accept the terms and conditions.
- The applicant must answer the validation questions.
- Select Digital Certificate Qualified Professional. Note:
  - Documentation containing the applicant's biometric or sociodemographic information may be additionally requested if Olimpia deems it necessary
  - When identity validation by facial recognition is selected, the applicant will be asked for a copy of the identity document or the state document of the citizenship/foreigner identity card.
  - The subscriber will not be allowed to use the issued digital certificate until the effective date begins.

2.6.3.1 INFORMATION TO FILL IN THE APPLICATION:

- Type of Certificate: Qualified Professional
- Names and surnames
- Type of identity document
- Number of identity document
- Department of residence

- City of residence
- Residence address
- Cell phone
- Another phone
- Email
- Obtained title
- Professional card number or degree certificate
- Name of Entity where the professional card or degree certificate was obtained
- In the request for the digital certificate, the applicant must inform the effective date, if not completed, the effective date will be the issuance date of the digital certificate.

2.6.3.2 DOCUMENTS TO REQUEST:

- Legible image of the identity document
- Public service bill image
- Degree certificate or professional card (legible)

2.6.3.3 PAYMENT AND ACTIVATION:

The applicant must follow the instructions described in the service portal to make the payment by the established means and enter their personal password to proceed to activate the service.

2.6.4 BELONGING TO COMPANY

- The applicant must accept the terms and conditions.

- The applicant must answer the validation questions.
- Select Digital Certificate Belonging to a
  ompany.
- Note:
  - Documentation containing the applicant's biometric or sociodemographic information may be additionally requested if Olimpia deems it necessary
  - When identity validation by facial recognition is selected, the applicant will be asked for a copy of the identity document or the state document of the citizenship/foreigner identity card..
  - The subscriber will not be allowed to use the issued digital certificate until the effective date begins.

2.6.4.1 INFORMATION TO FILL IN THE APPLICATION:

- Type of Certificate: Belonging to Company
- Name or business name of the company
- Company's NIT
- Department of the judicial notification address according to the certificate of existence and legal representation
- City of the judicial notification address according to the certificate of existence and legal representation
- Address of the judicial notification address according to the certificate of existence and legal representation
- Company Email
- Company's Telephone
- Names and surnames of the employee

- Type of the employee's identity document
- Employee Cell Phone
- Number of the employee's identity document
- Area of the company to which the employee belongs
- Position held by the employee
- In the request for the digital certificate, the applicant must inform the effective date, if not completed, the effective date will be the issuance date of the digital certificate.

2.6.4.2 DOCUMENTS TO REQUEST:

- Legible image of the employee's identity document ()
- Labor Certificate (validity no older than 30)
- Certificate of Existence and Legal Representation (validity no older than 30 days.)

2.6.4.3 PAYMENT AND ACTIVATION:

The applicant must follow the instructions described in the service portal to make the payment by the established means and enter their personal password to proceed to activate the service.

2.6.5 CIVIL SERVICE

- The applicant must accept the terms and conditions.
- The applicant must answer the validation questions.
- Select Civil Service Digital Certificate.

Note:

- Documentation containing the applicant's biometric or sociodemographic information may be additionally requested if Olimpia deems it necessary
- When identity validation by facial recognition is selected, the applicant will be asked for a copy of the identity document or the state document of the citizenship/foreigner identity card.
- The subscriber will not be allowed to use the issued digital certificate until the effective date begins.

2.6.5.1 INFORMATION TO FILL IN THE APPLICATION:

- Type of Certificate: Civil Service
- Company name
- Company Address (Department)
- Company Address (City)
- Company Address (Address)
- Company Email
- Company telephone
- Area of the company to which the employee or contractor belongs
- Position held by employee or contractor
- Names and surnames of the employee or contractor
- Type of the employee's or contractor's identity document
- Number of the employee's or contractor's identity document
- Employee or Contractor Email
- Employee or contractor Cell Phone
- In the request for the digital certificate, the applicant must inform the

effective date, if not completed, the effective date will be the issuance date of the digital certificate.

2.6.5.2 DOCUMENTS TO REQUEST:

- Legible image of the employee's or contractor's identity document
- Labor Certificate, administrative act of appointment, or contract for the provision of services (Valid for no more than 30 days).

2.6.5.3 PAYMENT AND ACTIVATION:

The applicant must follow the instructions described in the service portal to make the payment by the established means and enter their personal password to proceed to activate the service.

2.6.6 LEGAL REPRESENTATIVE

- The applicant must accept the terms and conditions.
- The applicant must answer the validation questions.
- Select Legal Representative's Digital Certificate. Note:
  - Documentation containing the applicant's biometric or sociodemographic information may be additionally requested if Olimpia deems it necessary
  - When identity validation by facial recognition is selected, the applicant will be asked for a copy of the identity document or the state document of the citizenship/foreigner identity card..
  - The subscriber will not be allowed to use the issued digital certificate until the effective date begins.

2.6.6.1 INFORMATION TO FILL IN THE APPLICATION:

- Type of Certificate: Legal Representative
- Name or business name of the company
- Company's NIT
- Department of the judicial notification address according to the certificate of existence and legal representation
- City of the judicial notification address according to the certificate of existence and legal representation
- Address of the judicial notification address according to the certificate of existence and legal representation
- Company Email
- Company's Telephone
- Names and surnames of the legal representative
- Type Identity document of the Legal Representative
- Identity document number of the Legal Representative
- Email of the legal representative
- Cell phone of the legal representative
- Area of the company to which the legal representative belongs.
- In the request for the digital certificate, the applicant must inform the effective date, if not completed, the effective date will be the issuance date of the digital certificate.

2.6.6.2 DOCUMENTS TO REQUEST:

- Legible image of the Legal Representative's identity document
- Certificate of Existence and Legal Representation (validity no older

than 30 days.)

2.6.6.3 PAYMENT AND ACTIVATION:

The applicant must follow the instructions described in the service portal to make the payment by the established means and enter their personal password to proceed to activate the service.

2.7.1 DOCUMENTS TO REQUEST:

• Certificate of citizenship/immigration card status (issued by the National Registry of Civil Status/Colombian Migration Administrative Department)
• Image of the identity document (legible)
• Image of public service bill.
2.7.2.3. Identity authentication (Certified electronic signature)
Olimpia will validate the identity of the applicants, in accordance with the internal document of the life cycle of the digital certificate, which consists, in summary, of applying one of the following methods:

iii. Validation through a third party (Delegated Validation): A third party delegated by the applicant and who previously authenticated the applicant's identity, makes the request for the certified electronic signature through the website.
iv. Validation through OTP: An OTP will be sent to the applicant to their email and/or cell phone number to authenticate the service

2.7.1. Payments and Activation:
The applicant must follow the instructions described in the service portal to make the payment by the established means and enter their personal password to proceed with the activation of the service.

2.8. PLATFORM SECURITY POLICIES
The platform delivered addresses the different aspects of security:

- Sure

The system does not allow unauthorized access to information, both through the platform and through direct attacks on the servers on which it operates.

Authorization check in all operations that the user can perform.

- Traceable

 All user actions that involve a modification to a document are recorded.

2.7. CRYPTOGRAPHIC DEVICES OFFERED BY OLIMPIA

2.7.1. STANDARDS FOR HSMS

OlimpiaIT 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".

2.7.2. CRYPTOGRAPHIC MODULE CERTIFICATION

The cryptographic modules acquired by OlimpiaIT (HSM) for the ROOT CA and the subordinate CA comply with the FIPS140-2 LEVEL 3 standard or higher.
Note: The risks and commitments of the cryptographic devices offered by Olimpia IT are described in Numeral 5 of the Certification Practices Statement CERTIFICATION PRACTICES STATEMENT.

2.8. LIABILITY DISCLAIMER

The limits of Olimpia IT's responsibility for each signed document are described in the Certification Practice Statement in the section "EXEMPTION OF LIABILITY".

2.9. CHANGES IN THE CERTIFICATE'S CONTENT

The procedure for updating the information contained in the certificates can be found in the Certification Practice Statement, Numeral 3.3 "UPDATE FREQUENCY OF THE INFORMATION CONTAINED IN THE DIGITAL CERTIFICATES".

3. 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.