DPC-001 Declaración De Prácticas De Certificación

Versión Nro. 25

CONTENIDO

1. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
1	2021-02-05	• Creación del Documento
2	2021-02-15	• Se modifica el nombre representación empresa por representante legal en todo el documento.
3	2021-02-17	• Se modifica el numeral 7.1.7, corrigiendo que las llaves de los certificados de la CA Raíz y las CA subordinadas tienen como función firmar certificados digitales y CRL.
4	2021-02-19	• Se actualiza el numeral 2.3, con la versión actual del documento, se incluye información relacionada con proveedores relacionados en el alcance acreditado, (2.3.3.1) y se incluye que no se establece una tarifa para revocación de certificados (11.1).
5	2021-04-26	Se actualiza el numeral 3.3.2., con la forma adecuada y técnica de actualizar los registros de la CRL. Se actualiza el numeral 7.3.1, determinando que existe un control, en un procedimiento interno para el almacenamiento de las llaves de la CA. Se adiciona al numeral 20.1 entrega del token físico el siguiente párrafo al final del numeral. "El suscriptor, podrá consultar las instrucciones de uso del token, las cuales se encuentran en el sitio web www.micertificado.olimpiait.com , enlace descargas, "Olimpia Sign". •
6	2021-05-11	Acción 8153: Actualiza el numeral 3.3.2., las condiciones para actualizar la CRL. Acción 8157: Adiciona en el numeral 20.1 donde el suscriptor encuentra las instrucciones de instalación y uso de la entrega del token Acción 8187: Modifica en el numeral 7.3.1, el control de archivo de la llave pública.

VERSIÓN	FECHA	DESCRIPCIÓN
		Actualiza numeral el 2.8.2 y 2.8.3 nombre del cargo del CEO y del responsable por la DPC respectivamente Actualiza en el numeral 6.2.1 el nombre del rol de la alta dirección de la ECD. Modifica el numeral 7.2 y 7.3 cambiando el termino de "clave" por "llave" y ajustando aplicabilidad a lo establecido por la organización. Complementa numeral 12.2 con "Los datos personales, excepto aquellos de naturaleza pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva"
7	2021-08-05	Agrega al numeral 4.2.1, en ampliación de los mecanismos utilizados por la organización para la identificación del suscriptor.
8	2021-12-09	Agrega Condiciones de generación de clave para el uso del Token Físico en el numeral 5.3.8 Agrega numeral 26.4 "Driver Token" y 26.5 "Generador CSR" Agrega al Numeral 5.1.1 Literales f y G Vigencia de los certificados digitales. Elimina referencia a la identificación de los procedimientos internos de los numeral 6.4.4, 6.7.1, 7.1.1, 7.2.2, 7.2.6, 7.2.9, 11.4.1 y 12 Complementa tarifas de los servicios en el Numeral 11
9	2022-02-28	Se elimina del numeral 6.8 el aviso a la Superintendencia de industria y Comercio, en caso de cesación de actividades. Se agregan los literales pp), qq), rr), ss), tt), uu), vv), ww), xx), yy), zz), aaa), bbb) al numeral 14.1., se agrega

VERSIÓN	FECHA	DESCRIPCIÓN
		el literal z), aa), bb), cc) y dd) al numeral 14.2. en cumplimiento de los artículos 32 a 33 de la Ley 527 de 1999. Deberes de la ED, terminación unilateral. Se agrega una nota al numeral 2.6.2.2., en el sentido de dar cumplimiento a lo descrito en el artículo 35 de la Ley 527/99, en el contenido mínimo del certificado. Se adiciona un párrafo al numeral 5.4., para dar cumplimiento al art 36 de la Ley 527/99. Aceptación de un certificado. Se incluye numeral 5.11 sobre tipos de HSM de Olimpia IT. Se agrega un párrafo en el numeral 5.3.1.1. sobre sobre la forma de comunicación entre la RA y la CA. Se agrega un párrafo al numeral 5.8.3 en el sentido de informar al suscriptor que no podrá solicitar la revocación de un certificado digital si el mismo no ha entrado en vigor. Se agrega el siguiente texto al numeral 2.7.4. "los instaladores o drivers no son compatibles con sistemas operativos macOs"
10	2022-04-06	Incluye en el numeral 5.4.1 el texto "dicho certificado", para aclarar que la aceptación del certificado se da cuando la entidad de certificación ha guardado el certificado en un repositorio. Modifica el Numeral 6.8, (4) dando alcance a la comunicación que se debe remitir a la Superintendencia de Industria y Comercio, según la Circular Externa 30 del 14 de octubre de 2021 de ONAC. Modifica el texto del literal qq del Numeral 14.1 que indicaba "esta Ley", por "el Artículo 29 de la Ley 527 de 1999". Aclarar que los instaladores o drivers requeridos para el uso de token físico no son compatibles con sistemas operativos macOs, dentro de los numerales 2.7.4, 20.1 y 26.1.
11	2022-05-04	Suprime la palabra "revocación" del Numeral 2.4.6.3.

VERSIÓN	FECHA	DESCRIPCIÓN
		Agrega el Numeral 4.2.1. para indicar que en los HSM Centralizado, la clave privada se genera en el HSM en el instante previo a la emisión del certificado, y que cuando el certificado se emite en Otros Dispositivos, el método de prueba de la posesión de la clave privada será la entrega a la RA de una petición de certificado en formato PKCS #10 Debido a la inclusión de un nuevo Numeral 4.2.1., se corre el Numeral 4.2.1 anterior a 4.2.2. Retira la palabra "automática" del Numeral 4.2.1 (ahora numeral 4.2.2.) Agrega un texto adicional al Numeral 4.2.1 (ahora numeral 4.2.2.) para indicar que OlimpiaIT podrá solicitar documentos adicionales o eximir de documentos, cuando lo requiera para validar la identidad de los solicitantes y se indican los documentos adicionales que pueden solicitarse. Debido a la inclusión de Numeral 4.2.1., se corre el Numeral 4.2.2. a 4.2.3. Agrega el texto "contra bases de datos propias o de terceros, ya sean oficiales o privadas" dentro del Numeral 5.1 Agrega dos bullets al Numeral 5.1, indicando que el documento requerido para emitir certificados solicitados por un menor de edad es la tarjeta de identidad y señalando que OlimpiaIT se reserva el derecho de emisión de certificados cuando a su juicio se pueda poner en riesgo a la ECD. Se agrega un texto al Numeral 5.2.2 indicando que, si OlimpiaIT decide rechazar la solicitud de expedición

VERSIÓN	FECHA	DESCRIPCIÓN
		del certificado de firma digital, lo notificará mediante notificación con los motivos para ello
12	2022-06-24	Modifica los siguientes términos de las definiciones (numeral 2.2.1) y se organizan alfabéticamente: Firma digital, Autoridad de Sellado de Tiempo (TSA), Suscriptor, Autoridad de Registro (RA), Log, Neutralidad Tecnológica, PKI, Queja, Revocación, Solicitante y Token. Adiciona en el Numeral 2.6.1. y 2.6.2 que el certificado contiene el Código de Acreditación. Adiciona las funciones de la RA en el Numeral 5.3.1., de acuerdo con el Numeral 10.11.2 del CEA-3.0-07. Se incluye la nota en el Numeral 5.8.4.1. de que en caso de que se revoque un certificado con relación a las firmas electrónicas o digitales, posteriormente el mismo no podrá ser rehabilitado por la OlimpiaIT. Modifica el tiempo de disponibilidad PKI y CRL del Numeral 6.1.3. Adiciona el Numeral 6.1.7. sobre el uso exclusivo de los sistemas de certificación. Adiciona el literal ccc en el Numeral 14.1. que incluye la responsabilidad de la EDC en la toma de decisiones, conservando el poder de decisión al otorgar, mantener, cancelar o retirar (revocar) la certificación. Aclara el Numeral 14.2, literal s, sobre la prohibición de usar la marca de Olimpia IT sin consentimiento previo. Adiciona derechos de los solicitantes y suscriptores en el Numeral 14.5.

VERSIÓN	FECHA	DESCRIPCIÓN
		Los tiempos de emisión ya no son 10 días hábiles si no 2 días hábiles. Se deja claro que, para token, los tiempos de entrega se deben sumar a estos 2 días dependiendo del destino. Se actualiza la norma de acreditación CEA-4.1-10 por CEA-3.0-07.
13	2022-08-02	Elimina la actividad de apelación en el proceso de PQRS, en el Numeral 2.2.1. y 28. Se eliminar la letra "A" de la palabra "PQRSA" en todo el texto. Incluye la definición de "tercero confiante" al Numeral 2.2.1. Elimina palabra repetida del Numeral 5.1., literal a Agrega aclaración en el Numeral gener.1. indicando que los certificados de persona natural o jurídica se someten a la Política de Certificados. Se incluye al Numeral 5.6. la claridad de que no se permite la suspensión de certificados que no conduzca a un estado de revocación y, por ende, no existe el estado de suspensión. En el Numeral 5.8.3.1., modifica el teléfono de contacto para la revocación de certificados por el correo electrónico servicioalcliente@olimpiait.com. Modifica el Numeral 5.9.2. y 6.7, indicando que el tiempo de disponibilidad de la lista de certificados revocados es del 99.8%. Adiciona el texto de operación de estampado cronológico en el Numeral 10.2. Modifica el término de 10 días, por 2, en el Numeral 5.1, 5.2.3 y 10.3.

VERSIÓN	FECHA	DESCRIPCIÓN
		Modifica el tipo de calendario del Numeral 10.1, de Juliano a Gregoriano. Se adiciona texto al literal b del Numeral 14.2.
14	2022-12-26	Incluye los métodos de validación de identidad en el Numeral 4.2.2. Se aclara que la entrega de la documentación se realizará para los servicios de certificación digital en el Numeral 5.3.8. Adiciona Numeral 8.4 de estándares técnicos vigentes. Se eliminan las restricciones e indica que interviene un proveedor para el servicio de correo electrónico certificado en el Numeral 24.9.
15	2023-01-24	Se incluye que la DPC cumplirá los criterios del programa Webtrust en el Numeral 2.1 Se aclara en el numeral 2.6.1. CA Raíz, donde se define mediante una matriz el contenido del certificado de CA Raíz Se aclara en el numeral 2.6.2.1. El contenido del certificado de la CA Subordinadas es., donde se define mediante una matriz el contenido del certificado de la Sub Se aclara en el numeral 2.6.2.2. El contenido del certificado del suscriptor es, donde se define mediante una matriz el contenido del certificado del suscriptor. Se aclara en 2.7. El uso permitido de los certificados digitales

VERSIÓN	FECHA	DESCRIPCIÓN
		Se aclara en el numeral 3.2. PUBLICACIÓN DE LA INFORMACIÓN, se corrige la url de la página de Olimpia y se describe los puntos de descarga, donde se identifica que documentos se pueden descargar, la crl, la CA raíz, la subsordinada entre otras. Se aclara en el numeral 5.3.1. Actividades de la Autoridad de Registro (RA) en el literal i, se deja claro que después de la validación de identidad y documental se firma esta solicitud para que la CA genere el certificado. Se aclara en el numeral 5.8.3 deja como contenido define que personas pueden solicitar la revocación de un certificado y que al momento de realizar esta actividad genera una notificación. Se aclara en el numeral 5.8.4 adiciona notificación de la revocación del suscriptor. Se aclara en el numeral 5.8.4.1. Describiendo los medios las alternativas para realizar la solicitud de revocación. Se aclara en el numeral 6.1.8. Protección en centro de Datos se afirma que los Data center tienen aislamiento contra electromagnetismo (Faraday) Se aclara en el numeral "6.5.2. Tiempo de almacenamiento de la información", donde se define el tiempo de conservación de la información que genera el ciclo de vida del certificado. Se aclara en el numeral 6.7.3 OlimpiaIT notificará la revocación a los suscriptores cuando comprometa la llave privada. Se aclara en el numeral 7.1.1. Generación del par de llaves, donde se menciona los mecanismos que

VERSIÓN	FECHA	DESCRIPCIÓN
		validan la autenticidad e integridad en la ceremonia de llaves Se aclara en el numeral 7.1.4 Entrega de la llave pública de CA a partes confiables OlimpiaIT permite la descarga de la llave pública desde su portal web de la Entidad de Certificación Digital a través del acceso a la descarga del certificado digital autofirmado que contiene la lleva pública. Se aclara en el numeral 7.2.9. Procedimiento de destrucción de la llave privada, que el borrado se podrá realizar cuando no tenga obligaciones comerciales o legales y el borrado o destrucción donde se encuentre la información de la llave privada. Se aclara en el numeral 8.2.2 se elimina la frase "no se realiza almacenamiento de CRL anteriores" Se elimina el numeral 26.3 Mail SIGN ya que el servicio se presta por un tercero. En los numerales que define el número de teléfono se realizó la actualización del indicativo telefónico a 601
16	2023-03-30	Actualización de las tarifas para 2023 en los capítulos 11.1.1.1. Emisión de Certificado Digital con Token Físico, 11.1.1.2. Emisión de Certificado Digital por Solicitud de Certificación PKCS#10, 11.1.2. Tarifas Estampado Cronológico y 11.1.3. Tarifas Servicio Firma centralizada, 11.1.4. Tarifas Servicio Correo electrónico certificado y 11.1.5. Tarifas Servicio SMS Certificado Modificación del número telefónico corporativo.
17	2023-05-29	Modifica el nombre del datacenter (de Centurylink Colombia S.A.S., a Cirion Technologies Colombia S.A.S.) en el numeral 2.3.3.1

VERSIÓN	FECHA	DESCRIPCIÓN
		Cambia la forma de realizar actualización de los certificados, de manera "automática" a "Manual" en el numeral 3.3.3. Se Incluye la posibilidad de presentar firma a ruego notaria en el numeral 4.2.2 Se Incluye la discapacidad como factor que puede generar discriminación en el numeral 21.1 Se Modifica el nombre "OlimpiaIT" por "Olimpia IT" y realiza otros ajustes de forma
18	2023-07-21	Modifica el nombre del CEO en el numeral 2.8.2. Incluye nota en el numeral 5.3.6 aclarando que los servicios a través de token operan de la misma manera que la firma centralizada. En el numeral 5.3.8 se deja claro que, tanto para los token físicos como virtuales, se notifica al suscritor a través de correo electrónico la generación del pin aleatorio para su posterior modificación a través del "Driver token" publicado en la página web. Igualmente, se incluye nota indicando que la documentación formal de los servicios de certificación digital debe dar cumplimiento a lo establecido en el Reglamento de uso de los símbolos de Acreditado y/o Asociado del ONAC. Incluye la descripción técnica de los HSM y los Token en el numeral 5.11.
19	2023-09-14	Incluye lineamiento sobre la actualización del certificado de existencia y representación legal en el sitio web, dentro del numeral 2.3.3.1 Incluye las situaciones en las que la ECD realizará notificación a ONAC por cambios organizacionales, en el numeral 3.3.4.

VERSIÓN	FECHA	DESCRIPCIÓN
		Elimina la referencia a listas restrictivas en el numeral 5.2.2. Actualiza el número de referencia de validación de identidad en el numeral 5.3.1.1. Modifica el numeral 11.4.1 indicando que los cobros son anuales. Aclara que el correo certificado utiliza certificado digital de Olimpia IT en numeral 24.9. Incluye declaración de la prevalencia de la versión en español sobre la versión en inglés de la DPC, en el apartado 29. Incluye ajustes de forma.
20	2024-01-31	Agrega definición de "firma electrónica" en el numeral 2.2.1. Agrega el servicio de Firma Electronica Certificada para persona natural o persona jurídica y nota aclaratoria en el numeral 2.3.2. Agrega el término de "firma electrónica", "electrónica" o "electrónicamente" en los siguientes numerales: • Numeral 2.6.2.2, literal v • Numeral 2.6.4.5 • Numeral 2.7.1, literal b • Numeral 3.2 • Numeral 5.2.2 • Numeral 5.3 • Numeral 5.3.1.1 • Numeral 14.2, literales j, t, aa y cc • Numeral 14.4, literal a • Numeral 14.4.1 • Numeral 14.4.2 • Numeral 14.4.3

VERSIÓN	FECHA	DESCRIPCIÓN
		• Numeral 14.5 • Numeral 15.1, literales h y j • Numeral 15.2 • Numeral 15.3 Modifica el cargo de "Digital Identity & E-Signature Business Director" por "Product Director". Realiza aclaración de Comprobación del Estado del Certificado (OCSP) en el Numeral 3.3.3. Aclara que el Numeral 4.2.2. no aplica para Firma Electrónica Certificada, y adiciona numeral 4.2.3 sobre autenticación de la identidad para Firma Electrónica Certificada. Adiciona el siguiente texto a la solicitud por internet del numeral 5.1: "o a través de cualquier otro portal que Olimpia IT, o a través de API debidamente integrada al portal de la Entidad de Certificación Digital". Así mismo, adiciona la posibilidad de realizar validación a través de delegado. Agrega el texto "o cualquier documento que permita validar de manera confiable la calidad e identificación del suscriptor" en el Numeral 5.3.1.1, literales a, b, d, e y f. Adiciona la forma de uso de firma electrónica certificada, por portal web, API y otros mecanismos en el Numeral 5.3.5. Suprime texto "El solicitante podrá incrustar una estampa de tiempo en una firma digital con un servicio de certificado digital de Olimpia IT" en el Numeral 10.8.3.

VERSIÓN	FECHA	DESCRIPCIÓN
		Ajusta las tarifas de los servicios para el año 2024 (numeral 11) y agrega las tarifas de firma electrónica certificada en el Numeral 11.1.5. Ajusta texto del Numeral 14.1, literales zz y bb, Numeral 14.4 y Numeral 14.4.1, aclarando que aplica para los servicios de certificación digital en general. Ajusta forma de Numeral 14.5, eliminando texto redundante "los derechos se detallan" Agrega OID de Firma Electrónica Certificada de persona natural y de persona jurídica en el Numeral 22 Agrega servicio de Firma Electrónica Certificada de persona natural o persona jurídica y nota aclaratoria en el Numeral 23. Adiciona numeral 24.1 con la descripción del servicio de firma electrónica certificada de persona natural o persona jurídica.
21	2024-02-16	Ajusta el tipo de firma electrónica certificada en los numerales 2.3.2, 23 y 24.10. Agrega la opción de validación de identidad delegada a través de tercero en el numeral 4.2.2. Modifica las formas de validación de identidad de la firma electrónica certificada del numeral 4.2.3. Agrega la posibilidad de enmendar errores en el numeral 14.3, literal c. Ajusta el OID de la firma electrónica certificada en el numeral 22.

VERSIÓN	FECHA	DESCRIPCIÓN
		Incluye la descripción de los requisitos y procedimientos para la emisión de la firma electrónica certificada en el numeral 24.10.1. Elimina referencia "firma electrónica" en los siguientes apartes: • Numeral 2.7.1, literal b • Numeral 3.2 • Numeral 14.4, literal a • Numeral 14.4.1 • Numeral 14.4.2 • Numeral 14.4.3 • Numeral 14.5 Numeral 15.1, literal j
22	2024-04-04	Adiciona el numeral 4.2.3 y 4.2.3.1 que incluye la validación de identidad delegada realizada por entidades del Sector de la Función Pública a través de convenio. Adiciona el numeral 5.8.3.2 sobre la revocatoria de certificados en cumplimiento de un convenio.
23	2024-05-20	Se suprimen las tarifas de los servicios de certificación digital del numeral 11.1 de la DPC dejando la referencia de que se publicarán las tarifas en el portal de Mi Certificado dando cumplimiento a la NC1 de ONAC, ID 241 de la herramienta Kawak y corrección 268.
24	2024-06-27	Se ajusta el numeral 4.2.2. indicando los casos en los que existen procesos específicos de autenticación. Se agrega los textos "y siguientes" y "o las normas que los modifiquen o adicione" en el numeral 4.2.3.1.

"A partir de la versión 25, el control de cambios se reflejará en la herramienta de gestión que está definida para el SIG."

2. INTRODUCCIÓN

2.1. DESCRIPCIÓN GENERAL

Olimpia IT pone de manifiesto a todos los interesados, de acceso libre en su página web esta Declaración de Prácticas de Certificación -DPC, cuyo propósito es erigir los lineamientos generales para los servicios de certificación.

Esta Declaración de Prácticas de Certificación tendrá plena validez tanto para los suscriptores, terceros y demás intervinientes durante todo el ciclo de vida del certificado digital y la prestación de los servicios que como Entidad de Certificación Digital abierta presta Olimpia IT. El contenido de esta Declaración de Prácticas de Certificación está basado en el Decreto 333 de 2014, los estándares RFC 3647, RFC 3628, los requerimientos del CEA 3.0-07, los requerimientos del Organismo Nacional de Acreditación de Colombia (ONAC), la normatividad colombiana que le aplique y los controles del programa Webtrust que se encuentren vigentes; y su aplicación está acogida a las leyes del territorio colombiano.

Cualquier modificación, aclaración, supresión, adición o complementación que Olimpia IT realice de esta Declaración de Prácticas de Certificación se realizará de conformidad con el procedimiento que para ello ha establecido Olimpia IT.

Sin perjuicio de lo anterior, cada una de las alteraciones que se surtan en esta DPC pasará por el control de versiones y cada versión deberá ser aprobada por el Comité de Políticas de Olimpia IT.

El solicitante de la modificación deberá ajustarse a lo descrito en el numeral 3.2 de esta DPC, y si la modificación solicitada es aprobada, requerirá que la nueva versión sea publicada e informada a los consumidores y público en general en la página web

https://micertificado.olimpiait.com, botón “marco legal”, link “Declaración de prácticas de certificación”, botón “Detalle”.

Esta Declaración de Prácticas de Certificación se encuentra publicada para su consulta a los consumidores y público en general en la página web https://micertificado.olimpiait.com, botón “marco legal”, enlace “Declaración de prácticas de certificación”, botón “Detalle”.

2.2. DEFINICIONES Y ABREVIATURAS

2.2.1. DEFINICIONES

i. Algoritmo: es un conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien deba realizar dicha actividad. Dado un estado inicial y siguiendo los pasos sucesivos, se llega a un estado final y se obtiene una solución.
ii. Autoridad de Registro (RA): Es la encargada de recibir las solicitudes relacionadas con certificación digital, para registrar las peticiones que hagan los solicitantes para obtener un certificado, comprobar la veracidad y corrección de los datos que aportan los usuarios en las peticiones y enviar las peticiones que cumplen los requisitos a una CA para que sean procesadas.
iii. Autoridad de Sellado de Tiempo (TSA): Entidad de confianza que emite sellos de tiempo.
iv. CA raíz: Autoridad certificadora de primer nivel, base de confianza.
v. CA subordinada: Autoridad certificadora de segundo nivel o más niveles.
vi. Caracterización de procesos y servicios: Descripción documentada de las características generales del proceso o servicio que establece la relación con los demás procesos internos o externos de la organización, los insumos y salidas del proceso, los proveedores y suscriptores, los riesgos y controles, y su interacción.

vii. Certificado Digital: mensaje de datos electrónico firmado por la Entidad de Certificación Digital, el cual identifica tanto a la Entidad de Certificación que lo expide, como al suscriptor y contiene la llave pública de este último.

viii. Datos de Creación de Firma (Llave privada): son valores numéricos únicos que, utilizados juntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos.

ix. Datos de Verificación de Firma (Llave pública): son los datos, como códigos o llaves criptográficas públicas, que son utilizados para verificar que una firma digital fue generada con la llave privada del suscriptor.

x. Declaración de Prácticas de Certificación (DPC): Es el documento en el que consta de manera detallada los procedimientos que aplica la ECD para la prestación de sus servicios. Una declaración de las prácticas que una ECD emplea para emitir, gestionar, revocar y renovar certificados sin y con cambio de llaves.

xi. Entidad de Certificación Digital (ECD): De acuerdo con lo indicado en la Ley 527 de 1999, Artículo 2, Literal d, es aquella persona natural o jurídica que, está facultada para emitir certificados digitales en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

xii. Entidad de Certificación Abierta: Entidad que ofrece al público en general, servicios propios de las ECD, tales que su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, y recibe remuneración.

xiii. Firma Digital: Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del suscriptor y al texto del mensaje, permite determinar que este valor se ha obtenido

exclusivamente con la clave del suscriptor y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

xiv. Firma Electrónica: Se refiere a métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente. De acuerdo con el artículo 161 del Decreto 19 de 2012, las Entidades de Certificación Digital podrán emitir certificados en relación con las Firma Electrónicas de personas naturales o jurídicas.

xv. Función Hash: Es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.

xvi. Lista de Certificados Revocados (CRL): Es aquella relación que debe incluir todos los certificados revocados por la Entidad de Certificación Digital.

xvii. Log: Servicio de registro de eventos del sistema de información, dejando la información anterior y la actual, identifica quién y cuándo se realizó el evento.

xviii. Neutralidad Tecnológica: principio contemplado en la Ley 1341 del 2009 y el Artículo 2.2.2.47.2. del DURSCIT, según el cual no debe existir preferencia o restricción de ninguna índole de las diversas técnicas o tecnologías que pueden utilizarse para firmar, generar, comunicar, almacenar o archivar electrónicamente información. De acuerdo con la Sentencia C-403/10 de la Corte Constitucional, "[e]s la libertad que tienen los proveedores de redes y servicios de usar las tecnologías para la prestación de todos los servicios sin restricción distinta a las posibles interferencias perjudiciales y el uso eficiente de los recursos escasos". Este principio es aplicable a la actividad adelantada por las Entidades de Certificación Digital, siempre y

cuando se dé cumplimiento a los criterios establecidos en el CEA 3.0-07.

xix. Niveles de Seguridad: Son los diversos niveles de seguridad que ofrecen las variables de firma electrónica cuyos beneficios y riesgos deben ser evaluados por la persona, empresa o institución que piensa optar por una modalidad de firma electrónica para enviar o recibir mensajes de datos o documentos electrónicos.

xx. OID: Identificador único de objeto (Object identifier). Acrónimo del término en idioma inglés "Object Identifier", que consiste en un número único de identificación asignado el cual está basado en estándares internacionales y comúnmente utilizado para identificar documentos, sistemas, equipos, etc., con la finalidad, entre otros, de conocer el origen, la titularidad y la antigüedad del objeto identificado.

xxi. PKI: Infraestructura de llave pública (Public Key Infrastructure): es el conjunto de hardware, software, políticas, procedimientos y elementos tecnológicos que, mediante la utilización de un par de llaves criptográficas, una privada que sólo posee el suscriptor del servicio y una pública, que se incluye en el certificado digital, logran:

- Identificar al emisor de un mensaje de datos electrónico.
- Impedir que terceras personas puedan observar los mensajes que se envían a través de medios electrónicos.
- Impedir que un tercero pueda alterar la información que es enviada a través de medios electrónicos.
- Evitar que el suscriptor del servicio de certificación digital que envió un mensaje electrónico pueda después negar dicho envío.

xxii. Política de certificado (PC): Es el conjunto de reglas que indica los requisitos de un certificado en una comunidad y/o clase en particular, en el marco de los requisitos legales, reglamentarios, y con requisitos de seguridad comunes.

xxiii. Proveedor: El término "proveedor", incluye a organizaciones, personas, fabricantes, distribuidores, ensambladores de tecnología y otros que suministran productos, bienes y servicios. Entre los proveedores de las ECD están las entidades recíprocas y empresas de tecnología que prestan servicios en sus diferentes modalidades como son: hosting, colocation, repositorio documental (electrónico o físico), proveedor de dispositivos, proveedor de telecomunicaciones, etc.

xxiv. Queja: Expresión de insatisfacción, diferente de la apelación, presentada por una persona u organización a una ECD o a un organismo de acreditación, relacionada con las actividades de uno de los dos, para la cual se espera respuesta.

xxv. Requisitos de certificación: Es el conjunto de obligaciones establecidas en la ley colombiana, que el solicitante del servicio de certificación digital debe demostrar ante la ECD, para ser suscriptor del certificado que solicita.

xxvi. Revocación: Para los efectos de este documento, es el proceso por el cual se inhabilita el Certificado Digital emitido y se da por terminado su periodo de validez de uso a partir de la fecha de revocación al presentarse alguna de las causas establecidas en la Declaración de Prácticas de Certificación.

xxvii. Servicio del estado del certificado en línea OCSP (Online Certificate Status Protocol): Actividad de consulta en tiempo real al sistema de la ECD, sobre el estado de un certificado digital a través del protocolo OCSP.

xxviii. Servicio de Certificación Digital: Conjunto de actividades de certificación que ofrece la ECD para certificar el origen e integridad de mensajes de datos, basados en las firmas digitales o electrónicas, estampado de tiempo, así como en la aplicabilidad de estándares técnicos admitidos y vigentes en infraestructura de llave pública – PKI.

xxix. Servicio de generación de firma digitales: Se entenderá para todos los efectos de la Entidad de Certificación Digital Olimpia IT, el servicio de firma centralizada.

xxx. Solicitante: Persona natural o jurídica que solicita el servicio de certificación digital a la ECD con el propósito de obtener servicios de certificación digital.

xxxi. Suscriptor: En los servicios de certificación digital, el término suscriptor identifica a la persona natural o jurídica que contrata el servicio de certificación digital a la ECD. En el caso de la actividad de emisión de certificados digitales, también será la persona natural o jurídica a cuyo nombre se expide un certificado.

xxxii. Tercero confiante: Persona natural o jurídica que decide aceptar y confiar en un certificado digital emitido por Olimpia IT.

2.2.2. ABREVIATURAS

CA: Certification Authority
DPC: Declaración de Prácticas de Certificación
CRL: Certificate Revocation List
PC: Política de Certificado
OCSP: Servicio del estado del certificado en línea (Online Certificate Status Protocol)
RA: Autoridad de Registro (Registration Authority)
PKI: Infraestructura de llave Pública (Public Key Infrastructure)
ECD: Entidad de Certificación Digital
ONAC: Organismo Nacional de Acreditación de Colombia
OID: Object Identifier
TSA: Time Stamp Authority (Autoridad de Estampado Cronológico)

2.3. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

Nombre	**DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN**
Código:	DPC – 001
Fecha Aprobación:	23 de febrero de 2022
Versión:	16

Descripción	El presente documento contiene la Declaración de Prácticas de Certificación para los certificados, servicios y TSA, para Olimpia IT asociadas a la emisión de certificados digitales las cuales son aprobadas por el Comité de Políticas de Olimpia IT y están a disposición de todo el público.
Enlace	https://micertificado.olimpiait.com

2.3.1. ALCANCE

El alcance de esta Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC), se encuentra limitada a las actividades de certificación para las cuales el Organismo Nacional de Acreditación de Colombia, haya dado viabilidad en su realización, así como para la prestación de servicios también viables de prestar por parte de Olimpia IT como Entidad de Certificación Digital Abierta.

Cada una de las actividades o servicios acreditados a ser desarrollados por Olimpia IT como Entidad de Certificación Digital Abierta, cuentan con un detalle del límite de obligaciones, responsabilidades, derechos y seguridad que puede prestar cada uno, los cuales se desarrollan con amplitud en cada uno de los puntos de los servicios tratados en esta DPC.

2.3.2. SERVICIOS QUE OFRECE LA ECD

Certificado digital persona natural, Certificado digital persona jurídica, Certificado digital profesional titulado, Certificado digital pertenencia a empresa, Certificado digital función pública, Certificado digital representante legal, Servicio correo electrónico certificado, Servicio de estampado cronológico, Servicio de firma centralizada, Servicio de Firma Electrónica Certificada.

Nota: Se aclara que el servicio de Firma Electrónica Certificada no se encuentra acreditado.

2.3.2.1. INFORMACIÓN PARA CONSUMIDORES Y PÚBLICO EN GENERAL

Desde la página web www.olimpiait.com podrá acceder a https://micertificado.olimpiait.com, botón "Productos", en el link "Certificados Digitales" se informan los diferentes tipos de certificados ofrecidos y en el link "Servicios Digitales" se informan los servicios ofrecidos de acuerdo con lo establecido en el documento RAC-3.0-07 de ONAC.

Se informa a los consumidores y al público las actividades de la ECD y el alcance acreditado, en la página web https://micertificado.olimpiait.com.

En la página web www.olimpiait.com, en el enlace "Acerca de nosotros" se encuentra la información como lo es naturaleza, tipo de empresa, entre otros aspectos de relevancia.

Todos los servicios prestados y la emisión de certificados acreditados por Olimpia IT ante ONAC, se prestan con independencia e imparcialidad. Así mismo, cada una de las políticas de certificados contenidas en esta Declaración de Prácticas de Certificación se someten al cumplimiento de la prestación de los servicios con independencia e imparcialidad, y sus condiciones se tratan y desarrollan en el mecanismo de imparcialidad establecido por Olimpia IT denominado Comité de Imparcialidad y asociado a los riesgos que este comité identifique y mitigue o acepte.

2.3.3. ACERCA DE OLIMPIA IT

Olimpia IT S.A.S. es una sociedad comercial constituida en su totalidad por capital privado mediante escritura pública # 1513 de la notaria 32 del círculo de Bogotá del primero de julio de 2005, inscrita el 12 de julio de 2005 bajo el # 01000696 del libro IX cuyo NIT es 900.032.774-4. Olimpia IT, es una sociedad inscrita ante la Cámara de Comercio de Bogotá y cuyo estado es activo.

El domicilio social y de correspondencia de Olimpia IT, se encuentra ubicado en la ciudad de Bogotá D.C., en la Calle 24 No. 7- 43 Piso 16 Edificio Siete24, que corresponde al registrado en el certificado de existencia y representación expedido por la Cámara de Comercio de Bogotá, cuyo teléfono principal es (+57 601) 742 7878, y correo electrónico es notificaciones.gerencia@olimpiait.com, sociedad que le corresponde el registro de matrícula mercantil No# 01505286 del 12 de julio de 2005 y cuya actividad como Entidad de Certificación Digital fue otorgada por el Organismo Nacional de Acreditación de Colombia (ONAC) mediante certificado de acreditación emitido por ONAC, acreditación que se puede consultar en el directorio oficial de acreditaciones para entidades de certificación digital: www.onac.org.co/modulos/contenudo/defuaul.asp?idmodulo=599

2.3.3.1. CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL DE OLIMPIA IT

Olimpia IT declara e informa al público en general que el certificado de existencia y representación legal de Olimpia IT S.A.S, expedido por la Cámara de Comercio de Bogotá, se encuentra disponible en el sitio web https://micertificado.olimpiait.com. en el botón marco legal, enlace "certificado de existencia y representación legal" clic en botón "Detalle". Olimpia IT realizará la actualización de este documento en el sitio web, cada vez que se presente una actualización en la información relevante de este documento (razón social, objeto social u representación legal) y, en todo caso, por lo menos una vez al año y antes del 31 de diciembre de cada año.

Otras entidades subcontratas se relacionan a continuación:
Proveedor data Center: BT Colombia Ltda., con NIT 830.045.126-4, matrícula mercantil No. 00854381, cuyo estado es activo en la Cámara de Comercio de Bogotá, con domicilio social y de correspondencia Cl 113 No. 7 - 21 Torre A Oficina 1112, de la ciudad de Bogotá, con correo electrónico ricardo.daza@bt.com y teléfono: (57 601) 6292240, cuyo certificado de

existencia y representación legal, se encuentra en https://micertificado.olimpiait.com, link "certificado de existencia y representación legal data center".

Proveedor data Center: Cirion Technologies Colombia S.A.S., con NIT 800.136.835-1, matrícula mercantil No. 00464163, cuyo estado es activo en la Cámara de Comercio de Bogotá, con domicilio social y de correspondencia es Calle 185 No. 45-03 Centro Comercial Santafe Torre Empresarial P, de la ciudad de Bogotá, con correo electrónico german.garcia@centurylink.com y teléfono: (57 601) 6119000, cuyo certificado de existencia y representación legal, se encuentra en https://micertificado.olimpiait.com, link "certificado de existencia y representación legal data center".

2.4. INFORMACIÓN SOBRE EL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN CON EL FIN DE EXPEDIR LOS CERTIFICADOS

Olimpia IT, ha implementado el sistema de seguridad de la información basado en la norma internacional NTC-ISO/IEC 27001 en su versión vigente.

2.5. REQUISITOS DEL SISTEMA DE GESTIÓN

Olimpia IT, ha implementado el sistema de gestión basado en las normas Internacionales ISO/IEC 9001 y 27001.

2.6. PARTICIPANTES Y ESTRUCTURA EN EL PROCESO DE CERTIFICACIÓN DIGITAL

A continuación, se muestran cómo está organizado el **Sistema de Certificación Digital de Olimpia IT.** Para estos efectos se entenderá que el sistema está compuesto por una estructura y unos participantes, entre otros, por la CA raíz, la CA subordinada, un comité de imparcialidad, la RA, suscriptores y partes confinantes.

2.6.1. CA RAÍZ

Autoridad certificadora de primer nivel, base de confianza.

2.6.1.1. EL CONTENIDO DEL CERTIFICADO GENERADO ES:

Campo del certificado		Valor
version		v3
serialNumber		Número entero positivo único con respecto a la CA que emite el certificado
signature		Parámetros del algoritmo de firma
signature algorithm		SHA 256 RSA
issuer		DN de la CA que emite el certificado
validity	**notBefore**	Fecha y hora de inicio de validez del certificado, tiempo UTC
	notAfter	Fecha y hora de fin de validez del certificado, tiempo UTC
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

Campo del certificado	Valor
	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

Nota: El Certificado digital es generado en formato CRT.

2.6.2. CA SUBORDINADA

Autoridad certificadora de segundo nivel o más niveles.

2.6.2.1. EL CONTENIDO DEL CERTIFICADO DE LA CA SUBORDINADAS ES:

Campo del certificado		Valor
version		v3
serialNumber		Número entero positivo único con respecto a la CA que emite el certificado
signature		Parámetros del algoritmo de firma
signature algorithm		SHA 256 RSA
issuer		DN de la CA que emite el certificado
validity	**notBefore**	Fecha y hora de inicio de validez del certificado, tiempo UTC
	notAfter	Fecha y hora de fin de validez del certificado,tiempo UTC

Campo del certificado	Valor
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
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. EL CONTENIDO DEL CERTIFICADO DEL SUSCRIPTOR ES:

Campo del certificado		Descripción	Valor
version		N° de versión	v3
serialNumber		N° de serie	Número entero positivo único con respecto a la CA que emite el certificado
signature		Algoritmo de firma	OID y parámetros del algoritmo de firma
signature algorithm		Algoritmo hash de firma	funciones hash criptográficas
issuer		Emisor (DN)	DN de la CA que emite el certificado
validity	**notBefore**	Válido desde	Fecha y hora de inicio de validez del certificado, tiempo UTC
	notAfter	Válido hasta	Fecha y hora de fin de validez del certificado, tiempo UTC
subjectPublicKeyInfo		Clave pública	parámetros del algoritmo y valor de la clave pública
Parámetros de clave pública			05 00
Identificador de la clave en la entidad emisora		Identificador de la clave en la entidad emisora	Id. de clave=eeb5ba8bc455b5b7b1f773f32079f3feab67a85e
Identificador de clave del titular		identificador de clave del titular	identificador de clave del titular
Restricciones básicas		Entidad final - ninguna	Tipo de asunto=Entidad final Restricción de longitud de ruta=Ninguno
Directivas del certificado			[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.50890.2.1.7.

Campo del certificado	Descripción	Valor
		3 [1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://micertificado.olimpiait.com/recursos/archivos/declaraciondepracticasdecertificacion.pdf
Nombre alternativo del emisor	Código de acreditación ONAC	Nombre DNS=21-ECD-001
Puntos de distribución CRL	Puntos de validación de los certificados revocados	La url de la CRL
Acceso de la información de la entidad emisora	Datos de la entidad	[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

Campo del certificado	Descripción	Valor
		URL=http://crt.olimpiait.com/olimpiaitroot.crt
Restricciones básicas	Entidad de certificación (CA)	Tipo de asunto= Entidad de certificación (CA) Restricción de longitud de ruta=Ninguno
Uso de la clave	Propósitos para los cuales se debe utilizar el certificado.	Sin repudio, Firma de certificados, Firma CRL sin conexión, Firma de lista de revocación de certificados (CRL) (46 00)
Huella digital	La síntesis o huella digital de los datos del certificado	Línea alfanumérica 89ebb74b4b2c

Nota: Olimpia IT declara que los certificados digitales del suscriptor contienen la información requerida por el artículo 35 de la Ley 527 de 1999 y que se describe a continuación:

i. Nombre, dirección y domicilio del suscriptor.
ii. Identificación del suscriptor nombrado en el certificado.
iii. El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
iv. La clave pública del usuario.
v. La metodología para verificar la firma digital o firma electrónica del suscriptor impuesta en el mensaje de datos.
vi. El número de serie del certificado.
vii. Fecha de emisión y expiración del certificado.

2.6.3. TIME STAMP AUTHORITY (AUTORIDAD DE SELLADO DE TIEMPO)

Garantiza la integridad de un momento (fecha y hora), con la imposición de una firma digital en dicho mensaje de datos, por el cual Olimpia IT, da certeza de que dicha marca de tiempo es un mensaje de datos confiable, que no ha sido alterado desde su creación. La fecha y hora son tomadas del Instituto Nacional de Metrología (INM).

2.6.3.1. LA ESTRUCTURA DE LOS DATOS DE LA TSA SUBORDINADAS ES:

- Versión
- Número de serie
- Algoritmo de firma
- Algoritmo hash de firma
- Emisor
- Válido desde
- Válido hasta
- Sujeto
- Clave pública
- Parámetros de clave pública
- Identificador de clave del titular
- Directivas del certificado
- Restricciones básicas
- Uso de la clave
- Uso mejorado de claves
- Algoritmo de identificación
- Huella digital

2.6.4. PARTICIPANTES

2.6.4.1. SUSCRIPTOR

Es aquella persona, natural o jurídica, la cual figura como titular del certificado digital emitido por Olimpia IT, según se establece en la PC establecida para cada uno de los certificados.

2.6.4.2. PARTES CONFIANTES

Persona u organización que recibe, hace uso o confía de cualquier manera en los certificados digitales emitidos por Olimpia IT y que por lo tanto se vincula jurídicamente en virtud de los términos de la presente DPC.

2.6.4.3. AUTORIDAD DE REGISTRO (RA)

La autoridad de registro designada por Olimpia IT es la encargada de la recepción de solicitudes, validación de identidad, aprobación, rechazo de solicitudes de emisión, y comunicación con el suscriptor según lo establecido por la normativa colombiana vigente.

2.6.4.4. AUTORIDAD DE CERTIFICACIÓN

La autoridad de certificación designada por Olimpia IT es la encargada de tomar la decisión respecto de la emisión de certificados digitales y/o servicios asociados, así como de la generación de los certificados digitales, tanto para Olimpia IT, como para los suscriptores.

2.6.4.5. ESTRUCTURA DE LA PKI

Combinación de hardware, software, políticas y procedimientos de seguridad, que permiten la ejecución con garantías de operaciones criptográficas como el cifrado de la firma digital o firma electrónica y el no repudio de transacciones electrónicas.

Componentes de la PKI:

a) Autoridad de Certificación (CA)
b) Autoridad de Registro (RA)
c) Autoridad de Sellado de Tiempo (TSA)
d) Solicitantes y suscriptores
e) Partes confiantes
f) Repositorios de información

2.7. USOS PERMITIDOS PARA LOS CERTIFICADOS DIGITALES

Los certificados podrán ser utilizados según lo estipulado en esta DPC y la PC respectiva. Las extensiones Key Usage y Extended Key Usage podrán ser utilizadas para establecer límites técnicos a los usos de la clave privada del certificado correspondiente.

El certificado digital raíz sólo puede utilizarse para la identificación de la propia autoridad de certificación raíz y para la distribución de su clave pública de forma segura. El uso de los certificados emitidos por la CA raíz estará limitado a la firma de certificados digitales y la firma de las listas de certificados revocados correspondientes.

2.7.1. REGLAS DE OLIMPIA IT PARA LOS CERTIFICADOS DIGITALES EMITIDOS

a) Los usos permitidos para el Certificado Digital expedido por Olimpia IT serán los que se estipulen en esta DPC. Cualquier uso diferente que se dé al Certificado Digital se considerará una justa causa de revocación de este y la terminación de la relación comercial con el suscriptor.

b) El uso del certificado digital y los mensajes de datos que se firmen digitalmente son responsabilidad del suscriptor, por ende, Olimpia IT, en su calidad de ECD se exonera de toda responsabilidad sobre la verificación o función fedante que puedan ostentar los mensajes de datos firmados digitalmente por el suscriptor.

c) En su condición de aceptante del certificado digital las partes confiantes deberán:

- Verificar la idoneidad del certificado digital que se encuentra en uso por parte del suscriptor a través de los medios expuestos por Olimpia IT, así mismo Olimpia IT en su calidad de Entidad de Certificación Digital (ECD) revisará la demás

información que sea sujeta de validación y que pueda ser dispuesta por Olimpia IT.

- Las partes confiantes deberán consultar las listas de certificados revocados suministradas por Olimpia IT en su página de internet.

Suscriptores y partes confiantes aceptan y reconocen que la clave pública del suscriptor se entiende como un recurso tecnológico apropiado para encriptar o cifrar mensajes de datos, con el propósito de identificar que únicamente el tenedor de una llave privada es el responsable de su custodia. De igual manera el suscriptor declara conocer que en caso de pérdida de la misma, ocasionará la imposibilidad de recuperar el mensaje de datos encriptado o cifrado. Por lo anterior, Olimpia IT no asume ninguna responsabilidad por este hecho y los intervinientes (suscriptor y partes confiantes) reconocen esta situación.

d) Una vez el suscriptor verifique que parte de la información del certificado digital ha perdido su vigencia o su eficacia, deberá solicitar la renovación de su certificado.

e) El almacenamiento de los certificados independientemente del estado en el que se encuentre se desarrollará por parte de Olimpia IT de forma indefinida.

f) El uso de los certificados digitales estará predeterminado a cumplir los siguientes propósitos:

- **No repudio:** Es aquella virtud emanada de la ley y depositada en una Entidad de Certificación Digital para determinar la imposibilidad de que un suscriptor se sustraiga del reconocimiento de los actos que ha firmado digitalmente con su certificado digital.

- **Integridad:** es aquella virtud emanada de la ley y depositada en una Entidad de Certificación Digital para que un tercero confiante en el certificado digital tenga la seguridad jurídica de que el mensaje de datos firmado digitalmente por el suscriptor al momento de su recepción no ha sido alterado o modificado de tal forma que su contenido corresponde al inicialmente enviado.

- **Identificación:** Procedimiento por medio del cual se reconoce que una persona natural o jurídica es quien realmente dice ser, mediante un proceso de autenticación ante un proceso informático y que esta persona actúe en su condición de firmante respecto del certificado digital emitido.

- **Confidencialidad:** Con el propósito de evitar la intervención o intrusión no autorizada del mensaje de datos, la clave pública del suscriptor podrá ser utilizada para cifrar los mensajes de datos y garantizar su envío de forma confidencial, siempre y cuando las técnicas de encriptación o cifrado de información correspondan a las avaladas para un sistema de certificación digital adoptado por Colombia o por acuerdos internacionales públicos o privados que suscriba Colombia o la Entidad de Certificación Digital.

En virtud de lo anterior, el convenio público o privado que se haya suscrito entre entidades de certificación digital exonera de responsabilidad por esta actividad de encriptación o cifrado a Olimpia IT. Para ello Olimpia IT, procura que la seguridad de la clave privada del suscriptor cumpla con los parámetros exigidos por ONAC. Olimpia IT no es responsable, no tiene injerencia, ni la capacidad de recuperar los datos cifrados que por causa del

suscriptor por la pérdida de la clave privada no puedan ser descifrados o desencriptados.

g) Las obligaciones adicionales entre Olimpia IT y el suscriptor y/o de las partes confiantes será de exclusiva responsabilidad del suscriptor, sin embargo, dichas obligaciones deberán ser informadas previamente a las partes involucradas o afectadas con dichas obligaciones.

2.7.2.USOS PERMITIDOS Y RESTRICCIONES

2.7.2.1. SOLICITUDES DE VARIOS CERTIFICADOS

El suscriptor puede realizar una nueva solicitud de un certificado (con token físico), aun cuando ya tenga un tipo de certificado de la misma naturaleza al que está solicitando.

2.7.2.2. EMISIÓN DE CERTIFICADOS A DISTINTOS SERVICIOS

Para los servicios que utilizan firma centralizada y certificado digital Persona Natural, Persona Jurídica o Función Pública: Olimpia IT emitirá máximo un tipo de certificado por servicio.

2.7.2.3. MULTIPLICIDAD DE CARGOS O FUNCIONES

Para los servicios que utilizan firma centralizada y tipo de certificado Profesional titulado y Pertenencia a empresa: Cuando el suscriptor tenga multiplicidad de cargos, profesiones y/o representaciones legales, podrá tener máximo un certificado por cada función, profesión o representación legal que ejerza.

2.7.3. USOS INDEBIDOS DE LOS CERTIFICADOS DIGITALES

a) Queda prohibido el uso de los certificados digitales por parte del suscriptor, de los terceros intervinientes o de quien ostente la

calidad de tenedor del certificado digital para la realización, planeación, concertación u otro tipo de actividades encaminadas a la ejecución de cualquier actividad considerada como ilícita por la legislación colombiana, por los convenios internacionales que suscriba Colombia, por las normas supranacionales, o por las nomas de terceros países en donde pueda ser verificado o usado el certificado digital emitido por Olimpia IT, o que contravenga las buenas costumbres, a las sanas prácticas comerciales y a todas las normas contenidas en esta Declaración de Prácticas de Certificación.

b) Así mismo, el uso del sistema de certificación digital y el uso de los certificados digitales se encuentra proscrito en actividades relacionadas con los sistemas de control para actividades de alto riesgo o para sistemas a prueba de error, sin limitarse a los siguientes:

- Sistemas de navegación de transporte terrestre, aéreo o marítimo.
- Sistemas de control de tráfico aéreo.
- Sistemas de control de armas.

Olimpia IT, podrá en cualquier momento definir mecanismo, políticas, procesos o procedimientos encaminados a establecer nuevas actividades de alto riesgo e informarlas acorde con lo exigido por la ley y las normas al público en general.

c) El uso de los certificados digitales se encuentra limitado a la ejecución de actividades que no estén relacionadas de forma directa o indirecta con sistemas informáticos que puedan ocasionar por acción u omisión la muerte o lesión de personas u ocasionar un perjuicio al medio ambiente.

d) Cuando con el suscriptor se haya pactado que la clave privada del suscriptor será almacenada en un medio físico custodiado por el suscriptor, este dispositivo solo podrá ser utilizado en actividades con referencia directa al Sistema informático de Certificación Digital. No podrá incorporarse en el soporte físico suministrado por Olimpia IT información diferente a aquella expresamente autorizada por Olimpia IT, ni usarse por fuera del Sistema informático de Certificación Digital.

2.7.4. RESTRICCIÓN PARA FIRMAR DOCUMENTOS

La firma de documentos tipo *.pdf, protegidos por contraseña de modificación, solo se podrá hacer desde la aplicación en ambiente web y con formato *.p7z.

Los instaladores o drivers requeridos para el uso de token físico no son compatibles con sistemas operativos macOs.

2.8. POLÍTICAS DE ADMINISTRACIÓN

2.8.1. ORGANIZACIÓN ADMINISTRATIVA DE OLIMPIA IT

Nombre: Olimpia IT S.A.S.
Correo electrónico: servicioalcliente@olimpiait.com/ gerencia@olimpiait.com
Dirección comercial y de notificaciones judiciales: Calle 24 No. 7- 43 Piso 16 Edificio Siete24
matrícula mercantil No# 01505286 del 12 de julio de 2005

2.8.2. PERSONA DE CONTACTO

Nombre: Simbad Ceballos – CEO
Correo electrónico: simbad.ceballos@olimpiait.com
Dirección: Calle 24 No. 7- 43 Piso 16 Edificio Siete24, Bogotá (Colombia).
Número de teléfono: (+57 601) 742 7878

2.8.3. RESPONSABLE POR LA DPC

Product Director
Correo electrónico: dgiraldo@olimpiait.com.

Legal Counsel Specialist
Correo electrónico: santiago.ramirez@olimpiait.com.

Dirección: Calle 24 No. 7- 43 Piso 16 Edificio Siete24, Bogotá (Colombia).
Número de teléfono: (+57 601) 742 7878.

3. REPOSITORIOS DE INFORMACIÓN DE LA ENTIDAD DE CERTIFICACIÓN DIGITAL

3.1. REPOSITORIOS

Olimpia IT garantiza la disponibilidad de la información en su repositorio acorde con los niveles de disponibilidad exigidos por ONAC y contenidos en la normatividad legal y técnica aplicada para este ítem, este repositorio contiene información de los Certificados de la CA raíz, CA Subordinada y lista de certificados revocados CRL, en caso de interrupción por causa de fuerza mayor, el servicio se restablecerá en los tiempos establecidos por Olimpia IT;

3.1.1. INFORMACION DE LOS CERTIFICADOS DE LA ECD Y DE LOS CERTIFICADOS REVOCADOS

En la página web https://micertificado.olimpiait.com, se tiene dispuesto la consulta del estado del certificado por medio de OCSP, en el link "Validaciones", botón "Validar firma", adjuntando el archivo tipo p7z, desde la ubicación en que se tenga guardado y haciendo clic en el botón "validar firma" de la parte inferior; y la consulta de la lista de certificados revocados por medio de CRL, en el link "Validaciones", botón "Estado del certificado (OCSP)" adjuntando el certificado y haciendo clic en el botón "buscar" de la parte inferior

3.2. PUBLICACIÓN DE LA INFORMACIÓN

- El Chief Legal Officer es responsable de revisar la DPC junto con el equipo de trabajo que así lo requiera.
- El Comité de Políticas tiene la autoridad de aprobar el presente documento.
- La Alta dirección de la ECD es la responsable de publicar el presente documento al público.

La siguiente información estará disponible en la página web https://micertificado.olimpiait.com

En el menú de Validaciones

- La Lista de Certificados Revocados (CRL) en el botón
  - olimpiaitroot.crl
  - olimpiaitecdsub.crl
- Estado del Certificado (OCSP)
- Validar Firma ***"En este módulo se puede validar y detallar la Firma Digital de los archivos en formato p7z"***
- Certificados Suscriptores ***"En este módulo se puede realizar la consulta y descarga de los certificados en estado vigente de los suscriptores".***
- Certificados CA
  - Certificados Raiz olimpiaitroot
  - Certificados Subordinada OlimpiaIT ECD Sub
  - Certificados TSA olimpiaitecdtsa

En el menú de Marco legal

- Declaración de Prácticas de Certificación
- Políticas de Certificados
- Política de Protección de Datos
- Política del Sistema Integrado de Gestión
- Política de Imparcialidad, No Discriminación e Independencia
- Consentimiento de responsabilidad ECD
- Póliza de responsabilidad civil Olimpia IT
- Certificado de existencia y representación legal DataCenter
- Certificado de existencia y representación legal Olimpia IT
- Autorización para el tratamiento de datos personales

El Comité de Políticas tiene la autoridad de aprobar el presente documento a través del formato que para ello se designe.

3.3. FRECUENCIA DE ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN LOS CERTIFICADOS DIGITALES

3.3.1. CERTIFICADOS EMITIDOS POR LA CA RAÍZ DE OLIMPIA IT

La publicación del certificado se realizará con anterioridad a su puesta en vigencia a través de la página web de Olimpia IT y se actualizará cada vez que se requiera.

3.3.1.1. PROCEDIMIENTO PARA LA ACTUALIZACIÓN DE LA INFORMACION CONTENIDA EN LOS CERTIFICADOS

Para realizar la actualización de la información de los certificados, Olimpia IT, emitirá un nuevo certificado, siguiendo las reglas de expedición para un nuevo certificado digital descritas tanto en esta DPC como en la PC y dando cumplimiento a la Política de Protección de Datos Personales.

La vigencia del nuevo certificado se sujetará a los descrito en el numeral 19 de esta DPC.

3.3.2. CRL – LISTA DE CERTIFICADOS REVOCADOS

La CRL debe ser actualizada de forma automática antes de la fecha de "próxima actualización" informada en la CRL sin revocaciones o cuando se realice alguna revocación, así:

- La fecha efectiva de la CRL es actualizada una vez se efectúe la revisión para la fecha y hora de la próxima actualización y no se han realizado revocaciones.

- La fecha efectiva se actualiza al generar la CRL después de realizar alguna revocación.

- La fecha de próxima actualización de la CRL siempre corresponde a 48 horas posteriores a la fecha efectiva.

3.3.3. PROTOCOLO DE COMPROBACIÓN DEL ESTADO DE UN CERTIFICADO (OCSP)

La comprobación del Estado de un Certificado (OCSP) se realiza en la página web de Olimpia IT.

3.3.4. DPC

La DPC se encuentra publicada en el sitio web https://micertificado.olimpiait.com, en el botón "Marco Legal" en el link "Declaración de prácticas de certificación, en el botón "Detalle", se actualiza según lo establecido por Olimpia IT con la debida aprobación del Comité de Políticas.

Los procesos de actualización serán informados a ONAC, cuando sea necesario. Serán informados a ONAC todas los cambios en la plataforma de los servicios de certificación digital relacionados en el alcance de acreditación, y en especial se comunicará a ONAC los cambios en relación con: **1.** la situación jurídica, de propiedad, comercial u organizativa; **2.** organización y gestión (por ejemplo, personal clave); **3.** instalaciones de Olimpia IT y otros recursos cuando sean relevantes; **4.** documentos normativos especificados en el alcance de acreditación, cuando estos no sean reglamentos técnicos o normas técnicas nacionales o internacionales; **5.** cualquier otro cambio fundamental que se produjese en las condiciones iniciales en que se concede la acreditación.

3.4. CONTROL DE ACCESO A LA INFORMACIÓN ALMACENADA

El control de acceso a la información contenida en los repositorios está limitado a cualquier persona natural y jurídica los cuales deseen realizar consulta de la información la cual Olimpia IT establece como Pública.

4. AUTENTICACIÓN E IDENTIFICACIÓN DE LA INFORMACIÓN

4.1. DENOMINACIÓN EN LOS NOMBRES

4.1.1. ESTANDAR DE LOS NOMBRES

Olimpia IT establece en el presente documento un Objeto Identificador (OID) y un Distinguished Name (DN) definido para cada uno de los certificados generados y al suministrado por IANA, firmados acordes al estándar X-509 v3.

4.1.2. DISTINCIÓN DE NOMBRES

Olimpia IT garantiza a sus suscriptores la total identificación de este y de su certificado generado mediante la asignación de un nombre distintivo (DN).

4.1.3. INTERPRETACIÓN DE FORMATOS DE NOMBRES

Las normas utilizadas para la interpretación de la nomenclatura en los certificados emitidos están basadas en la reglamentación dada por el estándar ISO/IEC 9595 (X.500) Distinguished Name (DN).

4.1.4. SINGULARIDAD DE LOS NOMBRES

Olimpia IT garantiza mediante la aplicabilidad de sus políticas y procedimientos la unicidad en los nombres de cada uno de los certificados generados utilizando el sistema de Distinguished Name (DN).

4.1.5. SOLUCIÓN DE DISPUTAS RELATIVO A LOS NOMBRES

Olimpia IT establece en la presente Declaración de Prácticas de Certificación la abstinencia en resolución de conflictos respecto a la titularidad de personas jurídicas o naturales.

4.2. PROCEDIMIENTOS DE IDENTIFICACIÓN DEL SUSCRIPTOR (VALIDACIÓN DE IDENTIDAD)

4.2.1. MÉTODO DE PRUEBA DE POSESIÓN DE LA CLAVE PRIVADA

Cuando un certificado se emite en HSM Centralizado, la clave privada se genera en el HSM en el instante previo a la emisión del certificado, mediante un procedimiento que garantiza su confidencialidad y su vinculación con el Solicitante. Cuando un certificado se emite en Otros Dispositivos, el método de prueba de la posesión de la clave privada será la entrega a la RA de una petición de certificado en formato PKCS #10 que contiene la correspondiente clave pública.

4.2.2. AUTENTICACION DE LA IDENTIDAD

A excepción de la autenticación o validación contemplados en el Numeral 4.2.3 y 4.2.4 de esta DPC, Olimpia IT declara que valida la identidad de las personas que realizan las solicitudes de certificados digitales contra la base de datos biográfica que administra y produce la Registraduría Nacional del Estado Civil o el Departamento Administrativo Migración Colombia.

Para validar el estado de vigencia del documento de identidad del solicitante, Olimpia IT establece dos métodos alternativos, que se implementan de manera independiente según el tipo de servicio o producto solicitado:

a) El solicitante deberá adjuntar un certificado de estado de cédula de ciudadanía o extranjería, para los servicios que así lo requieran, con el cual se validará la vigencia de su documento de identidad.

b) Cuando no se requiera el certificado de estado de cédula de ciudadanía al solicitante, la validación de la vigencia de su documento de identidad se realizará mediante una consulta al

Archivo Nacional de Identificación de la Registraduría Nacional del Estado Civil (ANI).

Los métodos de autenticación de Identidad de los solicitantes podrán ser complementados con otra información adicional, ya sea producto de un convenio o como parte de una solicitud; teniendo en cuenta lo anterior, Olimpia IT podrá solicitar información que contenga datos biométricos o sociodemográficos del solicitante para autenticar la identidad. Dicha validación tendrá en cuenta el resultado del cotejo biométrico y la autenticidad de la información biométrica o sociodemográfica suministrada, al finalizar este proceso el equipo de la RA realiza la recomendación para la emisión o rechazo de la solitud.

Olimpia IT realizará la validación de la identidad de los solicitantes, de acuerdo con el documento interno de ciclo de vida del certificado digital, que consiste, en resumen, en aplicar alguno de los siguientes métodos:

i. Validación por reconocimiento facial: El solicitante podrá capturar fotografía de rostro y cargar la imagen del documento de identidad por ambas caras.

ii. Llamada del operador RA: Se realizarán preguntas demográficas al solicitante vía telefónica para confirmar su identidad.

iii. Validación de identidad mediante documento con huella: El solicitante podrá adjuntar documento notariado (incluyendo documento con firma a ruego en el caso de no poder o no saber firmar) o consentimiento de responsabilidad disponible en el proceso de solicitud del certificado.

iv. Validación de identidad delegada a través de un tercero: Validación a través de tercero delegado por el solicitante y que previamente

realizó la autenticación de identidad del solicitante. El delegado realizará la solicitud del certificado por medio de la página web.

Olimpia IT verificará y garantizará que el tercero delegado está realizando una validación de identidad adecuada de los solicitantes, para lo ejecutará los siguientes controles con los delegados:

- Contrato de la ECD con el tercero delegado: Olimpia IT suscribirá contrato con el tercero delegado, a través del cual se incluirán obligaciones del delegado referentes a: a) realizar una validación de identidad del solicitante que incluye solicitar y almacenar copia de la Cédula de Ciudadanía, y para personas jurídicas, Certificado de Existencia y Representación Legal y RUT; según el tipo de certificado y fin o propósito de uso del mismo, y de acuerdo con el análisis de riesgo, también se podrán adicionar controles adicionales de validación de identidad; b) posibilidad del delegado de ser auditado por Olimpia IT o por cualquier autoridad pública o de certificación incluyendo ONAC para verificar sus obligaciones de validación de identidad, seguridad de la información, entre otros; y c) posibilidad de dar por terminado el contrato en caso de incumplimiento de las obligaciones de validación de identidad o auditoría del tercero delegado.

- Auditoría del tercero delegado: Se realizará anualmente auditoría al tercero delegado con el fin de verificar que este delegado cuente con lo siguiente: a) la documentación que permita verificar la identidad a los solicitantes (Cédula de Ciudadanía, y para el caso de personas jurídicas, Certificado de Existencia y Representación Legal y RUT) y los controles adicionales establecidos según el análisis de riesgo; b) contrato de mandato o similar celebrado con el solicitante que contemple una autorización expresa del solicitante de presentar una solicitud de certificado digital frente a una Entidad de Certificación Digital; c) cumplimiento de estándares

aceptados de seguridad de la información; y d) otros que sean requeridos por la auditoría.

- Certificado digital del tercero delegado: El tercero delegado deberá adquirir un certificado digital de Olimpia IT el cual le permitirá acreditar su identidad para la solicitud delegada frente a la ECD.

Olimpia IT se reserva el derecho de solicitar documentos adicionales a los que sean exigidos en el formulario de solicitud cuando así lo considere necesario para verificar la identidad o cualquier calidad del solicitante. Olimpia IT podrá exonerar de la presentación de cualquiera documento adicional cuando la identidad del solicitante haya sido suficientemente verificada por otros medios.
Olimpia IT podrá exigir adicionalmente uno, alguno o varios de los siguientes documentos cuando lo considere necesario:

- Referencias comerciales
- Referencias personales
- Certificados laborales
- Certificaciones bancarias
- Licencia de conducción válida
- Certificado de antecedentes judiciales
- Pasaporte vigente
- Libreta militar
- Documento de afiliación al Régimen de Seguridad Social en Salud
- Documento de afiliación a la empresa Administradora de Riesgos Profesionales
- Acta de nombramiento y/o posesión a un cargo
- Certificaciones de autoridades de inspección, vigilancia y control.

- Otros documentos que permitan verificar la identidad o facultades del suscriptor o de la entidad, para la emisión de cualquiera de los tipos de certificados que emite Olimpia IT

4.2.3. VALIDACIÓN DE IDENTIDAD DELEGADA REALIZADA POR ENTIDADES DEL SECTOR DE LA FUNCION PUBLICA A TRAVES DE CONVENIO

Se admitirá este método, siempre que una entidad del Sector de la Función Pública (según el objeto el artículo 2.1.1.1 de Decreto 1083 de 2015, Decreto Único Reglamentario del Sector de Función Pública) haya realizado previamente un proceso de autenticación de identidad del solicitante y Olimpia IT hubiese suscrito un convenio, acuerdo, contrato o alianza con la entidad del Sector de la Función Pública.

La entidad del Sector de la Función Pública debe contar con una habilitación para la validación de identidad, que puede comprender lo siguiente:

- Se encuentra legalmente o reglamentariamente habilitada para realizar el proceso de validación de identidad del solicitante.
- Cuenta con una autorización de tipo contractual, o de otra clase que le permita realizar la validación de identidad del solicitante.

Olimpia IT podrá solicitar certificación, procedimientos escritos y otra documentación que permita acreditar la autenticación de identidad realizada por la entidad del Sector de la Función Pública, en caso de considerarlo necesario.

4.2.3.1. VALIDACIÓN DE IDENTIDAD REALIZADA POR LA DIAN PARA LA PLATAFORMA GRATUITA DE FACTURACIÓN ELECTRONICA

Olimpia IT admitirá la validación de identidad realizada por la DIAN, para la emisión de certificados digitales de persona natural o persona jurídica, destinados a la firma de documentos en la Solución Gratuita del Sistema de Facturación Electrónica de la DIAN. La validación de identidad será la admitida para la inscripción o actualización del Registro Único Tributario – RUT, según los requisitos legales establecidos en el Estatuto Tributario (Artículo 555-2 y siguientes) y el Decreto 1625 de 2016 o las normas que los modifiquen o adicionen.

Olimpia IT aceptará la validación de identidad para la emisión de certificados digitales en la Solución Gratuita del Sistema de Facturación Electrónica de la DIAN, una vez se realice la autenticación de los solicitantes a través del envío de token al correo electrónico registrado en el RUT, o por medio de metodología similar o equivalente.

Para este proceso de validación de identidad, y la emisión de los certificados digitales, Olimpia IT almacenará alguno(s) de los siguientes números de identificación del solicitante:

- Cédula de Ciudadanía
- Cédula de Extranjería
- NIT
- Permiso por Protección Temporal - PPT
- Pasaporte
- Tarjeta de identidad, siempre que lo permita la DIAN en su Solución Gratuita del Sistema de Facturación Electrónica

4.2.4. AUTENTICACIÓN DE LA IDENTIDAD (FIRMA ELECTRONICA CERTIFICADA)

Olimpia IT realizará la validación de la identidad de los solicitantes, de acuerdo con el documento interno de ciclo de vida del certificado digital, que consiste, en resumen, en aplicar alguno de los siguientes métodos:

i. Validación mediante OTP: Se realizará la validación de identidad a través de autenticación de acceso al número celular que se registre en el portal, al cual será enviado una clave numérica de un único uso vía SMS.

ii. Validación por reconocimiento facial: El solicitante podrá capturar fotografía de rostro y cargar la imagen del documento de identidad por ambas caras y mediante este mecanismo la plataforma realizará un cotejo biométrico facial para confirmar la identidad del suscriptor. Este mecanismo incluye entre otras cosas una prueba de rostro vivo.

4.2.5. DEMOSTRACIÓN DE LA POSESION DE LA CLAVE PRIVADA

Olimpia IT mediante la aplicación del sistema de certificación digital implementado, realiza el control, posesión y emisión de la llave privada mediante el uso de dispositivos criptográficos certificados en FIPS 140 -2 nivel 3, esto se logra por medio del formato PKCS#11.

5. OPERACIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS DIGITALES

Olimpia IT define los estados para la emisión de certificados digitales, los cuales no pueden tener un periodo de vigencia superior a 2 años y no pueden ser activados después de estar vencidos o revocados.

5.1. SOLICITUD DE EMISIÓN DE CERTIFICADOS DIGITALES

Olimpia IT establece en el presente documento la forma de solicitar un certificado digital, a través de los siguientes medios:

- **Internet:** A través de la página web de la Entidad de Certificación Digital https://micertificado.olimpiait.com, o través de cualquier otro portal web que Olimpia IT defina como canal de venta de sus servicios de certificación digital, siempre que dichos portales estén debidamente integrados al portal de la Entidad de Certificación Digital.
- El solicitante deberá registrarse en el portal web en el botón "registro" o a través de cualquier otro portal que Olimpia IT, o a través de API debidamente integrada al portal de la Entidad de Certificación Digital, e ingresar la información allí requerida:
    - Tipo de identificación
    - Número del documento
    - Fecha de expedición del documento
- Se realizará una validación de la información ingresada contra la Base de datos biográfica de la Registraduría Nacional del Estado Civil, contra bases de datos propias o de terceros, sean oficiales o privadas

- Si la información no es válida, la aplicación informará que la información no es válida.
- Si la información es válida, el solicitante o quien ese delegue deberá ingresar la siguiente información:

    - Dirección de correo electrónico
    - Número de teléfono celular y confirmación del mismo.
    - Leer y aceptar los términos y condiciones de uso

- Al suscriptor o quien este delegue le llegará un mensaje a su correo electrónico, en el que se solicitará la activación de su cuenta por un enlace contenido en el mismo correo electrónico.
- El suscriptor deberá iniciar sesión en el portal web https://micertificado.olimpiait.com, en el botón "Registrarse/iniciar sesión" en el enlace "Iniciar sesión" e ingresar la siguiente información:

    - Tipo de documento de identidad
    - Número de documento de identidad

- Se enviará al número de teléfono celular registrado por el solicitante un OTP (One Time Password) compuesto por un código de 4 dígitos de un solo uso, para que el solicitante lo ingrese en el espacio dispuesto para ello, en la parte inferior de la ventana de inicio de sesión con el fin de generar una autenticación ante el portal.
- Una vez la autenticación sea efectiva, el portal web, informará al solicitante que ya se encuentra en su cuenta privada, el solicitante podrá solicitar certificados digitales desde el enlace "Certificados" o "Servicios" desde el enlace "Servicios".

- Cuando el servicio es solicitado por un menor de edad, su identidad será asegurada con el documento de identidad (tarjeta de identidad) autenticado y documento que respalde el vínculo del solicitante y el menor de edad (cuando este vínculo sea requerido según la normatividad).
- Olimpia IT se reserva el derecho de emisión de certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial o idoneidad legal o moral de la Entidad de Certificación Digital

Nota: La página Web de la Entidad de Certificación Digital podrá ser desplegada en los navegadores Chrome en su versión 71.0.3578.98 y Microsoft EDGE versión 38.14393.2068.0. El uso de cualquier otro navegador puede ocasionar inconvenientes con el uso del portal, la solicitud de certificados o servicios.

- **Telefónicamente:** Comunicándose con la línea de atención al cliente (+57 601) 742 7878, en donde el operador remitirá al solicitante al registro de la página web https://micertificado.olimpiait.com, descrita en el ítem anterior.

a) El solicitante podrá consultar el estado de su solicitud en página web https://micertificado.olimpiait.com. Si el usuario cumple con la documentación solicitada y con los requerimientos establecidos, Olimpia IT procederá a realizar la emisión del certificado en un lapso máximo de 2 días hábiles, contados desde la decisión de certificación de aceptar la solicitud, y sin contabilizar el tiempo que el solicitante se tarde en responder las solicitudes de subsanación de información, en caso de que apliquen.

Nota: Cuando se emite el certificado en Token físico, a los 2 días de emisión se les debe sumar el tiempo que tome la entrega, el cual dependerá del lugar de donde reside el suscriptor.

b) Las solicitudes son registradas desde la página Web https://micertificado.olimpiait.com.

c) Olimpia IT tiene la potestad de solicitar aclaración de la información suministrada o de la documentación; en caso de que no se logre aclarar la información o documentación, la decisión de certificación por parte de la CA será de rechazar la solicitud.

d) Toda documentación entregada por el solicitante debe ser almacenada de forma segura siguiendo los estándares establecidos por Olimpia IT bajo las certificaciones de NTC-ISO/IEC ISO 9001 y NTC-ISO/IEC 27001 en su versión vigente.

5.1.1. REALIZACIÓN DE LA SOLICITUD

El solicitante evacua de forma satisfactoria el registro en la página web https://micertificado.olimpiait.com y realiza una solicitud de un certificado o servicio.

El solicitante selecciona una opción de certificado o servicio en la página web https://micertificado.olimpiait.com, en una de las dos pestañas que contienen los certificados o servicios que Olimpia IT emite o presta.

A continuación, se listan de forma representativa los pasos que debe seguir el solicitante. De acuerdo con cada tipo de producto o servicio solicitado, se puede establecer un orden diferente en los pasos aquí descritos:

a) El solicitante da clic en el botón adquirir del certificado o servicio que desea adquirir.
b) El solicitante acepta los términos y condiciones para poder continuar con la solicitud.

c) El solicitante diligencia la información que solicita el portal web
d) El solicitante adjunta la documentación que solicita el portal web
e) El solicitante diligencia la información si requiere el servicio con token físico
f) Selecciona la vigencia del certificado que desea (máximo 2 Años)
g) Selecciona la fecha de inicio de la vigencia (Opcional)
h) El solicitante indica el paquete que desea adquirir
i) El solicitante genera el pago del paquete que indicó desea adquirir
j) El solicitante adjunta el comprobante de pago en un archivo, en los formatos permitidos para el cargue de documentos

- Si el solicitante realizó el pago en línea, la aplicación tomará el pago realizado y dará continuidad al paso de activación del certificado.

k) Olimpia IT realiza una validación automática o manual del pago, contrastando la referencia de la solicitud con el registro bancario, y almacena el registro o evidencias de la validación realizada.

Nota: La fecha de vigencia del certificado no podrá ser menor a la fecha actual, sino se selecciona fecha de inicio de vigencia, por defecto la fecha de vigencia será la fecha de emisión del certificado, la fecha de inicio de vigencia no podrá ser superior a 30 días.

5.1.2. REVISION DE LA SOLICITUD Y DECISIÓN DE LA CERTIFICACIÓN

5.1.2.1. REVISIÓN DE LA SOLICITUD

La RA revisará la solicitud del certificado presentada acorde con el procedimiento establecido para ello al interior de la ECD.

La RA remitirá la revisión de la solicitud al operador de la CA, quien la revisará y decidirá sobre la certificación.

5.1.2.2. DECISIÓN DE LA CERTIFICACIÓN

El operador de la CA, una vez la RA haya realizado la revisión de la solicitud, tomará la decisión de la certificación, acorde con el procedimiento establecido para ello al interior de la ECD.

Si la decisión de la certificación es de rechazar la solicitud, se le informará al solicitante por correo electrónico de esta decisión.

La RA tramita únicamente las solicitudes que se encuentran en el alcance de la acreditación otorgado por ONAC.

5.1.3. PERSONAS QUE PUEDEN SOLICITAR UN CERTIFICADO

Las personas que pueden solicitar un certificado digital son aquellas personas naturales o representantes legales de jurídicas nacionales o extrajeras la cuales sean mayor de edad bajo la ley Colombia (Aplica para persona natural) que residan en el territorio colombiano y tengan un correo electrónico activado.

5.1.4. PROCESO DE INSCRIPCIÓN

El proceso de inscripción para solicitud de un certificado digital se realiza mediante la página web de la Entidad de Certificación Digital, las responsabilidades las acepta el solicitante cuando realiza la aceptación del acuerdo de términos y condiciones y la aceptación de la DPC.

5.2. PROCESAMIENTO DE SOLICITUD DE CERTIFICADO

5.2.1. REALIZAR FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

El procesamiento de la solicitud se realiza desde la aplicación separando la RA (Autoridad de registro) y CA (Autoridad de certificación) por medio de permisos y responsabilidades, autenticando a los solicitantes por medio de los datos demográficos solicitados y soportes de las

restricciones implementadas por Olimpia IT para la validación de identidad

5.2.2. APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADOS

Una vez realizadas las validaciones correspondientes según lo especificado en los procedimientos de operación del sistema de gestión de la ECD el operador de la CA con la revisión realizada por la RA y sus revisiones complementarias aprueba o rechaza solicitudes realizadas por los solicitantes. Si Olimpia IT decide rechazar la solicitud de expedición del certificado de firma digital o firma electrónica, lo notificará mediante correo electrónico al solicitante indicando los motivos que justifican esta decisión.

Los motivos de rechazo pueden ser, entre otros los siguientes:

- Documentación no correspondiente al solicitante del certificado
- Información y/o documentación falsa
- Documentación incompleta
- Peligro Reputacional para la empresa
- Documentación incompleta
- Otros

Previamente a que las solicitudes sean rechazadas, la RA por medio del canal digital de Olimpia o área que haga sus veces, informará al solicitante sobre la inconsistencia documental o registral, así como, la imposibilidad de prestar el servicio, si el servicio solicitado se encuentra por fuera del alcance de la acreditación otorgado.

5.2.3. TIEMPO PARA PROCESAR LAS SOLICITUDES DE CERTIFICADO

Los tiempos establecidos por Olimpia IT para generar el certificado es de máximo dos (2) días hábiles a partir de la finalización de la solicitud, sin contabilizar el tiempo que el solicitante se tarde en responder las solicitudes de subsanación de información, en caso de que apliquen.

5.3. PROCEDIMIENTO PARA LA EXPEDICIÓN DE CERTIFICADO DIGITAL

Solicitud por parte del solicitante de un certificado digital o servicio ofrecido por la ECD.

Inicia con el registro del solicitante en el portal web https://micertificado.olimpiait.com, descrito en el numeral 5.1 de esta DPC y finaliza con la generación del certificado y entrega de firma digital o firma electrónica al suscriptor o prestación del servicio solicitado.

5.3.1. ACTIVIDADES DE LA AUTORIDAD DE REGISTRO (RA)

El control de seguridad de la RA (en ambiente físico y lógico), se realiza a través del proceso en donde la RA se identifica ante la CA mediante el uso de certificado digital.

La RA tiene la función de garantizar que:

a) La revisión de la solicitud debe asegurar la identificación inequívoca de la identidad del suscriptor (persona natural o jurídica), la veracidad y autenticidad de la información, que permita dar una recomendación para la toma de decisión.
b) La ECD debe mantener registros de los procesos de validación de identidad para demostrar el cumplimiento eficaz de la

identificación inequívoca del suscriptor y permitir una evaluación de dichos registros.

c) Se resuelve cualquier diferencia de entendimiento conocida entre la ECD y el solicitante, incluyendo el acuerdo con respecto a la DPC, documentos normativos u otros documentos reglamentarios.
d) Se define el alcance del servicio de certificación digital solicitado.
e) Se dispone de los medios para realizar todas las actividades de verificación.
f) La ECD tiene la competencia y la capacidad para llevar a cabo la actividad y servicios de certificación digital.
g) La ECD debe declinar una solicitud de un servicio de certificación digital, si el mismo no se encuentra en el alcance de la acreditación que le fue otorgado por ONAC.
h) La ECD debe documentar los procesos y los resultados relacionados con la revisión de la solicitud, incluyendo la recomendación para la decisión sobre la certificación con base en la revisión.
i) La RA realiza las validaciones documentales y de identidad de las diferentes solicitudes y emite una recomendación donde se define, la emisión o no emisión del certificado, esta solicitud es firmada digitalmente para que la CA genere el certificado.

5.3.1.1. REVISIÓN DE LA SOLICITUD

El procedimiento para la expedición de certificados digitales involucra la validación de la identidad y la calidad en la que actúa el solicitante por parte de la RA.
La RA validará la identidad del solicitante acorde a lo establecido en esta DPC en el numeral 4.2.

La RA validará la calidad en la que el solicitante pide sea concedido el servicio de la siguiente forma:

a) Si es persona Natural con lo establecido en el numeral 4.2 de esta DPC, y cuando aplique, con la información que reposa en el Registro Único Tributario (RUT) y los documentos y procedimientos establecidos en la Política de Certificados o cualquier documento que permita validar de manera confiable la calidad e identificación del suscriptor.
b) Si es persona jurídica, con la información que reposa de ella en el certificado de existencia y representación legal de la Cámara de Comercio (del domicilio de la persona jurídica), o con la información que reposa en el Registro Único Tributario (RUT), y los demás documentos y procedimientos internos que determine Olimpia IT en la Política de Certificados, o cualquier documento que permita validar de manera confiable su calidad e identificación del suscriptor.
c) Si es profesional titulado, con la entidad que expidió el título que acredita el solicitante o el banco de datos oficial que se haya determinado para ello y por los procedimientos internos que determine Olimpia IT para ello.
d) Si es de perteneciente a empresa, con la entidad que acredita que el solicitante ostenta la calidad que pide en el certificado de empleado o contratista y por los procedimientos internos que determine Olimpia IT para ello o cualquier documento que permita validar de manera confiable la calidad e identificación del suscriptor.
e) Si es función pública, con la información de la entidad que otorgó la función pública o acto administrativo de su nombramiento y por los procedimientos internos que determine Olimpia IT para ello o cualquier documento que permita validar de manera confiable la calidad e identificación del suscriptor.
f) Si es de representante legal, con la información que reposa de la sociedad en la Cámara de Comercio del domicilio de la sociedad y por los procedimientos internos que determine Olimpia IT para ello

o cualquier documento que permita validar de manera confiable la calidad e identificación del suscriptor.

Siempre que lo considere oportuno, el operador RA podrá solicitar la subsanación de la información inicialmente proporcionada por el solicitante en su solicitud, necesaria para la correcta validación y aprobación del producto o servicio. El tiempo que llegase a tardar el solicitante en responder las solicitudes de subsanación no será contabilizado dentro del plazo máximo de entrega, que ha establecido Olimpia IT para sus servicios.

La RA se comunica con la CA a partir de anotaciones realizadas en cada revisión de cada solicitud que la RA envía a la CA, junto con la recomendación de expedir un certificado digital.

5.3.2. DECISIÓN DE LA CERTIFICACIÓN

El operador de la CA una vez recibida la revisión antes descrita, tomará la decisión de certificación en sentido de aceptar o rechazar la solicitud.

La decisión se notificará acorde con lo establecido en el numeral 5.1.2. de esta DPC.

5.3.3. SOLICITUD EXPEDICIÓN DEL CERTIFICADO

El portal interno notificará a la CA la solicitud de emisión del Certificado Digital, esta procederá acorde con el procedimiento establecido para ello.

5.3.4. EMISIÓN DEL CERTIFICADO

La CA subordinada de Olimpia IT generará el Certificado Digital.

5.3.5. FORMA DE USO

La firma digital del suscriptor deberá ser usada desde un dispositivo HSM (Hardware Secure Module) certificado FIPS 140 -2 nivel 3.

La firma electrónica certificada podrá ser usada desde el portal web de la ECD, a través de API o por cualquier otro mecanismo que la ECD disponga para la prestación del servicio.

5.3.6. ENTREGA DE TOKEN AL SUCRIPTOR

En caso de que la solicitud requiera la entrega de la firma digital en token físico, el operador de la CA guardará la firma digital del certificado solicitado en un dispositivo HSM (Hardware Secure Module) certificado FIPS 140 -2 nivel 3, que será guardado en una bolsa de seguridad y entregado por una empresa de mensajería contratada para ello.

Nota: Para los servicios a través de token virtual, estos tienen el mismo funcionamiento que la firma centralizada.

5.3.7. ACTIVIDADES DE LA AUTORIDAD DE CERTIFICACIÓN PARA LA EMISION DEL CERTIFICADO

Las acciones de la CA (Autoridad de Certificación) se realizan después de realizar las validaciones correspondientes por parte del RA (Autoridad de Registro) y se limitan a:

- Generación de los certificados de forma segura (en ambiente físico y lógico), autenticando a los administradores y operadores con un doble factor de autenticación biométrica como control de acceso físico y usuario y contraseña para control de acceso lógico.

- Almacenado de la llave privada de forma segura.

5.3.8. NOTIFICACIÓN AL SOLICITANTE

Olimpia IT realiza la notificación a los solicitantes respecto al otorgamiento del servicio de certificación digital, por medio del envío de un correo electrónico a la dirección de correo electrónico especificada en el registro.

Una vez aprobado el Servicio de Certificación Digital, el suscriptor recibirá una notificación de aprobación con un Documento formal que contiene la siguiente información:

a) El nombre y la dirección de la ECD;
b) La fecha en que se otorga la certificación digital (esta fecha no debe ser anterior a la fecha en la cual se tomó la decisión sobre la certificación digital);
c) El nombre y la dirección del suscriptor;
d) El alcance de la certificación digital;
e) El término o la fecha de expiración de la certificación digital;
f) Toda otra información exigida para el servicio de certificación.

Para certificados emitidos mediante token físico y virtual, se notifica al suscritor a través de correo electrónico la generación de un pin de 4 dígitos de manera aleatoria e indicándole que debe generar el cambio del mismo mediante el uso del "Driver token" publicado en la página web de mi certificado en la sección de descargas.

Nota: La documentación formal de los servicios de certificación digital debe dar cumplimiento a lo establecido en el Reglamento de uso de los símbolos de Acreditado y/o Asociado del ONAC que se encuentre vigente.

5.4. ACEPTACIÓN DEL CERTIFICADO DIGITAL

5.4.1. CONDUCTA QUE CONSTITUYE LA ACEPTACIÓN DEL CERTIFICADO DIGITAL

Olimpia IT en su calidad de Entidad de Certificación Digital establece que se da por aceptado el certificado digital generado por la jerarquía de confianza establecida en Olimpia IT, en dos niveles desde la CA Raíz a la Sub CA, cuando el solicitante o suscriptor recibe la notificación de generación de su certificado por medio de correo electrónico.

Salvo acuerdo entre las partes, se entiende que un suscriptor ha aceptado un certificado cuando la entidad de certificación, a solicitud de éste o de una persona en nombre de éste, ha guardado dicho certificado en un repositorio.

5.4.2. PUBLICACIÓN DEL ESTADO DE LOS CERTIFICADOS DIGITALES

Olimpia IT realiza la publicación del estado de los certificados digitales emitidos en la página web de la Entidad de Certificación Digital https://micertificado.olimpiait.com, los cuales pueden ser consultados por cualquier persona.

5.5. CONDICIONES DE USO DEL CERTIFICADO DIGITAL Y LA CLAVE GENERADA

La responsabilidad de Olimpia IT para el uso del certificado se encuentra establecida en lo previsto por la normativa colombiana correspondiente.

5.5.1.USO DE LA CLAVE PRIVADA

Olimpia IT establece en la presente Declaración de Prácticas de Certificación el uso de las llaves privadas por parte de suscriptores dueños de la llave, siempre y cuando se realice un uso efectivo de alguno de los servicios o certificados expuestos por la Entidad de Certificación Digital.

5.5.2. USO DE LA CLAVE PÚBLICA

El uso de la llave pública de los certificados digitales emitidos por Olimpia IT es de confiabilidad pública, en los cuales el usuario deberá previamente validar el estado del certificado en el portal de servicios de la Entidad de Certificación Digital en la cual se obtiene la vigencia de la llave pública expuesta.

5.6. RENOVACIÓN DEL CERTIFICADO DIGITAL

Se establece en la presente Declaración de Prácticas de Certificación que en ninguna circunstancia se realizará la renovación de un certificado digital, se entiende que un suscriptor solicita la renovación de un certificado cuando este se ha vencido o está próximo a vencerse, por este motivo es necesario realizar una nueva solicitud cumpliendo los requisitos establecidos por la ECD en el momento de la nueva solicitud.

Asimismo, no se permite la suspensión de certificados que no conduzca a un estado de revocación inmediato. En este sentido, Olimpia IT no realiza suspensiones de certificados.

5.7. MODIFICACIÓN DE CERTIFICADOS

Olimpia IT establece en la presente Declaración de Prácticas de Certificación que no se pueden realizar modificaciones sobre los certificados digitales generados, en caso de requerir alguna modificación es necesario realizar la revocación del certificado y emitir uno nuevo.

5.8. REVOCACIÓN DE CERTIFICADOS DIGITALES Y CAUSALES DE REVOCACIÓN

5.8.1. REVOCACIÓN

Olimpia IT realizará la revocación de certificados digitales por una de las siguientes causales:

5.8.2. CAUSALES DE REVOCACIÓN

i. Compromiso de la seguridad en cualquier motivo, modo, situación o circunstancia.
ii. Muerte o incapacidad sobrevenida del suscriptor.
iii. Liquidación de la persona jurídica representada que consta en el certificado digital

iv. Confirmación que alguna información en el certificado digital es falsa.
v. Por la ocurrencia de hechos nuevos que provoquen que los datos originales no correspondan a la realidad.
vi. Orden judicial o de entidad administrativa competente.
vii. Pérdida, inutilización del certificado digital que haya sido informado a la ECD.
viii. Terminación del contrato de suscripción, de conformidad con las causales establecidas en el contrato.
ix. Por cualquier causa que razonablemente que se ponga en duda la confiabilidad del certificado digital.
x. Por el incumplimiento del Contrato del Servicio de Certificación Digital proporcionado por la ECD al suscriptor o de la persona jurídica.
xi. Por perdida de clave asignada por el suscriptor.
xii. Por el manejo indebido por parte del suscriptor del certificado digital.
xiii. Mal uso (bloqueo) del certificado.
xiv. Otras

5.8.3. SOLICITUD DE REVOCACIÓN (PERSONAS QUE INVOCAN LAS CAUSALES DE REVOCACION DE LOS CERTIFICADOS)

La solicitud de revocación de un certificado la puede solicitar:

El suscriptor y/o solicitante, quien deberá solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias o causas de revocación establecidas.

Cualquier persona o ente podrá solicitar la revocación de un certificado o de los certificados en caso de tener conocimiento de alguna de las circunstancias o causas de revocación establecidas.

Los colaboradores autorizados por Olimpia IT.
El suscriptor debe considerar que no podrá solicitar la revocación de un certificado digital, cuando dicho certificado no ha entrado en vigencia.

5.8.3.1. EN CUMPLIMIENTO DE UNA ORDEN JUDICIAL O ADMINISTRATIVA

En cumplimiento de una orden judicial o administrativa emitida por funcionario competente, se podrá realizar la revocación de cualquier certificado digital.

5.8.3.2. EN CUMPLIMIENTO DE UN CONVENIO

Las entidades del Sector de la Función Pública con convenios pueden solicitar la revocación de certificados tramitados bajo el convenio haciendo uso de servicios web o por medio del envío de un correo electrónico de solicitud indicando las causas o motivos para la revocación.

5.8.4. PROCESO DE REVOCACIÓN DE CERTIFICADOS DIGITALES Y VERIFICACIONES DE LA SOLICITUD DE REVOCACIÓN

El proceso de revocación de un certificado digital podrá iniciarse de manera oficiosa por parte de Olimpia IT, siempre que antecede a dicha revocación una justa causa legal, contractual o que se encuentre en esta Declaración de Prácticas de Certificación.

El procedimiento para la revocación de certificados denominado “Revocación de Certificados” y lista las siguientes actividades a desplegar:

a. Solicitud de la revocación

b. Validación de identidad del suscriptor
c. Validación de solicitud
d. Revocar certificado
e. Registros

En la revocación del certificado se enviará comunicado por correo electrónico al Suscriptor.

En este procedimiento se detallan las verificaciones de identidad y del estado del certificado que se deben hacer, a fin de ejecutar la solicitud de revocación

5.8.4.1. MEDIOS PARA LA RECEPCIÓN DE SOLICITUDES DE REVOCACIÓN

Olimpia IT habilita la revocación de los Certificados digitales de forma fácil y segura así:

- En la página web https://micertificado.olimpiait.com el suscriptor, se registra con usuario y contraseña e indicar cual es el certificado a revocar, debe utilizar el botón de revocación selecciona y describe en las observaciones el motivo, una vez confirme la solicitud la CA revoca el certificado de manera inmediata el certificado.

- Por vía telefónica (+57 601) 742 7878 el horario de atención será de 8AM a 5PM.

Olimpia IT se reserva el derecho de validar la identidad del suscriptor o entidad solicitante de la revocación, mediante los mecanismos establecidos por la Entidad de Certificación Digital.

Nota: En caso de que se revoque un certificado con relación a las firmas electrónicas o digitales, posteriormente el mismo no podrá ser rehabilitado por Olimpia IT.

5.8.5. OPORTUNIDAD PARA INVOCAR LAS CAUSALES DE REVOCACIÓN DE LOS CERTIFICADOS

La solicitud de revocación de un certificado podrá hacerse en cualquier momento, siempre que el certificado se encuentre en estado activo.

5.8.6. CONSECUENCIAS DE LA REVOCACIÓN DEL CERTIFICADO

Olimpia IT, en aras de garantizar la confiabilidad y demás atributos legales y técnicos otorgados a los certificados digitales, previo a la revocación o cancelación de un servicio otorgado deberá verificar el cumplimiento de una cualquiera de las causales de revocación o cancelación llamada prosperar de las que se encuentren pactadas contractualmente o descritas en esta Declaración de Prácticas de Certificación.

La culminación satisfactoria del proceso de revocación del certificado digital, dando lugar a la revocación del certificado digital, no implica la negación de nuevos servicios al suscriptor ni de los servicios/certificados revocados o cancelados, pudiendo el suscriptor solicitar nuevamente uno cualquiera de los servicios/certificados a Olimpia IT en las mismas condiciones técnicas, jurídicas y para los propósitos para los cuales se requiera el nuevo servicio/certificado.

Una vez se ha efectuado la revocación del certificado digital a partir de ese momento, dicho certificado no gozará del atributo de confiabilidad otorgado por la ley, imposibilitando el uso de este certificado digital revocado para cualquier uso legal incluidos los servicios para los cuales fue obtenido.

Como consecuencia de la revocación del certificado digital queda prohibido el uso de este o de sus componentes físicos o lógicos que se le hallan proporcionado al suscriptor para el uso de dicho certificado.

Si el certificado ha sido revocado por decisión imputable a la Entidad de Certificación Digital, esta tendrá la obligación de emitir un nuevo certificado digital con las mismas condiciones y partes involucradas en el certificado digital revocado, con exclusión del periodo de vigencia, el cual será por el faltante del tiempo de vigencia establecido para el certificado digital que se encuentra revocado.

5.8.7. PUBLICACIÓN DE LA REVOCACIÓN DE CERTIFICADOS

Olimpia IT se compromete a informar a los suscriptores sobre la revocación de los certificados digitales mediante los medios de comunicación acordados y publicados en la CRL, que se encuentra en la página https://micertificado.olimpiait.com.

La vigencia de la revocación del certificado iniciará cuando el certificado quede publicado en la CRL y la llave privada sea destruida. Olimpia IT deberá actualizar su CRL (Lista de certificados revocados) y publicarlo según los tiempos establecidos en la presente DPC (Declaración de prácticas de Certificación).

Olimpia IT garantiza la retención de los certificados digitales mientras Olimpia IT preste servicios como ECD, después de la perdida de vigencia del certificado o de la revocación el mismo; en caso de ser necesario.

5.8.8. FRECUENCIA DE PUBLICACIÓN DE LA CRL

La frecuencia de publicación de la CRL está determinada según el numeral 3.3.2 de la presente Declaración de Prácticas de Certificación.

5.8.9. DISPONIBILIDAD DE COMPROBACIÓN DE ESTADO

El estado de los certificados se puede consultar en línea mediante el uso de la CRL o del protocolo OCSP cuyas características se especifican en el

numeral 3.3.3 de la presente Declaración de Prácticas de Certificación, dispuestos en la página https://micertificado.olimpiait.com.

5.9. ESTADO DE LOS CERTIFICADOS

5.9.1.CARACTERÍSTICAS

Los estados de los certificados digitales se encuentran en línea y se realiza la validación de cada uno de los certificados por medio de la implementación del protocolo OCSP (Online Certificate Status Protocol) el cual permite al suscriptor, partes confiantes y terceros interesados, conocer el estado actual de su certificado.

5.9.2. DISPONIBILIDAD

La disponibilidad del servicio de actualización de la lista de certificados revocados de Olimpia IT está alineada a lo requerido por ONAC en el cual se especifica el 99.8% de disponibilidad al año.

5.10. FINALIZACIÓN DEL SERVICIO

La finalización del servicio de certificación digital se produce en los siguientes casos:

- Revocación del certificado por cualquier causa de revocación.
- Finalización de la vigencia del certificado.
- Por consumo total del paquete adquirido.

Una vez el servicio ha finalizado, por cualquiera de sus causas, la conservación de los certificados digitales emitidos será de mínimo diez (10) años, contados a partir del día siguiente a la finalización del servicio

5.11. TIPOS DE HSM OFRECIDOS

Olimpia IT, ofrece al suscriptor que el uso de la llave privada se pueda realizar desde los HSM alojados en los datacenter de Olimpia IT o en un dispositivo criptográfico HSM "token" portátil que es entregado al suscriptor y que contiene la clave privada del suscriptor, en ambos casos el dispositivo criptográfico es certificado FIPS 140-2 nivel 3.

Las características técnicas del dispositivo entregado al suscriptor se detallan a continuación y en el siguiente enlace: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/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. RIESGOS Y COMPROMISOS DE LOS DISPOSITIVOS CRIPTOGRÁFICOS QUE OFRECE OLIMPIA IT

A continuación, se listan los riesgos y compromisos técnicos que tiene los dispositivos criptográficos que ofrece Olimpia IT, están basados en la información suministrada por el fabricante y que se encuentra en el siguiente enlace:

https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2434

Los riesgos asociados son:

- Obsolescencia tecnológica
- Ausencia de soporte técnico del fabricante o proveedor
- Riesgos por fuera de la política de seguridad del fabricante

5.13. CUSTODIA DEL PAR DE LLAVES

La custodia del par de llaves generados en la CA Raíz y la CA subordinada se almacenan en la infraestructura tecnológica de Olimpia IT, la cual contiene dispositivos criptográficos HSM y a los cuales solo se puede tener acceso por medio de la combinación de las claves asignadas a custodios de Olimpia IT.

La contraseña para la generación del par de llaves se encuentra dividida en dos partes cada una a cargo de una gerencia al interior de Olimpia IT.

Los caracteres de las contraseñas se encuentran en sobres sellados, los cuales a su vez se encuentran bajo la seguridad física de cada una de las gerencias encargadas de la custodia de las partes de la contraseña de generación de los certificados de la CA Raíz y la CA Subordinada.

6. CONTROLES DE SEGURIDAD

6.1. CONTROLES DE SEGURIDAD FÍSICA

6.1.1. UBICACIÓN Y CONSTRUCCIÓN

Todas las operaciones relacionadas con la Entidad de Certificación Digital están protegidas físicamente con un sistema de acceso biométrico el cual tiene una funcionalidad de 24X7X365 lo cual permite identificar a las personas que requieran acceso a las instalaciones donde se contiene los activos de información de tal forma se garantiza que solo el personal autorizado puede acceder a ellos. Además, cuenta con equipos ubicados en el centro de datos equipados con las protecciones necesarias determinadas por el acuerdo contractual entre el centro de datos y Olimpia IT.

6.1.2. CONTROL DEL ACCESO

El control para el acceso físico a las instalaciones de la compañía está definido por las políticas internas en la que se establecen perímetros de seguridad correspondientes al nivel de confidencialidad de la información a la cual se quiere acceder, adicionalmente el personal que ingresa cuenta con permisos de acceso predefinidos de acuerdo con los requerimientos de acceso por perfil o cargo, adicionalmente las instalaciones se monitorean a través de CCTV.

El ingreso a los centros de datos se controla y lleva a cabo teniendo en cuenta las políticas de control de acceso y protocolos definidos por la compañía.

6.1.3. SEGURIDAD DE LA INFRAESTRUCTURA

Atendiendo los requerimientos de ONAC, de uptime del 99.8% para la PKI y para la CRL, Olimpia IT, cuenta con la implementación de la infraestructura PKI en alta disponibilidad mediante el resguardo de sus equipos críticos en dos centros de datos los cuales cuentan con los controles de seguridad de acceso físico y lógico, un plan de continuidad en caso de alguna emergencia y un mantenimiento periódico a la infraestructura interna mejora la seguridad de los equipos.

6.1.4. SISTEMA DE ALMACENAMIENTO

La información física relacionada con la emisión de certificados digitales se almacena de forma segura en cajas fuertes y cajoneras protegidas con llave según la evaluación del nivel de importancia determinado por el propietario o custodio del activo.

6.1.5. ELIMINACIÓN DE INFORMACIÓN

Olimpia IT garantiza la eliminación optima de información sensible mediante la aplicación de un procedimiento interno el cual está basado

en las recomendaciones brindadas por estándares internacionales con la generación de evidencias de la total destrucción de la información.

6.1.6. ALMACENAMIENTO DE COPIAS DE SEGURIDAD

El almacenamiento de las copias de seguridad se realiza después de realizar la generación de las llaves privadas y públicas de la CA RAÍZ y la CA SUBORDINADA, una vez generadas las claves se realiza la copia de seguridad de todo el dispositivo criptográfico en las "SmartCard" las cuales quedan bajo custodia de Olimpia IT.

6.1.7. USO EXCLUSIVO DE LOS SISTEMAS DE CERTIFICACIÓN

Se establece como control de seguridad que los sistemas que cumplan las funciones de certificación solo son y serán utilizados con ese propósito y por lo tanto, no realizan ninguna otra función.

6.1.8. PROTECCIÓN EN CENTRO DE DATOS

Las instalaciones de los centros de datos están construidas en materiales de concreto que garantizan la protección frente a ataques por fuerza bruta, y se encuentran ubicadas en una zona de bajo riesgo de desastres que permite un rápido acceso, posee falso suelo, sistemas de detección y extinción de incendios, sistemas antihumedad, sistema de refrigeración y sistema de suministro eléctrico, el centro de datos tiene protección contra ondas electromagnéticas.

6.2. CONTROLES PROCEDIMENTALES

6.2.1. ROLES DE CONFIANZA

Olimpia IT, posee actualmente roles y responsabilidades relacionados con los procesos de emisión de certificados digitales los cuales se definen de la siguiente forma:

Administrador de la CA debe realizar las funciones acordes a su rol en la ECD.
Operador de la CA debe realizar las funciones acordes a su rol en la ECD.
Administrador RA debe realizar las funciones acordes a su rol en la ECD.
Operador RA debe realizar las funciones acordes a su rol en la ECD.
Alta Dirección de la ECD debe realizar las funciones acordes a su rol en la ECD.
Administrador de PKI debe realizar las siguientes funciones acorde a su rol en la ECD.

6.2.2. NÚMERO DE PERSONAS REQUERIDAS POR ACTIVIDAD

Se garantiza que se dispone por lo menos 1 persona para realizar la tarea que se requiere.

6.2.2.1. CONTINUIDAD

En caso de ausentismo total o parcial del rol definido anteriormente, éste será retomado por un trabajador que ostente un rol paralelo y que posea un perfil similar.

6.2.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Los usuarios encargados de cada uno de los roles descritos en los apartados anteriores se autentican mediante del directorio activo de Olimpia IT, el cual cuenta con un usuario único de autenticación y una clave sólida generada bajo las mejores prácticas de la industria, adicionalmente la seguridad de la información sensible se limita solo al personal autorizado mediante la negación de permisos de acceso a la cuenta de ingreso.

6.3. CONTROLES DE SEGURIDAD PERSONAL

6.3.1. REQUISITOS, CALIFICACIONES Y EXPERIENCIA

Olimpia IT garantiza que sus empleados designados a trabajar en la emisión de certificados digitales deben poseer:

- Nivel mínimo de desarrollo de competencias blandas de acuerdo con el nivel del cargo.
- Aprobación de pruebas técnicas de desempeño y conocimientos.
- Conocimientos en SGSI y SIG.
- Título académico de acuerdo con el cargo a ocupar en la compañía.
- Entrevista de selección.

6.3.2. COMPROBACIÓN DE ANTECEDENTES

Olimpia IT establece en su proceso de contratación la validación de antecedentes penales, civiles y judiciales de cada uno de sus trabadores los cuales son validados y aceptados.

6.3.3. REQUISITOS DE FORMACIÓN AL PERSONAL

Olimpia IT contempla dentro de su plan de formación, la capacitación al personal involucrado en el proceso de emisión de certificados digitales para el correcto desarrollo
de las funciones dentro de la empresa el cual incluye como mínimo:

- Seguridad de la información física y lógica.
- Servicios prestados por la ECD.
- Conceptos Generales de la DPC.
- Conceptos básicos sobre el monitoreo y gestión de incidentes.
- Marco legal y disciplinarios para tener en cuenta.

6.3.4. FRECUENCIA CON LA QUE SE REALIZA LA FORMACIÓN AL PERSONAL

Olimpia IT valida las acciones de formación de motivación individual o corporativa en los
temas definidos anteriormente anualmente en:

- Aspectos de seguridad de la empresa incluyendo la emisión de certificados digitales, Curso virtual en seguridad de la información
- Curso Virtual de Atención al Cliente
- Inducción virtual y presencial

6.3.5. FRECUENCIA DE ROTACIÓN DE RESPONSABILIDADES EN OLIMPIA IT

Olimpia IT actualmente no realiza rotación en los roles definidos para la ejecución de las actividades ya que éstas son inherentes al cargo, aunque cada persona habilitada, en la formación e inducción a las actividades asociadas a un rol cuenta con un recurso de respaldo en caso de ausencia del principal asociado al rol.

6.3.6. SANCIONES A LOS TRABAJADORES

Olimpia IT define dentro de su Reglamento Interno de Trabajo las acciones a tomar por
sospecha o por evidencia de acciones no autorizadas para la implementación de las labores para las cuales el empleado fue contratado, dichas sanciones pueden ir desde
un llamado de atención, la reubicación del recurso hasta la desvinculación del trabajador involucrado.

6.3.7. DOCUMENTACIÓN SUMINISTRADA A LOS TRABAJADORES DE OLIMPIA IT

Olimpia IT cuenta con un Sistema de Gestión de Calidad NTC-ISO/IEC ISO 9001 y de Seguridad de la Información NTC-ISO/IEC 27001 en su versión vigente, que proporciona a sus empleados toda la documentación y buenas prácticas necesarias para el correcto desempeño de sus tareas. Entre la documentación provista se encuentra la siguiente:

- Declaración de Prácticas de Certificación
- Política de Seguridad de la Información

- Política de seguridad y Salud en el Trabajo
- Política de Gestión de Calidad
- Organigrama Institucional
- Procedimientos y caracterizaciones

6.4. CONTROL DE EVENTOS DE SEGURIDAD

6.4.1. REGISTROS DE AUDITORIA (LOGS)

Olimpia IT cuenta con plataformas tecnológicas a fin de garantizar el monitoreo de los eventos transaccionales y de seguridad acorde a la necesidad del servicio; en caso de existir algún incidente de seguridad se seguirá el procedimiento interno el cual incluye la revisión de cada registro de eventos y los siguientes datos relativos:

- Fecha y hora del incidente de seguridad
- Identificación del incidente por medio de un número de identificación
- Identificación de las causas del incidente de seguridad
- Monitoreo y generación de eventos sobre los componentes críticos del sistema
- Identificación de la criticidad del incidente de seguridad
- Respuesta a incidentes de forma reactiva y proactiva

Los logs se revisan al interior de Olimpia IT, por lo menos una vez al año.

6.4.2. FRECUENCIA DE ALMACENAMIENTO PARA LOS LOGS

Olimpia IT garantiza la frecuencia de almacenamiento de logs y el monitoreo de la información en tiempo real mediante el uso de las herramientas tecnológicas para el monitoreo y registro de logs

6.4.3. ALMACENAMIENTO DE REGISTROS DE AUDITORÍA

El sistema de recopilación de pistas de auditoría se ejecuta de forma automática en la aplicación, la cual, de cumplimiento a lo definido por la entidad de vigilancia y control, el ente regulador o mínimo de 3 años.

6.4.4. ALERTAMIENTO DE EVENTOS DE SEGURIDAD

El servicio de monitoreo de Olimpia IT alerta al Administrador de la CA respecto a la generación de actividades no autorizadas o registros de eventos potencialmente peligrosos en la infraestructura de la Entidad de Certificación Digital; el Administrador de la CA debe realizar el escalamiento a las unidades correspondientes y ejecutar el procedimiento interno de Olimpia IT cuando:

- La seguridad de la llave privada se ha visto comprometida
- Cuando el sistema de seguridad ha sido vulnerado
- Cuando se presenten fallas en el sistema que comprometan la prestación del servicio
- Cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratado por el suscriptor
- Cuando se presente cualquier otro evento o incidente de seguridad de la información.

6.4.5. ANÁLISIS DE VULNERABILIDADES

El equipo de ciberseguridad de Olimpia IT realiza un análisis de vulnerabilidades de forma periódica a la infraestructura critica de la Entidad de Certificación Digital realizando el correspondiente informe respecto a las vulnerabilidades encontradas durante el análisis.

6.5. REGISTRO DE EVENTOS DE AUDITORÍA

6.5.1.TIPOS DE REGISTROS ALMACENADOS

Se realiza el monitoreo de los siguientes parámetros dentro del ciclo de los certificados digitales:

- Formulario de solicitud
- Registro de revisión por parte de la RA
- Registro de decisión por parte de la CA
- Generación del certificado digital
- Almacenamiento de la llave privada
- Notificaciones a los solicitantes
- Uso del certificado digital o servicios adquiridos
- Registro de revocación
- Destrucción de las claves criptográficas
- OCSP
- CRL

Para la CA RAÍZ y CA Subordinada:

- Generación de las claves
- Administración de los dispositivos criptográficos (HSM)
- Almacenamiento de las claves criptográficas
- Destrucción de claves criptográficas

Monitoreo de la información pública:

- Actualización o modificación de la Declaración de Prácticas de Certificación
- Actualización o modificación de los acuerdos de términos y condiciones
- Actualización o modificación de la documentación del sistema de gestión
- Autorización de acceso a los sistemas de información.

6.5.2. TIEMPO DE ALMACENAMIENTO DE LA INFORMACIÓN

La información requerida en el ciclo de vida de los certificados se conservará durante el periodo que establezca la legislación vigente cuando sea aplicable.

El almacenamiento de los registros de auditoria transaccional y de seguridad da cumplimiento a lo definido por la entidad de vigilancia y control, el ente regulador o mínimo de 3 años.

6.5.3. PROTECCIÓN DE LA INFORMACIÓN

La seguridad de la información resguardada por Olimpia IT es de acceso restringido y tanto el almacenamiento físico como lógico se realiza de forma segura siguiendo las políticas de la Entidad de Certificación Digital en seguridad de la información.

6.5.4. PROCEDIMIENTOS DE BACKUP DE LA INFORMACIÓN

Las copias de seguridad de la información se realizan en los servidores de la Entidad de Certificación Digital mediante un proceso automático de sincronización con servidores ubicados en el Datacenter alterno.

6.5.5. PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Los registros de auditoría generados por Olimpia IT para la ejecución de actividades como Entidad de Certificación Digital están protegidos por acceso físico y lógico mediante la implementación de dispositivos biométricos para el acceso físico a la información confidencial, la asignación de permisos por parte del responsable de la Entidad de Certificación Digital y realizando el monitoreo de acceso a los registros de auditoría.

La comprobación de la seguridad implementada se realiza mediante la acción de auditoría interna y externa realizada por el personal competente para esta actividad y validada por el Oficial de Seguridad con el fin de tener los controles necesarios para el resguardo de las pistas de auditoría.

6.6. RE-CREACIÓN DE LA LLAVE DE LA CA RAÍZ

La re-creación de la clave de la CA RAÍZ se realiza por medio de un proceso de auto firmado siempre y cuando se dé el vencimiento del par de llaves generadas previamente o exista un proceso de revocación de las mismas, Olimpia IT se compromete a realizar el alertamiento oportuno al ente Organismo Evaluador de la Conformidad (ONAC) con el fin de dar cumplimiento a lo establecido en la normas legales y técnicas y cumplir con todos los parámetros de seguridad establecidos por la Entidad de Certificación Digital.

6.7. CONTINUIDAD Y CONTINGENCIA

Olimpia IT, ha desarrollado el plan de continuidad para recuperar todos los sistemas después de un desastre según los procedimientos internos de la organización, donde se tiene identificado un BIA – DRP y la gestión de riesgos asociada a estas actividades.

6.7.1. PROCEDIMIENTOS DE SEGURIDAD PARA EL MANEJO DE EVENTOS E INCIDENTES

Se establece un procedimiento interno para gestión de incidentes en cumplimiento del anexo A de la norma NTC-ISO/IEC 27001 en su versión vigente, transversal a la organización para el alertamiento y solución de posibles incidentes de seguridad de la información en la Entidad de Certificación Digital unido al plan de continuidad de negocio en caso de ser necesario, en el cual se le dan prioridad a la solución del alertamiento de incidentes entre otros se puede tener:

- Afectación de la disponibilidad de los servicios
- Alteración de la información de la Entidad de Certificación Digital
- Divulgación de información de tipo restringido o privado de la Entidad de Certificación Digital

Olimpia IT mantiene su compromiso con la seguridad de la información acorde con la Política General de su Sistema Integrado de Gestión.

6.7.1.1. EVENTOS DE SEGURIDAD QUE SE DEBEN REGISTRAR

Se tendrán en cuenta entre otros los siguientes eventos:

a) Cuando la seguridad de la llave privada de la entidad de certificación se ha visto comprometida.
b) Cuando el sistema de seguridad de la entidad de certificación ha sido vulnerado.
c) Cuando se presenten fallas en el sistema de la entidad de certificación que comprometan la prestación del servicio.
d) Cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratado por el suscriptor.
e) Cuando se presente cualquier otro evento o incidente de seguridad de la información.

6.7.2. CAMBIOS NO AUTORIZADOS EN LOS RECURSOS

Olimpia IT dispone en su plan de continuidad de negocio los tiempos necesarios para recuperar la integridad de la información alterada en su infraestructura critica el cual se revisa y prueba periódicamente (al menos una vez al año) con el fin de validar su eficacia ante los posibles incidentes de seguridad, adicionalmente se establece la prioridad a la información de los certificados digitales emitidos, revocados o vencidos según establecido por el ente auditor.

6.7.3. PROCEDIMIENTO ANTE EL COMPROMISO DE LA LLAVE PRIVADA

Cuando se presente el compromiso de la seguridad de la llave privada sea de la CA RAÍZ, CA Subordinada o de los suscriptores, Olimpia IT deberá

ejecutar el procedimiento de revocación a los certificados afectados, en el caso en donde sea de la CA RAÍZ o CA subordinada se debe emitir el nuevo par de llaves según lo especificado en la presente Declaración de Prácticas de Certificación.

Olimpia IT notificará la revocación a los suscriptores cuando comprometa la llave privada.

6.7.4. CONTINUIDAD DE NEGOCIO ANTE UN DESASTRE NATURAL

El plan de continuidad de negocio de Olimpia IT contempla resguardo de información en ubicaciones diferentes teniendo una redundancia en los servicios prestados en caso de que se presente el acontecimiento, adicionalmente se realizará una supervisión periódica al estado de los servicios prestados.

6.8. FINALIZACIÓN DE LA ACTIVIDADES COMO ENTIDAD DE CERTIFICACIÓN DIGITAL

De conformidad con el artículo 17 del Decreto 333 de 2014, las entidades de certificación acreditadas por el ONAC podrán cesar en el ejercicio de sus actividades, en las condiciones establecidas en el artículo 34 de la Ley 527 de 1999, modificado por el artículo 163 del Decreto-ley 19 de 2012 y deberán informar a ONAC.

En el evento en que Olimpia IT deba por cualquier circunstancia cesar sus actividades deberá:

- Informar a todos los suscriptores mediante dos avisos publicados en diarios o medios de amplia circulación nacional, con un intervalo de 15 días, sobre:

    i. La terminación de su actividad o actividades y la fecha precisa de cesación.

ii. Las consecuencias jurídicas de la cesación respecto de los certificados expedidos.
iii. La posibilidad de que un suscriptor obtenga el reembolso equivalente al valor del tiempo de vigencia restante del certificado.
iv. La comunicación enviada a la Superintendencia de Industria y Comercio, y si es el caso, el operador de la CRL responsable de la publicación de los certificados emitidos por la ECD, hasta cuando expire el último de ellos.

En todo caso los suscriptores podrán solicitar la revocación y el reembolso equivalente al valor del tiempo de vigencia restante del certificado, si lo solicitan dentro de los dos (2) meses siguientes a la segunda publicación.

La terminación de la actividad o actividades se hará en la forma y siguiendo el cronograma presentado por la ECD al ente de vigilancia y control y que éste apruebe.

7. CONTROLES DE SEGURIDAD TÉCNICA

7.1. CREACIÓN E INSTALACIÓN

7.1.1. GENERACIÓN DEL PAR DE LLAVES

La generación de las claves de la CA Raíz y la CA Subordinada se realiza con autenticidad e integridad de acuerdo con el procedimiento de ceremonia de llaves, en un dispositivo criptográfico hardware (HSM) certificado FIPS 140-2 nivel 3, y con la participación de diferentes involucrados que incluye el rol auditor.

En los casos en que Olimpia IT, pueda garantizar que las claves criptográficas del Suscriptor han sido creadas en un dispositivo

criptográfico que cumpla con los requisitos mínimos (si el tipo de soportes Tarjeta/Token o HSM Centralizado),

El par de llaves de cada una de las anteriores CA ha sido generado de acuerdo con el procedimiento de Ceremonias de Generación de llaves.

El algoritmo de generación del par de llaves es RSA (Rivest, Shamir y Adlemar) un algoritmo de firma SHA (Secure Hash Algortim).

7.1.2. ENTREGA DE LA LLAVE PRIVADA AL SUSCRIPTOR

Olimpia IT cuenta con un método de entrega de la llave privada al suscriptor, el cual consiste en que por medio de un HSM con seguridad FIPS 140 – 2 Nivel 3 se almacena la llave privada la cual es entregada al suscriptor según lo establecido en la presente Declaración de Prácticas de Certificación.

7.1.3. ENTREGA DE LA LLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

La llave pública será almacenada y publicada por Olimpia IT cuando su forma de solicitud sea distinto al PKCS#10, cuando la solicitud del servicio se realice por la forma PKCS#10, Olimpia IT no almacenará ni publicará la llave pública, por cuanto la misma es de responsabilidad del solicitante que la suministra por un CSR (*Certificate Signing Request*).

Olimpia IT podrá emitir certificados digitales a partir de una solicitud de certificación digital radicada por el suscriptor o por un tercero autorizado. Por lo cual, el tercero deberá garantizar que los parámetros utilizados para la llave pública son el algoritmo criptográfico SHA 256 + RSA, y que estas llaves tengan un tamaño de 2048 bits.

7.1.4. ENTREGA DE LA LLAVE PÚBLICA DE CA A PARTES CONFIABLES

Olimpia IT permite la descarga de la llave pública desde su portal web de la Entidad de Certificación Digital a través del acceso a la descarga del certificado digital autofirmado que contiene la lleva pública.

7.1.5. TAMAÑO DE LAS LLAVES

Olimpia IT utiliza como tamaño de las llaves de la CA RAÍZ y de la CA subordinadas una longitud de 4096 bits basadas en el algoritmo RSA.

Olimpia IT utiliza como tamaño de las llaves para los suscriptores de 2048 bits basadas en el algoritmo RSA.

7.1.6. PARÁMETROS DE LLAVE PÚBLICA Y VERIFICACIÓN DE LA CALIDAD

Los parámetros utilizados para la llave pública son el algoritmo criptográfico SHA256 + RSA.

7.1.7. USOS DE LA LLAVE

El uso de la llave de la CA RAÍZ será para firmar el certificado de las CA Subordinadas, garantizando autenticidad, integridad no repudio, la CA Raíz permanecerá en estado apagado.

El uso de la llave de la CA subordinada es para firmar certificados digitales de los suscriptores, firma de CRL, garantizando autenticidad y no repudio.

El uso de los certificados digitales de los suscriptores será el permitido por la ley, esta DPC, el alcance acreditado y lo pactado con el suscriptor.

7.2. SEGURIDAD DE LA LLAVE PRIVADA

Olimpia IT establece la protección de la llave privada de la CA subordinada y de la CA raíz mediante el módulo criptográfico (Hardware Secure Module) ubicado en la infraestructura tecnológica de Olimpia IT, con su respectiva copia de seguridad almacenado en las tarjetas inteligentes (SmartCards) las cuales están en custodia de Olimpia IT.

7.2.1. ESTÁNDARES PARA LOS HSM

Olimpia IT establece en sus módulos criptográficos la aplicabilidad del estándar FIPS 140-2 nivel 3 descrito por el NIST (National Institute of Standards and Technology) para dispositivos criptográficos de referencia "Luna PCI-e cryptographic module safenet.inc".

7.2.2.CONTROL DE ACCESO A LA LLAVE PRIVADA

El control de acceso a la llave privada de la CA RAÍZ y CA Subordinada se realiza mediante un control multi personal de roles involucrados definidos por Olimpia IT para la ejecución de este proceso.

7.2.3. CUSTODIA DE LA LLAVE

La custodia de la llave privada de la CA RAÍZ y CA subordinadas se realiza mediante la utilización de la metodología establecida por Olimpia IT para el manejo de llaves criptografías y se almacena de forma segura en la infraestructura o dispositivo designada.

La custodia de las llaves privadas las cuales son entregadas directamente a los suscriptores por medio del servicio de entrega autorizado y son de responsabilidad del suscriptor mediante la custodia de esta.

7.2.4. BACKUP DE LA LLAVE PRIVADA

Las copias de seguridad de las llaves privadas de la CA RAÍZ y CA subordinada de los suscriptores quedan debidamente almacenadas en las SmartCards de Olimpia IT las cuales son custodiadas y resguardas en las oficinas de Olimpia IT.

7.2.5. ARCHIVO DE LA LLAVE PRIVADA

El archivo de la llave privada se resguarda en la infraestructura tecnología de Olimpia IT ubicado en dos centros de datos diferentes y se encuentran en dispositivos criptográficos FIPS 140-2 nivel 3, los cuales cumplen con los requerimientos de seguridad física establecidos por Olimpia IT.

7.2.6. ALMACENAMIENTO DE LA LLAVE PRIVADA EN LOS HSM

La llave criptográfica de la CA Raíz, CA Subordinada y TSA se crea y almacena en el módulo HSM, las copias de seguridad y la recuperación se describen en el procedimiento interno de Olimpia IT.

7.2.7.PROCEDIMIENTO DE ACTIVACIÓN DE LA LLAVE PRIVADA

La activación de la llave privada se realiza en un procedimiento multi personal ejecutado
en los HSM, en el cual los involucrados (trabajadores y observadores) validan y dejan evidencia del proceso realizado para la activación de la llave privada.

Nota: La responsabilidad de la custodia de la llave privada permanecerá en Olimpia IT o en caso de entregar el HSM (token) al solicitante, este se responsabilizará por su llave privada.

7.2.7.1. PROCEDIMIENTO PARA LA GENERACIÓN DE LA LLAVE PRIVADA DE LA CA RAÍZ Y SUBORDINADAS.

Para la generación de la nueva llave privada en caso de vencimiento de las llaves privadas de la CA raíz y las subordinadas se debe:

- Realizar la destrucción de las claves privadas de los dispositivos criptográficos
- Destrucción de las copias de seguridad
- Realizar nuevamente la ceremonia de llaves
- Asignar nuevas contraseñas de acceso

- Custodiar de forma segura la nueva llave privada
- Ejecutar el backup de la llave privada

Adicionalmente el sistema debe rechazar cualquier intento de generar o firmar un certificado si la llave se encuentra en estado de vencimiento

7.2.8. PROCEDIMIENTO DE DESACTIVACIÓN DE LA LLAVE PRIVADA

La desactivación de la llave privada se realiza una vez el servicio ha finalizado por cualquier causa legal o contractual y el estado del certificado pasará a ser revocado.

7.2.9. PROCEDIMIENTO DE DESTRUCCIÓN DE LA LLAVE PRIVADA

La llave privada de la CA no se destruye hasta que el propósito comercial haya dejado de tener valor o las obligaciones legales hayan caducado.

Existen 3 mecanismo para realizar el borrado de los HSM, el responsable de la ECD aprueba el mecanismo de borrado a implementar acorde a lo requerido por el control de cambios gestionado

i. Borrar desde la aplicación
ii. Borrar desde las herramientas que vienen con el HSM
iii. Se puede forzar el jumper para el borrado seguro de la información (Acorde a la configuración del HSM)

Se destruirán físicamente o reinicializarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de la clave privada de firma de certificados de la CA Raíz y de la CA Subordinada, o de los datos de activación de estas, incluyendo también los dispositivos que contengan copias de dichas claves o de sus datos de activación

7.2.9.1. PROCEDIMIENTO DE DESTRUCCIÓN DE LA LLAVE PRIVADA DEL SUSCRIPTOR

La destrucción de la llave privada del suscriptor se realiza mediante el uso de borrado seguro de información por software de la base de datos en donde se encuentra almacenada la llave privada del suscriptor.

Esto está asociado a la revocación del certificado, al vencimiento del certificado digital o cualquier otra causa que impida hacer uso del certificado.

7.2.10. VULNERABILIDADES SISTEMAS DE CIFRADO

Olimpia IT establece para mitigar la perdida de la vigencia de la llave de cifrado por método de intrusión un tamaño de RSA de 2048 el cual actualmente es uno de los métodos más seguros de cifrado conocido.

7.2.11. CERTIFICACIÓN DEL MÓDULO CRIPTOGRÁFICO

Los módulos criptográficos adquiridos por Olimpia IT (HSM) para la CA RAÍZ y la CA subordinada dan cumplimiento al estándar FIPS140-2 NIVEL 3 o superior.

7.3. INFORMACIÓN ADICIONAL RESPECTO A LA ADMINISTRACIÓN DEL PAR DE LLAVES

7.3.1. ARCHIVO DE LA LLAVE PÚBLICA

Los certificados emitidos por Olimpia IT, y por tanto las claves públicas, se conservarán durante el periodo exigido por la legislación vigente cuando sea aplicable, o al menos durante 3 años desde su expiración.

7.3.2. TIEMPO OPERACIONAL DE LOS CERTIFICADOS

El tiempo de validez de los certificados está determinado por la vigencia otorgada por Olimpia IT y se puede reducir en caso de que se realice el proceso de revocación del certificado el cual se puede evidenciar al

consultar la lista de certificados revocados (CRL) en la página web de la entidad.

El periodo de uso de un certificado será determinado por la validez temporal del mismo. Un certificado no debe ser usado después del periodo de validez del mismo, aunque la parte confiante pueda usarlo para verificar datos históricos teniendo en cuenta que no se garantiza un servicio de verificación en línea válido para ese certificado

7.4. DATOS DE ACTIVACIÓN

7.4.1. GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación de la CA RAÍZ y CA Subordinada se deben generar y almacenar en los HSM y cuya protección se encuentra en cabeza de 2 o más trabajadores de Olimpia IT.

7.4.2. PROTECCIÓN DE DATOS DE ACTIVACIÓN

Únicamente el personal autorizado posee las claves de acceso a los dispositivos criptográficos. Para lo cual se debe tener la presencia de 2 personas los cuales custodian una parte de la llave y con esto poder acceder al dispositivo.

La clave de acceso es confidencial, personal e intransferible y es el parámetro que protege las claves privadas permitiendo la utilización de los certificados de CA RAÍZ y CA Subordinada; por lo tanto, deben tenerse en cuenta unas normas de seguridad para su custodia definidas por Olimpia IT.

7.5. CONTROLES DE SEGURIDAD INFORMÁTICA

7.5.1. REQUISITOS DE LA SEGURIDAD INFORMÁTICA

Olimpia IT, ha definido como requisitos técnicos aplicables a su infraestructura lo siguiente:

- Control de acceso físico y lógico
- Monitoreo de acciones
- Eliminación de cuentas de usuario por defecto
- Criptografía segura
- Auditorías periódicas a los sistemas
- Análisis de riesgos sobre la operación

7.5.2. NIVELES DE SEGURIDAD INFORMÁTICA OLIMPIA IT

Olimpia IT cuenta con un nivel de seguridad basado ITSEC, NIST, CIS entre otros.

7.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

7.6.1. CONTROLES EN EL DESARROLLO DE SISTEMA

Olimpia IT establece un sistema de seguridad para los sistemas de CA RAÍZ, CA subordinada y portal de la RA en físico y lógico acorde a lo establecido por las mejores prácticas de la industria y mejorando continuamente según las necesidades de negocio. A su vez el sistema de seguridad está basado en el estándar NTC-ISO/IEC 27001 en su versión vigente, dando cumplimiento a los requerimientos establecidos.

7.6.2. CONTROLES DE GESTIÓN DE LA SEGURIDAD

Olimpia IT mantiene un sistema de seguridad de la información en el cual se incluyen controles como capacitación a todo el personal en seguridad, mantenimiento de la información actualizada, sistema monitoreo activo para el servicio, se realiza un análisis de riesgos de acuerdo con el

procedimiento de gestión de riesgos de la organización y se llevan a cabo los planes de acción correspondientes.

7.6.3. EVALUACIÓN DE SEGURIDAD DURANTE EL CICLO DE VIDA

Olimpia IT implementa y mantiene los controles de seguridad establecidos en la presente declaración de prácticas de certificación, en las políticas y procedimientos establecidos en su Sistema Integrado de Gestión.

7.7. CONTROLES DE SEGURIDAD EN LA RED

La seguridad en la red de Olimpia IT está determinada por la implementación de trasmisión de datos de forma segura, infraestructura en alta disponibilidad, análisis de ethical hacking y auditorías periódicas internas y externas, actualizaciones de seguridad en la infraestructura (firewall, switch, bases de datos) entre otros controles dando una alta confiabilidad sobre el servicio prestado.

8. ESTÁNDARES TÉCNICOS DE LOS CERTIFICADOS

8.1. PERFIL DEL CERTIFICADO

8.1.1. NÚMERO DE VERSIÓN

Los certificados digitales de Olimpia IT, soportan y emiten certificados bajo el estándar RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile, para perfiles de certificado y CRL.

8.1.2. EXTENSIONES DEL CERTIFICADO

Olimpia IT establece en la presente Declaración de Prácticas de Certificación, la utilización de por lo menos las siguientes extensiones de los certificados:

- Identificador de clave de entidad emisora
- Identificador de clave del titular
- Restricciones básicas
- Directivas del certificado
- Puntos de distribución CRL
- Acceso a la información de la entidad emisora
- Uso de la clave
- Uso mejorado de claves

8.1.3. ALGORITMO CRIPTOGRÁFICO UTILIZADO EN LOS CERTIFICADOS

El algoritmo criptográfico utilizado por Olimpia IT en la generación del par de llaves es:

- SHA256 con encriptación de RSA.

8.1.4. FORMATOS DE NOMBRES

Olimpia IT está alineado a lo establecido por el estándar X.500 para la generación de los distinguished names (DN) identificando al titular del certificado digital

8.1.5. RESTRICCIONES DE NOMBRE

Los nombres contenidos en los certificados están restringidos a distinguished names X.500, únicos y no ambiguos.

8.1.6. OBJETO IDENTIFICADOR DE LA POLÍTICA DE CERTIFICACIÓN

La CA raíz tiene definida una política de asignación de OIDs dentro de su árbol privado de numeración.

Los OID, se encuentran señalados en el numeral 22 de esta DPC.

8.2. PERFIL DE LA CRL

8.2.1. NÚMERO DE VERSIÓN

La ECD realiza la emisión de los certificados revocados (CRL) en referencia al formato con formato X. 509 v.3.

8.2.2. CRL Y SUS EXTENSIONES

Se establece que la lista de certificados revocados (CRL) está basada en el estándar RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

Olimpia mantiene actualizada la CRL de forma automática.

8.3. VALIDEZ DE LOS CERTIFICADOS POR OCSP

Este protocolo permite validar en línea el estado de los certificados digitales.

Olimpia IT entrega respuesta general del estado del certificado a petición de un tercero, parte confinante o titular de la información mediante una respuesta general y de consulta pública expuesta y sin firmar en el portal de servicios de la ECD.

8.3.1. ESTÁNDAR DE REFERENCIA PARA EL OCSP

Olimpia IT implementa como referencia de versión estándar para el OCSP RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

8.3.2. EXTENSIONES DEL CERTIFICADO UTILIZADO EN LA FIRMA DEL PROTOCOLO OCSP

- Identificador de clave de entidad emisora
- Identificador de clave del titular

- Restricciones básicas
- Directivas del certificado
- Puntos de distribución CRL
- Acceso a la información de la entidad emisora
- Uso de la clave
- Uso mejorado de claves

8.4. ESTÁNDARES TÉCNICOS VIGENTES

Olimpia IT establece en el documento POL-030 POLÍTICA DE CERTIFICADOS los estándares técnicos vigentes aplicables definidos en los Criterios Específicos de Acreditación de acuerdo con las actividades del artículo 161 que hacen referencia al Decreto Ley 019 del 2012 para los servicios de certificación de digital.

9. AUDITORÍA DE CUMPLIMIENTO

9.1. PERIODICIDAD DE LA AUDITORÍA

El sistema de acreditación de la Entidad de Certificación Digital se someterá a una auditoría de tercera parte de acuerdo con la normatividad legal y técnica vigente. De esta manera se asegura su adecuado funcionamiento y operatividad con las estipulaciones incluidas en esta DPC y en concordancia con la acreditación otorgada por ONAC.

9.2. EQUIPO AUDITOR

Olimpia IT seleccionará el equipo de auditores a ejecutar las actividades, los cuales deberán cumplir con los siguientes requisitos:

- Experiencia comprobada en auditorías de Seguridad de la Información, Seguridad en PKI, con conocimientos en Sistemas de Gestión de Riesgos.

9.3. RELACIÓN ENTRE LA ENTIDAD AUDITADA Y EL AUDITOR

La relación entre el auditor y la entidad auditada se limitará estrictamente a los procesos e información requerida para la auditoría, con lo cual se garantiza la inexistencia de conflictos de intereses y se deja evidencia de la relación en la cual se especifica en el acuerdo contractual entre Olimpia IT y la empresa auditora.

9.4. CONTROL DE CONFORMIDAD

Se establece el alcance de la auditoría a la operación y mantenimiento de los servicios mencionados en la presente declaración de prácticas de certificación en los cuales se verifican los siguientes aspectos:

- Documentación del sistema integrado de gestión
- Controles de seguridad física y lógica
- Temas técnicos
- Cumplimiento del ciclo de vida de los certificados digitales
- Plan de Continuidad del negocio
- Roles y funciones del personal

9.5. ACCIONES PREVENTIVAS O DE MEJORA COMO RESULTADO DE NO CONFORMIDADES

Olimpia IT ante la identificación de cualquier incumplimiento en la auditoría implementará acciones correctivas llevadas a cabo en el menor tiempo posible junto con un plan de acción continuo el cual servirá como control para evitar que se presente el incumplimiento nuevamente.

9.6. INFORME DE RESULTADOS

El Auditor comunicará los resultados de la auditoría a la Gerencia General de Olimpia IT y a los dueños de procesos en los cuales se detecten no conformidades.

9.7. REGISTRO DE AUDITORÍA

En cumplimiento con lo señalado en el artículo del el Decreto 333 de 2014, Olimpia IT como Entidad de Certificación Digital abierta, deberá cumplir con la auditoría de tercera parte en los términos previstos en los criterios específicos de acreditación que establezca ONAC.

10. ESTAMPADO CRONOLÓGICO

El servicio de estampado cronológico da certeza de la integridad de la fecha y hora de un documento tomando la hora legal colombiana del Instituto Nacional de Metrología, o quien haga sus veces, adhiriendo una firma digital de la TSA.

Este servicio se prestará para los siguientes tipos de certificado:

- Certificado Digital - Persona Natural
- Certificado Digital - Persona Jurídica
- Certificado Digital - Profesional Titulado
- Certificado Digital - Pertenencia a Empresa
- Certificado Digital - Función Pública
- Certificado Digital - Representante Legal

El servicio podrá ser usado en otros certificados, sin embargo, ello no implica reciprocidad de certificados, ni se garantiza que su visualización pueda ejecutarse de la misma forma en que se ejecuta con los certificados emitidos por Olimpia IT.

Las estampas cronológicas podrán usarse en documentos sin firma, pero su visualización no podrá detectarse a simple vista por lo que el suscriptor deberá contar con las herramientas adecuadas para ello.

10.1. TIME STAMP AUTHORITY (TSA)

El servicio de estampado cronológico es generado por la TSA, y su administración está en cabeza de Olimpia IT.

La información que se obtiene del Instituto Nacional de Metrología es firmada digitalmente por Olimpia IT en su calidad de TSA, basada en el certificado expedido por la sub-CA que se le ha emitido a Olimpia IT, para este propósito. Este servicio permite imponer una estampa de tiempo de un documento firmado digitalmente por medio de uno de los certificados que emite Olimpia IT como ECD, con la certeza de su integridad y autenticidad.

La información contenida en una estampa de tiempo permite establecer dos características esenciales:

i. El tiempo expresado en horas, minutos y segundos, acorde con la hora emitida por el Instituto Nacional de Metrología, según Decreto 4175 de 2011.

ii. Fecha expresada en día, mes y año, de acuerdo con el calendario Gregoriano, que es el oficialmente aceptado por la República de Colombia.

10.2. OPERACIÓN DEL ESTAMPADO CRONOLÓGICO

Una Autoridad de Registro (RA) es la responsable de la gestión de las solicitudes, identificación y registro de los solicitantes del servicio de estampado cronológico y cualquier responsabilidad específica establecida en esta DPC y las Políticas de Certificación. Las RA son autoridades delegadas por la ECD para el servicio de estampado cronológico, aunque la ECD es en última instancia la responsable del servicio. La ECD puede ejercer en cualquier momento las labores de RA.

La CA es la responsable de la toma de la decisión de emitir, revocar o cancelar un servicio de estampado cronológico.
Los requisitos para el servicio son:

- Documento de identificación: Cédula de ciudadanía, Cédula de extranjería, o Pasaporte vigente
- Certificado de Cámara de comercio no mayor a 30 días
- Registro único tributario – RUT del año vigente

10.3. MEDIOS PARA LA SOLICITUD DEL SERVICIO

Olimpia IT establece en el presente documento la forma de acceder al servicio de estampado cronológico el cual puede ser solicitado a través del siguiente medio:

- Página web de Olimpia IT https://micertificado.olimpiait.com en la cual se debe seleccionar el servicio de estampa de tiempo.

Olimpia IT, se compromete con los suscriptores a habilitar en un plazo no superior a dos (2) días hábiles el servicio de estampado cronológico, a menos que exista un acuerdo legal distinto con el solicitante, y sin contabilizar el tiempo que el solicitante se tarde en responder las solicitudes de subsanación de información, en caso de que apliquen.

El certificado con el cual se firma digitalmente una estampa de tiempo corresponde a uno de los certificados emitidos por Olimpia IT como ECD.

10.4. ESTAMPADO CRONOLÓGICO PARA UN MENSAJE DE DATOS

El servicio de estampado cronológico establece la custodia de la llave privada del suscriptor en los servidores de Olimpia IT de forma segura, y una vez el suscriptor tiene el servicio de estampado cronológico, se le asignará un usuario, que estará vinculado a una clave de 4 dígitos que será creada por el suscriptor y con la cual podrá acceder al portal de Olimpia IT, y usar el servicio de estampado cronológico.

10.5. POLÍTICAS PARA LA PRESTACIÓN DEL SERVICIO DE ESTAMPADO CRONOLÓGICO

Olimpia IT establece, las siguientes políticas necesarias para el servicio:

a) Toda solicitud gestionada debe ser documentada y almacenada en los logs del sistema.
b) Se deberá mantener informado al solicitante el estado de su solicitud
c) Se debe dar cumplimiento a los establecido en la DPC "Declaración de Prácticas de Certificación.
d) El equipo de soporte corporativo realiza validaciones de estado del servicio y de la documentación de los solicitantes cuando se realiza la revisión de forma automática
e) Todas las actividades realizadas por el rol de "portal de servicios", corresponden a actividades ejecutadas automáticamente por la aplicación.
f) La validación de la identidad del solicitante se realiza en el proceso de emisión de certificado digital.
g) Para realizar la solicitud del servicio el usuario debe estar autenticado en el portal de servicios.
h) El sello de tiempo (o marca de tiempo) se aplica antes del final del periodo de validez del certificado del firmante.
i) Toda estampa de tiempo se emite con una precisión de tiempos inferiores a un segundo.
j) El tiempo de vida esperado de la firma utilizada para firmar el tiempo token de sello (depende del algoritmo de hash que se esté utilizando, el algoritmo de firma utilizado y la longitud de la clave privada).
k) Si no se encuentra un servidor NTP con el cual generar la estampa cronológica el sistema no generará ninguna estampa cronológica.

10.6. NÚMERO DE ESTAMPAS DE TIEMPO

Para el servicio de estampado cronológico Olimpia IT tiene a disposición un número de estampas limitado o ilimitado según el paquete del servicio adquirido.

10.7. PROCEDIMIENTO PARA LA HABILITACIÓN DEL SERVICIO PARA EL SUSCRIPTOR

El procedimiento para la habilitación del servicio para el solicitante, en el servicio de estampado cronológico, será el establecido en el procedimiento interno que Olimpia IT ha establecido para ello, y que lista las siguientes actividades:

a) Tramitar solicitud
b) Validar consignación
c) Validar recaudo
d) Evidencia de pago
e) Envío de correo electrónico al solicitante
f) Validar solicitud
g) Emitir decisión
h) Registros

10.8. REQUISITOS DEL SERVICIO DE ESTAMPADO CRONOLÓGICO (DOCUMENTO E INFORMACIÓN SOLICITADA)

- El solicitante deberá aceptar los términos y condiciones.
- El solicitante deberá contestar las preguntas de validación.

Para la prestación del servicio de estampado cronológico se establece la siguiente documentación:

10.8.1. DOCUMENTACIÓN A SOLICITAR

- Certificado de estado de cédula de ciudadanía/extranjería/Certificado de existencia y representación expedido por la cámara de comercio (Expedido por la Registraduría Nacional del Estado Civil/Departamento Administrativo Migración Colombia)
- Imagen **legible** del documento de identidad

10.8.2. INFORMACIÓN A DILIGENCIAR EN LA APLICACIÓN

- Nombres y apellidos
- Tipo de documento de identidad
- Número documento identidad
- Departamento de residencia
- Ciudad de residencia
- Dirección de residencia
- Teléfono celular
- Correo electrónico
- Otro teléfono (campo no obligatorio)

El solicitante deberá seleccionar uno de los paquetes ofertados para este servicio y pagar por los medios establecidos en esta DPC, el valor del paquete seleccionado.

Si se realizó un pago en línea, la aplicación tomará el pago y permitirá al solicitante continuar con el proceso de activación.
Si el pago se hizo por consignación, el solicitante deberá adjuntar el comprobante de la consignación y podrá validar el estado de la solicitud en la página web https://micertificado.olimpiait.com

Para que el solicitante asocie un certificado digital con este servicio, podrá adquirirlo por el servicio de firma centralizada y pagar el costo del paquete acorde con las formas establecidas para ello en esta DPC.

Si la generación del certificado es exitosa, el solicitante deberá activar el mismo acorde con lo especificado en la aplicación, para el servicio de firma centralizada.

10.8.3. REQUISITOS DEL SERVICIO DE ESTAMPADO CRONOLÓGICO

El solicitante deberá haber adjuntado la información requerida por la aplicación y diligenciado la información solicitada, así mismo deberá haber seleccionado uno de los paquetes ofertados para este servicio y si el mismo tiene costo haber pagado el valor del paquete seleccionado.

Si el solicitante, requiere que el servicio de estampado cronológico sea usado con un certificado digital de otra entidad de certificación, Olimpia IT no suministra los componentes tecnológicos para este tipo de integración.

Si el solicitante requiere el estampado cronológico para un documento sin firmar, deberá disponer de la tecnología adecuada para su visualización, pues, aunque la estampa de tiempo quede incrustada en el documento, no se garantiza su visualización sin una firma digital que acompañe el sello de tiempo.

10.9. PROCEDIMIENTO PARA LA HABILITACIÓN DEL SERVICIO DE ESTAMPADO CRONOLÓGICO PARA EL SOLICITANTE/SUSCRIPTOR

Olimpia IT establece a continuación, la forma de solicitar el servicio de estampado cronológico, a través de los siguientes medios:

- **Internet:** A través de la página web de la Entidad de Certificación Digital https://micertificado.olimpiait.com, o través de cualquier otro portal web que Olimpia IT defina como canal de venta de sus

servicios de certificación digital, siempre que dichos portales estén debidamente integrados al portal de la Entidad de Certificación Digital.

- El solicitante deberá registrarse en el portal web en el botón "registro" e ingresar la información allí requerida:

    - Tipo de identificación
    - Número del documento
    - Fecha de expedición del documento

- Se realizará una validación de la información ingresada contra la Base de datos biográfica de la Registraduría Nacional del Estado Civil.

    - Si la información no es válida, la aplicación informará que la información no es válida.
    - Si la información es válida, el solicitante deberá ingresar la siguiente información:

        - Dirección de correo electrónico
        - Número de teléfono celular
        - Leer y aceptar los términos y condiciones de uso

    - Al suscriptor le llegará un mensaje a su correo electrónico, en el que se solicitará la activación de su cuenta por un enlace contenido en el mismo correo electrónico.
    - El suscriptor deberá iniciar sesión en el portal web https://micertificado.olimpiait.com, en el botón "Registrarse/iniciar sesión" en el enlace "Iniciar sesión" e ingresar la siguiente información:

        - Tipo de documento de identidad

- Número de documento de identidad

- Se enviará al número de teléfono celular registrado por el solicitante un OTP (One Time Password) compuesto por un código de 4 dígitos de un solo uso, para que el solicitante lo ingrese en el espacio dispuesto para ello, en la parte inferior de la ventana de inicio de sesión con el fin de generar una autenticación ante el portal.
- Una vez la autenticación sea efectiva, el portal web, informará al solicitante que ya se encuentra en su cuenta privada, el solicitante podrá solicitar certificados digitales desde el enlace "Certificados" o "Servicios" desde el enlace "Servicios".

Nota: La página Web de la Entidad de Certificación Digital podrá ser desplegada en los navegadores Chrome en su versión 71.0.3578.98 y Microsoft EDGE versión 38.14393.2068.0. El uso de cualquier otro navegador puede ocasionar inconvenientes con el uso del portal, la solicitud de certificados o servicios.

- **Telefónicamente:** Comunicándose con la línea de atención al cliente (+57 601) 742 7878, en donde el operador remitirá al solicitante al registro de la página web https://micertificado.olimpiait.com, descrita en el ítem anterior.

El suscriptor acepta la conformidad con las siguientes políticas y procedimientos establecidos por Olimpia IT:

a) El solicitante podrá consultar el estado de su solicitud en la página web https://micertificado.olimpiait.com. Si el usuario cumple con la documentación solicitada y con los requerimientos establecidos, Olimpia IT procederá a realizar la habilitación del servicio en un lapso máximo de 2 días hábiles, contados desde la decisión de aceptar la solicitud, y sin contabilizar el tiempo que el solicitante se tarde en

responder las solicitudes de subsanación de información, en caso de que apliquen.

b) Las solicitudes son registradas desde la página Web https://micertificado.olimpiait.com.
c) Olimpia IT tiene la potestad de solicitar aclaración de la información suministrada o de la documentación; en caso de que no se logre aclarar la información o documentación, la decisión de certificación por parte de la RA será de rechazar la solicitud.
d) Toda documentación entregada por el solicitante debe ser almacenada de forma segura siguiendo los estándares establecidos por Olimpia IT de NTC-ISO/IEC ISO 9001 y NTC-ISO/IEC 27001 en su versión vigente, la cual debe tener una disponibilidad de al menos 2 años.

10.10. LAPSO DE ACTIVACIÓN DEL SERVICIO

Olimpia IT a continuación establece los tiempos de prestación del servicio y el lapso de vigencia cuando el servicio se encuentra asociado a firmas digitales:

- Si se realiza la revocación del certificado digital del suscriptor por motivos de uso indebido del certificado inmediatamente se cancela el servicio de estampado cronológico.

- Por vencimiento del servicio de estampado cronológico

- Por incumplimiento en las políticas de seguridad de Olimpia IT puede llegar cancelar el servicio de estampado cronológico

- Por motivos legales relacionados con las normas y leyes colombianas

- Cuando se genere la cancelación del certificado digital asociado a este servicio, por vencimiento del término, el servicio de estampado

cronológico seguirá activo, pero para acceder a este el suscriptor deberá asociar un nuevo certificado digital al servicio de estampado cronológico.

En caso de la generación de un nuevo certificado para reemplazar uno que fue revocado, se podrá seguir usando el servicio de estampado cronológico contratado.

10.11. FUNCIONAMIENTO DEL SERVICIO DE ESTAMPADO CRONOLÓGICO

El mensaje de datos que se compone de la información horaria, expresada en el calendario Juliano y en horas, minutos y segundos, es firmado digitalmente por el certificado digital de la TSA.

Este mensaje de datos, que contiene una estampa de tiempo firmada digitalmente, podrá ser usado por el suscriptor en un documento electrónico a fin de que se tenga la certeza de cuando fue firmado dicho documento.

10.12. RESPONSABILIDADES POR CADA DOCUMENTO QUE OLIMPIA IT ESTAMPA

Cada documento que sea estampado por Olimpia IT, se limita a testificar por medios técnicos, idóneos y seguros que la fecha y hora en que se ha estampado un documento corresponde a la fecha y hora legal para la República de Colombia, y que dicha estampa de tiempo corresponde al momento en que se ha firmado digitalmente un documento, cuando la estampa de tiempo sea utilizada con un certificado digital emitido por Olimpia IT.

Olimpia IT se hace responsable por la veracidad, integridad, autenticidad y no repudio de la estampa que es suministrada y que es certificada por la TSA de Olimpia IT, tal como se acredita en la información del certificado

digital que se suministra de la estampa de tiempo que se ha impuesto en el documento firmado digitalmente.

Los riesgos derivados del servicio serán de responsabilidad de Olimpia IT, siempre que los sellos de tiempo se encuentren en poder de Olimpia IT y no hayan sido entregados al suscriptor, una vez los sellos de tiempo son puestos a disposición del suscriptor para su consumo, el suscriptor será el responsable de su uso y buen manejo acorde con esta DPC.

Los suscriptores y partes confiantes de este servicio, se acogen al régimen de responsabilidades que les correspondan respecto de este servicio y que se encuentran contenidas en esta DPC.

10.13. FUENTE DE TIEMPO

Olimpia IT realiza un proceso de Identificación para la infraestructura requerida para lo cual se debe realizar la debida sincronización de tiempos (Servidor de Horario Central), dicha conexión se realiza por medio de un Servidor Controlador de Dominio Maestro que sincroniza su hora con la hora legal colombiana: horalegal.inm.gov.co por ultimo las máquinas del cliente y los servidores sincronizan su hora contra el servidor Controlador de Dominio Maestro por medio de GPO.

La TSA no generará sincronización de la hora sus relojes con la hora legal colombiana, ya que la hora legal colombiana se tomará de la página web oficial del Instituto Nacional de Metrología.

11. CONDICIONES COMERCIALES

11.1. POLÍTICA TARIFARIA DE EXPEDICIÓN Y REVOCACIÓN DE CERTIFICADOS

Las tarifas definidas por la entidad de certificación digital, para cada uno de los servicios dentro del marco acreditado pueden ser consultadas en el sitio web de la entidad de certificación, en la subpágina de "Productos" dentro de la opción "ver planes y precios" de cada tipo de certificado.

Olimpia IT, establece que no cuenta con una tarifa para la revocación de certificados.

11.2. TARIFAS PARA SERVICIOS DIGITALES EN PROYECTOS

Olimpia IT podrá establecer condiciones especiales de emisión de certificados digitales o servicios acreditados por ONAC, los cuales previamente deberán estar pactadas con el suscriptor y en las que se podrán establecer condiciones específicas que requiera el suscriptor, siempre que este ceñido a esta Declaración de Prácticas de Certificación y la normatividad vigente colombiana.

11.3. FORMA DE PAGO

Pago en efectivo: Se realiza mediante Recaudo Bancolombia al Convenio 76321 a nombre de OLIMPIA IT S.A.S., indicando como número de referencia el número de documento de identificación del solicitante y, en caso de que aplique, el número único de referencia de la solicitud.

Pago en Línea: Pago Online, el proceso de pago se realizará mediante la entidad bancaria del solicitante, por medio de la pasarela de pago dispuesta por Olimpia IT, dentro de la página web https://micertificado.olimpiait.com

11.4. POLÍTICAS PARA EL REEMBOLSO DE DINERO

Los suscriptores y/o solicitantes de certificados digitales podrán solicitar reembolso de dinero en los siguientes casos:

11.4.1. EVENTOS PARA EL REEMBOLSO DEL DINERO

- **Cuando un suscriptor solicite un servicio y su solicitud sea rechazada:** El operador de la RA informará a Servicio al Cliente, para que este ejecute el reembolso al usuario o solicitante.
- **Cuando Olimpia IT lo considere necesario debido a una afectación del solicitante durante el proceso de solicitud, o del suscritor en el uso de los servicios:** El operador de la RA podrá determinar un reembolso, informando a Servicio al Cliente los causales del mismo, para que este ejecute el reembolso al usuario o solicitante.
- **Cuando Olimpia IT realice la cesación de actividades como Entidad de Certificación Digital:** en este caso el suscriptor puede solicitar el reembolso del dinero el cual será proporcional al tiempo de vigencia usufructuado del certificado digital hasta el momento de la cesación de actividades.

11.4.2. VALOR A REEMBOLSAR

Los suscriptores y/o solicitantes tendrán derecho al reembolso del cincuenta por ciento (50%) del valor pagado por la solicitud del certificado o servicio que hayan realizado. Cuando la emisión de un certificado digital o la prestación de un servicio no se pueda efectuar por causas imputables a Olimpia IT, el área de Servicio al Cliente evaluará acorde con el procedimiento interno, el reembolso de un valor mayor al 50%.

11.5. RESPONSABILIDAD FINANCIERA

Olimpia IT cuenta con la estabilidad financiera y de los recursos necesarios para su operación según lo establecido en el Decreto 333 de 2014, lo cual se evidencia mediante el cumplimiento de los estados

financieros validados por el revisor fiscal y el seguro de responsabilidad civil adquirido desde julio del 2018 esto con el fin de poder indemnizar los daños o perjuicios que se puedan causar en la operación de Olimpia IT como Entidad de Certificación Digital.

12. CONFIDENCIALIDAD DE LA INFORMACIÓN

Olimpia IT cataloga dentro de su sistema integrado de gestión toda aquella información no pública como información confidencial (etiquetamiento según su nivel de publicidad en público, interno, restringido o reservado) según las políticas de seguridad de la información dispuestas por la compañía.

El tratamiento que se le da a la información confidencial, así como los usos autorizados de la misma están determinados por el etiquetado que se le otorga.

NIVEL DE CONFIDENCIALIDAD USO AUTORIZADO

Transporte: Mediante cualquier medio utilizado por Olimpia.

Almacenamiento: Usualmente esta información es transitoria, y cuando corresponda a información del Sistema Integrado de Gestión se realiza de acuerdo con los procedimientos internos

Transporte: Se puede transportar por cualquier medio que forme parte de la infraestructura tecnológica interna de Olimpia.

Almacenamiento: Se mantendrá dentro de los límites de Olimpia, física o lógicamente.

Transporte: Se debe llevar esta información dentro de los medios designados por el dueño del proceso.

Almacenamiento: Se mantendrá almacenada en los medios o lugares designados por el dueño del proceso.

Transporte: Es obligatorio transportar esta información usando medios seguros, encriptados y siempre se ha de considerar una confirmación de acuse de recibo.

Almacenamiento: Se mantendrá cifrada en un medio protegido con controles de acceso o bajo llave (acceso sólo al Propietario).

El acceso a la información confidencial (uso interno, restringido o reservado) solo será permitido a las personas autorizadas por el propietario del activo de información correspondiente, esta información se encuentra relacionada en el inventario de activos de Olimpia IT.

La información que sea de carácter confidencial e inherente a las actividades de la Entidad de Certificación Digital, se revelarán acorde con el párrafo anterior y cuando medie una orden judicial o administrativa emitida por funcionario público competente que requiera la revelación de dicha información. Cuando se presente petición de autoridad judicial o administrativa, dicha solicitud deberá ser elevada al área legal, la cual dará respuesta al requerimiento de revelación de la información confidencial.

Cuando se exija a Olimpia IT, por ley o autorización en las disposiciones contractuales, la divulgación de información confidencial, el suscriptor o la persona implicada debe, a menos que lo prohíba la ley, ser notificada de la información suministrada.

Olimpia IT garantiza a los suscriptores que acorde con esta DPC y su política de protección de datos personales, los datos personales de los solicitantes y suscriptores son tratados adecuadamente y bajo los límites de la autorización que los solicitantes y suscriptores han dado para ello.

La información suministrada por los solicitantes y suscriptores se clasifica como restringida y acorde con ello se dará su tratamiento al interior de Olimpia IT.

La información recopilada con el fin de prestar los servicios de adquisición de cualquiera de los tipos de certificados, los servicios de correo electrónico certificado, firma centralizada, al certificado y estampado cronológico se someten a la protección de información que se declara en esta DPC.

12.1. ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

Se considera información confidencial:

- Información de registro, todos los datos relativos al registro de certificados.
- La información de negocio suministrada por sus proveedores y otras personas con las que Olimpia IT tiene el deber de guardar secreto establecida legal o convencionalmente.
- Información sobre la vida de los certificados, todos los datos relativos a la emisión y revocación (salvo su publicación en la CRL) de certificados de la ECD.
- Toda la información clasificada como “Confidencial”

12.2. INFORMACIÓN QUE NO ESTÁ DENTRO DEL ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

Olimpia define como información no confidencial la siguiente:

- Lista de Certificados Revocados (CRL)
- La clave pública de los certificados digitales emitidos por Olimpia IT
- Las versiones de la DPC
- El procedimiento de PQRS para el suscriptor
- Información de la empresa que reposa en el certificado de existencia y representación expedido por la correspondiente Cámara de Comercio del domicilio de la empresa.
- Los datos personales, excepto aquellos de naturaleza pública

12.3. RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Los trabajadores y aliados de Olimpia IT son los responsables de proteger la información confidencial quienes se acogen a la normativa contractual adquirida y a la normatividad vigente colombiana.

12.4. MANEJO DE LA INFORMACIÓN SUMINISTRADA POR LOS SUSCRIPTORES

Olimpia IT, en su calidad de Entidad de Certificación Digital cumple con lo establecido en la normatividad colombiana para la protección de la información de los solicitantes o suscriptores mediante la implementación y cumplimento de la Política de Protección de Datos Personales, en la cual se especifican los lineamientos a los cuales se acoge Olimpia IT, la cual está disponible al público en el portal de la Entidad de Certificación Digital.

La información acerca del suscriptor obtenida en fuentes diferentes del suscriptor (por ejemplo, de un reclamante o de los reguladores) debe ser tratada como confidencial.

13. DERECHOS DE PROPIEDAD INTELECTUAL

El presente documento está protegido por las normas de derechos de autor, cualquier reproducción, distribución o modificación total o parcial a usuarios no autorizados o cualquier uso indebido de la información confidencial será considerado un delito conforme a lo establecido por el Código Penal y Leyes vigentes del estado colombiano.

14. OBLIGACIONES Y GARANTÍAS

Olimpia IT establece a continuación las obligaciones y deberes de cada una de las partes involucradas, enmarcado dentro de las exigencias hechas por el Decreto 333 de 2014, las normas que lo modifiquen aclaren o sustituyan, así como el CEA 3.0-07.

14.1. OBLIGACIONES Y DEBERES DE LA ENTIDAD DE CERTIFICACIÓN DIGITAL

Olimpia IT asegura que todos los suscriptores y clientes han cumplido los requisitos definidos en las leyes colombianas y las disposiciones emitidas por los entes reguladores para obtener el servicio de certificación digital solicitado.

Olimpia IT declara que se sujeta al cumplimiento de las siguientes obligaciones y deberes para la prestación de los servicios que como ECD, se estipulan las siguientes obligaciones:

a) En cuanto a los sistemas de seguridad necesarios para el correcto funcionamiento del servicio, será obligación de Olimpia IT, procurar su óptima funcionalidad en todo momento y tomar las medidas contingentes y técnicas para lograr dicho funcionamiento.

b) En cuanto a la infraestructura necesaria para el correcto funcionamiento como ECD, los mismos deberán estar implementados y en funcionamiento, y será necesario realizar los mantenimientos requeridos para su adecuado rendimiento.

c) Acoger, respetar y aplicar en su integridad **la Declaración de Prácticas de Certificación** (DPC) y honrar los acuerdos con los usuarios de los servicios de ECD.

d) Dar a conocer y/o poner a disposición de los usuarios el contenido de los términos y condiciones, así como de las políticas de manera adecuada y suficiente, sobre el servicio a prestar, así como sus características generales y particulares, el contrato a suscribir y/o la aceptación que dé el usuario de los servicios a prestar, informando de forma clara y veraz la condición de ECD de que goza Olimpia IT y los servicios para los cuales se encuentra autorizado a prestar.

e) Dar a conocer y/o poner a disposición de los usuarios las responsabilidades u obligaciones que le competen como adquiriente de los servicios puestos a disposición o contratados para ejecución de Olimpia IT en su calidad de ECD.

f) A través del Comité de Políticas, aprobar el contenido de esta Declaración de Prácticas de Certificación (DPC), que contiene las reglas para la TSA y las Políticas de Certificados.

g) Inhibirse de almacenar y/o acceder a la clave privada del suscriptor.

h) Mantener la guarda y protección del soporte físico del certificado digital hasta que se verifique por cualquier medio la entrega de este al suscriptor (si aplica).

i) Ayudar, colaborar y facilitar el acceso tanto a las instalaciones como a los demás espacios en los que Olimpia IT tenga control, al Organismo Nacional de Acreditación de Colombia para el desarrollo de auditorías ya sean presenciales o remotas.

j) Emitir certificados digitales acorde con lo estipulado en esta declaración de Prácticas de Certificación y lo acordado con el suscriptor, fijando como límite la legalidad y autorización que para el evento se requiera.

k) Llevar el registro de los certificados expedidos y publicarlos acorde con lo definido en esta Declaración de Prácticas de Certificación.

l) Cuando se tenga conocimiento de un evento que pueda comprometer la prestación del servicio informar por los medios más eficaces e idóneos de dicha eventualidad el Organismo Nacional de Acreditación de Colombia.

m) Cuando se generen cambios modificatorios, supletorios, introductorios o de supresión en la PKI, que puedan afectar la prestación del servicio, informar por los medios más eficaces e idóneos de dicho cambio el Organismo Nacional de Acreditación de Colombia.

n) Cuando ocurran por cualquier motivo cambios de estado del certificado del suscriptor informar de dicho cambio de forma eficaz al suscriptor, informando de forma suficiente y de fondo los motivos del cambio y el sustento legal del mismo.

o) Tomar todas las medidas de seguridad y control suficientes y razonables que no comprometan la divulgación de su clave privada.

p) Realizar todos los esfuerzos necesarios para la prestación permanente e ininterrumpida de los servicios de certificación digital.

q) Mantener actualizada la base de datos de certificados digitales revocados acorde con lo instruido en esta Declaración de Prácticas de Certificación y efectuar los avisos y publicaciones requeridos por ley para satisfacer la notificación de las actualizaciones dadas.

r) Efectuar la revocación de los certificados digitales acorde con lo establecido en la sección 5.8 de esta Declaración de Prácticas de Certificación.

s) Una vez se efectúe la revocación de un certificado digital por parte de Olimpia IT, se deberá informar al suscriptor al día hábil siguiente de dicha eventualidad.

t) Procurar que los administradores no se encuentren incursos en las causales establecidas en el literal c del artículo 29 de la Ley 527 de 1999, y una vez algún administrador se encuentre incurso, realizar su remoción inmediata.

u) Poner a disposición de los suscriptores un mecanismo de comunicación permanente que les permita resolver de forma oportuna las consultas e inquietudes que se generen en cuanto a los certificados digitales y su revocación.

v) Colaborar oportuna y eficazmente con las autoridades judiciales o administrativas cuando así lo requieran en todos los aspectos relativos a las firmas y certificados digitales expedidos y en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración.

w) Conservar en cualquier medio idóneo y legalmente permitido la documentación soporte de los certificados digitales expedidos, por el término previsto en la ley para los papeles de los comerciantes y tomar las medidas necesarias para garantizar la integridad y la confidencialidad que le sean propias.

x) A petición del suscriptor, de una persona autorizada por este o de cualquier autoridad judicial o administrativa que tenga competencia para ello, suministrar, transferir o transmitir la información entregada por el suscriptor e informar de dicha operación a más tardar al día hábil siguiente en que la operación de la información requerida se ejecute o inicie su ejecución en caso de ser una operación de tracto sucesivo.

y) Cumplir con los Criterios de Acreditación CEA-3.0-07 emitidos por el Organismo Nacional de Acreditación de Colombia.

z) Informar al suscriptor de las obligaciones en el cuidado, custodia y responsabilidad que le compete, en cuanto al uso adecuado, legal y acorde con las buenas costumbres mercantiles de los servicios de certificación digital.

aa) Siempre que un solicitante de los servicios ofertados por Olimpia IT como Entidad de Certificación Digital, cumpla con los requisitos legales y los establecidos tanto en esta Declaración de Prácticas de Certificación como en las políticas generales de Olimpia IT, esta última no podrá negarse a prestar el servicio de forma injustificada. El ejercicio del suscriptor de actividades ilícitas o la vinculación pública o judicial del suscriptor en calidad de sujeto activo a actividades ilícitas podrá ser causal de rechazo de la solicitud del solicitante de los servicios ofrecidos por Olimpia IT.

bb) Cumplir con lo dispuesto en la Ley Estatutaria 1581 de 2012, sus decretos reglamentarios, demás normas que la modifiquen, adicionen, sustituyan o complementen, respecto de todos los datos de los intervinientes en los servicios de certificación digital o conexos, en especial los datos personales de los suscriptores.

cc) Los proveedores del servicio de Datacenter, que son considerados como críticos para la operación de Entidad de Certificación Digital, se someten al cumplimiento de los requisitos establecidos para ellos como proveedores de este servicio en el documento de Criterios de Acreditación CEA-3.0-07 emitido por el Organismo Nacional de Acreditación de Colombia (ONAC).

dd) Olimpia IT informa a sus proveedores del servicio de Datacenter, que son considerados como críticos para la operación de Entidad de Certificación Digital, que hace extensivo el cumplimiento de los requisitos del documento de Criterios de Acreditación CEA-3.0-07 emitido por el Organismo Nacional de Acreditación de Colombia (ONAC), cuando les corresponda.

ee) Olimpia IT ha establecido un protocolo de protección de datos personales y un manual de tratamiento de datos personales como sistema de seguridad para proteger la información que se recopila con el fin de prestar el servicio de estampado cronológico, emisión de certificados digitales y servicios de firma centralizada, correo electrónico certificado, archivo, conservación, registro, custodia y anotación.

ff) Olimpia IT tiene un procedimiento documentado para recibir, evaluar y tomar decisiones acerca de las quejas y reclamos. Debe registrar y rastrear las quejas y reclamos, así como las acciones que se han emprendido para resolverlas.

gg) Olimpia IT registra y confirma si un reclamo se relaciona con las actividades de certificación digital de las cuales es responsable y, si es así, debe tratarlas y dar respuesta.

hh) Olimpia IT es responsable de reunir y verificar toda la información necesaria para alcanzar una decisión sobre la queja y reclamo.

ii) La decisión que resuelve la queja o reclamo debe ser tomada, revisada y aprobada por personas que no estén involucradas en las actividades de certificación digital relacionadas con el reclamo.

jj) Olimpia IT debe suministrar al reclamante una notificación formal sobre el resultado y la finalización del proceso de reclamación.

kk) Olimpia IT debe emprender las acciones posteriores necesarias para resolver el reclamo.

ll) Olimpia IT deberá atender con los reclamos hechos por los suscriptores respecto de los certificados emitidos, los servicios prestados y el servicio de estampado cronológico.

mm) La alta dirección de la ECD de asegurarse de que esta DPC se implemente adecuadamente.

nn) Olimpia IT ejerce control, sobre los servicios de certificación digital acreditados, respecto a la propiedad y el uso de símbolos, certificados, cualquier otro mecanismo para indicar que el servicio de certificación digital está acreditado.

oo) Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación;

pp) Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en el Artículo 29 de la Ley 527 de 1999;

qq) a) Emitir certificados conforme a lo solicitado o acordado con el suscriptor;

rr) Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas digitales, la conservación y archivo de certificados y documentos en soporte de mensaje de datos;

ss) Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor;

tt) Garantizar la prestación permanente del servicio de entidad de certificación.

uu) Atender oportunamente las solicitudes y reclamaciones hechas por los suscriptores.

vv) Efectuar los avisos y publicaciones conforme a lo dispuesto en la ley.

ww) Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas digitales y certificados emitidos y en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración.

xx) Permitir y facilitar la realización de las auditorías por parte del Organismo Nacional de Acreditación de Colombia. Es responsabilidad de la entidad de certificación pagar los costos de la acreditación y los de las auditorias de vigilancia, conforme con las tarifas del Organismo Nacional de Acreditación de Colombia.

yy) Elaborar los reglamentos que definen las relaciones con el suscriptor y la forma de prestación del servicio.

zz) Llevar un registro de los certificados.

aaa) Salvo acuerdo entre las partes, la entidad de certificación podrá dar por terminado el acuerdo de vinculación con el suscriptor dando un preaviso no menor de noventa (90) días. Vencido este término, la entidad de certificación revocará los certificados que se encuentren pendientes de expiración.

bbb) Ser responsable de sus decisiones relacionadas con la certificación digital, conservando el poder de decisión al otorgar, mantener,

cancelar o retirar (revocar) la certificación, obligaciones que no son delegadas ni contratadas con terceros.

14.2. CONDICIONES Y OBLIGACIONES DE LOS SUSCRIPTORES

Las obligaciones que a continuación se describen, estarán a cargo del suscriptor

a) Cumplir con los requisitos del servicio de certificación digital respectivo incluyendo la implementación de los cambios cuando los comunica Olimpia IT.

b) Que la información suministrada para el certificado sea coherente con el servicio solicitado y suministrar a la RA la información real, verdadera y necesaria para realizar una correcta identificación.

c) No utilizar su certificación digital de manera que contravenga la ley u ocasione mala reputación o perjuicios para la ECD, y no hace ninguna declaración relacionada con su certificación digital que la ECD pueda considerar engañosa o no autorizada.

d) Que inmediatamente después de la cancelación o la terminación de la certificación digital, el suscriptor deje de utilizarla en todo el material publicitario que contenga alguna referencia a ella, y emprende las acciones exigidas por el servicio de certificación digital (por ejemplo, la devolución de los documentos de la certificación) y cualquier otra medida que se requiera.

e) Que, al hacer referencia al servicio de certificación digital en medios de comunicación, tales como documentos, folletos o publicidad, el suscriptor informe que cumple con los requisitos especificados en las Políticas de Certificados.

f) Informar a la ECD, acerca de los cambios que pueden afectar la información del certificado que le fue otorgado o que se encuentra en proceso de emisión.

g) Realizar un uso adecuado, legal y acorde con las buenas costumbres mercantiles de la clave privada, así como utilizarla sólo para los fines establecidos y de acuerdo con lo pactado en el contrato celebrado y con lo estipulado en esta Declaración de Prácticas de Certificación.

h) Informar a los terceros intervinientes y que tengan interés en el proceso, la calidad en la que se firman los mensajes de datos de acuerdo con la clasificación dada al suscriptor contractualmente. Cuando el mensaje de datos o documento electrónico firmado por el suscriptor con su certificado digital. La calidad en la que firma el suscriptor será la que determine el contexto contractual y de costumbre de uso que se dé entre las partes y de acuerdo con el documento firmado.

i) Una vez cumplido uno cualquiera de los supuestos requeridos para realizar la revocación del certificado digital que le ha sido entregado, solicitar la inclusión de dicho certificado digital en las listas de certificados revocados que administre y lleve Olimpia IT.

j) Dar un uso adecuado y acorde con lo contractualmente pactado y con lo establecido en esta Declaración de Prácticas de Certificación, aceptando que la clave privada es personal e intransferible, por lo cual el uso por parte de terceras personas distintas al suscriptor, sin que ello esté pactado contractualmente, implica una aceptación del suscriptor en el uso que el tercero le dé a la clave privada. Esta infracción no afectará las cualidades jurídicas de la firma digital o firma electrónica.

k) El suscriptor declara que toda la información contenida en el certificado digital es cierta y veraz, y dado el caso de que dicha información consignada no corresponda a la realidad, es obligación

del suscriptor informar de manera inmediata a Olimpia IT, la corrección, modificación, adición o supresión a que haya lugar.

l) Si el suscriptor conoce de alguna condición de cualquier naturaleza o índole que pueda llegar a afectar la confiabilidad o alguna otra de las virtudes jurídicas del certificado digital, deberá informarla inmediatamente a Olimpia IT. Cuando la firma o el certificado digital se encuentren almacenados o direccionados por un soporte físico, se deberá notificar cualquier daño, deterioro sustancial pérdida o robo que impida el uso de los servicios ofrecidos por Olimpia IT.

m) Cuando la firma o el certificado digital se encuentren almacenados en un soporte físico, destruir el soporte físico cuando así lo exija Olimpia IT, ya sea por la sustitución por otro o cuando termine el periodo del servicio adquirido, siguiendo para ello las instrucciones de Olimpia IT.

n) Cuando el certificado digital y su llave privada se encuentren almacenados en la infraestructura física de un tercero, destruir el certificado junto con sus llaves pública y privada cuando así lo exija Olimpia IT, ya sea por la sustitución por otro o cuando termine el periodo del servicio adquirido.

o) Devolver el soporte físico del certificado digital cuando así lo exija Olimpia IT.

p) Inhibirse de violentar por cualquier forma los derechos de propiedad industrial e intelectual de Olimpia IT en el uso de los certificados digitales. El suscriptor garantiza que la información incluida en el certificado digital por su instrucción no constituye vulneración alguna a los derechos de propiedad intelectual o industrial de Olimpia IT o de cualquier tercero, y se obliga a mantener indemne a Olimpia IT de cualquier llamamiento por la ocurrencia de este tipo de hechos. A su vez el uso inadecuado que el suscriptor haga de la firma o del certificado digital se entenderá es de su entera responsabilidad.

q) Cualquier otra que se derive de la ley o del contenido de esta Declaración de Prácticas de Certificación.

r) Abstenerse de realizar copias, modificar, alterar, reproducir, adaptar, traducir, utilizar técnicas de ingeniería inversa, descompilar o desensamblar, alterar, o interferir en cualquier otra forma con la prestación del servicio prestado por Olimpia IT.

s) El suscriptor no podrá usar el nombre y/o enseña comercial de Olimpia IT, así como la marca de Olimpia IT o de los servicios acreditados de la compañía, en programas de publicidad o Marketing, ni podrá referirse a Olimpia IT directa o indirectamente ante terceros sin el previo consentimiento por escrito de Olimpia IT. El uso de la marca y de la propiedad intelectual de Olimpia IT sin que exista una autorización previa, licencia o cesión, podrá acarrear el inicio de acciones legales y el cobro de los perjuicios que se ocasionen a Olimpia IT.

t) Cuando el suscriptor utilice los servicios de Olimpia IT, y requiera o desee comunicar la utilización del servicio prestado por Olimpia IT, deberá informar en los medios en que se cite el servicio, que este cumple con todos los parámetros legales exigidos tanto para el certificado digital como para la firma digital y la firma electrónica.

u) Cumplir las obligaciones que se pacten en cuanto uso de marcas comerciales en la prestación de los servicios y en consecuencia respetar los derechos marcarios que se encuentren en cabeza de Olimpia IT.

v) Todo cambio tecnológico voluntario realizado por el suscriptor que pueda afectar la prestación del servicio deberá ser informado a Olimpia IT.

w) El suscriptor debe consultar, conocer y aceptar esta DPC, así como su alcance tanto para los certificados digitales, los servicios prestados y el servicio de estampado cronológico.

x) Al obtener una estampa cronológica, el suscriptor debe verificar que se haya firmado correctamente y que el certificado no se encuentre revocado.

y) El suscriptor y los clientes garantizan que han cumplido los requisitos definidos en las leyes colombianas y las disposiciones emitidas por los entes reguladores para obtener el servicio de certificación digital solicitado.

z) El suscriptor podrá dar por terminado el acuerdo de vinculación con la entidad de certificación dando un preaviso no inferior a treinta (30) días.

aa) Recibir la firma digital o firma electrónica por parte de la entidad de certificación o generarla, utilizando un método autorizado por ésta.

bb) Suministrar la información que requiera la entidad de certificación.

cc) Mantener el control de la firma digital y la firma electrónica.

dd) Solicitar oportunamente la revocación de los certificados.

14.3. OBLIGACIONES DEL SOLICITANTE

a) El solicitante se obliga para con Olimpia IT a leer los "Términos y Condiciones", aceptarlos en su integridad y cumplirlos cabalmente durante la vigencia de la relación comercial objeto de este documento y después de la terminación de la relación comercial, en cuanto a los

aspectos que por la ley las a partes estén obligados, tales como, pero sin limitarse al cuidado y custodia de la información, etc.

b) El solicitante se adhiere a lo establecido en la Política de Protección de Datos Personales de Olimpia IT, expuesta al público en la página de la ECD

c) Garantiza que toda la información suministrada antes, durante y después del proceso de emitir certificados digitales y/o prestar servicios acreditados por ONAC, es veraz y que cualquier falsedad en la información suministrada será motivo de suspender por término indefinido los servicios y los certificados emitidos. Igualmente, el solicitante acepta que en caso de que se presenten errores, yerros, o *typos* evidentes en la redacción o presentación de la información de la solicitud, la ECD podrá ajustar o corregir esta información con el fin de proveer efectivamente el servicio, siempre que no se presenten situaciones que razonablemente permitan concluir que existe intensión de presentar información falsa, o mala fe del solicitante.

d) Es compromiso del solicitante usar el mecanismo de autenticación establecido por Olimpia IT como único método de ingreso al portal, en caso de tener dificultades con el ingreso el solicitante puede comunicarse con la línea de servicio al cliente de Olimpia IT.

e) Queda prohibido por parte de los solicitantes el ingreso de software nocivo u otro similar al portal web de la entidad de certificación digital el cual pueda provocar algún daño o perjuicio para Olimpia IT o terceras partes involucradas en la prestación del servicio, o partes confiantes del servicio.

f) Se exige a los solicitantes tener una cuenta de correo electrónico activa y número de celular activo, en caso de no tener uno de estos dos

servicios, se le indicará al solicitante que deberá adquirir uno de ellos para la prestación del servicio.

Los términos y condiciones de uso del correo electrónico que adquiera el solicitante serán de exclusivo cumplimiento del solicitante.

g) Olimpia impide el uso de su portal interno para actividades consideradas como ilícitas según la normatividad vigente colombiana.

h) Al solicitante se le suspenderá la cuenta por inactividad prolongada por más 2 años, contados desde su fecha de creación.

14.4. OBLIGACIONES Y PRECAUCIONES DE LAS PARTES CONFIANTES

El servicio de certificación digital integra la utilización de un conjunto de elementos para la eficaz prestación de un servicio para los suscriptores y que a su vez repercute en la confianza legal y contractual que tienen los terceros respecto de los certificados digitales emitidos por Olimpia IT.

La confiabilidad basada en el no repudio de la operación es un factor de confianza en los terceros receptores del certificado digital expedido por Olimpia IT y bajo el resguardo presuntivo de la ley el tercero entiende y acepta que el acto celebrado surte la equivalencia funcional al de un documento firmado manuscritamente, esa tercera persona se convierte en un interviniente del Sistema de Certificación Digital, en calidad de parte confiante, y por ello asume las obligaciones que se establecen a continuación:

a) Verificar que tanto el certificado digital como la firma digital, no se encuentren listados en las listas de revocación de certificados que maneja y administra Olimpia IT disponible en el sitio de web de Olimpia IT.

b) Aceptar y reconocer a los certificados digitales solamente el uso que se permite darles de conformidad con lo establecido en la sección de Uso de los certificados digitales.

c) Dar cumplimiento al capítulo 15.3 de esta Declaración de Prácticas de Certificación dirigido a la parte confiante.

d) Informar a Olimpia IT de cualquier evento que pueda afectar la utilización del Sistema de Certificación Digital.
e) Abstenerse de realizar copias, modificar, alterar, reproducir, adaptar, traducir, utilizar técnicas de ingeniería inversa, descompilar o desensamblar, alterar, o interferir en cualquier otra forma con la prestación del servicio prestado por Olimpia IT.
f) La parte confiante debe consultar, conocer y aceptar esta DPC, así como su alcance tanto para los certificados digitales, los servicios prestados y el servicio de estampado cronológico.
g) Al obtener una estampa cronológica, el suscriptor debe verificar que se haya firmado correctamente y que el certificado no se encuentre revocado.

14.4.1. ESTADO DE CONFIANZA DE LOS CERTIFICADOS Y FIRMAS DIGITALES

El **Sistema de Certificación Digital** de Olimpia IT cumple y continua en cumplimiento a cabalidad con todos los requerimientos legales, técnicos y tecnológicos que dan certeza de los atributos otorgados por la ley para ofrecer certificados confiables que gozan de no repudio y de las demás características que otorga la ley para que estos servicios ofrecidos por Olimpia IT, cumplan a entera satisfacción tanto de las autoridades habilitantes, como de los suscriptores y partes confiantes, con el principio de equivalencia funcional que permite adherir la firma digital a un mensaje de datos y documentos electrónicos, así como la emisión de sus

certificados digitales equiparables a los documentos físicos, para obtener así la seguridad jurídica deprecada de este tipo de procedimientos.

14.4.2. ESTADO DE CONFIANZA DE LAS FIRMAS DIGITALES Y FIRMAS ELECTRÓNICAS

Para garantizar la confiabilidad adquirida por la parte confiante respecto de la firma digital, esta parte deberá previo voto de confiabilidad, conocer esta Declaración de Prácticas de Certificación, en especial la parte que le compete a la parte confiante, haber hecho el proceso de confiabilidad del certificado digital que a continuación se describe y que su creación corresponda a un acto anterior del acto a firmar y verificar el certificado raíz de la firma digital de Olimpia IT que contiene la clave pública.

14.4.3. ESTADO DE CONFIANZA DE LOS CERTIFICADOS DIGITALES

Para garantizar la confiabilidad adquirida por la parte confiante, respecto del certificado digital, esta parte previo voto de confiabilidad deberá, verificar que el certificado no se encuentre incluido en las listas de revocación que administra Olimpia IT, que el certificado digital se encuentre al momento del acto a realizar con una fecha de expiración posterior al acto a ejecutar y haber agotado el proceso de confiabilidad de firma digital.

Es entendido que un certificado digital será válido siempre que no se encuentre en las listas de revocación que administra Olimpia IT, su creación es anterior al momento de su utilización y se encuentra asociada al certificado raíz de la firma digital de Olimpia IT.
El uso de un certificado digital por cualquier interviniente está sujeto al estricto cumplimiento de los siguientes parámetros:

- El acuerdo contractual celebrado con el suscriptor del servicio de certificación digital, y cuyo contenido se encuentra en el siguiente

enlace que hace parte de la página web oficial de Olimpia IT, https://micertificado.olimpiait.com
- Esta Declaración de Prácticas de Certificación.

14.5. DERECHOS ASOCIADOS A CADA UNO DE LOS SERVICIOS PRESTADOS COMO ECD

Las políticas de certificados acogerán los siguientes derechos para cada uno de los servicios que describen a continuación:

- El suscriptor tiene derecho a utilizar la firma digital asociada al certificado que le haya expedido Olimpia IT como ECD, en todos los documentos que requiera.
- El suscriptor y el solicitante tienen derecho a informar a los terceros confiantes en la firma digital y firma electrónica que Olimpia IT es la ECD que presta el servicio.
- El suscriptor tiene derecho a usar la estampa de tiempo que le haya otorgado Olimpia IT, en cualquier documento que haya firmado o emplear su uso de forma legal.
- El suscriptor tiene derecho a acceder a los servicios de correo electrónico certificado y firma centralizada a través de los canales que para ello disponga Olimpia IT, como ECD.
- El solicitante y el suscriptor tienen derecho a recibir información clara respecto de los valores o precios, certificados o servicios que emite Olimpia IT.
- El solicitante y el suscriptor tienen derecho a que se realice el tratamiento de sus datos personales de acuerdo con la normatividad vigente, en particular la Ley 1581 de 2012 y el Decreto 1377 de 2013.

El suscriptor, las partes confiantes y demás involucrados, tienen derecho a presentar peticiones, quejas o reclamos de forma respetuosa a Olimpia IT, y a obtener respuesta a las mismas.

15. EXENCIÓN DE RESPONSABILIDAD

15.1. LIMITES DE RESPONSABILIDAD POR EL EJERCICIO DE LA ACTIVIDAD

a) El servicio ofrecido por parte de Olimpia IT como Entidad de Certificación Digital, compone por parte de Olimpia IT una obligación de medio y no de resultado. Por lo que Olimpia IT pondrá a disposición del servicio, del suscriptor y demás terceros intervinientes o con legítimo interés la debida diligencia con su profesionalismo, y experiencia en la prestación del servicio de certificación digital, y será responsable únicamente por la culpa leve en sus actuaciones como Entidad de Certificación Digital. Olimpia IT no puede asegurar ni garantizar que la actividad de certificación tenga un resultado determinado. Olimpia IT sólo responderá por aquellos errores que ocurridos hubieran podido evitarse por su diligencia profesional.

b) El incumplimiento de cualquiera de las obligaciones por parte del suscriptor o del tercero confiante, sus consecuencias de toda índole correrán por cuenta de estos, esto incluido los daños que incluso por circunstancias ajenas a su voluntad de se haya producido, en igual aplicación para la pérdida del dispositivo físico cuando aplique.

c) Cuando el incumplimiento de cualquiera de las obligaciones por parte del suscriptor o el tercero confiante, sea la causa de una prestación del servicio defectuosa, Olimpia IT no será responsable de la prestación defectuosa de este servicio, ni de las consecuencias de la pérdida de las cualidades jurídicas otorgadas por la ley a la firma digital.

d) Olimpia IT no será responsable por los perjuicios causados por el incumplimiento de sus obligaciones por fuerza mayor, caso fortuito

y en general, cualquier circunstancia sobre la que Olimpia IT no pueda tener un control razonable, incluyendo pero sin limitarse a los siguientes:, el corte de suministro eléctrico y/o telefónico, los virus informáticos, las deficiencias en los servicios de telecomunicaciones (Internet, canales de comunicación, etc.) o el compromiso de las llaves asimétricas derivado del riesgo tecnológico imprevisible.

e) El límite de responsabilidad patrimonial por responsabilidad civil contractual o extracontractual independientemente de la causa u origen de su responsabilidad, por parte de Olimpia IT se fija como cuantía máxima para la indemnización de perjuicios por los daños ocasionados por certificado digital emitido, el amparo o cubrimiento otorgado en la póliza de responsabilidad civil profesional tomada por Olimpia IT. En consecuencia, Olimpia IT solo indemnizará a las personas perjudicadas por un certificado digital emitido por ésta, independientemente del número de veces que el mismo se haya utilizado o del número de perjudicados por dichos usos. En caso de que existan varios perjudicados, el monto máximo indemnizable se distribuirá a prorrata entre ellos. Si habiéndose distribuido la indemnización, surgieren nuevos perjudicados, estos deberán dirigirse contra las personas ya indemnizadas para efectos de obtener a prorrata su indemnización.

f) Olimpia IT solo responderá por los perjuicios que se ocasionen por la utilización de los servicios de certificación digital dentro del año siguiente a la expiración o revocación del certificado digital. Olimpia IT no ofrece ningún tipo de garantía que no esté expresamente estipulada, ni responderá por evento que no esté expresamente contemplado en esta Declaración de Prácticas de Certificación.

g) Cuando las leyes concernientes al servicio de certificación digital establezcan la ineficacia de toda cláusula que implique limitar el

monto de los perjuicios derivados de la responsabilidad civil contractual o extracontractual, la nulidad de las cláusulas no afectará las demás cláusulas de esta declaración de Prácticas de Certificación.

h) Los certificados de firmas digitales y electrónicas emitidos por entidades de certificación extranjeras podrán ser reconocidos, en los mismos términos y condiciones exigidos en la ley, para la emisión de certificados por parte de Olimpia IT, siempre y cuando tales certificados sean reconocidos por una entidad de certificación autorizada que garantice en la misma forma que lo hace con sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia.

i) Con el propósito de viabilizar la imparcialidad que, como Entidad de certificación Digital, requiere Olimpia IT, esta ha diseñado, implementado y acogido una política de imparcialidad- no discriminación e independencia, con el fin de identificar los riesgos que puedan afectar a esta, así como los controles necesarios para el resguardo de la imparcialidad al interior de la entidad de certificación digital.

j) Olimpia IT como ECD limita su responsabilidad por cada documento firmado así: el contenido de cada uno de los documentos firmados, su compromiso y legalidad son de entera y exclusiva responsabilidad del suscriptor por lo que Olimpia IT se limita a suministrar un certificado digital para el uso de firma digital por parte del suscriptor y que dicho certificado puede ser verificado por los medios dispuestos para ello por parte de Olimpia IT.

15.2. RESPONSABILIDADES DE LOS SOLICITANTES Y SUSCRIPTORES

De conformidad con lo establecido en el artículo 40 de la Ley 527 de 1.999, el suscriptor será responsable por la falsedad, error u omisión en la información suministrada a la entidad de certificación y por el incumplimiento de sus deberes como suscriptor.

El suscriptor que haya ocasionado algún perjuicio a Olimpia IT deberá indemnizarlo, así como si con su actuar haya ocasionado perjuicios a los demás involucrados o receptores.

También será responsable el suscriptor por la indemnización de perjuicios a que hubiere lugar por la violación de esta Declaración de Prácticas de Certificación, el incumplimiento de los términos y condiciones de la página https://micertificado.olimpiait.com, y demás documentos que se establezcan para el cumplimiento de la relación comercial que nace de la prestación de los servicios de Olimpia IT como ECD, asumiendo los gastos judiciales en que incurra Olimpia IT por esta causa, incluyendo los costos de abogados.

Independientemente de la causa por la cual haya entregado dicha información falsa, inexacta o insuficiente. El suscriptor asumirá los perjuicios que sufra como consecuencia de eventos de caso fortuito o fuerza mayor.

Será de entera responsabilidad del suscriptor la custodia y cuidado del soporte físico (tarjeta inteligente, token, disco duro, USB u otro suministrado o no por Olimpia IT) del certificado digital.
Independientemente de si los medios empleados por la parte confiante validan o no las condiciones de vigencia del certificado digital y de la firma digital, así como la calidad en la que actúa, el suscriptor está en la obligación de informar a la parte confiante sobre la condición o calidad en la que se está utilizando el certificado digital. Este deber de información

será asumido de forma exclusiva por el suscriptor y no habrá solidaridad del deber de esta información respecto de Olimpia IT para con los partes confiantes.

Los actos ejecutados por el suscriptor en el amparo del certificado digital otorgado, bajo el marco contractual celebrado, serán de su entera y exclusiva responsabilidad, así como que su capacidad para obligarse es excluyente con la capacidad obligacional de la Entidad de certificación Digital Olimpia IT, por lo que los efectos de los actos o negocios jurídicos corresponderán de forma exclusiva al suscriptor.

15.3. RESPONSABILIDAD DE PARTES CONFIANTES

Las partes confiantes, tienen la responsabilidad de verificar el estado del certificado, a fin de garantizar que la firma digital en el documento que ha recibido es válida.

El estado del certificado se puede validar en el siguiente enlace https://micertificado.olimpiait.com

15.4. CUMPLIMIENTO DE LAS OBLIGACIONES DE OLIMPIA IT

a) Olimpia IT ha suscrito una póliza de seguro con una entidad aseguradora autorizada para funcionar en el territorio colombiano y bajo la legislación colombiana, que ampara todos los perjuicios contractuales y extracontractuales de los suscriptores y terceros de buena fe exenta de culpa derivados de errores y omisiones, o de actos de mala fe de los administradores, representantes legales o empleados de Olimpia IT en el desarrollo de las actividades para las cuales solicita o cuenta con acreditación.

b) En la página web https://micertificado.olimpiait.com se encuentran publicadas las actividades y servicios acreditados atendiendo lo establecido para reglamento de uso de los símbolos de acreditado y/o asociado de ONAC.

c) Las Condiciones de la póliza de seguro:

Dando cumplimiento al artículo 9 del Decreto 333 de 2014, la póliza de seguros adquirida por Olimpia IT, cubre todos los perjuicios contractuales y extracontractuales de los suscriptores y terceros de buena fe, derivados de errores y omisiones, o de actos de mala fe de los administradores, representantes legales o empleados de la ECD en el desarrollo de las actividades para las cuales cuenta con acreditación.

La póliza de seguros adquirida por Olimpia IT le da cumplimiento a los siguientes literales del artículo 9 del Decreto 333 de 2014.

"c) Cubre los anteriores riesgos por una cuantía asegurada por evento de 7.500 salarios mínimos mensuales legales por evento;
d) Incluye cláusula de restitución automática del valor asegurado;
e) Incluye una cláusula que obliga a la entidad aseguradora, al tomador y al asegurado a informar previamente a ONAC la terminación del contrato de seguro o las modificaciones que reduzcan el alcance o monto de la cobertura."

La póliza es de responsabilidad civil profesional, el tomador es Olimpia IT S.A.S., la aseguradora es SBS Seguros de Colombia S.A.S., los beneficiarios son terceros afectados y su vigencia se encuentra disponible al público para consulta en portal de la entidad de certificación digital https://micertificado.olimpiait.com

d) Olimpia IT cuenta con la estabilidad financiera y los recursos necesarios para su operación según lo establecido en el Decreto 333 de 2014, lo cual se puede evidenciar por medio de sus Estados Financieros.

16. RESOLUCIÓN DE CONTROVERSIAS Y MINUTA CONTRACTUAL PARA LA PRESTACIÓN DE SERVICIOS COMO ECD

Cualquier controversia que se sucinte entre las partes como consecuencia del contrato que se celebre y/o de la aplicación de esta Declaración de Prácticas de Certificación (DPC) o de las Políticas de Certificados (PC), así como de los demás convenios y/o reglas para la prestación de los servicios, de su interpretación, de su ejecución, de domicilio y en general de su construcción, se señala como domicilio la ciudad de Bogotá D.C., y se regirá por las leyes que regulan la materia en la República de Colombia. Por lo tanto, las disputas que surjan se regirán en lo no previsto por las normas del Código de Comercio Colombiano, y a falta de éstas, por normas análogas del ordenamiento jurídico colombiano, así como por los principios generales del derecho, de manera que, en todo caso, toda situación que resulte de la ejecución pueda ser resuelta de manera jurídica. De ser necesario, se aplicará igualmente la costumbre mercantil local.

Las diferencias o controversias que surjan entre las partes, con ocasión de la firma, ejecución, interpretación, prorroga o terminación del contrato y demás normas o reglamentos que regulen la prestación del servicio serán resueltas de la siguiente forma, y con base en los siguientes parámetros:

a) Cualquier conflicto suscitado por causa o respecto del contrato y demás normas o reglamentos que regulen la prestación del servicio se resolverá como primera medida según el trámite señalado a continuación.

b) Las Partes intentarán de buena fe resolver con prontitud cualquier conflicto suscitado por causa o respecto del contrato y demás normas o reglamentos que regulen la prestación del servicio a

través de una negociación entre los Representantes Legales y/o quienes estos designen para que puedan resolver la controversia.

TRÁMITE:

a) Cualquiera de las Partes puede dar aviso por escrito a la otra, de cualquier conflicto o diferencia que no haya sido resuelta en el curso normal de su trato comercial.

b) En un plazo no mayor de diez (10) días calendario contados a partir de la entrega de la notificación del conflicto y/o diferencia, la parte receptora del aviso entregará a la otra una respuesta por escrito. El aviso y la respuesta incluirán: a) los argumentos que fundamentan su respuesta; y b) El nombre y cargo del representante de los intereses, a esta parte y de cualquier otra persona que haya de acompañarlo.

c) Recibida la respuesta, dentro de los diez (10) días calendario siguientes, los representantes de ambas partes deberán reunirse en tiempo y lugar mutuamente acordados, en la ciudad de Bogotá D.C., con el fin de buscar una solución al conflicto.

Toda controversia o diferencia relativa a este contrato que las partes no puedan resolver en negociación directa se someterá a la justicia ordinaria.

16.1. CONTRATO CELEBRADO ENTRE LA ECD Y LOS SOLICITANTES Y/O SUSCRIPTORES

En https://micertificado.olimpiait.com los solicitantes y/o suscriptores encontrarán el contrato a celebrar con la ECD, el cual se encuentra en formato de aceptación o rechazo de términos y condiciones, a fin de prestar los servicios y/o emisión de certificados digitales que requieran.

Si el solicitante y/o suscriptor, rechaza los términos y condiciones el proceso de solicitud finalizará.

16.2. LEY APLICABLE

Olimpia IT se acoge a toda ley aplicable colombiana evidenciando su cumplimiento en los documentos de la Entidad de Certificación Digital.

17. POLÍTICA DE MANEJO DE LOS CERTFICADOS

OLIMPIA IT, declara que cuenta con un documento independiente a esta Declaración de Prácticas de Certificación, el cual contiene la Política de Certificados (PC).

17.1. EMISIÓN DE CERTIFICADOS DIGITALES – REQUISITOS Y PROCEDIMIENTOS

Olimpia IT establece que, en su Política de Certificados, en el numeral 2, se encuentran los requisitos y procedimientos para la emisión de certificados digitales.

17.2. CUMPLIMIENTO DE LEY APLICABLE

Olimpia IT, establece que en el documento denominado Política de Certificados, en su numeral 2, se encuentra el cumplimiento de la ley aplicable.

17.3. CUMPLIMIENTO DE LOS REQUISITOS LEGALES

Olimpia IT, establece que en el documento denominado Política de Certificados, en su numeral 2, se encuentra el cumplimiento de los requisitos legales.

18. ACUERDO DE TÉRMINOS Y CONDICIONES

Olimpia declara que el solicitante previo a adquirir un certificado digital lee y acepta los términos y condiciones que deben cumplidos por todas aquellas personas que deseen interactuar con Olimpia IT S.A.S., como Entidad de Certificación Digital abierta, para el registro en la página web de Olimpia IT, https://micertificado.olimpiait.com en el cual el solicitante y/o suscriptor se obliga a leerlas y acogerlas.

Una vez el suscriptor y/o solicitante ha aceptado los términos y condiciones expuestos en la página web https://micertificado.olimpiait.com se entenderá que el suscriptor y/o solicitante se obliga a las condiciones y obligaciones allí establecidas.

Este acuerdo puede ser objeto de modificaciones y su contenido se encuentra acorde con la legislación colombiana vigente al momento de su publicación.

19. VIGENCIA DE LOS CERTIFICADOS

19.1. VIGENCIA DEL CERTIFICADO RAÍZ

La vigencia del certificado raíz es de 20 años a partir de la generación del certificado autofirmado.

19.2. VIGENCIA DE LOS CERTIFICADOS SUBORDINADOS

La vigencia de los certificados subordinados de la CA subordinada y TSA son de 15 años a partir de la generación del certificado firmado por la CA Raíz.

19.3. VIGENCIA DE LOS CERTIFICADOS EMITIDOS A LOS SUSCRIPTORES

La vigencia de los certificados emitidos a los suscriptores para los certificados de personas natural, persona jurídica, perteneciente a empresa, representante legal, profesional titulado y función pública es de máximo 2 años a partir de la expedición del certificado emitido por Olimpia IT.

20. ENTREGA DE CERTIFICADO DIGITAL

20.1. ENTREGA DEL TOKEN FÍSICO

Olimpia IT en su calidad de Entidad de Certificación Digital Abierta se encuentra en la disposición de realizar la entrega de certificados digitales solicitados en un medio físico mediante la contratación de un servicio de mensajería cuya actividad sea la de mensajería en el territorio colombiano, al cual se le entregará la información debidamente almacenada dando cumplimiento a los requerimientos de seguridad y confidencialidad de la información enviada.

Adicionalmente se restringe el alcance del envió del token físico solo a las ciudades capitales, ciudades principales, municipios aledaños a dichas ciudades, y a los municipios con vías de acceso secundarias. Olimpia IT podrá evaluar casos especiales donde se requiera envíos a municipios fuera del alcance establecido.

El suscriptor, podrá descargar el manual de instalación y uso del token desde el sitio web https://micertificado.olimpiait.com, botón “Descargas”, y la opción de descargar “Olimpia Sign”.

Los instaladores o drivers requeridos para el uso de token físico no son compatibles con sistemas operativos macOs.

20.2. TIEMPOS MÁXIMOS DE ENTREGA

Olimpia IT establece en la presente Declaración de Prácticas de Certificación un tiempo de entrega del certificado en un máximo de 2 días hábiles a partir de la fecha de decisión de la certificación, sin contabilizar el tiempo que el solicitante se tarde en responder las solicitudes de subsanación de información (en caso de que apliquen), confirmándole que el certificado ya se encuentra emitido y el token criptográfico listo para ser enviado.

20.3. OBTENCIÓN DEL CERTIFICADO DESDE EL PORTAL WEB

En los servicios distintos al de entrega de token criptográfico al suscriptor, el suscriptor podrá solicitar a Olimpia IT que genere el almacenamiento seguro del certificado digital y que así lo pueda utilizar desde cualquier dirección IP, mediante una autenticación en el portal de Olimpia IT: https://micertificado.olimpiait.com; o mediante web services, APIs u otras formas de integración de software, según lo dispuesto en el numeral 26.6.

21. IMPARCIALIDAD, NO DISCRIMINACIÓN E INDEPENDENCIA EN LOS SERVICIOS

Olimpia IT establece en todas las actividades realizadas en la operación de la Entidad de Certificación Digital el cumplimiento de la política de imparcialidad, no discriminación e independencia establecida y la mitigación de los riesgos de imparcialidad mediante las sesiones del Comité de Imparcialidad, como mecanismo de control.

Olimpia IT, garantiza que los servicios prestados, son ejecutados bajo un marco de independencia de funciones, segregación objetiva de las mismas que permite que los roles y funciones, involucrados en la prestación del servicio, no se vean afectados o parcializados por factores externos.

21.1. FACTORES DE NO DISCRIMINACIÓN

Para cada una de las actividades realizadas, la Entidad de Certificación Digital actúa de forma tal que permite la presentación de una solicitud de servicio por cualquier persona sin distingo de sexo, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica o discapacidad.

Las limitaciones tecnológicas o de costo del servicio, así como las causales objetivas de rechazo del servicio, no son factores de discriminación y obedecen a las limitaciones tecnológicas, estimaciones financieras y características de los servicios que ha definido Olimpia IT para la prestación de sus servicios.

22. DIRECTIVA DEL CERTIFICADO

Olimpia IT a continuación presenta los OID, para la CA raíz, así como para el certificado de la sub-CA y de cada uno de los certificados y servicios prestados por Olimpia IT como ECD.

OID ECD
IANA
1.3.6.1.4.1.50890
Olimpia IT S.A.S.

La estructura de la directiva del certificado se realizará con base en la siguiente especificación:

OID ECD
IANA
1.3.6.1.4.1.50890
Olimpia IT S.A.S.

La estructura de la directiva del certificado se realizará con base en la siguiente especificación:

1.3.6.1.4.1 (Código estándar – No modificable)
50890 (Código IANA – Modificable solo si se adquiere uno nuevo)
50890.X (Certificado raíz de Olimpia – Se modifica acorde a la partición)
50890.2.X (Particiones en el HSM – Subordinadas - Se modifica acorde a la partición)
50890.2.X.X (Identificación de los servicios – Se modifica acorde a los servicios ofrecidos)
50890.2.X.X.X (Identificación de los Sub-servicios – Se modifica al alcance de cada servicio)

CERTIFICADOS EMITIDOS POR OLIMPIA
CA RAÍZ
1.3.6.1.4.1.50890.2
SUBCA PARA FIRMAR A LOS SUSCRIPTORES
1.3.6.1.4.1.50890.2.1
Persona Natural
1.3.6.1.4.1.50890.2.1.1
Persona Jurídica
1.3.6.1.4.1.50890.2.1.2
Profesional Titulado
1.3.6.1.4.1.50890.2.1.3
Pertenencia a Empresa
1.3.6.1.4.1.50890.2.1.4
Función Publica
1.3.6.1.4.1.50890.2.1.5
Representante Legal
1.3.6.1.4.1.50890.2.1.6
SERVICIOS PRESTADOS POR OLIMPIA
Firma Centralizada
1.3.6.1.4.1.50890.2.1.7

Firma Centralizada Persona Natural
1.3.6.1.4.1.50890.2.1.7.1
Firma Centralizada Persona Jurídica
1.3.6.1.4.1.50890.2.1.7.2
Firma Centralizada Profesional Titulado
1.3.6.1.4.1.50890.2.1.7.3
Firma Centralizada Pertenencia a Empresa
1.3.6.1.4.1.50890.2.1.7.4
Firma Centralizada Función Publica
1.3.6.1.4.1.50890.2.1.7.5
Firma Centralizada Representante Legal
1.3.6.1.4.1.50890.2.1.7.6
Reservado para Olimpia IT
1.3.6.1.4.1.50890.2.1.8
Correo Electrónico Certificado
1.3.6.1.4.1.50890.2.1.9
Correo Electrónico Certificado Persona Natural
1.3.6.1.4.1.50890.2.1.9.1
Correo Electrónico Certificado Persona Jurídica
1.3.6.1.4.1.50890.2.1.9.2
Correo Electrónico Certificado Profesional Titulado
1.3.6.1.4.1.50890.2.1.9.3
Correo Electrónico Certificado Pertenencia a Empresa
1.3.6.1.4.1.50890.2.1.9.4
Correo Electrónico Certificado Función Publica
1.3.6.1.4.1.50890.2.1.9.5
Correo Electrónico Certificado Representante Legal
1.3.6.1.4.1.50890.2.1.9.6

Los OID terminado en 2.1.10 y 2.1.11 están reservados a pruebas internas de Olimpia

TSA

1.3.6.1.4.1.50890.2.1.12

Certificado para cifrado de las llaves privadas de los suscriptores

1.3.6.1.4.1.50890.2.2

Estampado Cronológico TSA

1.3.6.1.4.1.50890.2.3

Firma Electrónica Certificada

1.3.6.1.4.1.50890.2.4

23. TIPOS DE CERTIFICADOS

Olimpia IT Ofrece los siguientes certificados y servicios:

- Certificado Digital Persona Natural
- Certificado Digital Persona Jurídica
- Certificado Digital Representante legal
- Certificado Digital Función Publica
- Certificado Digital Profesional Titulado
- Certificado Digital Pertenencia a Empresa
- Estampado Cronológico
- Firma Centralizada
- Correo Electrónico Certificado
- Firma Electrónica Certificada

Nota: Se aclara que el servicio de Firma Electrónica Certificada no se encuentra acreditado.

24. DESCRIPCIÓN DE LOS SERVICIOS

24.1. DESCRIPCIÓN DEL SERVICIO CERTIFICADO DIGITAL - PERSONA NATURAL

El certificado de Persona natural acredita la identidad del titular en la firma de documentos electrónicos garantizando la autenticidad del emisor de la comunicación, el no repudio del origen y la integridad del contenido. El poseedor de un certificado persona natural actúa en su propio nombre e interés.

Olimpia IT realiza su certificado digital – Persona natural acorde con lo establecido por la metodología de cifrado asimétrico para garantizar la incorruptibilidad de este, el cual tiene una validez en todo el territorio colombiano con un vencimiento máximo establecido en el presente documento.

Si el suscriptor desea utilizar este certificado con el servicio de firma centralizada, deberá tomar uno de los paquetes del servicio de firma centralizada.

Si el suscriptor desea disponer del certificado para ser usado a través de la plataforma tecnológica propia, o de un tercero autorizado, y con un uso en específico, deberá radicar una petición ante la ECD que cumpla con el estándar de solicitud de certificación *PKCS#10 - Formato de los mensajes enviados a una Autoridad de certificación para solicitar la certificación de una clave pública*. Por lo anterior, el suscriptor o el tercero autorizado deberá garantizar que los parámetros utilizados para la llave pública son el algoritmo criptográfico SHA256 + RSA. y que esta llave tenga un tamaño de 2048 bits.

24.2. DESCRIPCIÓN DEL SERVICIO CERTIFICADO DIGITAL - PERSONA JURÍDICA

El certificado de Persona Jurídica acredita la identidad del suscriptor y su condición como empresa o persona jurídica, y le permite al suscriptor firmar documentos digitalmente en la calidad que acredita su certificado.

Olimpia IT realiza su certificado digital – Persona jurídica acorde con lo establecido por la metodología de cifrado asimétrico para garantizar la incorruptibilidad de este, el cual tiene una validez en todo el territorio colombiano con un vencimiento máximo establecido en el presente documento.

Si el suscriptor desea utilizar este certificado con el servicio de firma centralizada, deberá tomar uno de los paquetes del servicio de firma centralizada.

Si el suscriptor desea disponer del certificado para ser usado a través de la plataforma tecnológica propia, o de un tercero autorizado, y con un uso en específico, deberá radicar una petición ante la ECD que cumpla con el estándar de solicitud de certificación *PKCS#10 - Formato de los mensajes enviados a una Autoridad de certificación para solicitar la certificación de una clave pública*. Por lo anterior, el suscriptor o el tercero autorizado deberá garantizar que los parámetros utilizados para la llave pública son el algoritmo criptográfico SHA256 + RSA y que esta llave tenga un tamaño de 2048 bits.

24.3. DESCRIPCIÓN DEL SERVICIO CERTIFICADO DIGITAL - PROFESIONAL TITULADO

El certificado de Profesional Titulado acredita la identidad del suscriptor y su título profesional, y le permite al suscriptor firmar documentos digitalmente en su propio nombre e interés.

Olimpia IT realiza su certificado digital –Profesional Titulado acorde con lo establecido por la metodología de cifrado asimétrico para garantizar la incorruptibilidad de este, el cual tiene una validez en todo el territorio colombiano con un vencimiento máximo establecido en el presente documento.

Si el suscriptor desea utilizar este certificado con el servicio de firma centralizada, deberá tomar uno de los paquetes del servicio de firma centralizada.

24.4. DESCRIPCIÓN DEL SERVICIO CERTIFICADO DIGITAL - PERTENENCIA A EMPRESA

El certificado de Pertenencia a Empresa acredita la identidad del suscriptor y su condición de pertenencia, función o empleo en una entidad o persona jurídica, y le permite al suscriptor firmar documentos digitalmente en la calidad que acredita su certificado.

Olimpia IT realiza su certificado digital –Pertenencia a Empresa acorde con lo establecido por la metodología de cifrado asimétrico para garantizar la incorruptibilidad de este, el cual tiene una validez en todo el territorio colombiano con un vencimiento máximo establecido en el presente documento.

Si el suscriptor desea utilizar este certificado con el servicio de firma centralizada, deberá tomar uno de los paquetes del servicio de firma centralizada.

24.5. DESCRIPCIÓN DEL SERVICIO CERTIFICADO DIGITAL - FUNCIÓN PÚBLICA

El certificado de Función Pública es emitido a nombre de personas naturales que acreditan la identidad del titular y su carácter de funcionario público o de particular en ejercicio de una función pública, ya

sea por designación o como resultado de la suscripción de un contrato que lo habilite como tal, en la firma de documentos electrónicos garantizando la autenticidad del emisor de la comunicación, el no repudio del origen y la integridad del contenido. El titular de un certificado de Función Pública actúa en la calidad acreditada en este.

Olimpia IT realiza su certificado digital –Función Pública acorde con lo establecido por la metodología de cifrado asimétrico para garantizar la incorruptibilidad de este, el cual tiene una validez en todo el territorio colombiano con un vencimiento máximo establecido en el presente documento.

Si el suscriptor desea utilizar este certificado con el servicio de firma centralizada, deberá tomar uno de los paquetes del servicio de firma centralizada.

24.6. DESCRIPCIÓN DEL SERVICIO CERTIFICADO DIGITAL – REPRESENTANTE LEGAL

El certificado de Representante Legal acredita la identidad del suscriptor y su condición como representante legal de una entidad o persona jurídica. Le permite al suscriptor firmar documentos digitalmente en nombre de la entidad o persona jurídica que representa.

Olimpia IT realiza su certificado digital –Representante Legal acorde con lo establecido por la metodología de cifrado asimétrico para garantizar la incorruptibilidad de este, el cual tiene una validez en todo el territorio colombiano con un vencimiento máximo establecido en el presente documento.

Si el suscriptor desea utilizar este certificado con el servicio de firma centralizada, deberá tomar uno de los paquetes del servicio de firma centralizada.

24.7. DESCRIPCIÓN DEL SERVICIO DE ESTAMPADO CRONOLÓGICO

El servicio de estampado cronológico da certeza de la integridad de la fecha y hora de un documento tomando la hora legal colombiana del Instituto Nacional de Metrología, o quien haga sus veces, adhiriendo una firma digital de la TSA.

El suscriptor debe adquirir uno de los paquetes comerciales ofertados para este servicio (ver sección 11.1).

24.8. DESCRIPCIÓN DEL SERVICIO DE FIRMA CENTRALIZADA

Es una gestión centralizada de los certificados digitales utilizados en una organización, donde los certificados digitales operan desde un repositorio único, controlado y seguro. Son certificados digitales generados y almacenados en el servidor de Olimpia IT, lo que permite al suscriptor utilizarlos desde cualquier ordenador.

Para ello, en el certificado de firma digital se utilizará la información que previamente ha suministrado el suscriptor a través del portal https://micertificado.olimpiait.com, el suscriptor realizará una autenticación (ingreso de código enviado a su correo o número celular en SMS, registrado al momento del registro del solicitante) en el portal https://micertificado.olimpiait.com, el suscriptor podrá solicitar el servicio desde cualquier IP, con servicio de internet.

Olimpia IT mediante la aplicación del sistema de certificación digital implementado, realiza la emisión y posesión de la llave privada mediante la generación del certificado de firma digital encriptado y complementado con una clave privada (PIN) que solo conoce el suscriptor de 4 dígitos; se realiza utilizando un módulo HSM (Hardware Security Module) certificado FIPS 140-2 Nivel 3. Se almacena en una infraestructura tecnológica independiente y aislada, que cumple el formato PKCS#11 y con los estándares internacionales de seguridad de la

información establecidos por la norma internacional NTC-ISO/IEC 27001 en su versión vigente. El suscriptor puede usar su certificado accediendo a esta tecnología (wrapping key), que consiste en llamar el servicio desde su alojamiento seguro y aislado, para ser usado desde un HSM (Hardware Security Module) certificado FIPS 140-2 Nivel 3.

Para el uso del servicio, el suscriptor deberá vincular un certificado digital emitido por Olimpia IT que contiene la información del suscriptor (el suscriptor deberá seleccionar al momento de la adquisición del servicio, el certificado digital con el cual hará uso de este servicio), este procedimiento se realizará en el portal https://micertificado.olimpiait.com. El costo de este servicio que incluye la emisión del certificado digital respectivo se define en el acápite de tarifas.

En los archivos tipo .pdf, la firma se integrará al archivo y cuando sea otro tipo de archivo la firma no se integra, pero sí se entregará junto con el documento original en un archivo tipo p7z, el cual contiene la información del archivo original y la firma digital.

El suscriptor debe adquirir uno de los paquetes comerciales ofertados para este servicio.

24.8.1. ESTE SERVICIO TIENE LAS SIGUIENTES LIMITACIONES:

- El servicio funcionará correctamente utilizando los navegadores Chrome en su versión 71.0.3578.98 y Microsoft EDGE versión 38.14393.2068.0.

24.8.2. ESTE SERVICIO INCLUYE ADICIONAL A LOS REQUISITOS ESTABLECIDOS, LA SIGUIENTE OPERACIÓN:

- El suscriptor deberá digitar una clave de 4 dígitos (PIN), con el fin de generar una autenticación en la página https://micertificado.olimpiait.com, y posterior a ello poder hacer uso del servicio.

24.9. DESCRIPCIÓN DEL SERVICIO DE CORREO ELECTRÓNICO CERTIFICADO

Este servicio acredita la identidad del suscriptor y le permite enviar mensajes de datos tipo correo electrónico firmados digitalmente, garantizando la autenticidad del emisor de la comunicación, el no repudio del origen y la integridad del contenido.

El servicio de correo se prestará por intermedio de un proveedor que cumple con lo estipulado en la normatividad vigente, particularmente en los artículos 20 y 21 de la Ley 527 de 1999.

Los acuses de recibido son admisibles respecto del hecho de envío y entrega, así como la fecha y hora legal del envío, y la autenticidad de su contenido, de acuerdo con los artículos 12 y 20 de la Ley 527 de 1999.

Olimpia IT será la encargada de realizar el ciclo de vida completo para resguardar la información del Suscriptor y dar cumplimiento a los Criterios Específicos de Acreditación. Así mismo, mediante la plataforma del proveedor del servicio, se encargará de generar las credenciales con sus respectivas claves e incluirá la estampa y firma digital de Olimpia IT para que éstas den valor probatorio al correo electrónico o a su contenido, de acuerdo con el artículo 10 de la Ley 527 de 1999. Se aclara que el servicio de correo no requiere la emisión de certificado digital para el suscriptor.

Al otorgar el servicio por parte de la ECD, el Suscriptor recibirá correos con la aprobación del servicio, donde se especifica el alcance y el acceso a la documentación necesaria para uso del servicio, y correo con las credenciales de usuario y contraseña para que active el servicio e inicie su utilización.

El suscriptor debe adquirir uno de los paquetes comerciales ofertados para este servicio, según se define en el acápite de tarifas. El suscriptor deberá mantener activa la opción de notificación de acuse de recibido de

su cuenta de correo electrónico, durante la prestación del servicio de correo electrónico certificado.

24.10. DESCRIPCIÓN DEL SERVICIO FIRMA ELECTRÓNICA CERTIFICADA

La firma electrónica certificada contiene requisitos de confiabilidad y es apropiada para los fines con los cuales se generó o comunicó un mensaje de datos, acreditando que los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante y es posible detectar cualquier alteración no autorizada del mensaje de datos, hecha después del momento de la firma, por lo que tendrá la misma validez y efectos jurídicos que la firma.

Olimpia IT emite la firma electrónica acorde con lo establecido por la metodología de cifrado asimétrico para garantizar la incorruptibilidad de este, el cual tiene una validez en todo el territorio colombiano con un vencimiento máximo establecido en el presente documento.

Si el suscriptor desea disponer de la firma electrónica certificada para ser usada a través de la plataforma tecnológica propia, o de un tercero autorizado, y con un uso en específico, deberá radicar una petición ante la ECD que cumpla con el estándar de solicitud de certificación *PKCS#10 - Formato de los mensajes enviados a una Autoridad de certificación para solicitar la certificación de una clave pública*. Por lo anterior, el suscriptor o el tercero autorizado deberá garantizar que los parámetros utilizados para la llave pública son el algoritmo criptográfico SHA256 + RSA. y que esta llave tenga un tamaño de 2048 bits.

24.10.1. DESCRIPCIÓN DE LOS REQUISITOS Y PROCEDIMIENTOS PARA LA EMISIÓN DE LA FIRMA ELECTRONICA CERTIFICADA

Olimpia IT establece que el procedimiento interno para la expedición de las firmas electrónicas certificadas solicitadas se realiza según lo indicado a continuación.

24.10.1.1. SOLICITUD

- El solicitante deberá aceptar los términos y condiciones.
- Se podrá solicitar complementariamente documentación que contenga información biométrica o sociodemográfica del solicitante en caso de que Olimpia IT lo considere necesario.
- No se le permitirá al suscriptor usar el servicio emitido hasta que la fecha de inicio de vigencia inicie.

24.10.1.2. INFORMACIÓN A DILIGENCIAR EN LA APLICACIÓN

- Nombres y apellidos
- Tipo de documento de identidad
- Número documento identidad
- Departamento de residencia
- Ciudad de residencia
- Dirección de residencia
- Teléfono celular
- Correo electrónico
- Otro teléfono
- Correo electrónico alternativo
- Teléfono celular alternativo
- Número de documento alternativo

24.10.1.3. AUTENTICACIÓN DE LA IDENTIDAD

Según se describe en el Numeral 4.2.4 de esta DPC.

La validación de identidad da cumplimiento a los estándares técnicos *NIST Special Publication 800-63A*, en los niveles *Identity Assurance Level 1 – IAL1* (la validación se realiza con atributo proporcionado por el solicitante, quien lo confirma y cuenta con acuerdo de aceptación de dicho atributo) e *Identity Assurance Level 2 – IAL2* (existe evidencia de la identidad del solicitante).

24.10.1.4. DOCUMENTOS PARA SOLICITAR

- Imagen del documento de identidad (legible)
- Registro Único Tributario – RUT

24.10.1.5. LIMITACIONES PARA USO DE LOS SERVICIOS DE FIRMA ELECTRÓNICA CERTIFICADA

Las firmas electrónicas generadas en el ámbito de esta DPC pueden utilizarse con cualquier tipo de documentos en formato pdf, de acuerdo con las limitaciones de uso y restricciones derivadas de la presente DPC y lo dispuesto por el ordenamiento jurídico vigente.

Las firmas electrónicas garantizan la información de contacto del firmante de un documento, así como permiten comprobar la integridad del mismo, es decir que la información no ha sido alterada, aportando un atributo de seguridad adicional, como lo es la integridad de la información.

25. DISPOSITIVOS CRIPTOGRÁFICOS

Los lineamientos de los dispositivos criptográficos utilizados para la emisión de cada uno de los certificados digitales emitidos por Olimpia IT se encuentran descritos en los numerales 7.2.1 y 7.2.11 de la presente Declaración de Prácticas de Certificación.

26. SERVICIOS Y APLICACIONES PARA EL USO DE LOS SERVICIOS

26.1. VALIDEZ DE FIRMA

El servicio de validez de firma de Olimpia IT se encuentra expuesto en la página web y permite a los solicitantes, suscriptores, y partes confiantes entre otros, conocer la validez de una firma, así como la estampa de tiempo realizada por la Entidad de Certificación Digital, para lo cual el usuario debe realizar la carga de la firma en formato *.p7z y el sistema responde si la firma es validad o no. Los instaladores o drivers requeridos para el uso de token físico no son compatibles con sistemas operativos macOs.

26.2. OLIMPIA SIGN

El servicio de “Olimpia SIGN” es la aplicación de firma desarrollada por Olimpia IT para que sus suscriptores puedan realizar la firma de documentos cuando adquieren un token físico. Esta aplicación se puede descargar directamente desde la página web de la Entidad de Certificación Digital y solo funciona en equipos con sistema operativo Windows 10.

26.3. DRIVER TOKEN

Permite la interacción del sistema operativo con el dispositivo criptográfico token, facilita al usuario las operaciones de importación de certificados, autenticación en procesos de firmado y configuración de PIN de acceso.

26.4. GENERADOR CSR

Generador CSR: Software suministrado a los solicitantes de los servicios de certificación para facilitar la generación de una solicitud de certificado en formato PKCS#10.

26.5. EMISIÓN DE CERTIFICADOS DIGITALES POR SOLICITUDES PKCS#10

Olimpia IT podrá emitir certificados digitales a partir de una solicitud de certificación digital radicada por los suscriptores o terceros autorizados por los suscriptores, por la ley, o por entidad pública o privada competente.

En estos casos las peticiones radicadas deben cumplir con el estándar de solicitud de certificación *PKCS#10 - Formato de los mensajes enviados a una Autoridad de certificación para solicitar la certificación de una clave pública*. Y los suscriptores o terceros autorizados deberán garantizar que los parámetros utilizados para la llave pública son el algoritmo criptográfico SHA256 + RSA y que estas llaves tengan un tamaño de 2048 bits.

26.6. WEB SERVICES, APIS Y OTRAS FORMAS DE INTEGRACIÓN DE SOFTWARE

Dependiendo de las necesidades y requerimientos de los suscriptores sobre el uso de los certificados digitales, o el consumo de los servicios acreditados, Olimpia IT podrá poner a disposición de ellos web services, APIs y otras formas de integración de software, que podrán ser integradas en las plataformas o herramientas que para este fin tengan a disposición los suscriptores o terceros autorizados por los suscriptores, por la ley, o por entidad pública o privada competente.

27. UBICACIÓN

Dirección comercial y de notificación judicial: Calle 24 No. 7- 43 Piso 16 Edificio Siete24 Bogotá – Colombia.
Teléfono: (+57) 601 742 7878
Correo Electrónico: gerencia@olimpiait.com

28. POLÍTICA PARA RESOLVER PETICIONES, QUEJAS, RECLAMOS Y SUGERENCIAS

Olimpia IT pone a disposición del público en general y sus partes relacionadas para atender cualquier petición, queja o reclamo, los siguientes canales:

- Página web https://micertificado.olimpiait.com en donde se le dará una oportuna solución conforme a los tiempos establecidos.
- Línea de atención a PQRS: (+ 57 601) 742 7878

28.1. PROCEDIMIENTO PARA LA RESOLUCIÓN DE PETICIONES, QUEJAS, RECLAMOS Y SUGERENCIAS–PQRS-

Olimpia IT declara que los procedimientos para resolver las peticiones, quejas, reclamos y sugerencias se encuentran disponibles al público en la página web https://micertificado.olimpiait.com

29. PROPIEDAD DE OLIMPIA

El presente documento es de propiedad de Olimpia IT, así mismo, está protegido por las normas de derechos de autor, cualquier reproducción, distribución o modificación total o parcial a usuarios no autorizados o cualquier uso indebido de la información confidencial será considerado un delito conforme a lo establecido por el Código Penal y leyes vigentes del estado colombiano.

La presente versión de la Declaración de Prácticas de Certificación – DPC prevalecerá y tendrá prioridad sobre su versión en inglés y cualquier diferencia o controversia entre este documento y la versión en inglés, deberá resolverse de acuerdo con la interpretación y lectura de la presente DPC.