certicámara.

Código:	IDI-L-002
Fecha:	11/11/2026
Versión:	004
Etiquetado:	PÚBLICO

POLÍTICA DE CERTIFICACIÓN – CERTIFICADO DE FIRMA DIGITAL

USO EXCLUSIVO DE CERTICÁMARA S.A

certicámara.

Política de Certificación – Certificado de Firma Digital

certicámara.

Código:	IDI-L-002
Fecha:	11/11/2026
Versión:	004
Etiquetado:	PÚBLICO

POLÍTICA DE CERTIFICACIÓN – CERTIFICADO DE FIRMA DIGITAL

Contenido

1. INTRODUCCIÓN **5**
1.1 Nombre e identificación del documento 5
1.2 Alcance 5
1.3 Procedimiento para la actualización o aprobación de la política 6
1.4 Responsabilidades de publicación 6
2. IDENTIFICACIÓN DE POLÍTICAS **7**
2.1 Criterio de identificación de las políticas 7
2.2 OID de las políticas 7
2.3 Tipos de certificados ECD Certicámara 7
2.3.1 Certificado de Pertenencia a Empresa / Entidad en dispositivos locales y/o centralizados. 7
2.3.2 Certificado de Representación de Empresa / Entidad en dispositivos locales y/o centralizados. 9
2.3.3 Certificado de Titular de Función Pública en dispositivos locales y/o centralizados. 11
2.3.4 Certificado de Profesional Titulado en dispositivos locales y/o centralizados. 13
2.3.5 Certificado digital Persona Natural en dispositivos locales y/o centralizados. 15
2.3.6 Certificado digital Persona Natural / Persona Jurídica 16
3. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO **18**
3.1 Solicitud de certificado 18
3.1.1 ¿Quién puede presentar una solicitud de certificado? 21
3.2 Emisión de certificados 21
3.2.1 Acciones de la CA durante la emisión del certificado 21
3.2.2 Notificación al suscriptor por parte de la CA de emisión de certificado 22
3.2.3 Restauración de la clave privada 22
3.3 Entrega del certificado digital a los suscriptores por medio físico 22
3.3.1 Cubrimiento 22
3.3.2 Requisitos de entrega 22
3.3.3 Tiempo de gestión de entrega – Certificados Físicos 23
3.3.4 Tiempo de descarga 23
3.4 Aceptación del certificado 23
3.4.1 Publicación del certificado por la CA 24
3.4.2 Notificación de emisión de certificados por parte de la CA a otras entidades 24
3.5 Uso de pares de claves y certificados 24
3.5.1 Generación e instalación de pares de claves 24

USO EXCLUSIVO DE CERTICÁMARA S.A

3.5.2 Uso de certificado y clave privada del suscriptor 24
3.5.3 Uso del certificado y la clave pública del usuario de confianza 24
3.5.4 Método de destrucción de clave privada 25
3.6 Renovación del certificado 25
3.6.1 Tiempos para la renovación 25
3.6.2 ¿Quién puede solicitar la renovación? 25
3.6.3 Tramitación de solicitudes de renovación de certificados 25
3.6.4 Notificación de emisión de nuevo certificado al suscriptor 26
3.7 Renovación de llave de certificado 26
3.8 Modificación del certificado 26
3.9 Revocación y suspensión de certificados 26
3.9.1 Causales para la revocación 26
3.9.2 ¿Quién puede solicitar la revocación? 27
3.9.3 Procedimiento para solicitud de revocación 28
3.9.4 Período de gracia de la solicitud de revocación 28
3.9.5 Frecuencia de emisión de CRL 28
3.9.6 Disponibilidad de verificación de estado/revocación en línea 29
3.9.7 Requisitos de verificación de revocación en línea 29
3.9.8 Circunstancias de suspensión 29
3.10 Reposición de Certificados de firma Digital 29
3.10.1 Causales para la Reposición 30
3.11 Características de los certificados 31
3.11.1 Características operativas 31
3.11.2 Disponibilidad del servicio 32
3.12 Fin de la suscripción 32
3.13 Custodia y recuperación de llaves 32
3.13.1 Política y prácticas de custodia y recuperación de llaves 32
4. USOS DE LOS CERTIFICADOS 32
4.1 Usos apropiados del certificado digital 32
4.2 Usos prohibidos del certificado 33
4.3 Vigencia de los certificados 34
5. CARACTERÍSTICAS DE LOS CERTIFICADOS 34
5.1 Certificado digital en token físico 34
5.2 Certificado en token virtual 35
5.3 Certificado digital en PKCS#10 36
6. OBLIGACIONES Y RESPONSABILIDADES DE LOS INTERVINIENTES 37

USO EXCLUSIVO DE CERTICÁMARA S.A

7. DERECHOS DE LOS INTERVINIENTES **37**
8. CONFIABILIDAD DE LAS FIRMAS Y LOS CERTIFICADOS DIGITALES. **37**
9. CONFIDENCIALIDAD DE LA INFORMACIÓN **39**
9.1 Alcance de la información confidencial 39
9.2 Información fuera del alcance de la información confidencial 39
9.3 Responsabilidad de proteger la información confidencial 40
9.4 Tratamiento de Datos personales 40
9.5 Revelación en virtud de un proceso judicial o administrativo 41
10. TARIFAS DEL SERVICIO DE EMISIÓN DE CERTIFICADOS DIGITALES **42**
11. MODELOS Y MINUTAS DE LOS DOCUMENTOS DE TÉRMINOS Y CONDICIONES **44**
12. NORMATIVIDAD ASOCIADA **44**
13. CONTROL DE CAMBIOS **45**

USO EXCLUSIVO DE CERTICÁMARA S.A

POLÍTICA DE CERTIFICACIÓN – CERTIFICADO DE FIRMA DIGITAL

1. INTRODUCCIÓN

La presente Política de Certificación (PC) constituye la manifestación pública de la Entidad de Certificación Digital Abierta, en la cual se establecen las normas y prácticas adoptadas para el servicio de certificados de firma digitales que presta la Sociedad Cameral de Certificación Digital Certicámara S.A.

La presente **Política de Certificación (PC)** se ha elaborado siguiendo las recomendaciones de los estándares internacionales, tal como el RFC 3647, Adicionalmente, cumple con la legislación colombiana vigente, específicamente la Ley 527 de 1999, el Decreto Ley 019 de 2012, el Decreto 333 de 2014, y cualquier reglamento que los modifique o complemente.

Las condiciones de carácter general y aplicables a todos los servicios de certificación digital de Certicámara se encuentran en la **Declaración de Prácticas de Certificación (DPC)**. Esta DPC está disponible en la sección de "marco normativo" de nuestra página web.

1.1 Nombre e identificación del documento

Certicámara para la prestación de su servicio de certificado de firma digital, establece la siguiente información para el presente documento.

Nombre:	Políticas de Certificación – Certificado de firma digital
Fecha de publicación:	11/11/2026
Versión:	004
Código:	IDI-L-002
Ubicación:	https://web.certicamara.com/marco-normativo

1.2 Alcance

Este documento establece las normas y reglas a seguir por la Entidad certificadora **Certicámara** para ofrecer el servicio de Certificado de firma digital tal como se encuentra establecido en el certificado de acreditación expedido por el Organismo Nacional de Acreditación de Colombia ONAC en su página web https://onac.org.co/directorio3/index.php/acreditaciones/16-ECD-002

USO EXCLUSIVO DE CERTICÁMARA S.A

1.3 Procedimiento para la actualización o aprobación de la política

La actualización de la Política de Certificación se llevará a cabo cuando así lo exijan los requerimientos legales, normativos y/o aquellos aplicables a los servicios del alcance de este documento.

En este proceso, los responsables de las diversas áreas que participan en la prestación de los servicios comprendidos en el alcance se reunirán con el fin de evaluar las modificaciones a realizar. La aprobación final de dichos cambios se da por parte del Presidente.

La responsabilidad de gestionar la actualización de la PC en el sitio web de Certicámara, específicamente en el enlace https://web.certicamara.com/marco-normativo, corresponde al Director de Procesos.

1.4 Responsabilidades de publicación

Es obligación para la Entidad de Certificación publicar la información relativa a sus prácticas, sus certificados y el estado actualizado de dichos certificados. Las publicaciones que realice Certicámara de toda información clasificada como pública, se anunciará en su respectiva página Web de la siguiente manera:

a) La lista de Certificados Revocados (CRL), se encuentra disponible en formato CRL V2, en el repositorio de la CA raíz.
b) Las Políticas de Certificados de la CA raíz, se podrán ubicar en la versión actualizada del presente documento.
c) La última versión del presente documento es pública y se encuentra disponible en el sitio Web de la CA raíz https://web.certicamara.com/marco-normativo
d) Las llaves públicas de los certificados emitidos por la CA subordinada se encuentran disponibles en el repositorio público LDAP, en formato X.509 v3 y en la dirección https://ar.certicamara.com:8443/Search/, los cuales podrán ser consultados por un parámetro de búsqueda.
e) Los datos de contacto de Certicámara se encuentran descritos en la página web https://web.certicamara.com
f) Los instructivos de operaciones de la CA raíz y toda la información considerada relevante a los certificados emitidos se encuentra en la dirección https://web.certicamara.com/soporte/manuales-de-soporte-tecnico .
g) Estado de revocación de certificados OCSP, se encuentra disponible para su consulta vía web en la dirección http://ocsp.certicamara.com, http://ocsp.certicamara.co y http://ocsp4096.certicamara.co.

USO EXCLUSIVO DE CERTICÁMARA S.A

2. IDENTIFICACIÓN DE POLÍTICAS

2.1 Criterio de identificación de las políticas

Cada uno de los certificados emitidos por Certicámara cuenta con un identificador OID relacionado en la extensión, el cual se detalla en las propiedades del certificado. A través de este identificador OID se vincula el certificado emitido con la Política de Certificación correspondiente, que confirma el cumplimiento de las condiciones descritas.

2.2 OID de las políticas

Cada tipo de certificado se identificará por un OID (Object Identifier) único, incluido en el certificado como identificador de política, dentro de las propiedades del certificado.

OID	Tipo de Política
1.3.6.1.4.1.23267.50.1.1	Certificado de Pertenencia a Empresa / Entidad en dispositivos locales y/o centralizados
1.3.6.1.4.1.23267.50.1.2	Certificado de Representación de Empresa / Entidad en dispositivos locales y/o centralizados
1.3.6.1.4.1.23267.50.1.3	Certificado de Titular de Función Pública en dispositivos locales y/o centralizados
1.3.6.1.4.1.23267.50.1.4	Certificado de Profesional Titulado en dispositivos locales y/o centralizados
1.3.6.1.4.1.23267.50.1.5	Certificado digital persona natural en dispositivos locales y/o centralizados
1.3.6.1.4.1.23267.50.1.8.5	Certificado digital persona natural PKCS10
1.3.6.1.4.1.23267.50.1.8.4	Certificado digital persona jurídica PKCS10

2.3 Tipos de certificados ECD Certicámara

Buscando satisfacer las diferentes necesidades que surgen en el contexto del uso creciente de las tecnologías de la información y comunicaciones, Certicámara genera diversos tipos de **certificados digitales**, los cuales se emiten con una vigencia máxima de dos (2) años, de acuerdo con lo establecido en los Criterios de Específicos de Acreditación vigente lo cual se encuentra de conformidad en el numeral de Ciclo de vida de los certificados del presente documento.

2.3.1 Certificado de Pertenencia a Empresa / Entidad en dispositivos locales y/o centralizados.

Se expide a personas naturales nacionales o extranjeras que se han identificado plenamente ante Certicámara con documento(s) de identidad válido(s) y vigente(s)

USO EXCLUSIVO DE CERTICÁMARA S.A

expedidos por la autoridad competente de la República de Colombia, o con documento(s) equivalente(s) expedido(s) por la autoridad competente de cualquier Estado Extranjero, y permite identificarla como persona natural vinculándola como perteneciente a una determinada organización empresarial o entidad del Estado, pero sin que tenga la representación legal de la misma o facultad de comprometerla jurídicamente.

Los suscriptores de este tipo de certificados digitales son:

1) La persona natural que logre acreditar suficientemente, a juicio de Certicámara, que existe una relación jurídica, laboral o de cualquier otra índole, con la persona jurídica o entidad del Estado que vaya a aparecer en el certificado digital.

2) La persona jurídica que figura en el certificado digital.

Requisitos de expedición

- El solicitante debe diligenciar el formulario disponible en el sitio web, a través del enlace https://ventadigital.certicamara.com. Al ingresar la información correspondiente, el usuario garantiza que esta es **veraz, íntegra y actualizada**.

- Para este caso, debe adjuntar en el formulario el certificado laboral emitido por la empresa solicitante no mayor a 30 días, con membrete de la entidad, debe contener nombre, número de documento, cargo y firmado por el área de recursos humanos o representante legal. Para el caso de revisor fiscal o apoderado se acepta el certificado de existencia y representación legal no mayor a treinta (30) días, donde aparezca el nombramiento.

- Como parte del proceso, se debe **validar la identidad** del solicitante mediante los mecanismos dispuestos por Certicámara al momento de realizar la solicitud.

Nota: La información domiciliaria del suscriptor (dirección, municipio y departamento) no será objeto de validación externa. Bajo el principio de buena fe, los datos ingresados por el usuario en el formulario de solicitud se considerarán una declaración oficial.

Información publicada que aparecerá en el certificado digital:

1. Common Name (CN)	Nombre(s) y Apellido(s) del Suscriptor
2. Serial Number	Identificador Único del Certificado Digital
3. Organization (O)	Razón Social de la Organización del Suscriptor
4. 1.3.6.1.4.1.23267.2.1	Código del convenio
5. 1.3.6.1.4.1.23267.2.2	Número de Documento de Identificación del Suscriptor

USO EXCLUSIVO DE CERTICÁMARA S.A

6. 1.3.6.1.4.1.23267.2.3	Número de Identificación de la Organización
7. Title (T)	Nombre del Cargo del Suscriptor en la Organización
8. Organizational Unit (OU)	Convenio - Vigencia del Certificado – Token Físico / Virtual
9. Street Address (STREET)	Dirección de la Organización
10. Country (C)	País de Emisión del Certificado
11. State Or Province Name (S)	Ciudad / Municipio de la Organización del Suscriptor
12. Locality (L)	Departamento de la Organización del Suscriptor
13. Surname (SN)	Apellido (s) del Suscriptor
14. Given Name (G)	Primer Nombre de Suscriptor

2.3.2 Certificado de Representación de Empresa / Entidad en dispositivos locales y/o centralizados.

Se expide a personas naturales nacionales o extranjeras que se han identificado plenamente ante Certicámara con documento(s) de identidad válido(s) y vigente(s) expedidos por la autoridad competente de la República de Colombia, o con documento(s) equivalente(s) expedido(s) por la autoridad competente de cualquier Estado Extranjero, vinculándose con la calidad de representante legal de una persona jurídica o Entidad del Estado.

Los Certificados de Representación de Empresa/Entidad certifican la identidad de una persona natural vinculándola con la representación legal de una persona jurídica, una Entidad del Estado.

Los Certificados de Representación de Empresa/Entidad tienen como suscriptor tanto a la persona natural que actúa en nombre y representación legal de una persona jurídica, como a la persona jurídica representada que figura igualmente en el certificado digital.

Requisitos de expedición

- El solicitante debe diligenciar el formulario disponible en el sitio web, a través del enlace https://ventadigital.certicamara.com. Al ingresar la información correspondiente, el usuario garantiza que esta es **veraz, íntegra y actualizada**.

- Para este caso, debe adjuntar en el formulario el documento que acredita la existencia y representación legal de la empresa o entidad: Para empresas o entidades registradas en cámara de comercio se requiere Certificado de existencia y representación legal no mayor a 30 días y para empresas o entidades no registradas en cámara de comercio Certificado expedido por un

USO EXCLUSIVO DE CERTICAMARA S.A

organismo de control, tales como: Superintendencia financiera, Superintendencia de industria y comercio, Ministerio de educación, Alcaldías, entre otras. Para consorcios y uniones temporales el documento que acredita la existencia y representación legal es el acta de conformación consorcial o unión temporal.

- Como parte del proceso, se debe **validar la identidad** del solicitante mediante los mecanismos dispuestos por Certicámara al momento de realizar la solicitud.

Nota: La información domiciliaria del suscriptor (dirección, municipio y departamento) no será objeto de validación externa. Bajo el principio de buena fe, los datos ingresados por el usuario en el formulario de solicitud se considerarán una declaración oficial.

Información publicada que aparecerá en el certificado digital:

1. Common Name (CN)	Nombre(s) y Apellido(s) del Suscriptor (Representante Legal)
2. Serial Number	Identificador Único del Certificado Digital
3. Organization (O)	Razón Social de la Organización a la que pertenece el Suscriptor
4. 1.3.6.1.4.1.23267.2.1	Código del Convenio
5. 1.3.6.1.4.1.23267.2.2	Número de Documento de Identificación del Suscriptor
6. 1.3.6.1.4.1.23267.2.3	Número de Identificación de la Organización
7. Title (T)	Nombre del Cargo del Suscriptor en la Organización
8. Organizational Unit (OU)	Convenio - Vigencia del Certificado – Token Físico / Virtual
9. Street Address (STREET)	Dirección de la Organización
10. Country (C)	País de Emisión del Certificado
11. State Or Province Name (S)	Ciudad / Municipio de la Organización del Suscriptor
12. Locality (L)	Departamento de la Organización del Suscriptor
13. Surname (SN)	Apellido (s) del Suscriptor
14. Given Name (G)	Primer Nombre de Suscriptor

2.3.3 Certificado de Titular de Función Pública en dispositivos locales y/o centralizados.

Se expide a personas naturales nacionales o extranjeras que se han identificado plenamente ante Certicámara con documento(s) de identidad válido(s) y vigente(s)

USO EXCLUSIVO DE CERTICÁMARA S.A

expedidos por la autoridad competente de la República de Colombia, o con documento(s) equivalente(s) expedido(s) por la autoridad competente de cualquier Estado Extranjero, permitiendo identificar como persona natural y vinculándola como funcionario público perteneciente a una entidad del Estado en la República de Colombia.

Los suscriptores de este tipo de certificados digitales son las personas naturales que logren acreditar suficientemente, a juicio de Certicámara, que han obtenido el nombramiento como funcionarios públicos, trabajadores oficiales o son titulares legales del cargo de notario, cónsul, juez de la república, magistrado, registrador, servidor público en la República de Colombia y contratistas designados o autorizados por una entidad pública.

El Certificado de Titular de Función Pública no garantiza la calidad, idoneidad o cumplimiento efectivo de las funciones a cargo de su titular. Certicámara no garantiza que el suscriptor del certificado de Titular de Función Pública haya sido sujeto de sanciones disciplinarias, administrativas, penales o de cualquier otra clase en la República de Colombia o en el exterior. Para la emisión de Certificado de Titular de Función Pública Certicámara se basa en la documentación exhibida y las declaraciones efectuadas por el suscriptor al momento de solicitar el servicio. Mientras la ley o las normas aplicables no establezcan lo contrario, la solicitud de Emisión del Certificado de Función Pública no es obligatoria para los Titulares de Función Pública. La emisión del Certificado de Función Pública no limita al suscriptor para solicitar otros certificados digitales.

Requisitos de expedición

- El solicitante debe diligenciar el formulario disponible en el sitio web, a través del enlace https://ventadigital.certicamara.com. Al ingresar la información correspondiente, el usuario garantiza que esta es **veraz, íntegra y actualizada**.

- Para este caso, debe adjuntar en el formulario el documento que vincula a la persona con la entidad pública: Algunos de los siguientes documentos que acredita la vinculación son: Acta de posesión (artículo 2.2.5.1.8 del Decreto 1083 de 2015), Certificado laboral, Certificados de la Registraduría para alcaldes, Contrato de prestación de servicios Contratistas / captura de pantalla SECOPII.

- Como parte del proceso, se debe **validar la identidad** del solicitante mediante los mecanismos dispuestos por Certicámara al momento de realizar la solicitud.

Nota: La información domiciliaria del suscriptor (dirección, municipio y departamento) no será objeto de validación externa. Bajo el principio de buena fe, los datos ingresados por el usuario en el formulario de solicitud se considerarán una declaración oficial.

USO EXCLUSIVO DE CERTICÁMARA S.A

POLÍTICA DE CERTIFICACIÓN – CERTIFICADO DE FIRMA DIGITAL

Información publicada que aparecerá en el certificado digital:

1. Common Name (CN)	Nombre(s) y Apellido(s) del Suscriptor
2. Serial Number	Identificador Único del Certificado Digital
3. Organization (O)	Razón Social de la Organización a la que pertenece el Suscriptor
4. 1.3.6.1.4.1.23267.2.1	Código del Convenio
5. 1.3.6.1.4.1.23267.2.2	Número de Documento de Identificación del Suscriptor
6. 1.3.6.1.4.1.23267.2.3	Número de Identificación de la Organización
7. Title (T)	Nombre del Cargo del Suscriptor en la Organización
8. Organizational Unit (OU)	Convenio / Convenio - Vigencia del Certificado – Token Físico / Virtual *(Depende del convenio seleccionada para la solicitud)*
9. Street Address (STREET)	Dirección de la Organización
10. Country (C)	País de Emisión del Certificado
11. State Or Province Name (S)	Ciudad / Municipio de la Organización del Suscriptor
12. Locality (L)	Municipio / Ciudad de la organización Suscriptor
13. Surname (SN)	Apellido (s) del Suscriptor
14. Given Name (G)	Primer Nombre de Suscriptor

2.3.4 Certificado de Profesional Titulado en dispositivos locales y/o centralizados.

Se expide a personas naturales nacionales o extranjeras que se han identificado plenamente ante Certicámara con documento(s) de identidad válido(s) y vigente(s) expedidos por la autoridad competente de la República de Colombia, o con documento(s) equivalente(s) expedido(s) por la autoridad competente de cualquier Estado Extranjero identificándose como persona natural vinculándola a la obtención de un título profesional debidamente reconocido en la República de Colombia o en un Estado Extranjero, y que hayan obtenido el correspondiente registro, licencia, colegiatura o tarjeta profesional requerida para el ejercicio de su profesión en la República de Colombia o en un Estado Extranjero.

Los suscriptores de este tipo de certificados digitales son las personas naturales que logren acreditar suficientemente, a juicio de Certicámara, que ha obtenido un título profesional debidamente reconocido en la República de Colombia o en un Estado Extranjero convalidado por el Ministerio de Educación Nacional, y que han obtenido el correspondiente registro, licencia, colegiatura o tarjeta profesional requerido para el ejercicio de su profesión en la República de Colombia o en un Estado Extranjero.

USO EXCLUSIVO DE CERTICAMARA S.A

certicámara.

Código:	IDI-L-002
Fecha:	11/11/2026
Versión:	004
Etiquetado:	PÚBLICO

POLÍTICA DE CERTIFICACIÓN – CERTIFICADO DE FIRMA DIGITAL

Requisitos de expedición

- El solicitante debe diligenciar el formulario disponible en el sitio web, a través del enlace https://ventadigital.certicamara.com. Al ingresar la información correspondiente, el usuario garantiza que esta es **veraz, íntegra y actualizada**.

- Cuando no sea posible validar la profesión en fuentes confiables, se solicitará al interesado el Certificado de Profesional Titulado. Este requisito aplica para niveles técnico, tecnólogo y universitario (según la Ley 30 de 1992 y el concepto 059881 del Departamento Administrativo de la Función Pública). Se aceptarán documentos tales como: tarjeta profesional, diploma, acta de grado, matrícula profesional o certificación de título. En caso de títulos obtenidos en el exterior, el documento deberá estar debidamente convalidado por el Ministerio de Educación Nacional.
- Como parte del proceso, se debe **validar la identidad** del solicitante mediante los mecanismos dispuestos por Certicámara al momento de realizar la solicitud.

Nota: La información domiciliaria del suscriptor (dirección, municipio y departamento) no será objeto de validación externa. Bajo el principio de buena fe, los datos ingresados por el usuario en el formulario de solicitud se considerarán una declaración oficial.

Información publicada que aparecerá en el certificado digital:

1. Common Name (CN)	Nombre(s) y Apellido(s) del Suscriptor
2. Serial Number	Identificador Unico del Certificado Digital
3. Organization (O)	Razón Social de la Organización a la que pertenece el Suscriptor / Nombre(s) y Apellido(s) del Suscriptor. *(Depende de la información ingresada en la solicitud*)
4. 1.3.6.1.4.1.23267.2.1	Código del Convenio
5. 1.3.6.1.4.1.23267.2.2	Número de Documento de Identificación del Suscriptor
6. 1.3.6.1.4.1.23267.2.3	Número de Identificación de la Organización / Número de identificación del Suscriptor con o sin dígito de verificación (*Depende de la información ingresada en la solicitud*)
7. Title (T)	Nombre de la Profesión del Suscriptor
8. Organizational Unit (OU)	Convenio - Vigencia del Certificado – Token Físico / Virtual
9. Street Address (STREET)	Dirección de la Organización / Dirección del Suscriptor (*Depende de la información ingresada en la solicitud*)
10. Country (C)	País de Emisión del Certificado

USO EXCLUSIVO DE CERTICAMARA S.A

11. State Or Province Name (S)	Ciudad / Municipio de la organización / Suscriptor (*Depende de la información ingresada en la solicitud*)
12. Locality (L)	Departamento de la Organización / Suscriptor (*Depende de la información ingresada en la solicitud*)
13. Surname (SN)	Apellido (s) del Suscriptor
14. Given Name (G)	Primer Nombre de Suscriptor

2.3.5 Certificado digital Persona Natural en dispositivos locales y/o centralizados.

Se expide a personas naturales nacionales o extranjeras que se han identificado plenamente ante Certicámara con documento(s) de identidad válido(s) y vigente(s) expedidos por la autoridad competente de la República de Colombia, o con documento(s) equivalente(s) expedido(s) por la autoridad competente de cualquier estado Extranjero.

Los Certificados de Persona Natural tienen como suscriptor a la persona natural que, actuando en nombre propio, acredite su identidad ante Certicámara. Este certificado se puede utilizar a través de un dispositivo físico (token USB) conectado al equipo o de un dispositivo virtual (en la nube) mediante conexión a Internet.

Requisitos de expedición

- El solicitante debe diligenciar el formulario disponible en el sitio web, a través del enlace https://ventadigital.certicamara.com. Al ingresar la información correspondiente, el usuario garantiza que esta es **veraz, íntegra y actualizada**.

- Como parte del proceso, se debe **validar la identidad** del solicitante mediante los mecanismos dispuestos por Certicámara al momento de realizar la solicitud.

Nota: La información domiciliaria del suscriptor (dirección, municipio y departamento) no será objeto de validación externa. Bajo el principio de buena fe, los datos ingresados por el usuario en el formulario de solicitud se considerarán una declaración oficial.

Información publicada que aparecerá en el certificado digital:

1. Common Name (CN)	Nombre(s) y Apellido(s) del Suscriptor
2. Serial Number	Identificador Único del Certificado Digital
3. Organization (O)	Nombre(s) y Apellido(s) del Suscriptor
4. 1.3.6.1.4.1.23267.2.1	Código del Convenio

USO EXCLUSIVO DE CERTICÁMARA S.A

5. 1.3.6.1.4.1.23267.2.2	Número de Documento de Identificación del Suscriptor
6. 1.3.6.1.4.1.23267.2.3	Número de Documento de Identificación del Suscriptor (con o sin digito verificación) *(Depende de la información ingresada en la solicitud*)
7. Title (T)	Persona Natural
8. Organizational Unit (OU)	Convenio - Vigencia del Certificado – Token Físico / Virtual
9. Street Address (STREET)	Dirección del Suscriptor
10. Country (C)	País de Emisión del Certificado
11. State Or Province Name (S)	Ciudad / Municipio del Suscriptor
12. Locality (L)	Departamento del Suscriptor
13. Surname (SN)	Apellido (s) del Suscriptor
14. Given Name (G)	Primer Nombre de Suscriptor

2.3.6 Certificado digital Persona Natural / Persona Jurídica

Se expide a personas naturales nacionales, extranjeras o personas jurídicas que se han identificado plenamente ante Certicámara con documento(s) de identidad válido(s) y vigente(s) expedidos por la autoridad competente de la República de Colombia, o con documento(s) equivalente(s) expedido(s) por la autoridad competente de cualquier estado Extranjero.

Los Certificados de Persona Natural / Persona Jurídica tienen como suscriptor a la persona natural o persona jurídica que actuando en nombre propio logre acreditar suficientemente, a juicio de Certicámara, su identidad a través de la exhibición de la documentación que así lo acredite.

Requisitos de expedición

- El solicitante debe diligenciar el formulario disponible en el sitio web, a través del enlace https://ventadigital.certicamara.com. Al ingresar la información correspondiente, el usuario garantiza que esta es **veraz, íntegra y actualizada**.

- Para este caso, debe adjuntar en el formulario el documento que acredita la existencia y representación legal de la empresa o entidad: Para empresas o entidades registradas en cámara de comercio se requiere Certificado de existencia y representación legal no mayor a 30 días y para empresas o entidades no registradas en cámara de comercio Certificado expedido por un

USO EXCLUSIVO DE CERTICÁMARA S.A

organismo de control, tales como: Superintendencia financiera, Superintendencia de industria y comercio, Ministerio de educación, Alcaldías, entre otras. Para consorcios y uniones temporales el documento que acredita la existencia y representación legal es el acta de conformación consorcial o unión temporal.

- Como parte del proceso, se debe **validar la identidad** del solicitante mediante los mecanismos dispuestos por Certicámara al momento de realizar la solicitud.

Nota: La información domiciliaria del suscriptor (dirección, municipio y departamento) no será objeto de validación externa. Bajo el principio de buena fe, los datos ingresados por el usuario en el formulario de solicitud se considerarán una declaración oficial.

Nota: El formato PKCS#10 es una estructura estándar de solicitud que contiene la petición formal y las claves necesarias para integrar y generar la firma digital directamente desde los sistemas propios de la organización o suscriptor. Este tipo de certificado está orientado a entidades o personas que requieren gestionar el ciclo de firma dentro de su propia infraestructura tecnológica. Para su expedición, el cliente es responsable de garantizar la veracidad de la información ingresada, mientras que Certicámara S.A. verificará que los datos proporcionados coincidan exactamente con la documentación aportada.

Información publicada que aparecerá en el certificado digital:

1. Common Name (CN)	Razón social de la Organización
2. Serial Number	Identificador Único del Certificado Digital
3. Organization (O)	Razón social de la Organización
4. 1.3.6.1.4.1.23267.2.2	Número de Identificación del Suscriptor
5. 1.3.6.1.4.1.23267.2.3	Número de Identificación de la Organización
6. Organizational Unit (OU)	Uso del Certificado
7. Street Address (STREET)	Dirección del Suscriptor
8. Country (C)	País de Emisión del Certificado
9. State Or Province Name (S)	Ciudad / Municipio de la Organización
10. Locality (L)	Departamento del Suscriptor
11. Surname (SN)	Apellido (s) del Suscriptor
12. Given Name (G)	Primer Nombre de Suscriptor

USO EXCLUSIVO DE CERTICÁMARA S.A

3. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

3.1 Solicitud de certificado

El proceso de solicitud se podrá llevar a cabo por alguna de las siguientes formas:

1. Presencial dirigiéndose ante las instalaciones de Certicámara.
2. Por el Contact Center
3. O por cualquier otro medio electrónico que disponga Certicámara.

Las solicitudes recibidas serán objeto de revisión por parte de la Autoridad de Registro (RA), en concordancia con los criterios específicos de acreditación establecidos por ONAC y aquellos definidos internamente por Certicámara. Dicha revisión se llevará a cabo en un plazo máximo de dos (2) días hábiles, contados a partir de la recepción de la totalidad de los documentos requeridos, el comprobante de pago y la validación satisfactoria de la identidad del solicitante. Una vez completada la revisión, las solicitudes serán remitidas a la Autoridad de Certificación (CA) para su emisión, la cual se efectuará en un término máximo de un (1) día hábil.

De acuerdo con las políticas internas de Certicámara S.A., toda la documentación proporcionada por el solicitante debe estar en idioma español. Si un documento se presenta en otro idioma, deberá acompañarse de una traducción oficial realizada por un traductor avalado por el Ministerio de Relaciones Exteriores. La documentación se conservará según las tablas de retención documental de Certicámara. La información del solicitante no se hará pública sin su consentimiento explícito.

Al utilizar y suscribir electrónicamente el certificado de firma digital de CerticámaraS.A., el solicitante acepta plenamente y sin reservas los siguientes documentos, que hacen parte integral de esta DPC y del contrato de prestación de servicios: los Términos y Condiciones del servicio, las Declaraciones y Compromisos sobre prevención de LA/FT/FPDAM Y C/ST , la Política de Certificación (PC), el tratamiento de datos personales y las políticas organizacionales de Certicámara S.A., disponibles en el sitio web de Certicámara.

Los Términos y Condiciones del servicio de certificación de firma digital son aplicables desde el momento en que el solicitante expresa su interés en adquirir el certificado y continúan vigentes durante la validez del mismo, junto con las condiciones generales de contratación del servicio.

Los solicitantes deben tener en cuenta lo siguiente antes de solicitar cualquier servicio a Certicámara S.A.:

a) **Lectura de Documentación:** Haber leído íntegramente los Términos y Condiciones del servicio de certificación de firma digital, las Declaraciones y Compromisos de prevención LA/FT/FPDAM Y C/ST, la presente Declaración de Prácticas de Certificación (DPC), la Política de Certificación (PC) y el tratamiento de datos personales.

USO EXCLUSIVO DE CERTICÁMARA S.A

b) **Verificación de Información:** Verificar la información mencionada por Certicámara S.A. para tomar una decisión informada sobre la solicitud del certificado de firma digital, en cumplimiento de la Ley 527 de 1999, Decreto 019 de 2012, Ley 1341 de 2009, Ley 1978 de 2019, Ley 1581 de 2012, Decreto 1074 de 2015, Decreto 358 de 2020, Decreto 1538 de 2020 y Decreto 620 de 2020.

c) **Suministro de información:** El cliente deberá indicar información de contacto actualizada y disponible que permita contactarlo para llevar a cabo los procesos asociados a la emisión de firma digital, evitando que estas tengan configuraciones de restricción, filtros de seguridad o cualquier otro ajuste o autorización adicional en sus dominios. El correo electrónico y número de teléfono móvil vinculado a un dispositivo suministrado en la solicitud serán los canales de comunicación autorizados para el envío de notificaciones asociados al proceso, por lo tanto con el envío de estos datos se autoriza el envío para este fin.

d) **Asignación de contraseñas:** Para la utilización del certificado digital, es necesario que el titular asigne una contraseña. A continuación se detallan las implicaciones en caso de olvido o pérdida de la misma:

- **Token Virtual:** el restablecimiento de contraseña se podrá realizar a través de la página web, en el enlace https://ventadigital.certicamara.com/reset-password sin costo adicional hasta por diez (10) veces; posterior a este número de solicitudes implica costo asociado.
- **Token Físico:** debido a que Certicámara S.A. no dispone de mecanismos para su recuperación, dado que queda de forma local, será indispensable la adquisición de un nuevo certificado, lo cual implica un costo asociado.

El titular deberá recordar y custodiar la contraseña de forma segura. Dicha contraseña es el medio exclusivo para acceder al certificado emitido.

e) **Conocimiento Técnico y de Seguridad:** Conocer los requerimientos tecnológicos y de seguridad para el uso del certificado de firma digital. Estar informado sobre las características del certificado de Certicámara S.A., su nivel de confiabilidad, los límites de responsabilidad, las obligaciones del cliente y las medidas de seguridad necesarias para su utilización.

f) **Derecho de No Prestación del Servicio:** Tener en cuenta que Certicámara S.A. puede reservarse el derecho de no emitir un certificado de firma digital por condiciones técnicas, sin que esto genere responsabilidad alguna.

g) **Validación de Identidad por Certicámara S.A.:** Certicámara S.A., como Entidad de Certificación Digital Abierta, realizará previamente la comprobación de identidad utilizando fuentes confiables y datos proporcionados por terceros con contrato vigente para tal fin.

USO EXCLUSIVO DE CERTICÁMARA S.A.

h) **Solicitud de Documentos Adicionales:** Certicámara se reserva el derecho de solicitar documentos adicionales o copias de los exigidos en el formulario de solicitud cuando lo considere necesario para verificar la identidad o cualquier calidad del solicitante. También podrá exonerar la presentación de documentos si la identidad del solicitante ha sido suficientemente verificada por otros medios.
Estos documentos adicionales podrán incluir (sin limitación):

- Referencias comerciales de la empresa.
- Referencias personales del solicitante.
- Certificaciones bancarias.
- Licencia de conducción válida.
- Libreta militar.
- Documento de afiliación al régimen de seguridad social en salud.
- Documento de afiliación a la empresa administradora de riesgos profesionales.
- Otros documentos que permitan verificar la identidad o facultades del suscriptor o de la entidad para la emisión de cualquier tipo de certificado.

i) **Consulta de Bases de Datos:** Certicámara podrá consultar bases de datos de información de identidad de entidades públicas o privadas para realizar las validaciones necesarias para emitir el certificado digital.

j) **Cumplimiento SAGRILAFT:** Consultará las bases de datos necesarias para cumplir con el SAGRILAFT, previa aceptación por parte del solicitante de las Declaraciones y Compromisos de prevención de LA/FT/FPDAM Y C/ST, publicadas en el sitio web de Certicámara S.A.

k) **Vigencia de Certificados:** Los certificados de firma digital se emitirán con una vigencia máxima de dos (2) años.

l) **Negación o Declinación de la Solicitud:** Certicámara S.A. podrá negar la expedición de un certificado digital cuando no se encuentre dentro del alcance de la acreditación otorgada por ONAC, por incumplimiento de la ley y/o cuando a su juicio atente contra su buen nombre como ECD. En este caso, no habrá lugar a subsanación por parte del usuario. Si Certicámara decide negar o declinar la solicitud, notificará al solicitante por correo electrónico, indicando los motivos.

m) **Desarrollo para Mac OS:** Actualmente, Certicámara se encuentra desarrollando la infraestructura para la compatibilidad en la emisión de certificados de firma digital para el sistema operativo Mac OS.

3.1.1 ¿Quién puede presentar una solicitud de certificado?

La solicitud de un certificado digital podrá ser efectuada por cualquier persona natural en pleno ejercicio de su capacidad jurídica, así como por personas jurídicas a través de su

USO EXCLUSIVO DE CERTICÁMARA S.A.

representante legal, un apoderado, un empleado o un tercero debidamente autorizado, siempre que se acredite dicha calidad con los documentos exigidos por la Autoridad de Registro (RA). En el caso de menores de edad, la solicitud de firma digital deberá ser presentada por su representante, adjuntando el documento de identidad del menor y el documento que acredite la representación conforme a la normativa civil vigente.

3.2 Emisión de certificados

3.2.1 Acciones de la CA durante la emisión del certificado

Una vez que la solicitud de emisión ha sido aprobada, la Autoridad de Certificación (CA) procede a generar el certificado correspondiente, el cual se asocia a un par de claves y es firmado digitalmente mediante el certificado de la CA, que forma parte de la cadena de confianza Certicámara.

La emisión de los certificados requiere la autorización de la solicitud por parte del sistema de la CA Subordinada. Tras la aprobación, los certificados son emitidos de manera segura y se ponen a disposición del suscriptor.

En el proceso de emisión, la CA Subordinada realiza las siguientes acciones:

- Implementa un procedimiento de generación de certificados que establece un vínculo seguro entre el certificado y la información de registro, incluyendo la clave pública certificada.
- Garantiza la protección de la confidencialidad e integridad de los datos de registro.
- La vigencia de todos los certificados inicia una vez el titular realiza la descarga / activación de la firma digital bajo ninguna circunstancia se emitirá un certificado con un periodo de validez que preceda a la fecha actual.

3.2.2 Notificación al suscriptor por parte de la CA de emisión de certificado

El suscriptor sabrá sobre la emisión efectiva del certificado por medio de una notificación enviada a su correo electrónico registrado.

3.2.3 Restauración de la clave privada

Para el caso de certificados de firma digital en dispositivo virtual, Certicámara ha implementado mecanismos seguros que permiten al suscriptor gestionar el cambio o restablecimiento de su contraseña, a través del contact center, el cual no genera costo asociado, hasta máximo diez (10) solicitudes, posteriormente, esto tendrá un costo. Para el caso de certificado de firma digital en dispositivo físico, el suscriptor podrá realizar el cambio de ésta cuando lo requiera directamente desde el aplicativo, en caso de pérdida u olvido de la contraseña, deberá realizar el proceso de adquisición de una nueva firma.

USO EXCLUSIVO DE CERTICÁMARA S.A

3.3 Entrega del certificado digital a los suscriptores por medio físico

3.3.1 Cubrimiento

La entrega de los certificados digitales se efectuará de acuerdo con la matriz de cobertura del servicio de entrega del operador logístico que mantenga un contrato vigente con Certicámara para tal fin, o mediante entrega directa por parte de un colaborador del área logística de Certicámara. En ambos escenarios, se hará entrega del dispositivo físico y en el correo electrónico de aprobación enviado al titular se compartirá el enlace al instructivo para la descarga.

3.3.2 Requisitos de entrega

El dispositivo físico será entregado por el operador logístico en la dirección reportada o podrá ser retirado por el suscriptor en las instalaciones de Certicámara, de acuerdo con lo indicado en el formulario de solicitud. Cuando el titular autorice a un tercero para reclamar el dispositivo en las instalaciones, este deberá presentar en físico el formato de tercero autorizado, el cual podrá descargar desde la página de Certicámara en el siguiente enlace: https://web.certicamara.com/soporte/formatos

El formato denominado “Tercero autorizado” debe estar debidamente diligenciado y firmado por ambas partes. Adicionalmente, deberán presentar fotocopias de los documentos de identidad, tanto del titular como del tercero autorizado.

La guía del operador logístico servirá como evidencia del acuse de recibo del dispositivo físico y para el caso de entrega en las instalaciones de Certicámara se contará con la documentación formal de la entrega.

3.3.3 Tiempo de gestión de entrega – Certificados Físicos

En Bogotá y municipios cercanos al perímetro urbano el tiempo de entrega desde la emisión del certificado hasta la entrega al solicitante, será de dos (2) días hábiles aproximadamente.

Los tiempos de entrega estimados desde la emisión del certificado son:

- **Bogotá y municipios cercanos:** Aproximadamente dos (2) días hábiles.
- **Ciudades capitales de departamento:** Aproximadamente dos (2) a cuatro (4) días hábiles.
- **Otros municipios:** Aproximadamente cuatro (4) a cinco (5) días hábiles.
- **Municipios o destinos especiales:** Aproximadamente seis (6) a quince (15) días hábiles.

En caso de imposibilidad de entrega, se realizará un segundo intento. Si este también falla, el operador logístico devolverá el certificado digital a las instalaciones de Certicámara.

USO EXCLUSIVO DE CERTICÁMARA S.A

Si la entrega no es posible por causas atribuibles al suscriptor, Certicámara o el operador logístico lo contactarán para coordinar la entrega. Sin embargo, es importante tener en cuenta que si no se logra coordinar una fecha de entrega o recolección en un plazo de noventa (90) días calendario a partir de la fecha de emisión, se considerará que el bien ha sido abandonado. En este caso, Certicámara procederá a bloquear el enlace de descarga.

Si después de este período el titular requiere la firma digital, deberá iniciar un nuevo proceso de solicitud, lo cual generará costo según las políticas de Certicámara.

3.3.4 Tiempo de descarga

Una vez aprobada la solicitud de certificado de firma, el titular recibirá automáticamente un correo electrónico con el enlace de descarga, un manual detallado y recomendaciones importantes, para lo cual dispondrá de noventa (90) días calendario para realizar este proceso, de lo contrario, se entenderá que el bien ha sido abandonado y Certicámara procederá al bloqueo definitivo del enlace. En tal caso, si desea obtener el certificado de firma, deberá iniciar un nuevo proceso de solicitud, lo cual generará un costo según las tarifas de Certicámara.

3.4 Aceptación del certificado

No se exige una confirmación por parte del suscriptor como aceptación del servicio recibido. Se entiende que el servicio de certificado de firma digital es aceptado a partir del momento en que se solicita su expedición. En consecuencia, si la información contenida en la comunicación de activación del servicio no se ajusta a su estado actual o no fue proporcionada correctamente, el suscriptor deberá informar a Certicámara a través de cualquiera de los canales de atención disponibles para llevar a cabo los trámites de corrección pertinentes en caso que apliquen.

3.4.1 Publicación del certificado por la CA

La autoridad de registro, a través de su servidor, incorporará las claves públicas de los certificados digitales emitidos por la autoridad de certificación subordinada en la estructura de directorio LDAP (Lightweight Directory Access Protocol) de la PKI en el instante en que el certificado sea emitido.

En caso de presentarse alguna dificultad técnica que obstaculice su publicación, ésta se llevará a cabo dentro del mes siguiente a la fecha de emisión del certificado, de acuerdo con las conclusiones del análisis técnico que haya impedido su publicación oportuna.

3.4.2 *Notificación de emisión de certificados por parte de la CA a otras entidades*

Certicámara dispone de un repositorio de certificados digitales LDAP, a través del cual entidades, organismos gubernamentales, empresas del sector privado y demás partes interesadas tienen la posibilidad de consultar la emisión de los certificados. Este repositorio

USO EXCLUSIVO DE CERTICÁMARA S.A

se encuentra accesible en la siguiente dirección web: https://ar.certicamara.com:8443/Search/. La información se publica en este repositorio una vez que el certificado ha sido emitido.

3.5 Uso de pares de claves y certificados

3.5.1 Generación e instalación de pares de claves

La CA Raíz, genera el par de claves (Pública y Privada) utilizando un dispositivo de hardware criptográfico (HSM) que cumple con los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica de autoridad de certificación normalizado, de acuerdo con FIPS 140-3 Nivel 3 o superior nivel de seguridad, y la creación de llaves de la CA utiliza un algoritmo de generación de números seudo aleatorio.

3.5.2 Uso de certificado y clave privada del suscriptor

En la sección de *Identificación de políticas* de este documento se detallan los usos y finalidades para cada uno de los tipos de certificados emitidos por Certicámara.

3.5.3 Uso del certificado y la clave pública del usuario de confianza

Los terceros de buena fe únicamente podrán depositar su confianza en los certificados para los fines que se definen en la presente DPC, la PC y la normativa vigente.

Dichos terceros podrán llevar a cabo operaciones de clave pública de forma satisfactoria al confiar en los certificados emitidos por la cadena de confianza. No obstante, deberán actuar con diligencia y asumir la responsabilidad de verificar el estado de los certificados empleando los mecanismos que se detallan en esta DPC.

3.5.4 Método de destrucción de clave privada

El componente RSE de la infraestructura PKI de Certicámara eliminará la identidad asociada a la clave privada del certificado del suscriptor emitido en token virtual cuando expire su plazo de vigencia o haya sido revocado. La destrucción se realizará utilizando los comandos establecidos para borrar físicamente de la memoria del HSM la parte en la que estaba grabada la llave.

3.6 Renovación del certificado

3.6.1 Tiempos para la renovación

Certicámara notificará a sus suscriptores la terminación de la vigencia de su certificado digital con una antelación mínima de treinta (30) días calendario. Dicha notificación podrá efectuarse a través de correo electrónico a la dirección suministrada por el suscriptor o

USO EXCLUSIVO DE CERTICÁMARA S.A.

mediante cualquier otro medio de comunicación idóneo que Certicámara estime conveniente.

Sin embargo, no constituye una obligación para Certicámara asegurar la efectividad de la notificación sobre la finalización de la vigencia del certificado ni confirmar su recepción. Es deber del suscriptor conocer la fecha de expiración de su certificado digital y gestionar los trámites pertinentes ante Certicámara para la emisión de una nueva firma.

La renovación se entenderá como la emisión de un certificado digital nuevo, lo cual conlleva el registro de una solicitud renovada, la aceptación por parte del solicitante de los Términos y Condiciones del servicio de certificación de firma digital de Certicámara S.A., las Declaraciones y Compromisos en materia de prevención de LA/FT/FPDAM Y C/ST, la validación previa de la identidad y la generación de un nuevo par de claves.

3.6.2 ¿Quién puede solicitar la renovación?

Los suscriptores pueden solicitar la renovación de su certificado cuando esté próximo a vencer y deseen seguir utilizando un certificado digital que acredite las mismas condiciones aprobadas en el certificado actual.

3.6.3 Tramitación de solicitudes de renovación de certificados

Para efectos de la renovación de un certificado, el suscriptor deberá someterse nuevamente al proceso de validación de identidad. En consecuencia, el procedimiento de solicitud para la renovación de un certificado es idéntico al de la emisión por primera vez, con la salvedad de que no se requerirá adjuntar documentos a la solicitud, a menos que estos hayan expirado (en caso de que corresponda).

3.6.4 Notificación de emisión de nuevo certificado al suscriptor

La emisión efectiva del nuevo certificado será comunicada al suscriptor a través de un correo electrónico enviado a la dirección que haya suministrado.

3.7 Renovación de llave de certificado

Certicámara no contempla la renovación del par de claves dentro del ciclo de vida de sus certificados. En todos los casos, la emisión de un certificado implica la generación de un nuevo par de claves.

3.8 Modificación del certificado

Durante la vigencia de un certificado, no se permite la modificación o actualización de la información que contiene. Si se requiere cambiar algún dato del certificado emitido, será necesario revocar el certificado actual y solicitar la emisión de uno nuevo con los datos correctos y pagar el valor correspondiente.

USO EXCLUSIVO DE CERTICÁMARA S.A

3.9 Revocación y suspensión de certificados

La revocación de un certificado digital constituye el mecanismo por el cual se inhabilita un certificado emitido, dando por concluido su periodo de validez, bien sea por la expiración de su vigencia o al acontecer alguno de los eventos de revocación estipulados en la presente Declaración de Prácticas de Certificación. Es de aclarar que, la revocación no tiene ningún costo asociado.

Certicámara no maneja el estado de suspensión para sus certificados digitales.

3.9.1 Causales para la revocación

Certicámara revocará el certificado digital de conformidad con el artículo 37 de la Ley 527 de 1999, cuando tenga conocimiento de que se ha producido alguno de los siguientes hechos:

a) Por compromiso de la seguridad en cualquier motivo, modo, situación o circunstancia.
b) Compromiso o pérdida de la clave privada del suscriptor por cualquier motivo o circunstancia.
c) La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.
d) Por muerte del suscriptor.
e) Por incapacidad sobreviniente del suscriptor.
f) Por liquidación de la persona jurídica representada que consta en el certificado digital.
g) Por actualización de la información contenida en el certificado digital.
h) Por la confirmación de que alguna información o hecho contenido en el certificado digital es falso, así como la ocurrencia de hechos nuevos que provoquen que los datos originales no se adecuen a la realidad.
i) Por el compromiso de la clave privada de Certicámara o de su sistema de seguridad de manera tal que afecte la confiabilidad del certificado digital, por cualquier circunstancia, incluyendo las fortuitas.
j) Por el cese de actividades de Certicámara, salvo que los certificados digitales expedidos sean transferidos a otra Entidad de Certificación.
k) Por orden judicial o de entidad administrativa competente.
l) Pérdida, inutilización o compromiso de la seguridad del soporte físico del certificado digital que haya sido debidamente notificada a Certicámara.
m) Por la terminación del contrato de suscripción, de conformidad con las causales establecidas en el contrato y en esta Declaración de Prácticas de Certificación.
n) Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto de que se ponga en duda la confiabilidad del certificado digital.
o) Por el manejo indebido por parte del suscriptor del certificado digital.
p) Por el incumplimiento del suscriptor o de la persona jurídica que representa o a la que está vinculado a través del Contrato del servicio de Certificación Digital proporcionado por Certicámara.

USO EXCLUSIVO DE CERTICÁMARA S.A

q) Por reporte de cartera vencida ocasionado por el pago no efectuado de los servicios que le está proporcionando Certicámara.
r) Por solicitud de reintegro de dinero por el suscriptor, de conformidad con las políticas de reintegro definidas por Certicámara
s) Por causas asociadas a Certicámara en el marco del cumplimiento normativo o reglamentario.
t) Por la concurrencia de cualquier otra causa especificada en la presente Declaración de Prácticas de Certificación.
u) Por terminación del contrato laboral o vínculo contractual del suscriptor con la entidad para la cual se emitió el certificado de firma digital.

3.9.2 ¿Quién puede solicitar la revocación?

El suscriptor está facultado para solicitar la revocación voluntaria de su certificado digital en cualquier momento. Dicha solicitud podrá ser presentada de forma directa o a través de un tercero debidamente autorizado. El procedimiento de revocación del certificado digital no generará costo alguno.

Certicámara podrá, asimismo, tramitar la revocación de un certificado si llegase a tener conocimiento o sospecha fundada de un compromiso de la clave privada del suscriptor, o de cualquier otro evento determinante que haga imperativa la revocación del certificado. En aquellos casos en que la revocación sea atribuible a razones inherentes a Certicámara, se procederá a la emisión de un nuevo certificado al suscriptor bajo las mismas condiciones y por el tiempo restante de vigencia. Para este fin, se utilizará la documentación previamente suministrada, con el fin de no afectar la disponibilidad del servicio.

3.9.3 Procedimiento para solicitud de revocación

Certicámara ha dispuesto los siguientes medios para recibir solicitudes de revocación:

- **Virtual:** Diligenciar el formulario de solicitud dispuesto en la página web: https://web.certicamara.com/soporte/formatos y posteriormente, radicar la solicitud a través del siguiente enlace: https://pqr.certicámara.com/registrar. Este mecanismo aplica cuando el certificado digital esté asociado a una persona jurídica o entidad y el suscriptor pierda su vínculo con dicha organización.
- **En línea:** A través de la página web de Certicámara, registrando la solicitud en la siguiente URL: https://ventadigital.certicamara.com/revocar-certificado

Si lo considera necesario, Certicámara realizará averiguaciones, verificaciones y gestiones pertinentes, personalmente o a través de terceros, para comprobar la existencia de la causal de revocación invocada. Estas gestiones podrán incluir comunicación directa con el suscriptor y la presencia física del tercero que invoca la causal.

USO EXCLUSIVO DE CERTICÁMARA S.A

Certicámara validará la identidad del suscriptor que invoca la causal de revocación. Si la persona que expone dicha no es el suscriptor o en caso de serlo no puede identificarse satisfactoriamente, podrá dirigirse personalmente a las oficinas de Certicámara en horarios de oficina 8:00 a.m. – 05:00 p.m. de lunes a viernes, con la prueba de la existencia de la causal de revocación respectiva para los casos en que aplique, sin perjuicio de que Certicámara disponga de las medidas que se establezcan para la seguridad del Sistema de Certificación Digital. Se aclara que una vez se reciba la solicitud de revocación y se compruebe la veracidad de dicha solicitud, se procederá a la revocación del certificado, sin periodos de gracia para dichas revocaciones.

En los casos en que se solicite la revocación por terminación del contrato laboral o vínculo contractual del suscriptor con la entidad para la cual se emitió el certificado de firma digital, Certicámara solicitará al encargado o responsable de la entidad una certificación donde conste la finalización del vínculo laboral.

Si la causal es comprobada, Certicámara incorporará el certificado de firma digital en la Base de datos de certificados digitales revocados como certificado digital revocado. De lo contrario, dará por terminado el proceso de revocación del certificado digital. Se aclara que Certicámara no ofrece el servicio de suspensión de certificados a los suscriptores.

3.9.4 Período de gracia de la solicitud de revocación

Certicámara debe informar al suscriptor, dentro de las 24 horas siguientes, la cancelación del servicio o revocación de su(s) certificado(s), de conformidad con la normatividad vigente.

3.9.5 Frecuencia de emisión de CRL

Se realiza la publicación de la lista de Certificados Revocados de la CA Subordinada Certicámara (CRL) y CA SUB CERTICÁMARA (CRL) con vigencia de tres (3) días:

- La publicación se podrá realizar máximo ocho (8) horas después de la última revocación, en cualquier momento del día.

3.9.6 Disponibilidad de verificación de estado/revocación en línea

Las listas de certificados revocados (CRL) y el servicio de validación sobre el estado del certificado en línea (OCSP) estarán disponible para su consulta los 365 días del año, durante las 24 horas del día, los 7 días de la semana. Este servicio se prestará con un acuerdo de disponibilidad de 99.8%.

Certicámara cuenta con el histórico de certificados revocados desde el inicio de la prestación del servicio.

3.9.7 Requisitos de verificación de revocación en línea

USO EXCLUSIVO DE CERTICÁMARA S.A

La verificación sobre el estado del certificado en línea debe realizarse mediante el servicio de OCSP de conformidad con el RFC 6960. Mediante el uso de ese protocolo se determina el estado actual de un certificado electrónico sin requerir las CRLs.

Un cliente de OCSP envía una petición sobre el estado del certificado a la AV, la cual, tras consultar su Base de Datos, ofrece una respuesta sobre el estado del certificado vía HTTP por medio de las direcciones http://ocsp.certicamara.com, http://ocsp.certicamara.co y http://ocsp4096.certicamara.co

3.9.8 Circunstancias de suspensión

Certicámara no considera dentro del ciclo de vida de los certificados la suspensión temporal de los mismos, en todos los casos un certificado revocado no podrá ser reactivado nuevamente.

3.10 Reposición de Certificados de firma Digital

Certicámara establece que la reposición de un certificado digital consiste en generar un nuevo certificado, de acuerdo con lo definido en el ciclo de vida de la presente Declaración de Prácticas de Certificación, la Política de Certificación y los valores establecidos en estos documentos.

Ahora bien, para hacer efectiva la reposición, se deberá tener en cuenta que el certificado inicial que se haya adquirido, cumpla con las siguientes condiciones:

- La vigencia del certificado digital debe ser igual o superior a un (1) año
- No se realizarán reposiciones de certificados digitales que se encuentren a menos de noventa (90) días calendario de su vencimiento.
- Se deberá mantener la misma política de certificación con la que se emitió inicialmente.

Esta nueva generación del certificado de firma digital, tendrá un costo asociado a su valor comercial al momento de la emisión, conforme con las tarifas estipuladas en la Política de Certificación. En el evento donde se hayan pactado acuerdos comerciales con el cliente, las tarifas a aplicar serán las establecidas en dicho documento.

Para la gestión de la reposición de certificados de firmas digitales, se debe contar con los siguientes requisitos:

- El suscriptor deberá generar la solicitud en la página web de Certicámara: https://ventadigital.certicamara.com solicitando la reposición del certificado digital, teniendo en cuentas las condiciones mencionadas en el numeral anterior.
- El suscriptor deberá realizar la revocación del certificado de firma digital, según lo definido en el numeral *Procedimiento para solicitud de revocación* de este documento.

USO EXCLUSIVO DE CERTICÁMARA S.A.

Adicionalmente, existen casos excepcionales, en donde por acuerdos comerciales se establece la obligación de Certicámara, de mantener custodia y manejo de cupos; en este escenario se debe contar con una comunicación por parte del supervisor y/o administrador del contrato, en la que se solicite la reposición de certificados y se justifique bajo alguna de las siguientes causales:

- Cambio de titular
- Cambio de cargo
- Cambio tipo de certificado (Físico/Digital)

A continuación, el titular del contrato enviará esta solicitud al área de registro y uso a través del formulario disponible en la página web: ttps://pqrf.certicamara.com/registrar, dónde se debe indicar el certificado que debe ser objeto de la reposición así como la información correspondiente a la revocación respectiva. Con base en la información suministrada se procederá a realizar el control de los cupos de la entidad.

3.10.1 Causales para la Reposición

Certicámara realizará la reposición del certificado de firma digital de conformidad con el numeral anterior, cuando se presenten alguna de las siguientes causales:

i. Pérdida del dispositivo físico.
ii. Exposición del PIN (Contraseña/clave) del certificado digital.
iii. Cambio en la información del certificado digital previamente emitido. (No aplica cambio de número de identificación).
iv. Cambio en la razón social de la empresa independientemente que conserve el mismo NIT.
v. Por error imputable a Certicámara.

Adicionalmente, se procederá con la reposición, cuando se haya producido alguno de los siguientes hechos, los cuales se encuentran tipificados en el artículo 37 de la ley 527 de 1999:

i. Por muerte del suscriptor.
ii. Por incapacidad sobreviniente del suscriptor.
iii. Por actualización de la información contenida en el certificado digital.
iv. Por pérdida, inutilización o compromiso de la seguridad del soporte físico del certificado digital que haya sido debidamente notificada a Certicámara.

En el caso que la reposición sea por error imputable a Certicámara, esta podrá utilizar la información previamente entregada por el solicitante para la emisión del certificado, sin que sea necesario la generación de una nueva solicitud por el suscriptor y bajo las mismas condiciones pactadas inicialmente.

USO EXCLUSIVO DE CERTICÁMARA S.A

3.11 Características de los certificados

3.11.1 Características operativas

Para la validación de los certificados digitales se dispone de varios prestadores de Servicios de Validación que proporcionan información sobre el estado de los certificados emitidos por la jerarquía de certificación. Se trata de un servicio de validación en línea (Autoridad de Validación, AV) que implementa el Online Certificate Status Protocol siguiendo la RFC 6960. Mediante el uso de ese protocolo se determina el estado actual de un certificado electrónico sin requerir las CRLs.

Un cliente de OCSP envía una petición sobre el estado del certificado a la AV, la cual, tras consultar su Base de Datos, ofrece una respuesta sobre el estado del certificado vía HTTP por medio de las direcciones http://ocsp.certicamara.com, http://ocsp.certicamara.co y http://ocsp4096.certicamara.co

También se dispondrá de los archivos CRL correspondientes a cada CA publicados en el sitio web de Certicámara en las siguientes URLs:

- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara.crl?crl=crl
- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica.crl?crl=crl
- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_2014.crl?crl=crl
- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_2014.crl?crl=crl
- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_4096.crl?crl=crl
- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_409 6.crl?crl=crl

3.11.2 Disponibilidad del servicio

El servicio de comprobación de estado de certificados se encuentra disponibles las 24 horas, los 365 días del año, el nivel de disponibilidad mínimo será del 99.8%.

3.11.3 Funciones opcionales

Para hacer uso del Servicio de validación en línea consultando las direcciones http://ocsp.certicamara.com y http://ocsp4096.certicamara.co, es responsabilidad del tercero de buena fe disponer de un Cliente OCSP que cumpla la RFC 6960.

3.12 Fin de la suscripción

La finalización de la suscripción de un certificado se produce en los siguientes casos:

- Revocación del certificado por cualquiera de las causas de revocación expresadas en el siguiente documento.

USO EXCLUSIVO DE CERTICAMARA S.A

- Caducidad de la vigencia del certificado.

3.13 Custodia y recuperación de llaves

3.13.1 Política y prácticas de custodia y recuperación de llaves

La llave privada de la CA raíz se custodia por un dispositivo criptográfico HSM. Para el acceso al repositorio de llaves privadas se usa el esquema umbral límite (k, n) de Shamir tanto en software como en dispositivos criptográficos.

4. USOS DE LOS CERTIFICADOS

4.1 Usos apropiados del certificado digital

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.

Usos generales aplicables a los certificados digitales emitidos por Certicámara:

a) El **suscriptor** sólo puede dar a los certificados digitales los usos que se especifiquen en el contrato que suscriba con Certicámara de manera individual, los permitidos en esta **Declaración de Prácticas de Certificación, en las Políticas de Certificación** y aquellos permitidos en virtud de la Ley 527 de 1999 y el Decreto 1074 de 2015 (que compila al Decreto 333 de 2014). El contrato celebrado con el suscriptor podrá limitar el alcance de los usos, en función del entorno dentro del cual se está utilizando el certificado digital, o de las características especiales del proyecto que se está desarrollando. Cualquier otro uso que se le dé se considerará una violación de esta **Declaración de Prácticas de Certificación** y **Políticas de Certificación** constituirá una causal de revocación del **certificado digital** y de terminación del contrato con el **suscriptor**, sin perjuicio de las acciones penales o civiles a las que haya lugar.

b) El **suscriptor** considera y acepta que los productos y servicios que se anuncian son tal y como se ofrecen individualmente, que los certificados digitales principalmente certifican la identidad de la persona natural que aparece como suscriptor del servicio, que no existe ningún tipo de información implícita que implique servicios o prestaciones adicionales a los expresamente mencionados y que la utilización de los mismos es de su exclusiva responsabilidad teniendo en cuenta lo previsto en la Ley 527 de 1999 y el Decreto 1074 de 2015 (que compila al Decreto 333 de 2014).

c) El uso del certificado digital y los mensajes de datos que se firmen digitalmente con él, incluyendo transacciones electrónicas monetarias, sin importar su monto, son TOTAL responsabilidad del correspondiente suscriptor y, por lo tanto, Certicámara no tiene responsabilidad alguna sobre la verificación o fe pública de los mensajes de datos firmados, pues no conoce ni tiene obligación legal de conocer los mensajes firmados digitalmente o el monto de las transacciones que se efectúen con el certificado digital en sistemas de transacciones electrónicas de terceros. En general, Certicámara como entidad de Certificación Digital Abierta y Tercero de Confianza no compromete su responsabilidad en el uso que realice el suscriptor de los certificados

USO EXCLUSIVO DE CERTICÁMARA S.A

de firma digital, por lo tanto, no se tienen límites financieros aplicables en este sentido. Para tal efecto, el suscriptor deberá dar cumplimiento a sus deberes previstos en la Ley 527 de 1999 y el Decreto 1074 de 2015 (que compila al Decreto 333 de 2014), así como deberá atender la carga de responsabilidad que le imponen dichas normas.

4.2 Usos prohibidos del certificado

a) Los certificados digitales no podrán ser utilizados bajo ninguna circunstancia para fines o en operaciones ilícitas bajo cualquier régimen legal del mundo.
b) Se encuentra terminantemente prohibido cualquier uso de los certificados digitales que resulte contrario a la legislación colombiana, a los convenios internacionales suscritos por el Estado colombiano, a las normas supranacionales, a las buenas costumbres, a las sanas prácticas comerciales, y a todo lo contenido en esta Declaración de prácticas de certificación y en los contratos que se firmen entre Certicámara y el Suscriptor.
c) Se encuentra prohibido cualquier uso de los certificados digitales cuya finalidad sea violar cualquier derecho de propiedad intelectual de Certicámara o de terceros.
d) El soporte físico del certificado digital suministrado por Certicámara (si aplica) sólo puede ser utilizado dentro del contexto del Sistema de Certificación Digital. No podrá incorporarse en el soporte físico suministrado información diferente a aquella expresamente autorizada por Certicámara, ni usarse por fuera del Sistema de Certificación Digital.

4.3 Vigencia de los certificados

Certicámara expide diversos tipos de certificados digitales, los cuales se emiten con una vigencia máxima de dos (2) años que equivalen a 730 días, de acuerdo con la normatividad vigente.

5. CARACTERÍSTICAS DE LOS CERTIFICADOS

5.1 Certificado digital en token físico (dispositivos locales)

Corresponde a un dispositivo físico que se conecta al puerto USB del equipo de cómputo, el cual contiene el certificado digital y el par de llaves pública y privada. También está protegido por una clave fija para ejecutar su uso. No se requiere tener el equipo conectado al servicio de Internet para dar uso del mismo. Es responsabilidad del cliente la salvaguarda del dispositivo entregado, así como el manejo de la respectiva contraseña.

Certicámara comprometida con el manejo del impacto ambiental de los dispositivos de almacenamiento físico entregados a los clientes, pondrá a disposición de los usuarios:

1. Una nueva opción de entrega de Token físico el cual ha pasado por un proceso de reacondicionamiento de revisión física y funcional de altos estándares.
2. Se ha practicado un proceso de borrado seguro para eliminar el certificado

USO EXCLUSIVO DE CERTICÁMARA S.A.

digital anterior, de acuerdo con las funcionalidades del aplicativo provistas por el proveedor.

3. Este nuevo proceso garantiza que el Token físico cumple con las condiciones de usabilidad adecuadas y de funcionamiento tecnológico.

i. Aspectos técnicos

- ✔ Longitud de la llave privada de 4096 bits.
- ✔ Algoritmo de firma de certificado con hash RSA-SHA-2 256 -2056
- ✔ Compatibilidad con API y estándares (PKCS#11, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE, MS minidriver, CNG)
- ✔ Capacidad de memoria 80K. Con retención de al menos 10 años.
- ✔ Dimensiones: 5110 - 16.4mm*8.5mm*40.2mm.
- ✔ Compatible con especificaciones ISO 7816-1 y 4.
- ✔ Plástico rígido moldeado, cierre antimanipulación.
- ✔ Windows (Server 2008/R2, Server 2012/R2, 7, 8 y 10).
- ✔ Linux.
- ✔ Conector USB.

ii. Cuidados del dispositivo criptográfico

- ✔ Temperatura de funcionamiento 0 °C a 70 °C (32 °F a 158 °F)
- ✔ Temperatura de almacenamiento -40°C a 85 °C (-40°F a 185 °F)
- ✔ Intervalo de humedad 0- 100% sin condensación
- ✔ Certificación de resistencia al agua IPX7 – IEC 60529

Para la asignación de las claves por parte del suscriptor, se debe tener en cuenta las siguientes recomendaciones y cuidados para su protección:

- ✔ La contraseña debe ser de uso personal y no debe ser transferida a un tercero.
- ✔ Almacene su contraseña en lugares seguros, se recomienda memorizarla para evitar que otras personas la conozcan.
- ✔ No dejar conectado el dispositivo al equipo cuando no esté en uso.
- ✔ Desconectar de manera correcta el dispositivo
- ✔ Evitar golpes y caídas.
- ✔ Utilizar las aplicaciones entregadas por Certicámara para el uso de su certificado.

iii. Riesgos asociados

Los riesgos a los cuales estarían expuestos los dispositivos criptográficos utilizados:

USO EXCLUSIVO DE CERTICÁMARA S.A

✔ Fluctuaciones fuera de los rangos de funcionamiento normales medioambientales, como, por ejemplo: voltaje y temperatura.
✔ Intentos de acceso físico por fuera de la ficha técnica del fabricante no autorizado

Para conocer el nivel de riesgos asociados de los dispositivos criptográficos, se puede consultar el documento NIST.FIPS.140-3

5.2 Certificado en token virtual (dispositivos centralizados)

Corresponde a una infraestructura dispuesta como servicio en la cual se custodian los certificados digitales emitidos junto con su par de llaves en la infraestructura tecnológica de Certicámara, los cuales están asociados a un nombre de usuario y contraseña dados por el titular del certificado. Para la realización de su uso se debe disponer de una conexión activa de Internet.

i. Características

✔ Llave privada de 4096 bits.
✔ Algoritmo de firma de certificado con hash SHA256.
✔ Certificados X.509 v3.
✔ Almacenamiento en infraestructura que cumple FIPS 140-3 Nivel 3.
✔ Firma de archivos firmado el hash del documento (no requiere el envío del documento para proteger su confidencialidad).
✔ Acceso de red al dominio *.certicamara.com por el puerto 443.
✔ Componente de firma que permita el consumo de Certitoken
✔ Java mínimo en Ver 7
✔ Windows 7 o superior
✔ Framework 4.0 o superior
✔ RSE: Doble factor de autenticación

ii. Cuidados del dispositivo

Cuidados físicos y tecnológicos del datacenter donde se encuentra ubicado el HSM, para asegurar su adecuado funcionamiento, donde se puede encontrar controles de humedad, electricidad, acceso no autorizado, detectores contra incendio, seguridad biométrica de acceso al rack y a la zona del datacenter otros.
Para la asignación de las claves por parte del suscriptor, se debe tener en cuenta las siguientes recomendaciones y cuidados para su protección:

✔ La contraseña debe contener entre ocho (8) y doce (12) caracteres alfanuméricos, utilizando mayúsculas y minúsculas.
✔ La contraseña debe ser de uso personal y no debe ser transferida a un tercero.
✔ Almacene su contraseña en lugares seguros, se recomienda memorizar para evitar

USO EXCLUSIVO DE CERTICÁMARA S.A

que otras personas la conozcan.

iii. Riesgos asociados

Para el certificado en token virtual los riesgos a los cuales se encuentra expuesto son aquellos en los que aspectos medioambientales impidan el adecuado funcionamiento del datacenter donde se encuentra instalado el HSM.

En temas lógicos, los riesgos asociados se encuentran definidos por ataques cibernéticos que impidan el acceso y/o disponibilidad respectiva.

5.3 Certificado digital en PKCS#10

Corresponde a un estándar de generación de llaves públicas y privadas desde la infraestructura del firmante y por responsabilidad del mismo, con el propósito de ser certificadas por una entidad de certificación digital.

i. Características

- ✔ Llave pública de 4096 bits.
- ✔ Algoritmo de firma de certificado con hash SHA256.
- ✔ Llave pública firmada en formato *.CER conforme a la cadena de confianza de Certicámara.
- ✔ Emisión haciendo uso del estándar PKCS#10.
- ✔ Generar un Certificate Signing Request – CSR – en formato PKCS#10.
- ✔ Capacidad de recibir y usar la llave pública en formato .CER.

ii. Cuidados del dispositivo

Cuidados físicos y tecnológicos del datacenter donde se encuentra ubicado el HSM, para asegurar su adecuado funcionamiento, donde se puede encontrar controles de humedad, electricidad, acceso no autorizado, detectores contra incendio, seguridad biométrica de acceso al rack y a la zona del datacenter otros.

Para la asignación de las claves por parte del suscriptor, se debe tener en cuenta las siguientes recomendaciones y cuidados para su protección:

- ✔ La contraseña debe contener entre ocho (8) y doce (12) caracteres alfanuméricos, utilizando mayúsculas y minúsculas.
- ✔ La contraseña debe ser de uso personal y no debe ser transferida a un tercero.
- ✔ Almacene su contraseña en lugares seguros, se recomienda memorizarla para evitar que otras personas la conozcan.

USO EXCLUSIVO DE CERTICÁMARA S.A

iii. Riesgos asociados

Para el certificado en PKCS#10 los riesgos a los cuales se encuentra expuesto son aquellos en los que aspectos medioambientales impidan el adecuado funcionamiento del datacenter donde se encuentra instalado el HSM.

En temas lógicos, los riesgos asociados se encuentran definidos por ataques cibernéticos que impidan el acceso y/o disponibilidad respectiva.

6. OBLIGACIONES Y RESPONSABILIDADES DE LOS INTERVINIENTES

Las obligaciones y responsabilidades de los intervinientes se encuentran definidos en el documento de Declaración de Prácticas de Certificación en el numeral 9.5.

7. DERECHOS DE LOS INTERVINIENTES

Los derechos de los intervinientes se encuentran definidos en el documento de Declaración de Prácticas de Certificación en el numeral 9.7.

8. CONFIABILIDAD DE LAS FIRMAS Y LOS CERTIFICADOS DIGITALES.

El Sistema de Certificación Digital de Certicámara es un sistema construido con base en el cumplimiento estricto de sus políticas y procedimientos. La confianza que genera en sus intervinientes depende en forma directa del cumplimiento de los mismos. Todos los intervinientes deberán prestar toda la colaboración a su alcance para la generación de la confianza propia del sistema de certificación digital, siguiendo en todo momento las políticas y procedimientos establecidos.

a. Confiabilidad de las firmas digitales

La parte confiante, antes de poder confiar en una firma digital certificada por Certicámara, tiene el deber de seguir estrictamente las indicaciones que se especifican a continuación:

1. La parte confiante debe determinar la confiabilidad del certificado digital, conforme a lo estipulado en la sección siguiente.
2. La parte confiante debe verificar que la firma digital se haya creado dentro del periodo de vigencia del certificado digital y que el mismo no se encuentra revocado.
3. La parte confiante deberá tener en cuenta todas las demás políticas y procedimientos que rigen la actividad de Certicámara y que se especifican en su Declaración de Prácticas de Certificación.

b. Confiabilidad del certificado digital

La parte confiante debe seguir las indicaciones que a continuación se enumeran si pretende confiar en un certificado digital emitido por Certicámara:

- La parte confiante debe verificar que el certificado digital no haya expirado, de

USO EXCLUSIVO DE CERTICÁMARA S.A

conformidad con la fecha de vigencia que figura en el mismo.

- La parte confiante debe verificar que el certificado digital no se encuentra en la base de datos de certificados digitales revocados de Certicámara que se encuentra publicada en el sitio de Internet de Certicámara. En todo caso, y sin ninguna excepción, está prohibido determinar el estado de revocación de un certificado digital con base en información distinta a la de la base de datos de certificados digitales revocados.
- La confiabilidad del certificado digital depende de que el mismo se encuentre firmado digitalmente por Certicámara. La parte confiante puede verificar la firma digital de Certicámara verificándola con el certificado raíz, que contiene la clave pública de Certicámara, el cual se encuentra disponible en el sitio de Internet de Certicámara.

El uso de un certificado digital por cualquier interviniente en el Sistema de Certificación Digital está sujeto al seguimiento estricto de las normas contenidas en:

- El contrato celebrado con cada suscriptor del servicio de certificación digital, que contiene las condiciones generales de contratación de los servicios de certificación digital de Certicámara S.A. cuyo clausulado se encuentra en el formulario de solicitud (https://ventadigital.certicamara.com/).

- La presente Declaración de Prácticas de Certificación con relación a las firmas digitales emitidas mediante sus certificados digitales. La parte confiante deberá tenerlas en cuenta siempre que pretenda confiar en un certificado digital.

9. CONFIDENCIALIDAD DE LA INFORMACIÓN

Certicámara, se compromete a proteger todos los datos a los que tenga acceso como consecuencia de su actividad como entidad de certificación.

No obstante, Certicámara se reserva el derecho a revelar a los empleados y consultores, externos o internos, los datos confidenciales necesarios para realizar las actividades dentro de Certicámara. En este caso los empleados y/o consultores son informados sobre las obligaciones de confidencialidad.

Estas obligaciones no se aplican si la información calificada como “confidencial” es requerida por los Tribunales u órganos administrativos competentes o impuesta por una ley, evento en el cual se revelará la información confidencial dada por el suscriptor, de acuerdo con las normas vigentes.

La información confidencial del suscriptor de servicios de certificación digital podrá ser expuesta por solicitud de éste, en su calidad de propietario de esta.

9.1 Alcance de la información confidencial

Se considera información confidencial:

USO EXCLUSIVO DE CERTICÁMARA S.A

- Documentos que tengan información relacionada con la administración, gestión y control de la infraestructura PKI.
- La información de negocio suministrada por sus proveedores y otras personas con las que Certicámara tiene el deber de guardar secreto establecida legal o convencionalmente.
- Información resultante de las consultas realizadas en las centrales de riesgo u otras entidades privadas o del sector público.
- Información laboral que contenga datos relacionados del suscriptor.
- Toda la información que sea remitida a Certicámara y que haya sido etiquetada como “Confidencial” por el remitente.

9.2 Información fuera del alcance de la información confidencial

Se considera información no confidencial:

- Contenido de los certificados emitidos
- Lista de Certificados Revocados (CRL)
- La clave pública de la AC Raíz y AC Subordinada
- La declaración de prácticas de certificación
- Políticas organizacionales

9.3 Responsabilidad de proteger la información confidencial

Como entidad de certificación digital abierta acreditada, Certicámara S.A. ha establecido un compromiso para salvaguardar la confidencialidad, integridad y disponibilidad de toda la información que gestiona en el marco de los servicios de certificación. Esto incluye, pero no se limita a, la información personal de los suscriptores, las claves privadas, los datos de los certificados digitales y cualquier otra información que, por su naturaleza, deba ser tratada con la máxima discreción.

Para garantizar la protección de esta información, nos comprometemos a:

- Implementar y mantener estrictas políticas y procedimientos de seguridad de la información que cumplan con los estándares nacionales e internacionales, incluyendo los requisitos de la ONAC y la legislación vigente en materia de protección de datos.
- Capacitar continuamente a todo nuestro personal sobre las mejores prácticas en seguridad de la información, la importancia de la confidencialidad y sus responsabilidades individuales en la protección de los datos.
- Utilizar tecnologías y sistemas de seguridad robustos y actualizados, incluyendo cifrado de datos, controles de acceso estrictos, sistemas de detección de intrusiones y mecanismos de respaldo y recuperación de información.
- Limitar el acceso a la información confidencial únicamente al personal autorizado que requiera dicha información para el desempeño de sus funciones. Todo acceso es monitoreado y registrado.
- Establecer acuerdos de confidencialidad con todos nuestros empleados, contratistas y terceros que puedan tener acceso a información sensible.

USO EXCLUSIVO DE CERTICÁMARA S.A

- Gestionar de forma segura y responsable la información de las claves privadas de los suscriptores, asegurando su protección contra el acceso no autorizado, la divulgación, la alteración o la destrucción.
- Notificar de manera oportuna a las autoridades competentes y a los afectados sobre cualquier incidente de seguridad que comprometa la confidencialidad, integridad o disponibilidad de la información, de acuerdo con los marcos regulatorios aplicables.
- Realizar auditorías internas y externas de forma regular para evaluar la efectividad de nuestros controles de seguridad y asegurar el cumplimiento continuo con nuestras políticas y los requisitos regulatorios.

La confianza de nuestros usuarios es fundamental. Por ello, la protección de su información confidencial es un pilar esencial de nuestras operaciones.

9.4 Tratamiento de Datos personales

En Certicámara S.A el tratamiento de datos personales se rige por los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, en estricto cumplimiento con la legislación colombiana vigente en materia de protección de datos, incluyendo la Ley 1581 de 2012 y sus decretos reglamentarios.

Para garantizar el adecuado tratamiento de los datos personales que Certicámara S.A recolecta o tiene acceso se compromete a:

- Recolectar los datos personales únicamente cuando sea necesario y pertinente para la prestación de sus servicios de certificación digital, la verificación de identidad, la emisión, renovación, suspensión o revocación de certificados, y el cumplimiento de nuestras obligaciones legales y contractuales.
- Informar a los titulares de los datos sobre la finalidad específica para la cual sus datos serán recolectados y tratados, obteniendo su consentimiento previo, expreso e informado, a menos que la ley exija o permita lo contrario.
- Utilizar los datos personales exclusivamente para las finalidades informadas y autorizadas, absteniéndose de utilizarlos para propósitos distintos a los establecidos en su política de tratamiento de datos personales, autorizaciones o aviso de privacidad dispuestos al momento de la recolección.
- Garantizar la veracidad, actualización y completitud de la información que reposa en nuestras bases de datos, implementando los mecanismos necesarios para que los titulares puedan actualizar o rectificar sus datos.
- Implementar medidas técnicas, humanas y administrativas rigurosas para salvaguardar la seguridad de los datos personales, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Permitir el acceso de los titulares a sus datos personales y a la información sobre el tratamiento de los mismos, así como facilitar el ejercicio de sus derechos a conocer, actualizar, rectificar y suprimir sus datos, y a revocar la autorización otorgada.

USO EXCLUSIVO DE CERTICÁMARA S.A

- Mantener la confidencialidad de los datos personales, incluso después de finalizada la relación con el titular, salvo en los casos en que la información sea requerida por una autoridad judicial o administrativa en ejercicio de sus funciones legales.
- No transferir ni comunicar datos personales a terceros sin la autorización expresa del titular, salvo en los casos que la ley lo permita o lo exija para el cumplimiento de una función legal o contractual.

Certicámara tiene a disposición del solicitante y suscriptor, la política de tratamiento de datos personales en la página web, en la siguiente ubicación en línea, https://web.certicamara.com/politicas

9.5 Revelación en virtud de un proceso judicial o administrativo

La información no está a disposición ni es revelada a individuos, entidades o procesos que no se encuentran autorizados. Solo podrá ser revelada cuando medie requerimiento de una autoridad judicial o administrativa, en ejercicio de sus funciones.

De acuerdo con lo establecido en la ley 1581 de 2012, no es necesaria la autorización del titular cuando la información sea requerida por una entidad pública o administrativa en el ejercicio de sus funciones legales o por orden judicial.

10. TARIFAS DEL SERVICIO DE EMISIÓN DE CERTIFICADOS DIGITALES

El valor que fija CERTICÁMARA para la prestación de los Servicios de Certificados de firma digital se establece de acuerdo con las condiciones contractuales acordadas con los solicitantes del servicio y serán adecuadamente calculados y liquidados por CERTICÁMARA.

La tarifa para la prestación del servicio de Certificados de firma digital será establecida con base en las necesidades del cliente y de acuerdo con la volumetría de certificados de firma digital que el cliente requiera, teniendo como precios venta público base de:

Tipo de dispositivo	Política	Cantidad	Tarifa		Tarifa Renovación / Reposición	
			1 año	2 años	1 año	2 años
Token Virtual (Certitoken)	Pertenencia a Empresa / Entidad Representación de Empresa / Entidad Titular de Función Pública Profesional Titulado persona natural	Unidad	$233.500	$310.500	$233.500	$310.500
Token Físico		Unidad	$313.500	$441.500	$313.500	$441.500
Token Físico (Reuso)		Unidad	$273.500	$362.500	$273.500	$362.500

USO EXCLUSIVO DE CERTICÁMARA S.A.

PKCS# 10	Persona Natural / Jurídica	Unidad	$625.500	$932.500	$625.500	$932.500

- El precio de la renovación de los certificados de firma digital corresponde al mismo mencionado en la tabla anterior.
- Los precios establecidos anteriormente no incluyen IVA.
- Las tarifas indicadas podrán variar según acuerdos comerciales especiales con entidades y suscriptores o por el desarrollo de campañas de promoción.
- Se determina que la vigencia de un certificado de un año es de 365 días calendario.

Los solicitantes tendrán la posibilidad de obtener las tarifas aplicables a través del siguiente link https://ventadigital.certicamara.com/, en donde dependiendo de los datos ingresados por el solicitante y de conformidad al proyecto y/o convenio al que pertenezcan, se liquidará la respectiva tarifa.

11. MODELOS Y MINUTAS DE LOS DOCUMENTOS DE TÉRMINOS Y CONDICIONES

El modelo de términos y condiciones para la suscripción que usa Certicámara en la prestación del servicio de certificado de firma digital se encuentra disponible en el siguiente enlace: https://ventadigital.certicamara.com/.

En caso de presentarse situaciones comerciales particulares con el cliente, entre Certicámara y este se podrá suscribir un contrato que detalle dichas situaciones.

12. NORMATIVIDAD ASOCIADA

Los certificados de firma digital son emitidos conforme a los documentos normativos o técnicos definidos en el alcance acreditado por el ONAC, el cual se encuentra publicado en https://onac.org.co/directorio-de-acreditados/

13. CONTROL DE CAMBIOS

Fecha	Razón de actualización
07/09/2022	• En el marco del cumplimiento de las disposiciones del capítulo 48 del DURSCIT, Artículo 2.2.2.48.3.1. Declaración de Prácticas de Certificación (DPC) y al estándar RFC 3647, se alinean los numerales con lo establecido en estos documentos y se crea el presente documento para dar mayor claridad al solicitante y suscriptor sobre las disposiciones, información, directrices, controles y demás aplicables para el servicio de certificado de firma digital. Teniendo en cuenta lo anterior, se asigna un nuevo código y versión del documento de acuerdo con la estructura de procesos de la organización.

USO EXCLUSIVO DE CERTICÁMARA S.A.

certicámara.

Código:	IDI-L-002
Fecha:	11/11/2026
Versión:	004
Etiquetado:	PÚBLICO

POLÍTICA DE CERTIFICACIÓN – CERTIFICADO DE FIRMA DIGITAL

Fecha	Razón de actualización
28/09/2022	✔ Se realizan los siguientes cambios al documento: o Cuidados para la protección de los dispositivos criptográficos físicos, virtuales y PKCS#10. o Información publicada en las plantillas para cada política. o Información para la restauración de la clave privada y la generación e instalación del par de claves.
31/10/2022	✔ Se incluye el numeral 9.3 Sistemas de seguridad para proteger la información, donde se informan los procedimientos que se tienen definidos para proteger la información que se recopila en la expedición de los certificados.
16/02/2023	Se realizan los siguientes cambios al documento: ● Actualización de tarifas para el 2023. ● Inclusión del numeral *3.10 Reposición de Certificados de firma Digital*, donde se aclara que se debe generar un nuevo certificado y las condiciones que debe tener en cuenta el suscriptor para su gestión. ● Se incorpora la definición como medio de entrega de token físico Reuso. ● Actualización de los nombres de las políticas de acuerdo con la acreditación ONAC.
21/07/2023	Se realizan los siguientes ajustes al documento: ● Claridad que la información en los OID´S de dirección, ciudad / municipio y departamento de todas las políticas, será la reportada en el RUT. ● Actualización de las tarifas de los certificados: Digital Token físico, Digital Token físico (rehuso) y Digital Certitoken. ● Actualización de las URL de los nuevos puntos de distribución 4026 para la lista de certificados revocados CRL.

USO EXCLUSIVO DE CERTICÁMARA S.A

POLÍTICA DE CERTIFICACIÓN – CERTIFICADO DE FIRMA DIGITAL

Fecha	Razón de actualización
18/09/2023	Se realizan los siguientes ajustes al documento: • Actualización de los canales para la solicitud de certificado. • En el numeral *"2.3 Tipos de certificados ECD Certicámara"* se especifican los documentos requeridos por tipo de política. • En la política "*2.3.5 Certificado digital Persona Natural / Persona Jurídica*" se da la claridad respecto a la plataforma dispuesta para la generación de la petición, unión de llaves y demás aspectos relacionados con la solicitud de firma. Así como, la responsabilidad del suscriptor en el certificado emitido bajo esta modalidad. • En el numeral *"3.1 Solicitud de certificado"* se da claridad frente a la suspensión temporal de certificados de firma digital en sistema operativo Mac OS.
15/01/2024	Se realizan los siguientes cambios al documento: • En el numeral *"3.1 Solicitud de certificado"* se incluye la aceptación plena, sin reservas y en su totalidad de los Términos y Condiciones del servicio, las Declaraciones y Compromisos en materia de prevención del lavado de activos financiación del terrorismo, financiamiento de la proliferación de armas de destrucción masiva, corrupción y soborno trasnacional. Así mismo, la validación de identidad que se realizará al solicitante durante el proceso de solicitud. • Aclaración en el numeral *"3.6.1 Tiempos para la renovación"* que la emisión de un nuevo certificado digital implica de manera previa la aceptación de Términos y Condiciones del servicio, de las Declaraciones y Compromisos en materia de prevención del lavado de activos financiación del terrorismo, financiamiento de la proliferación de armas de destrucción masiva, corrupción y soborno trasnacional y la validación de identidad en el registro de una nueva solicitud. • Actualización de las tarifas para el año 2024.

USO EXCLUSIVO DE CERTICÁMARA S.A

certicámara.

Código:	IDI-L-002
Fecha:	11/11/2026
Versión:	004
Etiquetado:	PÚBLICO

POLÍTICA DE CERTIFICACIÓN – CERTIFICADO DE FIRMA DIGITAL

Fecha	Razón de actualización
18/03/2024	Se realizan los siguientes ajustes al documento: • Eliminación del requisito de solicitud *"Certificado laboral cuando el contacto técnico es diferente al representante legal (Aplica Persona Jurídica y cuando el uso de la firma es diferente a facturación electrónica) requisitos PN"*. • En el numeral 3.1 solicitud de certificado, se aclara que la validación de la identidad hace parte de los requisitos que debe cumplir el suscriptor. • Actualización de los links de acuerdo con los cambios en la página web. • Actualización de la normatividad aplicada al servicio.
09/09/2024	Se realizan los siguientes ajustes al documento: • Actualización de los tiempos de gestión de entrega de los certificados digitales en medio físico. • Actualización de la longitud de clave 4096 bits en la emisión de certificados digitales. • Inclusión de las políticas: Certificado digital persona natural PKCS#10 y Certificado digital persona jurídica PKCS#10
05/08/2025	Se realizan los siguientes cambios al documento: • Ajuste integral de redacciones para dar mayor claridad y precisión en la información. • Ajuste del procedimiento de aprobación de los cambios en la DPC. • Ajuste de las condiciones de Tiempo de descarga • Inclusión que el procedimiento de revocación del certificado digital no genera costo alguno. • Eliminación de la línea nacional gratuita. • Actualización de enlaces. • Eliminación de la línea nacional gratuita. • Eliminación de la sección *"Políticas de reembolso para suscriptores"*, dado que estas condiciones se tienen establecidas en la ***Declaración de Prácticas de Certificación*** transversales para todos los productos. • Actualización de las tarifas.

USO EXCLUSIVO DE CERTICÁMARA S.A

certicámara.

Código:	IDI-L-002
Fecha:	11/11/2026
Versión:	004
Etiquetado:	PÚBLICO

POLÍTICA DE CERTIFICACIÓN – CERTIFICADO DE FIRMA DIGITAL

Fecha	Razón de actualización
26/09/2025	Se realizan los siguientes cambios al documento: • Aclaración en la sección de requisitos para cada política si el RUT corresponde a la persona natural o jurídica. • Claridad de los documentos equivalentes al RUT para la solicitud de certificado digital persona natural. • Ajuste del lineamiento para restablecer la contraseña de token virtual, el cual no genera costo hasta diez solicitudes. • Claridad que el tiempo para descarga del certificado digital son noventa (90) días calendario.
20/04/2026	Se realizan los siguientes cambios al documento: • Integralmente se actualizan los canales de atención. • Actualización de cargos responsables de acuerdo con los cambios en la estructura organizacional. • Modificación de la descripción y requisitos para la política de Certificado digital persona natural en dispositivos locales y/o centralizados. • Actualización de los requisitos de entrega de token físico a un tercero. • Cambio de código y versión del documento de acuerdo con los cambios en los procesos.
01/06/2026	Se realizan los siguientes cambios al documento: • Actualización integral de los links de acuerdo con los cambios en la página web. • Ajuste de los requisitos de expedición para cada una de las políticas. • Actualización del medio para restablecer la contraseña para token virtual. • Claridad de los medios para solicitar la revocación. • Actualización de las tarifas.
21/09/2026	Se realizan los siguientes cambios al documento: • Claridad del uso de certificado de persona natural en dispositivos locales y centralizados, y Certificado digital Persona Natural / Persona Jurídica, para brindar más claridad al solicitante. • Ajuste normatividad técnica de los certificados FIPS 140-3 en todo el documento.

USO EXCLUSIVO DE CERTICÁMARA S.A

POLÍTICA DE CERTIFICACIÓN – CERTIFICADO DE FIRMA DIGITAL

Fecha	Razón de actualización
	• Ajuste de las causales de revocación de acuerdo con el modelo operativo. • Como parte de las características técnicas de los certificados en token virtual, se incluye "RSE: Doble factor de autenticación".
11/11/2026	Se realizan los siguientes cambios al documento: • En el numeral 3.5.4 "Método de destrucción de clave privada", se ajusta el método utilizado para la destrucción de claves de certificados digitales emitidos en token físico.

USO EXCLUSIVO DE CERTICÁMARA S.A