Política de Certificación – Certificado de Firma Digital

Código: DYD-L-007

Fecha: enero 2024

Versión: 007

USO EXCLUSIVO DE CERTICÁMARA S.A.

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 Representación de Empresa / Entidad - Dispositivos locales y/o centralizados. 7
2.3.2 Certificado de Pertenencia a Empresa / Entidad - Dispositivos locales y/o centralizados. 9
2.3.3 Certificado de Profesional Titulado - Dispositivos locales y/o centralizados. 11
2.3.4 Certificado de Titular de Función Pública - Dispositivos locales y/o centralizados. 12
2.3.5 Certificado digital Persona Natural / Persona Jurídica - Dispositivos locales y/o centralizados. 14
3. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO 17
3.1 Solicitud de certificado 17
3.2 Emisión de certificados 19
3.2.1 Acciones de la CA durante la emisión del certificado 19
3.2.2 Notificación al suscriptor por parte de la CA de emisión de certificado 20
3.2.3 Restauración de la clave privada 20
3.3 Entrega del certificado digital a los suscriptores por medio físico 20
3.3.1 Cubrimiento 20
3.3.2 Requisitos de entrega 20
3.3.3 Tiempo de gestión de entrega – Certificados Físicos 20
3.3.4 Tiempo de descarga – Certificado Virtual 21
3.4 Aceptación del certificado 21
3.4.1 Publicación del certificado por la CA 22
3.4.2 Notificación de emisión de certificados por parte de la CA a otras entidades 22
3.5 Uso de pares de claves y certificados 22

USO EXCLUSIVO DE CERTICÁMARA S.A.

3.5.1 Generación e instalación de pares de claves 22
3.5.2 Uso de certificado y clave privada del suscriptor 22
3.5.3 Uso del certificado y la clave pública del usuario de confianza 22
3.5.4 Método de destrucción de clave privada 23
3.6 Renovación del certificado 23
3.6.1 Tiempos para la renovación 23
3.6.2 Quién puede solicitar la renovación 23
3.6.3 Tramitación de solicitudes de renovación de certificados 23
3.6.4 Notificación de emisión de nuevo certificado al suscriptor 24
3.7 Renovación de llave de certificado 24
3.8 Modificación del certificado 24
3.9 Revocación y suspensión de certificados 24
3.9.1 Causales para la revocación 24
3.9.2 ¿Quién puede solicitar la revocación? 25
3.9.3 Procedimiento para solicitud de revocación 26
3.9.4 Período de gracia de la solicitud de revocación 26
3.9.5 Frecuencia de emisión de CRL 26
3.9.6 Disponibilidad de verificación de estado/revocación en línea 27
3.9.7 Requisitos de verificación de revocación en línea 27
3.9.8 Circunstancias de suspensión 27
3.10 Reposición de Certificados de firma Digital 27
3.11 Características de los certificados 29
3.11.1 Características operativas 29
3.11.2 Disponibilidad del servicio 30
3.12 Fin de la suscripción 30
3.13 Custodia y recuperación de llaves 30
3.13.1 Política y prácticas de custodia y recuperación de llaves 30
4. USOS DE LOS CERTIFICADOS 30
4.1 Usos generales de los certificados digitales 30
5. CARACTERÍSTICAS DE LOS CERTIFICADOS 32
5.1 Certificado digital en token físico 32
5.1.1 Aspectos técnicos 32

USO EXCLUSIVO DE CERTICÁMARA S.A.

5.1.2 Cuidados del dispositivo criptográfico 33
5.1.3 Riesgos asociados 33
5.2 Certificado en token virtual 33
5.2.1 Características 33
5.2.2 Cuidados del dispositivo 34
5.2.3 Riesgos asociados 34
5.3 Certificado digital en PKCS#10 34
5.3.1 Características 34
5.3.2 Cuidados del dispositivo 35
5.3.3 Riesgos asociados 35
6. OBLIGACIONES Y RESPONSABILIDADES DE LOS INTERVINIENTES 35
7. DERECHOS DE LOS INTERVINIENTES 35
8. CONFIABILIDAD DE LAS FIRMAS Y LOS CERTIFICADOS DIGITALES. 35
8.1 Confiabilidad de las firmas digitales 36
8.2 Confiabilidad del certificado digital 36
9. CONFIDENCIALIDAD DE LA INFORMACIÓN 37
9.1 Alcance de la información confidencial 37
9.2 Información fuera del alcance de la información confidencial 37
9.3 Sistemas de seguridad para proteger la información 38
10. TARIFAS DEL SERVICIO DE EMISIÓN DE CERTIFICADOS DIGITALES 38
10.1 Políticas de Reembolso para Suscriptores 41
11. MODELOS Y MINUTAS DE LOS DOCUMENTOS DE TÉRMINOS Y CONDICIONES 41
12. NORMATIVIDAD ASOCIADA 41
13. CONTROL DE CAMBIOS 42

USO EXCLUSIVO DE CERTICÁMARA S.A.

POLÍTICA DE CERTIFICACIÓN – CERTIFICADO DE FIRMA DIGITAL

1. INTRODUCCIÓN

Este documento presenta una manifestación pública de la entidad de certificación digital abierta sobre las políticas y procedimientos específicos, normas y condiciones generales del servicio de certificados digitales que presta la Sociedad Cameral de Certificación Digital Certicámara S.A.

La presente política de certificación (PC) se ha estructurado conforme con las recomendaciones del RFC 3628, RFC 3161 y lo establecido en la Ley 527 de 1999, el Decreto Ley 0019 de 2012, el Decreto 333 de 2014 y los reglamentos que los modifiquen o complementen, en el territorio colombiano.

Las condiciones de carácter general y que tienen un alcance transversal a los diferentes servicios de certificación digital ofrecidos por Certicámara que se encuentran descritos en la **Declaración de Prácticas de Certificación (DPC)** publicada en la página web en la sección marco legal.

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	15/01/2024
Versión	007
Código	DYD-L-007
Ubicación	https://web.certicamara.com/marco_legal

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 ONAC en su página web https://onac.org.co/certificados/16-ECD-002.pdf

USO EXCLUSIVO DE CERTICÁMARA S.A.

1.3 Procedimiento para la actualización o aprobación de la política

La actualización de la política de certificación – Certificado de firma digital del servicio de Certificado de firma digital, se realizará cada vez que se requiera por cuestiones legales, reglamentarias y/o aplicables a los servicios acreditados.

Para lo anterior, el comité de cambios DPC y PC se reunirá para evaluar los cambios y/o modificaciones a realizar, los cuales serán aprobados por el Presidente Ejecutivo.

El Director de planeación y gestión es el responsable de gestionar la actualización en la página web de Certicámara, en el siguiente link https://web.certicamara.com/marco_legal

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_legal
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 en la dirección 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_tecnico.
g) Estado de revocación de certificados OCSP, se encuentra disponible para su consulta vía web en la dirección http://ocsp.certicamara.com y http://ocsp.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	Pertenencia a Empresa / Entidad
1.3.6.1.4.1.23267.50.1.2	Representación de Empresa / Entidad
1.3.6.1.4.1.23267.50.1.3	Titular de Función Pública
1.3.6.1.4.1.23267.50.1.4	Profesional Titulado
1.3.6.1.4.1.23267.50.1.5	Persona Natural
1.3.6.1.4.1.23267.50.1.2	Persona Jurídica

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 Representación de Empresa / Entidad - 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,

USO EXCLUSIVO DE CERTICÁMARA S.A.

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, o como comerciante persona natural en el ámbito de su actividad profesional o mercantil.

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 adjuntar los siguientes documentos:

    1. Registro Único Tributario (RUT): Será responsabilidad del suscriptor actualizar la información de domicilio (dirección, municipio y departamento) en el RUT. Las personas con domicilio fuera de Colombia que no se encuentren registrados ante la DIAN deberán adjuntar el documento que haga las veces de residente fiscal en su país y el mismo se deberá validar con la Dirección de Asuntos Legales y Contractuales quienes darán un concepto para la emisión.
    2. Documento de identificación: Cédula de ciudadanía, Pasaporte, Permiso con protección temporal (PPT), Certificado de Trámite del Permiso por Protección Temporal (PPT), Cédula de extranjería o Tarjeta de identidad.
    3. 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 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.

- El solicitante debe diligenciar el Formulario de prestación de servicios de certificación digital para el tipo Certificado de Representación de Empresa/Entidad adjuntando los documentos solicitados que se encuentran en el link: https://solicitudes.certicamara.com/SSPS/Solicitudes/RecomendacionesUso.aspx
- Validar la identidad del solicitante de acuerdo con los mecanismos dispuestos por Certicámara al momento de la solicitud.
- Dentro de la información publicada en el respectivo certificado se encuentra:

USO EXCLUSIVO DE CERTICAMARA S.A.

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

2.3.2 Certificado de Pertenencia a Empresa / Entidad - 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, 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.

USO EXCLUSIVO DE CERTICÁMARA S.A.

- Requisitos de expedición

  - El solicitante debe adjuntar los siguientes documentos:

    1. Registro Único Tributario (RUT): Será responsabilidad del suscriptor actualizar la información de domicilio (dirección, municipio y departamento) en el RUT. Las personas con domicilio fuera de Colombia que no se encuentren registrados ante la DIAN deberán adjuntar el documento que haga las veces de residente fiscal en su país y el mismo se deberá validar con la Dirección de Asuntos Legales y Contractuales quienes darán un concepto para la emisión.
    2. Documento de identificación: Cédula de ciudadanía, Pasaporte, Permiso con protección temporal (PPT), Certificado de Trámite del Permiso por Protección Temporal (PPT), Cédula de extranjería o Tarjeta de identidad.
    3. 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.

  - El solicitante debe diligenciar el Formulario de prestación de servicios de certificación digital para el tipo Certificado de Pertenencia a Empresa/Entidad adjuntando los documentos solicitados en el siguiente link: https://solicitudes.certicamara.com/SSPS/Solicitudes/RecomendacionesUso.aspx
  - Validar la identidad del solicitante de acuerdo con los mecanismos dispuestos por Certicámara al momento de la solicitud.
  - Dentro de la información publicada en el respectivo certificado se encuentra:

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
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

USO EXCLUSIVO DE CERTICÁMARA S.A.

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 Profesional Titulado - 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.

- Requisitos de expedición

  - El solicitante debe adjuntar los siguientes documentos:

  1. Registro Único Tributario (RUT): Será responsabilidad del suscriptor actualizar la información de domicilio (dirección, municipio y departamento) en el RUT. Las personas con domicilio fuera de Colombia que no se encuentren registrados ante la DIAN deberán adjuntar el documento que haga las veces de residente fiscal en su país y el mismo se deberá validar con la Dirección de Asuntos Legales y Contractuales quienes darán un concepto para la emisión.
  2. Documento de identificación: Cédula de ciudadanía, Pasaporte, Permiso con protección temporal (PPT), Certificado de Trámite del Permiso por Protección Temporal (PPT), Cédula de extranjería o Tarjeta de identidad.
  3. Certificado de Profesional Titulado: Aplica para Técnico, tecnólogo y universitario. Ley 30 de 1992 concepto 059 881 del Departamento administrativo de la función pública, tales como: Tarjeta profesional, Diploma, acta de grado o matrícula profesional, Certificación de título profesional. Cuando sea un profesional titulado

USO EXCLUSIVO DE CERTICÁMARA S.A.

en otro país, el documento debe ser convalidado por el Ministerio de Educación Nacional.

- El solicitante debe diligenciar el Formulario de prestación de servicios de certificación digital para el tipo **Certificado de Profesional Titulado** adjuntando los documentos solicitados en el siguiente link: https://solicitudes.certicamara.com/SSPS/Solicitudes/RecomendacionesUso.aspx
- Validar la identidad del solicitante de acuerdo con los mecanismos dispuestos por Certicámara al momento de la solicitud.
- Dentro de la información publicada en el respectivo certificado se encuentra:

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 / 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
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

2.3.4 Certificado de Titular de Función Pública - 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 adjuntar los siguientes documentos:

  1. Registro Único Tributario (RUT): Será responsabilidad del suscriptor actualizar la información de domicilio (dirección, municipio y departamento) en el RUT. Las personas con domicilio fuera de Colombia que no se encuentren registrados ante la DIAN deberán adjuntar el documento que haga las veces de residente fiscal en su país y el mismo se deberá validar con la Dirección de Asuntos Legales y Contractuales quienes darán un concepto para la emisión.
  2. Documento de identificación: Cédula de ciudadanía, Pasaporte, Permiso con protección temporal (PPT), Certificado de Trámite del Permiso por Protección Temporal (PPT), Cédula de extranjería o Tarjeta de identidad.
  3. 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.

  - El solicitante debe diligenciar el Formulario de prestación de servicios de certificación digital para el tipo **Certificado de Titular de Función Pública** adjuntando los documentos solicitados en el siguiente link:

USO EXCLUSIVO DE CERTICÁMARA S.A.

https://solicitudes.certicamara.com/SSPS/Solicitudes/RecomendacionesUso.aspx

- Validar la identidad del solicitante de acuerdo con los mecanismos dispuestos por Certicámara al momento de la solicitud.
- Dentro de la información publicada en el respectivo certificado se encuentra:

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

2.3.5 Certificado digital Persona Natural / Persona Jurídica - Dispositivos locales y/o centralizados.

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.

USO EXCLUSIVO DE CERTICÁMARA S.A.

POLÍTICA DE CERTIFICACIÓN – CERTIFICADO DE FIRMA DIGITAL

- Requisitos de expedición

  - El solicitante debe adjuntar los siguientes documentos:

1. Registro Único Tributario (RUT): Será responsabilidad del suscriptor actualizar la información de domicilio (dirección, municipio y departamento) en el RUT. Las personas con domicilio fuera de Colombia que no se encuentren registrados ante la DIAN deberán adjuntar el documento que haga las veces de residente fiscal en su país y el mismo se deberá validar con la Dirección de Asuntos Legales y Contractuales quienes darán un concepto para la emisión. Documento equivalente que certifique el domicilio de la persona natural, tales como: Contrato de arrendamiento, recibo de servicio público, certificado de residencia expedido por la autoridad municipal y el mismo se deberá validar con la Dirección de Asuntos Legales y Contractuales quienes darán un concepto para la emisión.
2. Documento de identificación: Cédula de ciudadanía, Pasaporte, Permiso con protección temporal (PPT), Certificado de Trámite del Permiso por Protección Temporal (PPT), Cédula de extranjería o Tarjeta de identidad.
3. Documentos con datos del cliente final (facturador): Este requisito aplica cuando su uso es para factura electrónica.
4. Documento que acredita la existencia y representación legal de la empresa o entidad (Aplica Persona Jurídica)
5. 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)

- El solicitante debe diligenciar el Formulario de prestación de servicios de certificación digital para el tipo de Certificado digital de Persona Natural / Persona Jurídica adjuntando los documentos solicitados en el siguiente link: https://solicitudes.certicamara.com/SSPS/Solicitudes/RecomendacionesUso.aspx
- Validar la identidad del solicitante de acuerdo con los mecanismos dispuestos por Certicámara al momento de la solicitud.
- Para las personas jurídicas y naturales obligados a facturar electrónicamente Certicámara S.A. dispondrá una plataforma para la generación de la petición, unión de llaves y demás aspectos relacionados con la solicitud de firma.
  De acuerdo con lo anterior, el solicitante será responsable de la información contenida en el Request cuando utilice una herramienta propia para la realización de la petición. Certicámara con sus sistemas de información, validará que la información contenida sea idéntica a la aportada en la petición de certificados digitales.
- Dentro de la información publicada en el respectivo certificado se encuentra, para Certificado de Persona Natural.

USO EXCLUSIVO DE CERTICÁMARA S.A.

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
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

- Dentro de la información publicada en el respectivo certificado se encuentra, para Certificado de Persona Jurídica

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

USO EXCLUSIVO DE CERTICÁMARA S.A.

10. Locality (L)	Departamento del Suscriptor
11. Surname (SN)	Apellido (s) del Suscriptor
12. Given Name (G)	Primer Nombre de Suscriptor

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 realizadas serán revisadas por la RA (autoridad de registro) de acuerdo con los criterios específicos de acreditación de ONAC y los definidos por Certicámara, para confirmar su veracidad e integridad. Esta revisión se ejecutará en un máximo de dos (02) días hábiles a partir de la completitud de los documentos, junto con el soporte de pago adjuntados por el solicitante. Posteriormente, las solicitudes serán escaladas a la CA (autoridad de certificación) para su emisión, la cual cuenta con un tiempo máximo de un (01) día hábil.

La documentación entregada por el solicitante será almacenada de acuerdo con las tablas de retención documental generadas por Certicámara. La información del solicitante no será publicada por Certicámara a no ser que se tenga su consentimiento explícito.

Los solicitantes que hacen uso y suscriben de manera electrónica el certificado de firma digital de CERTICÁMARA S.A. implica la aceptación plena, sin reservas y en su totalidad, 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 Declaración de Prácticas de Certificación (DPC), la Política de certificación - certificado de firma digital (PC) y de las políticas organizacionales de CERTICÁMARA S.A., publicados a través del sitio web de Certicámara S.A y que hacen parte integral del presente documento y en el contrato de prestación de servicios de certificación digital.

Los términos y condiciones aplican a partir del momento en el cual manifiesta a CERTICÁMARA S.A su interés por adquirir el certificado de firma digital y se mantendrá hasta la vigencia del certificado de firma digital junto con las condiciones generales de contratación del servicio.

Por ello, los solicitantes deberán tener en cuenta los siguientes puntos antes de solicitar el o los servicios a Certicámara:

USO EXCLUSIVO DE CERTICÁMARA S.A.

a) Haber leído en su integridad 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 presente Declaración de Prácticas de Certificación (DPC) y la Política de certificación - certificado de firma digital (PC).

b) Verificar la información mencionada por CERTICÁMARA S.A., la cual debe conocer para tomar una decisión informada sobre la prestación del certificado de firma digital, de conformidad con lo previsto en la Ley 527 de 1999, Decreto 019 de 2012, Ley 1341 de 2009, Ley 1978 de 2019, Decreto 1074 de 2015, Decreto 358 de 2020, Decreto 1538 de 2020 y en el Decreto 620 de 2020.

c) Conocer todos los requerimientos tecnológicos y de seguridad para la utilización del certificado de firma digital. Estar al tanto de las características del certificado de firma digital de CERTICÁMARA S.A., su nivel de confiabilidad, los límites de responsabilidad de los mismos, las obligaciones que asume como cliente y las medidas de seguridad que debe cumplir para su utilización.

d) Conocer que CERTICÁMARA S.A. puede reservarse el derecho de no prestar certificado de firma digital por condiciones técnicas, sin que esta decisión le genere algún tipo de responsabilidad.

e) CERTICÁMARA S.A., como Entidad de Certificación Digital Abierta, realizará previamente la comprobación de identidad, utilizando fuentes confiables y datos provistos por terceros con quienes CERTICÁMARA S.A. cuente con contrato vigente para tal fin.

f) Se reserva el derecho de solicitar documentos adicionales a los que sean exigidos en el formulario de solicitud o fotocopias de estos cuando así lo considere necesario para verificar la identidad o cualquier calidad del solicitante, así como de exonerar la presentación de cualquiera de ellos cuando la identidad del solicitante haya sido suficientemente verificada por Certicámara a través de otros medios. Sin limitarse a ellos, Certicámara podrá exigir adicionalmente alguno de los siguientes documentos:

- 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 cualquiera de los tipos de certificados que emite Certicámara.

g) Podrá consultar bases de datos de información de identidad dispuestos para tal fin por entidades privadas o del sector público con el fin de realizar las validaciones de identidad necesarias para emitir el certificado digital al suscriptor.

h) Consultará las bases de datos necesarias para dar cumplimiento al SAGRILAFT, previa aceptación del solicitante de las Declaraciones y Compromisos en materia de prevención del lavado de activos financiación del terrorismo, financiamiento de la

USO EXCLUSIVO DE CERTICÁMARA S.A.

proliferación de armas de destrucción masiva, corrupción y soborno trasnacional publicadas en el sitio web de Certicámara S.A. y que hacen parte integral del presente documento.

i) Emitirá certificados de firma digital con vigencia máxima de dos (2) años.
j) Certicámara S.A. declinará la expedición de un certificado digital a un solicitante, cuando no se encuentre dentro del alcance de la acreditación que le fue otorgado por ONAC, por el incumplimiento de la ley y/o cuando a su juicio atente contra el buen nombre de la ECD. En este caso, no habrá lugar a la subsanación por parte del usuario.
k) Si Certicámara decide negar o declinar la solicitud de expedición del certificado de firma digital, lo notificará por correo electrónico al solicitante, indicando los motivos que la justifican.
l) Actualmente nos encontramos en el desarrollo de la infraestructura que permita la compatibilidad para la emisión de los certificados de firma digital para el sistema operativo Mac OS.

- ¿Quién puede presentar una solicitud de certificado?

La solicitud del certificado puede ser realizada por cualquier persona, mayor de edad en capacidad de asumir las obligaciones y responsabilidades inherentes al tipo de certificado solicitado.

El certificado vinculado a la identidad de una persona jurídica puede ser solicitado por un representante legal, apoderado, empleado o persona autorizada por un representante legal de la Persona Jurídica que pueda sustentar correctamente la información requerida por la RA.

3.2 Emisión de certificados

3.2.1 Acciones de la CA durante la emisión del certificado

Una vez aprobada la solicitud de emisión del certificado, la CA genera el certificado correspondiente vinculado a un par de claves, el cual será firmado por el certificado de la CA que forma parte de la cadena de confianza de Certicámara.

La emisión de los certificados implica la autorización de la solicitud por parte del sistema de la CA Subordinada. Después de la aprobación de la solicitud se procederá a la emisión de los certificados de forma segura y se pondrán los certificados a disposición del suscriptor.

En la emisión de los certificados la CA Subordinada:

- Utiliza un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Protege la confidencialidad e integridad de los datos de registro.
- Todos los certificados iniciarán su vigencia al momento de la emisión por parte de la CA, dicha vigencia queda registrada en las propiedades del certificado.

USO EXCLUSIVO DE CERTICÁMARA S.A.

- Ningún certificado será emitido con un periodo de validez que se inicie con anterioridad de 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 medio virtual, Certicámara tiene implementado mecanismos seguros que permiten que el suscriptor gestione el cambio de su contraseña sin que implique el conocimiento de la contraseña por parte de ésta. Para el caso de certificado de firma digital en medio físico, el suscriptor no podrá restaurar su clave privada, sino que podrá realizar el cambio de ésta cuando lo requiera.

3.3 Entrega del certificado digital a los suscriptores por medio físico

3.3.1 Cubrimiento

La entrega de los certificados digitales se realizará de conformidad con la matriz de cubrimiento del servicio de entrega del operador logístico que tenga contrato vigente con Certicámara para efectuar esta tarea o mediante entrega directa por parte del colaborador del área logística de Certicámara, cumpliendo con los requisitos de seguridad necesarios para garantizar que la entrega es personal y que se mantiene en todo momento la confidencialidad de la llave privada del certificado del suscriptor.

Los certificados digitales serán enviados a través del operador logístico al destino diligenciado en el formulario de solicitud o podrán ser reclamados en las instalaciones de Certicámara, previa información del suscriptor.

3.3.2 Requisitos de entrega

La entrega se realiza en cualquiera de los eventos previa identificación del solicitante; ante la imposibilidad de entrega personal del certificado digital, el solicitante debe autorizar a un tercero para recibirlo a través de un poder firmado por el solicitante, anexando copia del documento de identificación del solicitante y del tercero autorizado. La guía del operador logístico servirá como evidencia del acuse de recibo del certificado de firma digital. En los eventos que exista por parte de la entidad contratante un coordinador encargado de la administración de los certificados digitales, este podrá recibir y distribuir los certificados previa validación de Certicámara.

3.3.3 Tiempo de gestión de entrega – Certificados Físicos

A nivel urbano y ciudades principales el tiempo de entrega desde la emisión del certificado hasta la entrega al solicitante, será aproximadamente de dos (2) días hábiles; ante la

USO EXCLUSIVO DE CERTICÁMARA S.A.

imposibilidad de ubicar al solicitante o tercero autorizado dicho término podrá ser de cinco (5) días hábiles.

A nivel nacional y ciudades intermedias, el tiempo de entrega desde la emisión del certificado hasta la entrega al solicitante, será aproximadamente de tres (3) días hábiles; ante la imposibilidad de ubicar al solicitante o tercero autorizado dicho término podrá ser de ocho (8) días hábiles.

Para los destinos especiales el tiempo de entrega desde la emisión del certificado hasta la entrega al solicitante, será aproximadamente de cuatro (4) días hábiles; ante la imposibilidad de ubicar al solicitante o tercero autorizado dicho término podrá ser de nueve (9) días hábiles.

En los eventos en los cuales la entrega del certificado no sea posible por una causa asociada al suscriptor, Certicámara y/o el operador logístico contactará al solicitante para coordinar el proceso de entrega. De no obtener respuesta expresa con la fecha de entrega o recolección del certificado de firma digital, Certicámara los mantendrá en custodia por un periodo de tres (3) meses a partir de la fecha de emisión. Una vez cumplido este término y sin haberse manifestado el suscriptor, se entenderá **que abandona el bien y Certicámara** procederá con la revocación. Si el solicitante requiere la emisión del certificado de firma digital deberá iniciar el proceso de solicitud de acuerdo con lo establecido por parte de Certicámara.

3.3.4 Tiempo de descarga – Certificado Virtual

En el caso de los certificados virtuales se entenderá que, con la notificación de descarga del certificado, el suscriptor puede hacer uso de su certificado digital.

En los eventos en los cuales la descarga del certificado no sea posible por una causa asociada al suscriptor, Certicámara contactará al solicitante para coordinar el proceso de descarga. De no obtener respuesta con la fecha de descarga del certificado de firma digital, Certicámara bloqueará el link de descarga y solo se reactivará previa solicitud del cliente por un periodo de tres (3) meses a partir de la fecha de emisión. Una vez cumplido este término y sin haberse manifestado el suscriptor, se entenderá que abandona el bien y Certicámara procederá con la revocación. Si el solicitante requiere la emisión del certificado de firma digital deberá iniciar el proceso de solicitud de acuerdo con lo establecido por parte de Certicámara.

3.4 Aceptación del certificado

No se requiere confirmación de parte del suscriptor como aceptación del servicio recibido. Se considera que el servicio de certificado digital es aceptado desde el momento que solicita su expedición, por ello, si la información contenida en la comunicación de activación del servicio no corresponde al estado actual de la misma o no fue suministrada correctamente,

USO EXCLUSIVO DE CERTICÁMARA S.A.

el suscriptor deberá notificar a Certicámara por cualquiera de nuestros canales para los trámites pertinentes de corrección.

3.4.1 Publicación del certificado por la CA

El servidor de la autoridad de registro introducirá las llaves 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 momento que el certificado sea emitido.

En caso que surja algún inconveniente técnico que impida su publicación, está ocurrirá dentro del siguiente mes a la emisión del certificado de acuerdo con el resultado del análisis técnico que haya impedido su publicación inmediata.

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

Certicámara posee un repositorio de certificados digitales LDAP, en el cual las entidades, organismos del gobierno, empresas privadas y demás partes interesadas podrán consultar la emisión de los certificados. El cual está disponible en la siguiente URL: https://ar.Certicamara.com:8443/Search/ . La publicación en este repositorio se realiza una vez se haya emitido el certificado.

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 140-2 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 **política de certificación** 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 sólo pueden depositar su confianza en los certificados para aquello que establece la DPC, PC y la normativa.

Los terceros de buena fe pueden realizar operaciones de clave pública de manera satisfactoria confiando en el certificado emitido por la cadena de confianza. Así mismo, deben asumir la responsabilidad de verificar el estado del certificado utilizando los medios que se establecen en la DPC y PC.

USO EXCLUSIVO DE CERTICÁMARA S.A.

3.5.4 Método de destrucción de clave privada

La CA Raíz y la CA Subordinada eliminarán su clave privada cuando expire su plazo de vigencia o haya sido revocada. 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. Lo mismo ocurrirá con sus copias de seguridad.

3.6 Renovación del certificado

3.6.1 Tiempos para la renovación

Certicámara notificará con al menos treinta días (30) calendario de anticipación a sus suscriptores la terminación de la vigencia de su certificado digital. Esta notificación podrá realizarse por correo electrónico a la dirección proporcionada por el suscriptor o por cualquier otro medio idóneo de comunicación cuando Certicámara lo considere pertinente.

Sin embargo, no es obligación de Certicámara garantizar la efectividad de la notificación sobre la terminación de la vigencia de su certificado o confirmar la recepción de la misma, pues es una obligación del Suscriptor conocer la vigencia de su certificado digital y adelantar los trámites pertinentes ante Certicámara para la emisión de su nueva firma.

La renovación se entenderá como la emisión de un nuevo certificado digital, por lo cual implica el registro de una nueva solicitud, la cual estará sujeta a la aceptación de 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, por parte del solicitante, a la previa validación de identidad y a la generación de un nuevo par de claves.

3.6.2 Quién puede solicitar la renovación

Los suscriptores están autorizados para solicitar la renovación de un certificado cuando se encuentre próximo a vencer el servicio y el suscriptor desee continuar utilizando un certificado digital que acredite las condiciones que le fueron aprobadas en el certificado digital.

3.6.3 Tramitación de solicitudes de renovación de certificados

El suscriptor deberá cumplir nuevamente con el proceso de validación de identidad para solicitar la renovación de un certificado. Por tal motivo, el procedimiento de solicitud para la renovación de un certificado es el mismo que el de emisión por primera vez. Salvo que no tendrá que adjuntar documentos a la solicitud a menos que estos hayan perdido vigencia en caso de que aplique.

USO EXCLUSIVO DE CERTICÁMARA S.A.

3.6.4 Notificación de emisión de nuevo certificado al suscriptor

Certicámara notificará al suscriptor sobre la emisión efectiva de un nuevo certificado por medio de un correo electrónico a la dirección suministrada.

3.7 Renovación de llave de certificado

Certicámara no considera dentro del ciclo de vida de sus certificados la renovación del par de claves, en todos los casos la emisión de un certificado conlleva la generación de un nuevo par de claves.

3.8 Modificación del certificado

Durante el ciclo de vida de un certificado, no se tiene prevista la modificación / actualización de los campos contenidos en el certificado. Si se requiere un cambio en los datos del certificado emitido, será necesario revocar el certificado y emitir uno nuevo con las modificaciones correspondientes.

3.9 Revocación y suspensión de certificados

La revocación de un certificado digital es el mecanismo por el que se inhabilita el certificado emitido y se da por terminado su periodo de validez ya sea por la finalización de su vigencia o al presentarse alguna de los eventos de revocación establecidos en la presente Declaración de Prácticas de Certificación, originando la pérdida de confianza en el mismo.

Adicionalmente, Certicámara no tiene permitido el estado de suspendido en los 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.

USO EXCLUSIVO DE CERTICÁMARA S.A.

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.
q) Por reporte de cartera vencida ocasionado por el pago no efectuado de los servicios que le está proporcionando Certicámara.
r) Por los eventos en los cuales la entrega del certificado no sea posible por una causa asociada al suscriptor.
s) Por causas asociadas a Certicámara y/o el operador logístico.
t) Por la concurrencia de cualquier otra causa especificada en la presente Declaración de Prácticas de Certificación.

3.9.2 ¿Quién puede solicitar la revocación?

El suscriptor podrá voluntariamente, en cualquier momento, de manera directa o a través de un tercero, solicitar a Certicámara la revocación del certificado digital emitido, en cuyo caso se iniciará el procedimiento de revocación del certificado digital.

Certicámara podrá tramitar la revocación de un certificado si tuviera conocimiento o sospecha del compromiso de la llave privada del suscriptor o cualquier otro hecho determinante que requiera proceder a revocar el certificado.

USO EXCLUSIVO DE CERTICÁMARA S.A.

3.9.3 Procedimiento para solicitud de revocación

El suscriptor en caso de requerir la revocación de su certificado de firma digital por alguna de las causales descritas anteriormente, podrá utilizarlos siguientes medios para la recepción de su solicitud:

- Telefónicamente llamando a la línea de atención (601) 7442727 lunes a viernes de 7:00 a.m. a 6:00 p.m. y sábados de 8:00 a.m. a 1:00 p.m.
- Revocación en línea a través de la página WEB de Certicámara registrando la solicitud de revocación en la siguiente URL:

https://solicitudes.Certicamara.com/SSPS/solicitudes/RevocarCertificadoClienteCF.aspx

Si Certicámara lo considera necesario realizará, personalmente o por intermedio de terceras personas, las averiguaciones, verificaciones y gestiones pertinentes para comprobar la existencia de la causal de revocación que sea invocada. Dichas gestiones podrán incluir la comunicación directa con el suscriptor y la presencia física del tercero que invoca la causal de revocación.

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, deberá dirigirse personalmente a las oficinas de Certicámara en horarios de oficina 08:00 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.

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:

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

USO EXCLUSIVO DE CERTICÁMARA S.A.

3.9.6 Disponibilidad de verificación de estado/revocación en línea

Las listas de certificados revocados (CRL) y el servicio de 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%.

3.9.7 Requisitos de verificación de revocación en línea

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 y http://ocsp.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 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:

USO EXCLUSIVO DE CERTICÁMARA S.A.

- El suscriptor deberá generar la solicitud en la página web de Certicámara: https://web.certicamara.com/soporte_tecnico, bajo el proyecto *reposición*.
- La generación de la nueva firma, se tendrá que hacer según lo contenido en el numeral 3.1 de la presente Política de Certificación.
- El suscriptor deberá realizar la revocación del certificado de firma digital. Para ello, tendrá dos posibilidades:

    i. Se deberá remitir -por parte del titular del certificado de firma digital, o un tercero autorizado- el formato correspondiente donde autoriza la revocación del Certificado digital al correo electrónico revocaciones@certicamara.com. El formato podrá ser solicitado, comunicándose con la línea de atención al cliente dispuesto por Certicámara (601) 7442727 opción 2, opción 1.

    ii. A través del siguiente link donde, aceptando los términos y condiciones, podrá realizar el proceso de forma personal https://solicitudes.certicamara.com/SSPS/solicitudes/RevocarCertificadoClienteCF.aspx

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 operaciones al correo revocaciones@certicamara.com, donde 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.

USO EXCLUSIVO DE CERTICAMARA S.A.

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.

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 y http://ocsp.certicamara.co

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

- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara.crl?crl=crl
- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica.crl?crl=crl
- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_2014.crl?crl=crl
- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_2014.crl?crl=crl
- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_4096.crl?crl=crl
- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_4096.crl?crl=crl

USO EXCLUSIVO DE CERTICÁMARA S.A.

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%.

***Funciones* opcionales**

Para hacer uso del Servicio de validación en línea consultando las direcciones http://ocsp.certicamara.com y, 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.
- 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 limite (k, n) de Shamir tanto en software como en dispositivos criptográficos.

4. USOS DE LOS CERTIFICADOS

4.1 Usos generales de los certificados digitales

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, aquellos usos permitidos en la 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 la 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.

USO EXCLUSIVO DE CERTICÁMARA S.A.

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 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 Prohibiciones de uso de los certificados

a) Los certificados digitales no podrán ser utilizados en 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 la Declaración de Prácticas de Certificación y Política de Certificación, y en los contratos que se firmen entre Certicámara y el Suscriptor.

c) Se encuentra prohibido el uso de los certificados digitales y del Sistema de Certificación Digital como sistema de control para actividades de alto riesgo o para sistemas a prueba de error, dentro de los que se incluyen, pero sin limitarse a los siguientes:
   - Sistemas de navegación de transporte terrestre, aéreo o marítimo.
   - Sistemas de control de tráfico aéreo.
   - Sistemas de control de armas.

d) Los certificados digitales no podrán utilizarse en ningún sistema cuyo fallo pueda ocasionar la muerte o lesión de personas, u ocasionar un serio perjuicio al medio ambiente.

e) 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 por Certicámara información diferente

USO EXCLUSIVO DE CERTICÁMARA S.A.

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 2 años que equivalen a 730 días, de acuerdo con lo establecido en el CEA Vigente.

5. CARACTERÍSTICAS DE LOS CERTIFICADOS

5.1 Certificado digital en token físico

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 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.

5.1.1 Aspectos técnicos

- ✓ Longitud de la llave privada de 2048 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.

USO EXCLUSIVO DE CERTICÁMARA S.A.

5.1.2 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.

5.1.3 Riesgos asociados

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

- ✓ Fluctuaciones fuero 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.140-2.pdf

5.2 Certificado en token virtual

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 el titular del certificado. Para la realización de su uso se debe disponer de una conexión activa de Internet.

5.2.1 Características

- ✓ Llave privada de 2048 bits.
- ✓ Algoritmo de firma de certificado con hash SHA256.
- ✓ Certificados X.509 v3.
- ✓ Almacenamiento en infraestructura que cumple FIPS 140-2 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.

USO EXCLUSIVO DE CERTICÁMARA S.A.

- ✓ Componente de firma que permita el consumo de Certitoken
- ✓ Java mínimo en Ver 7
- ✓ Windows 7 o superior
- ✓ Framework 4.0 o superior
- ✓ Acceso a las URL
  - https://certitoken.certicamara.com/certificate/list

5.2.2 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.

5.2.3 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.

5.3.1 Características

- ✓ Llave pública de 2048 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.

USO EXCLUSIVO DE CERTICÁMARA S.A.

5.3.2 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.

5.3.3 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 9.6.

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

USO EXCLUSIVO DE CERTICÁMARA S.A.

confianza propia del sistema de certificación digital, siguiendo en todo momento las políticas y procedimientos establecidos.

8.1 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.

8.2 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 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://solicitudes.certicamara.com/ssps/Solicitudes/AceptoLosTerminos.aspx).

USO EXCLUSIVO DE CERTICÁMARA S.A.

- 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 sus actividades. 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 este, en su calidad de propietario de esta.

9.1 Alcance de la información confidencial

Se considera información confidencial:

- 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 contengan datos relacionados con el salario 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)

USO EXCLUSIVO DE CERTICÁMARA S.A.

- La clave pública de la AC Raíz y AC Subordinada
- La declaración de prácticas de certificación
- Políticas organizacionales

Nota. Todos los datos personales del suscriptor relativos al registro de certificados son tratados de acuerdo con la política de Protección de Datos Personales definida por Certicámara para tal fin y en cumplimiento de la Ley Estatutaria 1581 de 2012 "Protección de Datos Personales", encontrándose dicha política publicada en la página web de Certicámara S.A.

9.3 Sistemas de seguridad para proteger la información

CERTICÁMARA cuenta con sistemas de seguridad tendientes a proteger la información que se recopila con el fin de expedir los certificados, los cuales se encuentran desarrollados a través de lineamientos para la gestión de activos de información que vinculan a todos los responsables respecto de la administración de estos datos, desde cada uno de sus roles. En complemento de lo anterior, CERTICÁMARA cuenta con un procedimiento para el etiquetado y manejo adecuado de información, cuyo objetivo principal consiste en establecer el paso a paso que se debe seguir para etiquetar la información y así asegurar que esta recibe un nivel apropiado de protección, de acuerdo con su nivel de importancia.

Así mismo, CERTICÁMARA cuenta con un sistema de gestión de seguridad de la información certificado bajo la norma ISO/IEC 27001:2013 y con una infraestructura robusta que permite garantizar la protección de la información.

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:

USO EXCLUSIVO DE CERTICÁMARA S.A.

POLÍTICA DE CERTIFICACIÓN – CERTIFICADO DE FIRMA DIGITAL

Producto	Artículo	Tipo	Precio
Certificado Digital Token Físico	Certificado Digital Persona Natural, vigencia (1) un año	Unidad	$ 306,000
	Certificado Digital Persona Natural, vigencia (2) dos años	Unidad	$ 428,000
	Certificado Digital Pertenencia a Empresa, vigencia (1) un año	Unidad	$ 306,000
	Certificado Digital Pertenencia a Empresa, vigencia (2) dos años	Unidad	$ 428,000
	Certificado Digital Profesional Titulado, vigencia (1) un año	Unidad	$ 306,000
	Certificado Digital Profesional Titulado, vigencia (2) dos años	Unidad	$ 428,000
	Certificado Digital Representación Legal, vigencia (1) un año	Unidad	$ 306,000
	Certificado Digital Representación Legal, vigencia (2) dos años	Unidad	$ 428,000
	Reposición Vigencia (1) un año sin token	Unidad	$ 306,000
	Reposición Vigencia (2) dos años sin token	Unidad	$ 428,000
Certificado Digital Token Físico (Reuso)	Certificado Digital Persona Natural, vigencia (1) un año	Unidad	$ 265,000
	Certificado Digital Persona Natural, vigencia (2) dos años	Unidad	$ 350,000
	Certificado Digital Pertenencia a Empresa, vigencia (1) un año	Unidad	$ 265,000
	Certificado Digital Pertenencia a Empresa, vigencia (2) dos años	Unidad	$ 350,000
	Certificado Digital Profesional Titulado, vigencia (1) un año	Unidad	$ 265,000
	Certificado Digital Profesional Titulado, vigencia (2) dos años	Unidad	$ 350,000
	Certificado Digital Representación Legal, vigencia (1) un año	Unidad	$ 265,000

USO EXCLUSIVO DE CERTICÁMARA S.A.

POLÍTICA DE CERTIFICACIÓN – CERTIFICADO DE FIRMA DIGITAL

Producto	Artículo	Tipo	Precio
	Certificado Digital Representación Legal, vigencia (2) dos años	Unidad	$ 350,000
Certificado Digital Certitoken	Certificado Digital Función Pública, vigencia (1) un año	Unidad	$ 226,000
	Certificado Digital Función Pública, vigencia (2) dos años	Unidad	$ 301,000
	Certificado Digital Persona Natural, vigencia (1) un año	Unidad	$ 226,000
	Certificado Digital Persona Natural, vigencia (2) dos años	Unidad	$ 301,000
	Certificado Digital Pertenencia a Empresa, vigencia (1) un año	Unidad	$ 226,000
	Certificado Digital Pertenencia a Empresa, vigencia (2) dos años	Unidad	$ 301,000
	Certificado Digital Profesional Titulado, vigencia (1) un año	Unidad	$ 226,000
	Certificado Digital Profesional Titulado, vigencia (2) dos años	Unidad	$ 301,000
	Certificado Digital Representación Legal, vigencia (1) un año	Unidad	$ 226,000
	Certificado Digital Representación Legal, vigencia (2) dos años	Unidad	$ 301,000
	Reposición Vigencia (1) un año	Unidad	$ 226,000
	Reposición Vigencia (2) dos años	Unidad	$ 301,000
Certificado Digital PKCS#10	Certificado Digital Persona Natural / Jurídica, vigencia (1) un año	Unidad	$ 606,000
	Certificado Digital Persona Natural / Jurídica, vigencia (2) dos años	Unidad	$ 903,000
	Reposición Vigencia (1) un año	Unidad	$ 606,000
	Reposición Vigencia (2) dos años	Unidad	$ 903,000

- 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.

USO EXCLUSIVO DE CERTICÁMARA S.A.

Los solicitantes tendrán la posibilidad de obtener las tarifas aplicables a través del siguiente link https://solicitudes.certicamara.com/ssps/Solicitudes/AceptoLosTerminos.aspx, 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.

Para tal efecto podrán ingresar a través de la página Web de Certicámara, www.certicamara.com al Sistema de solicitud de productos y servicios para generar el formulario de solicitud y la Orden de pedido correspondiente e iniciar su proceso de adquisición.

10.1 Políticas de Reembolso para Suscriptores

Los suscriptores de certificados digitales podrán solicitar reembolso de dinero en los siguientes casos:

- **Cuando se realiza una consignación por un valor mayor al establecido:** en este caso la Gerencia Administrativa y Financiera realiza las validaciones necesarias para confirmar el pago adicional, en el evento que la validación sea exitosa se efectuará el respectivo reembolso a la entidad o persona que haya realizado dicha solicitud.

- **Cuando se solicita un certificado digital que no aplique para el suscriptor**: la Dirección de Operaciones realiza verificación de los certificados digitales emitidos para el suscriptor y de acuerdo si el resultado de esta validación confirma que el certificado de firma digital no se requiere, autoriza a la Gerencia Administrativa y Financiera para proceder con el reembolso.

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://solicitudes.certicamara.com/ssps/Solicitudes/AceptoLosTerminos.aspx.

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

- RSA 2048, Entidad Final / RSA 4096, Root CA.
- FIPS PUB 180-4 Secure Hash Standard (SHS) 2015-08 - SHA 256

USO EXCLUSIVO DE CERTICÁMARA S.A.

- RFC 5280: mayo 2008 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- RFC 4523: junio 2006 - Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates.
- RFC 3647: noviembre 2003 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
- ETSI TS 102 042 Febrero 2013
- FIPS 140-2 Level 3 Mayo 2001
- ITU-T-X509: octubre 2019 - Tecnología de la información - Interconexión de sistemas abiertos - El directorio: Marcos para certificados de claves públicas y atributos.

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.
28/09/2022	✓ Se realizan los siguientes cambios al documento: ○ Cuidados para la protección de los dispositivos criptográficos físicos, virtuales y PKCS#10. ○ Información publicada en las plantillas para cada política. ○ 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

USO EXCLUSIVO DE CERTICÁMARA S.A.

Fecha	Razón de actualización
	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.
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: m) 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.

USO EXCLUSIVO DE CERTICÁMARA S.A.

POLÍTICA DE CERTIFICACIÓN – CERTIFICADO DE FIRMA DIGITAL

Fecha	Razón de actualización
	• 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.