certicámara.

Declaración de Prácticas de Certificación

Código: DYD-L-003

Fecha: Septiembre de 2025

Versión: 021

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Contenido

1. INTRODUCCIÓN **8**
1.1 Identificación de la entidad de certificación digital 8
1.2 Nombre e identificación del documento 9
1.3 Participantes de PKI 9
1.3.1 Autoridades de certificación 9
1.3.2 Autoridades de registro 11
1.3.3 Suscriptores 12
1.3.4 Partes que confían 12
1.3.5 Otros participantes 12
1.4 Uso de certificados 13
1.4.1 Usos apropiados del certificado 13
1.4.2 Usos prohibidos del certificado 14
1.5 Administración de políticas 14
1.5.1 Organización que administra el documento 14
1.5.2 Persona de contacto 14
1.5.3 Procedimiento para la actualización y aprobación de la DPC 15
1.6 Definiciones y siglas 15
2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO **18**
2.1 Repositorios 18
2.2 Publicación de información de certificación 18
2.3 Momento o frecuencia de publicación 19
2.3.1 Certificados de la CA Raíz 19
2.3.2 Lista de Certificados Revocados (CRL) 20
2.3.3 Estado de revocación de certificados OCSP 20
2.4 Controles de acceso a los repositorios 20
3. IDENTIFICACIÓN Y AUTENTICACIÓN **20**
3.1 Denominación 20
3.1.1 Tipos de nombres 20
3.1.2 Necesidad de que los nombres sean significativos 21
3.1.3 Anonimato o seudónimo de los suscriptores 21
3.1.4 Reglas para interpretar varias formas de nombres 21
3.1.5 Unicidad de los nombres 22
3.1.6 Reconocimiento, autenticación y función de las marcas 22
3.2 Validación de identidad inicial 22
3.2.1 Método para probar la posesión de la clave privada 22
3.2.2 Autenticación de la identidad de la organización o persona 22
3.2.3 Comprobación de las facultades de representación 22
3.2.4 Mecanismos de validación de identidad 22

3.2.5 Información del suscriptor no verificada 23
3.2.6 Criterios de interoperabilidad 23
3.3 Identificación y autenticación para solicitudes de renovación de claves 23
4. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO 23
4.1 Solicitud de certificado 23
4.1.1 ¿Quién puede presentar una solicitud de certificado? 26
4.2 Emisión de certificados 26
4.2.1 Acciones de la CA durante la emisión del certificado 26
4.2.2 Notificación al suscriptor por parte de la CA de emisión de certificado 27
4.3 Entrega del certificado digital a los suscriptores por medio físico 27
4.3.1 Cubrimiento 27
4.3.2 Requisitos de entrega 27
4.3.3 Tiempo de gestión de entrega – Certificados Físicos 28
4.3.4 Tiempo de descarga 28
4.4 Aceptación del certificado 28
4.4.1 Publicación del certificado por la CA 29
4.4.2 Notificación de emisión de certificados por parte de la CA a otras entidades 29
4.5 Desistimiento 29
4.6 No devolución del dinero 29
4.7 Uso de pares de claves y certificados 29
4.7.1 Generación e instalación de pares de claves 29
4.7.2 Uso de certificado y clave privada del suscriptor 30
4.7.3 Uso del certificado y la clave pública del usuario de confianza 30
4.8 Renovación del certificado 30
4.8.1 Tiempos para la renovación 30
4.8.2 ¿Quién puede solicitar la renovación? 31
4.8.3 Tramitación de solicitudes de renovación de certificados 31
4.8.4 Notificación de emisión de nuevo certificado al suscriptor 31
4.9 Renovación de llave de certificado 31
4.10 Modificación del certificado 31
4.11 Revocación de certificados 31
4.11.1 Causales para la revocación 31
4.11.2 ¿Quién puede solicitar la revocación? 32
4.11.3 Procedimiento para solicitud de revocación 33
4.11.4 Período de gracia de la solicitud de revocación 34
4.11.5 Frecuencia de emisión de CRL 34
4.11.6 Disponibilidad de verificación de estado/revocación en línea 34
4.11.7 Requisitos de verificación de revocación en línea 34

4.11.8 Circunstancias de suspensión 34
4.12 Reposición de Certificados de Firma Digital 34
4.12.1 Causales para la Reposición 36
4.13 Características de los certificados 36
4.13.1 Características operativas 36
4.13.2 Disponibilidad del servicio 37
4.13.3 Funciones opcionales 37
4.14 Fin de la suscripción 37
4.15 Custodia y recuperación de llaves 37
4.15.1 Política y prácticas de custodia y recuperación de llaves 37
5. CONTROLES DE INSTALACIONES, GESTIÓN Y OPERACIÓN 38
5.1 Controles físicos 38
5.1.1 Ubicación y construcción del sitio 38
5.1.2 Acceso físico 38
5.1.3 Energía y aire acondicionado 38
5.1.4 Exposiciones al agua 39
5.1.5 Prevención y protección contra incendios 39
5.1.6 Almacenamiento de medios 39
5.1.7 Eliminación de residuos 39
5.1.8 Copia de seguridad fuera del sitio 39
5.2 Controles de procedimiento 39
5.2.1 Roles de confianza 39
5.2.2 Número de personas requeridas por tarea 40
5.2.3 Identificación y autenticación para cada rol 40
5.2.4 Roles que requieren separación de funciones 40
5.3 Controles de personal 40
5.3.1 Calificaciones, experiencia y requisitos de autorización 40
5.3.2 Procedimientos de verificación de antecedentes 41
5.3.3 Requisitos de formación 41
5.3.4 Sanciones por acciones no autorizadas 41
5.3.5 Requisitos del contratista independiente 41
5.3.6 Documentación suministrada al personal 41
5.4 Procedimientos de registro de auditoría (Logs) 41
5.4.1 Tipos de eventos registrados 42
5.4.2 Frecuencia de procesamiento del registro 42
5.4.3 Período de retención para el registro de auditoría 42
5.4.4 Protección del registro de auditoría 42
5.4.5 Evaluaciones de vulnerabilidad 42

5.5 Archivo de registros 42
5.5.3 Protección del archivo 43
5.5.4 Procedimientos de copia de seguridad de archivos 43
5.5.5 Procedimientos para obtener y verificar información de archivo 43
5.6 Cambio de clave 43
5.7 Compromiso y recuperación ante desastres 43
5.7.1 Procedimientos de manejo de incidentes y compromisos 44
5.7.2 Capacidades de continuidad del negocio después de un desastre 44
5.8 Cese de actividades 44
6. CONTROLES DE SEGURIDAD TÉCNICA 45
6.1 Generación e instalación de pares de claves 45
6.1.1 Entrega de llave privada al suscriptor 45
6.1.2 Entrega de clave pública al emisor del certificado 46
6.1.3 Entrega de clave pública de la CA a partes de confianza 46
6.1.4 Tamaños de clave 46
6.1.5 Propósitos de uso de clave (según el campo de uso de clave X.509 v3) 46
6.2 Protección de clave privada e ingeniería de módulos criptográficos 47
6.2.1 Estándares y controles del módulo criptográfico 47
6.2.2 Clave privada (K de N) control multipersona 47
6.2.3 Custodia de la clave privada 48
6.2.4 Copia de seguridad de clave privada 48
6.2.5 Archivo de claves privadas 48
6.2.6 Almacenamiento de claves privadas en módulo criptográfico 48
6.2.7 Método de activación de clave privada 48
6.2.8 Método de desactivación de clave privada 48
6.2.9 Método de destrucción de clave privada 49
6.2.10 Calificación del módulo criptográfico 49
6.3 Otros aspectos de la gestión de pares de claves 49
6.3.1 Archivo de claves públicas 49
6.3.2 Períodos operativos del certificado y períodos de uso del par de claves 49
6.4 Datos de activación 49
6.4.1 Generación e instalación de datos de activación 49
6.4.2 Protección de datos de activación 49
6.5 Controles de seguridad informática 50
6.5.1 Requisitos técnicos específicos de seguridad informática 50
6.5.2 Calificación de seguridad informática 50
6.6 Controles técnicos del ciclo de vida 50
6.6.1 Controles de desarrollo del sistema 50

6.6.2 Controles de gestión de la seguridad 50
6.6.3 Controles de seguridad del ciclo de vida 51
6.7 Controles de seguridad de la red 51
6.8 Sellado de tiempo 51
7. PERFILES DE CERTIFICADO, CRL Y OCSP 51
7.1 Perfil de certificado 51
7.1.1 Número(s) de versión 51
7.1.3 Identificadores de objetos de algoritmo 52
7.1.4 Formas de nombre 52
7.1.5 Restricciones de nombre 52
7.1.6 Identificador de objeto de política de certificados 52
7.1.7 Sintaxis y semántica de calificadores de políticas 52
7.2 Perfil de lista de revocación de certificados 52
7.2.1 Número(s) de versión 52
7.2.2 CRL y extensiones de entrada de CRL 53
7.3 Perfil OCSP 53
7.3.1 Número(s) de versión 53
7.3.2 Extensiones OCSP 53
8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES 53
8.1 Frecuencia o circunstancias de la evaluación 53
8.2 Identidad/calificaciones del evaluador 54
8.3 Relación del evaluador con la entidad evaluada 54
8.4 Acciones tomadas como resultado de una no conformidad 54
8.5 Comunicación de resultados 54
9. OTROS ASUNTOS LEGALES Y COMERCIALES 54
9.1 Tarifas 54
9.1.1 Tarifas de emisión o renovación de certificados 54
9.1.2 Tarifas de acceso a la información de revocación o estado 54
9.1.3 Política de reintegro 55
9.2 Responsabilidad financiera 56
9.2.1 Cobertura de seguro 56
9.3 Confidencialidad de la información 56
9.3.1 Alcance de la información confidencial 57
9.3.2 Información fuera del alcance de la información confidencial 57
9.3.3 Responsabilidad de proteger la información confidencial 57
9.3.4 Tratamiento de Datos personales 58
9.3.5 Revelación en virtud de un proceso judicial o administrativo 59
9.4 Derechos de propiedad intelectual 59

9.5 Obligaciones y responsabilidades de los intervinientes 60
9.5.1 Obligaciones y deberes de Certicámara 60
9.5.2 Obligaciones y deberes del solicitante 62
9.5.3 Obligaciones y responsabilidades del suscriptor 62
9.5.4 Obligaciones y responsabilidades de la parte que confía 64
9.5.5 Obligaciones de los contratistas 65
9.6 Límites de responsabilidad 65
9.7 Derechos de los intervinientes 66
9.7.1 Derechos del solicitante 66
9.7.2 Derechos del suscriptor 66
9.8 Exclusión de garantías 67
9.9 Minutas de contratos 67
9.10 Política de manejo de otros servicios 68
9.11 Imparcialidad y no discriminación 68
9.12 Política de Peticiones, quejas, reclamos, sugerencias y felicitaciones 69
9.13 Disposiciones de resolución de disputas 70
9.14 Ley aplicable 71
9.15 Políticas de certificación 72
10. CONTROL DE CAMBIOS 72

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

1. INTRODUCCIÓN

La presente Declaración de Prácticas de Certificación (DPC) constituye la manifestación pública de la Entidad de Certificación Digital Abierta, en la cual se establecen las normas y prácticas adoptadas por la Autoridad de Certificación para la provisión de servicios de certificación digital. Esto se realiza en concordancia con la Ley 527 de 1999 y sus decretos compilatorios y modificatorios (Decreto 1074 de 2015, Decreto 620 de 2020), así como con la Ley 2106 de 2019, Ley 1581 de 2012, Ley 1898 de 2018 (Artículo 13.10) y el Decreto Ley 019 de 2012 (particularmente las actividades del artículo 161).

Este documento detalla las prácticas para los servicios acreditados ofrecidos por la Sociedad Cameral de Certificación Digital Certicámara S.A.: Certificado de firma digital, Estampado Cronológico, Huella Biométrica Certificada, Correo Electrónico Certificado, Generación De Firmas Digitales y Generación De Firmas Electrónicas Certificadas.

La DPC está destinada a personas naturales y jurídicas que solicitan o utilizan los servicios de certificación digital, así como a terceros que confían en su validez jurídica y probatoria en los diferentes contextos de su aplicación.

El presente documento se ha estructurado conforme al estándar RFC 3647.

1.1 Identificación de la entidad de certificación digital

La Sociedad Cameral de Certificación Digital Certicámara S.A. (en adelante, Certicámara) es una sociedad anónima constituida por las Cámaras de Comercio de Bogotá, Medellín, Cali, Bucaramanga, Cúcuta, Aburrá Sur y Confecámaras, con el fin de ofrecer servicios de certificación digital. Certicámara, filial de la Cámara de Comercio de Bogotá, opera como una Entidad de Certificación Digital Abierta, actuando como un tercero de confianza para la seguridad de productos y servicios electrónicos. Su propósito principal es proporcionar a empresarios y usuarios de Internet en el país las herramientas necesarias para realizar negocios electrónicos con seguridad jurídica.

Nombre:	Sociedad Cameral de Certificación Digital Certicámara S.A.
NIT:	830.084.433-7
Matrícula mercantil:	1079279
Certificado de existencia y representación legal:	https://web.certicamara.com/nosotros
Domicilio principal:	Bogotá
Dirección:	Carrera 7 N° 26-20 Pisos 18, 19 y 31
Teléfono (asuntos administrativos):	(601) 9157808

Correo Electrónico	info@certicamara.com
Teléfono (ventas, servicio al cliente y soporte técnico)	(601) 7442727 o (601) 7442725
Responsable de la recepción de las peticiones, consultas y reclamos de los suscriptores y usuarios	Dirección de Mejoramiento Continuo
Responsable de la revisión y aprobación de las respuestas a las peticiones, consultas y reclamos de los suscriptores y usuarios	Director de Mejoramiento Continuo
Correo Electrónico PQRS	certicamararesponde@certicamara.com
Dirección WEB	www.certicamara.com
N° Certificado de Acreditación	16-ECD-002
Certificado de Acreditación	https://onac.org.co/certificados/16-ECD-002.pdf

1.2 Nombre e identificación del documento

Certicámara para la prestación de sus diferentes servicios, establece la siguiente información para el presente documento.

Nombre	Declaración de Prácticas de Certificación – DPC
Fecha de publicación	26/09/2025
Versión	021
Código	DYD-L-003
Ubicación	https://web.certicamara.com/marco-normativo

Nota: En caso de requerir la consulta de una versión anterior de este documento, esta deberá solicitarse al correo de info@certicamara.com para que se atienda su solicitud.

1.3 Participantes de PKI

1.3.1 Autoridades de certificación

Es una entidad de confianza que presta servicios de certificación. Está facultada para emitir, gestionar y revocar los certificados digitales actuando como tercera parte de confianza entre el suscriptor y el usuario titular de un certificado, o los terceros de confianza.

Certicámara cuenta con la siguiente CA:

Autoridad de Certificación AC Raíz: La AC Raíz, es la Autoridad de Certificación origen de la jerarquía de certificación digital. Este componente de Certicámara es responsable de la emisión de los certificados digitales que acreditan su plataforma de emisión.

La estructura de sus datos es:

- Campo del Certificado Raíz
- Valor del Certificado Raíz
- Clave de la AC Raíz 4096 bits
- Vigencia hasta el 24 de mayo de 2031 01:39:46 pm
- Versión V3
- Número de serial del certificado
- Identificador único del certificado. Menor de 32 caracteres hexadecimales.
- Algoritmo de firma del certificado: SHA256withRSAEncryption
- SHA1: 54 63 28 3b 67 93 ff 55 27 7c ed e3 90 98 e8 04 22 f9 12 f7
- Número Serial: 43 1c 28 c6 74 0f ed 25 57 44 9f f2 fd 0e 5e 14

Certificadoras subordinadas

En el marco normativo colombiano, estos son derivados de la jerarquía de la AC Raíz, donde requieren que la AC Raíz les firme su certificado para que ellos a su vez emitan certificados a los suscriptores finales siguiendo con la cadena de confianza desde el punto raíz de Certicámara, como Entidad de Certificación Digital Abierta acreditada por ONAC bajo el Certificado de Acreditación número 16-ECD-002.

Para todas las CA's pertenecientes a la infraestructura de llave pública de Certicámara, aplica lo expresado en la DPC coherente con los requisitos generales establecidos por el marco jurídico descrito en el acápite sobre las referencias normativas.

La estructura de los datos del certificado para las autoridades subordinadas es:

- Campo del Certificado de la CA Raíz.
- Clave pública de la ENTIDAD SUBORDINADA 4096 bits
- Versión V3
- Número de serial del certificado
- Identificador único del certificado. Menor de 32 caracteres hexadecimales.
- Algoritmo de firma del certificado SHA256withRSAEncryption
- Datos del emisor
- CN
- Autoridad de Certificación Raíz de la cadena de certificación.
- SHA1: 26 c5 8f b4 36 4f f6 21 ce 2a 04 c7 3e bf b2 ac 09 c3 5f 56
- Número Serial: 58 1f 6a de 78 78 fe 8c 56 ac db d7 a6 77 58 10

Autoridad de estampado de tiempo

El "**Estampado cronológico**" es suministrado por **Certicámara** en un formato

electrónico seguro y adecuado definido de modo que se incorpora al mensaje de datos generado, transmitido o recibido por el suscriptor impidiendo su posterior alteración. El "**estampado cronológico**" de un mensaje de datos es único para este y no puede ser incorporado a otro u otros mensajes de datos diferentes.

El servicio de estampado se encuentra en la siguiente URL http://tsa.certicamara.com:9233/ donde el suscriptor deberá tener un usuario y contraseña para hacer consumo del servicio respectivo.

Esto se explica de la siguiente manera: (i) Un usuario quiere obtener un sello de tiempo para un documento electrónico que él posee; (ii) Un resumen digital (técnicamente un hash) se genera para el documento en el dispositivo que solicita el estampado; (iii) Este resumen forma la solicitud que se envía a la entidad de certificación que presta el **servicio de estampado cronológico**; (iv) La entidad de certificación que presta el **servicio de estampado cronológico** genera un sello de tiempo (o estampa cronológica) con este resumen digital, la fecha y hora obtenida de una fuente fiable y la firma digital. De esta manera, al estampar cronológicamente esta representación resumida del documento, lo que realmente se está haciendo es sellar el documento original; (v) El sello de tiempo se envía de vuelta al usuario; y (vi) La entidad de certificación que presta los servicios de **estampado cronológico** mantiene un registro de los sellos emitidos para su futura verificación. La estructura del servicio de Estampado Digital TSA (Time Stamp Authority) está descrito en el documento RFC 3628 y el Protocolo TSP (Time-Stamp Protocol) en el RFC 3161.

1.3.2 Autoridades de registro

Autoridad de Registro (RA): Es la encargada de recibir las solicitudes relacionadas con certificación digital, registrar las peticiones que hagan los solicitantes para obtener un certificado, comprobar la veracidad y corrección de los datos que aportan los usuarios en las peticiones, enviar las peticiones que cumplen los requisitos a una CA para que sean procesadas.

La autoridad de registro de Certicámara está compuesta por:

- **Software de la RA**: Facilita el registro de solicitudes y permite la gestión del ciclo de vida de la solicitud de certificación.
- **Agentes de la RA**: Usuarios de la RA con privilegios. Son los responsables de la revisión y validación de la información contenida en los documentos remitidos por el solicitante para la emisión de un servicio de la ECD.
- **Administrador RA**: La persona responsable de administrar y configurar la RA.
- **System Auditor**: Es la persona encargada de auditar el cumplimiento de los procedimientos y sistemas de la RA, validando que se cumpla lo establecido en la Declaración de Prácticas de Certificación (DPC) y Políticas de Certificación (PC).

1.3.3 Suscriptores

Suscriptor es la persona natural a la cual se emiten o activan los servicios de certificación digital y por tanto actúa como suscriptor y/o responsable del mismo, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en esta DPC y la política de certificación del servicio adquirido.

1.3.4 Partes que confían

Persona natural o jurídica diferente del suscriptor y/o responsable que decide aceptar y confiar en los servicios de certificación prestados por Certicámara.

1.3.5 Otros participantes

a. Proveedores de servicios

Los proveedores críticos seleccionados para la prestación del servicio de Datacenter satisfacen los requisitos mínimos establecidos en el documento Criterios Específicos de Acreditación CEA 3.0-7, disponible en la página web de ONAC. Por lo tanto, se les requerirá el cumplimiento de los requisitos detallados en dicho documento en los casos que corresponda.

Nombre:	Comunicación Celular S.A. Comcel S.A.
NIT:	800.153.993-7
Matrícula Mercantil:	487585
Certificado de Existencia y Representación Legal	https://web.certicamara.com/nosotros
Domicilio Principal	Bogotá
Dirección	Carrera 68 A N° 24 B 10
Teléfono	(601) 7480000 - 7500300
Correo Electrónico	notificaciones@claro.com.co
Sitio WEB	www.claro.com.co

Nombre	Sencinet Latam Colombia S.A.
NIT	800.255.754 - 1
Matrícula Mercantil	637298
Certificado de Existencia y Representación Legal	https://web.Certicámara.com/nosotros
Domicilio Principal	Bogotá
Dirección	Calle 113 N 7-21 Torre A Of 1112
Teléfono	(601) 6292262
Correo Electrónico	maria.diaz@sencinet.com
Sitio WEB	https://sencinet.com/

1.4 Uso de certificados

1.4.1 Usos apropiados del certificado

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

Usos generales aplicables a los certificados digitales emitidos por Certicámara:

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

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

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

1.4.2 Usos prohibidos del certificado

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

1.5 Administración de políticas

1.5.1 Organización que administra el documento

La totalidad de la información consignada en la presente **Declaración de Prácticas de Certificación (DPC)** y **Políticas de Certificación (PC)** constituye propiedad intelectual de Certicámara, cuya administración se realiza en concordancia con los lineamientos establecidos en su interior.

1.5.2 Persona de contacto

Dentro de Certicámara se ha establecido que la persona de contacto para los temas relacionados con la presente **Declaración de Prácticas de Certificación (DPC)** y **Políticas de Certificación (PC)** es el Director de Mejoramiento Continuo

Nombre:	Angela Viviana Leandro Herández
Cargo:	Director de Mejoramiento Continuo
Correo:	certicamararesponde@certicamara.com
Teléfono:	(601) 9157808
Dirección:	Carrera 7 N° 26-20 Piso 18

1.5.3 Procedimiento para la actualización y aprobación de la DPC

La actualización de la Declaración de Prácticas de Certificación se llevará a cabo cuando así lo exijan los requerimientos legales, normativos y/o aquellos aplicables a los servicios acreditados.

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

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

1.6 Definiciones y siglas

- **Algoritmo**: Es un conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien deba realizar dicha actividad. Dados un estado inicial y siguiendo los pasos sucesivos se llega a un estado final y se obtiene una solución.
- **Autoridad de Certificación (CA):** Entidad de confianza, responsable de emitir y revocar los certificados.
- **Autoridad de Sellado de Tiempo (TSA):** Time Stamp Authority, (Autoridad de sellado de tiempo)
- **Autoridad de Validación (VA):** Entidad de confianza que proporciona información sobre la validez de los certificados digitales.
- **CA Raíz:** Autoridad certificadora de primer nivel, base de confianza.
- **CA Subordinada:** Autoridad certificadora de segundo nivel o más niveles.
- **Certificado Digital:** Mensaje de datos electrónico firmado por la entidad de certificación digital, el cual identifica tanto a la entidad de certificación que lo expide, como al suscriptor y contiene la llave pública de éste último.
- **Cliente:** En los servicios de certificación digital, el término cliente identifica a la persona natural o jurídica con la cual la ECD establece una relación comercial.
- **Datos de Creación de Firma (Llave Privada):** Son valores numéricos únicos que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos.
- **Datos de Verificación de Firma (Llave Pública):** Son los datos, como códigos o claves criptográficas públicas, que son utilizados para verificar que una firma digital fue generada con la llave privada del suscriptor.
- **Declaración de Prácticas de Certificación (DPC):** Declaración de prácticas de certificación. Documento oficial presentado por la Entidad de Certificación

Digital, en el cual define normas y prácticas de la Autoridad de Certificación para la prestación de los servicios de certificación digital.

- **Declinación de la solicitud de servicio:** Es el rechazo de un servicio de certificación digital, el cual no se encuentra dentro del alcance de la acreditación que le fue otorgado por ONAC o por el incumplimiento de la ley. En este caso, no habrá lugar a la subsanación por parte del usuario.
- **Entidad de Certificación Abierta**: La que ofrece al público en general, servicios propios de las ECD, tales que: su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, y recibe remuneración.
- **Entidad de Certificación Digital (ECD):** Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.
- **Estampado Cronológico (Time Stamping):** Mensaje de datos firmado digitalmente y con sello de tiempo por una TSA que vincula a otro mensaje de datos con un momento de tiempo concreto, el cual permite establecer con una prueba que estos datos existían en ese momento y que no sufrieron ninguna modificación a partir del momento en que se realizó el estampado.
- **ETSI:** European Telecommunications Standards Institute
- **FIPS**: Federal Information Processing Standards (FIPS, en español Estándares Federales de Procesamiento de la Información) son estándares anunciados públicamente desarrollados por el gobierno de los Estados Unidos para la utilización por parte de todas las agencias del gobierno no militares y por los contratistas del gobierno. Muchos estándares FIPS son versiones modificadas de los estándares usados en las comunidades más amplias (ANSI, IEEE, ISO, etc.)
- **Firma Digital:** Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.
- **Firma Electrónica:** Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

    a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;
    b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.
- **Función HASH:** Es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos

de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.

- **HSM:** Hardware Security Module
- **LDAP:** Lightweight Directory Access Protocol
- **Lista de Certificados Digitales Revocados (CRL):** Es aquella lista de certificados digitales que han sido revocados por la Autoridad de Certificación (CA), que no han cumplido su fecha de vencimiento programada y que ya no deben ser confiables
- **Log:** Servicio de registro de eventos del sistema de información, dejando la información anterior y la actual, identifica quién y cuándo se realizó el evento.
- **Negación de la solicitud de servicio:** Se negará un servicio de certificación digital, por motivos ajenos a Certicámara S.A., y que se encuentren en cabeza del usuario, siempre y cuando, puedan ser subsanados por este último.
- **Neutralidad Tecnológica**: Principio de no discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente, así mismo la no discriminación, preferencia o restricción de ninguna de las diversas técnicas o tecnologías que pueden utilizarse para firmar, generar, comunicar, almacenar o archivar electrónicamente información.
- **OID:** Identificador único de objeto (Object Identifier). OID. acrónimo del término en idioma inglés “Object Identifier”, que consiste en un número único de identificación asignado en base a estándares internacionales y comúnmente utilizado para identificar documentos, sistemas, equipos, etc., con la finalidad, entre otras cosas, de conocer el origen, la titularidad y la antigüedad del objeto identificado.
- **PKI** (Public Key Infraestructure): Es el conjunto de hardware, software, políticas, procedimientos y elementos tecnológicos que, mediante la utilización de un par de claves criptográficas, una privada que sólo posee el suscriptor del servicio y una pública, que se incluye en el certificado digital.
- **Políticas de Certificado (PC):** Es el conjunto de reglas que indica los requisitos de un certificado en una comunidad y/o clase en particular, en el marco de los requisitos legales, reglamentarios, y con requisitos de seguridad comunes.
- **Recomendación para la decisión:** Comunicado emitido por parte de la Autoridad de Registro (RA) hacia la Autoridad de Certificación (CA), para aprobar la solicitud de prestación de servicios al solicitante por parte de Certicámara S.A.
- **Revocación**: Para este documento, es el proceso por el cual se inhabilita el certificado digital emitido y se da por terminado su periodo de validez de uso a partir de la fecha de revocación; al presentarse alguna de las causas establecidas en la declaración de prácticas de certificación.
- **Servicio de Certificación Digital**: Conjunto de actividades certificación que ofrece la ECD para certificar el origen e integridad de mensajes de datos, basados en las firmas digitales o electrónicas, estampado de tiempo, así como en la aplicabilidad de estándares técnicos admitidos y vigentes en infraestructura de llave pública – PKI.

- **Servicio del Estado del Certificado en Línea OCSP**: Actividad de consulta en tiempo real al sistema de la ECD, sobre el estado de un certificado digital a través del protocolo OCSP.
- **Solicitante**: Persona natural o jurídica que, con el propósito de obtener servicios de certificación digital de una ECD, demuestra el cumplimiento de los requisitos establecidos en la DPC y PC de éstas, para acceder al servicio de certificación digital.
- **Suscriptor**: Persona natural o jurídica a cuyo nombre se expide un certificado digital.
- **Token**: Dispositivo hardware criptográfico suministrado por una ECD, el cual contiene el certificado digital y la llave privada del suscriptor.
- **UpTime**: Compromiso en término de porcentaje de tiempo disponible de un sistema de información, que la empresa proveedora de éste se compromete a ofrecer a su cliente por año.
- **Usabilidad**: Es un término proveniente del inglés "Usability", empleado para denotar la forma en la que una persona puede emplear una herramienta particular de manera efectiva, eficiente y satisfactoria, en función de lograr una meta específica.

2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO

2.1 Repositorios

Los Certificados de la CA raíz, CA Subordinada y lista de certificados revocados CRL 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% y en caso de interrupción por causa de fuerza mayor, el servicio se restablecerá en el tiempo establecido de acuerdo con el porcentaje de disponibilidad. Para el caso de la PKI se establece una disponibilidad del 99,8%.

2.2 Publicación de información de certificación

a) Para los certificados de las AC Raíz y la Entidad Subordinada Acreditados**:**

- WEB:
  CA Raíz Certicámara S.A.
  http://www.certicamara.com/repositoriorevocaciones/ac_offline_raiz_certicamara_.cer

- CA Subordinada Certicámara S.A.
  http://www.certicamara.com/repositoriorevocaciones/ac_online_subordinada_certicamara_.crt
  http://www.certicamara.com/repositoriorevocaciones/ac_online_subordinada4096_certicamara_.crt

b) Para la lista de certificados revocados (CRL):

- WEB:
  - CA Raíz Certicámara S.A.
    http://www.certicamara.com/repositoriorevocaciones/ac_raiz_certicamara.crl

  - CA Subordinada Certicámara S.A.
    http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara.crl
    http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_2014.crl
    http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica.crl

    http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_2014.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

c) Para la DPC:
  - WEB:
    https://web.certicamara.com/marco-normativo

d) Para la verificación de estado de revocación de certificados OCSP
  - **o** WEB:
    http://ocsp.Certicamara.com

    http://ocsp.Certicamara.co

    http://ocsp4096.certicamara.co

A través de esta URL el usuario puede consultar directamente la revocación de un certificado, para esto se debe disponer de un Cliente OCSP que cumpla el RFC 6960. Si el usuario no cuenta con este Cliente OCSP, deberá descargar la lista completa de los certificados revocados (CRL).

El repositorio público de la AC raíz no contiene ninguna información confidencial o privada.

2.3 Momento o frecuencia de publicación

2.3.1 Certificados de la CA Raíz

La publicación del certificado se realizará con anterioridad a su puesta en vigencia a través de la página web de Certicámara. El periodo de validez es hasta el sábado, 24 de mayo de 2031 13:39:46.

2.3.2 Lista de Certificados Revocados (CRL)

Se realiza la publicación de la lista de Certificados Revocados de la CA Subordinada Certicámara S.A. (CRL) con vigencia de tres (3) días:

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

2.3.3 Estado de revocación de certificados OCSP

El servicio se encuentra disponible de manera continua las 24 horas, los 365 días del año para su consulta vía web y se actualiza automáticamente en los siguientes casos:

- Cada vez que se revoque un certificado digital.

2.4 Controles de acceso a los repositorios

El acceso a la información publicada por la CA Raíz será únicamente para consulta, y su modificación estará restringida a personal autorizado. La actualización de la información pública será realizada exclusivamente por el personal de Certicámara asignado a esta función.

Además, se garantiza la consulta a la CRL, a los certificados emitidos, al servidor OCSP y DPC en sus versiones anteriores y actualizadas.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 Denominación

Todos los certificados tienen una sección denominada Asunto o Subject cuyo objetivo es permitir identificar al suscriptor del certificado, esta sección contiene un DN o DistinguishedName caracterizado por un conjunto de atributos que conforman un nombre inequívoco y único para cada suscriptor de los certificados emitidos por Certicámara.

3.1.1 Tipos de nombres

Los atributos de cada tipo de certificado se establecen en la política de emisión de certificados. Cada tipo de certificado se identificará por un OID (Object Identifier) único, incluido en el certificado como identificador de política, dentro de las propiedades del certificado.

OID	Tipo de Política
1.3.6.1.4.1.23267.50.1.1	Certificado de Pertenencia a Empresa / Entidad en dispositivos locales y/o centralizados
1.3.6.1.4.1.23267.50.1.2	Certificado de Representación de Empresa / Entidad en dispositivos locales y/o centralizados
1.3.6.1.4.1.23267.50.1.3	Certificado de Titular de Función Pública en dispositivos locales y/o centralizados
1.3.6.1.4.1.23267.50.1.4	Certificado de Profesional Titulado en dispositivos locales y/o centralizados
1.3.6.1.4.1.23267.50.1.5	Certificado digital persona natural / jurídica en dispositivos locales y/o centralizados
1.3.6.1.4.1.23267.50.1.8.5	Certificado digital persona natural PKCS#10
1.3.6.1.4.1.23267.50.1.8.4	Certificado digital persona jurídica PKCS#10

3.1.2 Necesidad de que los nombres sean significativos

Las políticas definidas, garantizan que los nombres distintivos (DN) de los certificados son suficientemente significativos para vincular la clave pública con una identidad.

3.1.3 Anonimato o seudónimo de los suscriptores

Certicámara no admite anónimos ni seudónimos para identificar el nombre de una persona natural o jurídica. En el caso de una entidad o persona jurídica el nombre debe ser exactamente igual a la razón social, no se admiten nombres abreviados. En el caso de una persona natural el nombre debe estar conformado por nombres y apellidos tal como figura en el documento de identificación reconocido. Excepcionalmente, podrán utilizarse contracciones o abreviaciones siempre que exista consentimiento previo, expreso y por escrito del titular, y que se conserve evidencia documental de dicha autorización.

3.1.4 Reglas para interpretar varias formas de nombres

Las reglas utilizadas para la interpretación de los nombres distinguidos en los certificados emitidos están descritas en la ISO/IEC 9595 (X.500) Distinguished Name (DN). Adicionalmente todos los certificados emitidos utilizan codificación UTF8 para todos los atributos, según la RFC 5280 (“Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”).

3.1.5 Unicidad de los nombres

La AC raíz define como campo DN (Distinguished Name) del Certificado de Autoridad como único y sin ambigüedad. Para ello se incluirá como parte del DN, específicamente en el campo CN, el nombre o razón social del titular del certificado.

3.1.6 Reconocimiento, autenticación y función de las marcas

La ECD no asume compromisos en la emisión de certificados respecto al uso por los Suscriptores de una marca comercial, por lo cual, la ECD no está obligada a buscar evidencias de la posesión de marcas registradas antes de la emisión de los certificados.

Un solicitante de certificado retiene todos los derechos que posee (si los hubiera) en cualquier marca registrada, marca de servicio o nombre comercial contenida en cualquier solicitud de certificado y distinguished name dentro de cualquier certificado emitido a dicho solicitante de certificado.

3.2 Validación de identidad inicial

3.2.1 Método para probar la posesión de la clave privada

El sistema de certificación implementado y utilizado por Certicámara para la administración del ciclo de vida de sus certificados controla y garantiza de forma automática la emisión del certificado firmado al poseedor de la clave privada correspondiente a la clave pública incluida en la solicitud. Esta garantía se logra mediante el formato PKCS#10 que incluye en la propia solicitud una firma digital de la misma, realizada con la clave privada correspondiente a la clave pública del certificado.

3.2.2Autenticación de la identidad de la organización o persona

En el proceso de autenticación de la identidad de la organización o persona, el solicitante estará obligado a suministrar la documentación pertinente para cada servicio acreditado. Asimismo, el solicitante deberá proveer a Certicámara información que sea veraz, suficiente y adecuada en cumplimiento de los requisitos establecidos.

3.2.3Comprobación de las facultades de representación

La verificación de las facultades de representación del solicitante frente a Certicámara se efectuará a través de la consulta al Registro Único Empresarial y Social (RUES) o mediante la comprobación de los documentos legales que, de acuerdo con la legislación colombiana, acrediten y autoricen su rol como representante legal.

3.2.4 Mecanismos de validación de identidad

3.2.4.1 Verificación de identidad

Certicámara, como Entidad de Certificación Digital Abierta, realizará la comprobación de identidad por los mecanismos definidos, utilizando fuentes confiables y datos provistos por terceros con quienes Certicámara cuente con contrato vigente para tal fin.

3.2.4.2 Verificación de identidad por biometría

En caso de ser requerido, Certicámara podrá realizar la validación del solicitante a partir de la identificación biométrica dispuesta para asegurar que el solicitante es quien dice ser.

3.2.5Información del suscriptor no verificada

Certicámara, en su calidad de Entidad de Certificación Digital Abierta, verifica la información suministrada por el solicitante que pueda ser sustentada con evidencias probatorias. Respecto a aquella información que carezca de soporte documental, tal como dirección física, correo electrónico y datos similares, se aplicará el principio de buena fe del solicitante al momento de su entrega.

3.2.6 Criterios de interoperabilidad

Certicámara en su calidad de Entidad de Certificación Digital Abierta no contempla interoperabilidad con otras ECD externas. Solamente contempla la emisión de certificados digitales con su Subordinada.

No obstante, lo anterior, de presentarse la necesidad, por cuestiones comerciales y/o reglamentarias, de realizar la interoperabilidad con otra ECD, se deberá evaluar los diferentes escenarios para su ejecución garantizando la adecuada prestación del servicio.

3.3Identificación y autenticación para solicitudes de renovación de claves

Certicámara no contempla dentro de sus procesos la renovación de certificados digitales manteniendo el par de claves originales del suscriptor. En caso de ser necesaria la renovación de un certificado emitido con anterioridad, se deberá llevar a cabo un nuevo proceso de solicitud de emisión, que incluirá la generación de un nuevo par de claves.

4. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

4.1 Solicitud de certificado

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

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

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

solicitudes serán remitidas a la Autoridad de Certificación (CA) para su emisión, la cual se efectuará en un término máximo de un (1) día hábil.

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

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

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

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

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

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

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

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

- **Token Virtual:** el restablecimiento de contraseña se podrá solicitar a través del contact center sin costo adicional hasta por diez (10) veces; posterior a este número de solicitudes implica costo asociado.
- **Token Físico:** debido a que Certicámara S.A. no dispone de mecanismos para su recuperación, dado que queda de forma local, será indispensable la adquisición de un nuevo certificado a través de los medios definidos en este documento, lo cual implica un costo asociado.

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

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

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

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

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

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

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

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

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

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

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

4.1.1 ¿Quién puede presentar una solicitud de certificado?

La solicitud de un certificado digital podrá ser efectuada por cualquier persona natural en pleno ejercicio de su capacidad jurídica, así como por personas jurídicas a través de su representante legal, un apoderado, un empleado o un tercero debidamente autorizado, siempre que se acredite dicha calidad con los documentos exigidos por la Autoridad de Registro (RA). En el caso de menores de edad, la solicitud de firma digital deberá ser presentada por su representante, adjuntando el documento de identidad del menor y el documento que acredite la representación conforme a la normativa civil vigente.

4.2 Emisión de certificados

4.2.1 Acciones de la CA durante la emisión del certificado

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

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

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

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

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

El suscriptor será notificado de la emisión exitosa de su certificado a través de un correo electrónico enviado a su dirección registrada.

4.3 Entrega del certificado digital a los suscriptores por medio físico

4.3.1 Cubrimiento

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

4.3.2 Requisitos de entrega

El dispositivo físico será entregado por el operador logístico en la dirección reportada o podrá ser retirado por el suscriptor en las instalaciones de Certicámara, de acuerdo con lo indicado en el formulario de solicitud. Cuando el titular autorice a un tercero para reclamar el dispositivo en las instalaciones de Certicámara, éste deberá remitir un correo a la cuenta de logistica@certicamara.com previo a la entrega.

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

4.3.3 Tiempo de gestión de entrega – Certificados Físicos

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

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

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

Si la entrega no es posible por causas atribuibles al suscriptor, Certicámara o el operador logístico lo contactarán para coordinar la entrega. Sin embargo, es importante tener en cuenta que si no se logra coordinar una fecha de entrega o recolección en un plazo de tres (3) meses a partir de la fecha de emisión, se considerará que el bien ha sido abandonado. En este caso, Certicámara procederá a bloquear el enlace de descarga.

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

4.3.4 Tiempo de descarga

Una vez aprobada la solicitud de firma digital, el titular recibirá automáticamente un correo electrónico con el enlace de descarga, un manual detallado y recomendaciones importantes.

El enlace de descarga estará activo por treinta (30) días calendario. Después de este período, el sistema lo bloqueará por seguridad. Para reactivarlo, el titular deberá solicitarlo formalmente y dispondrá de dos (2) meses adicionales para realizar la descarga de su firma.

Si, transcurrido este plazo de tres (3) meses, no ha descargado su firma, se entenderá que el bien ha sido abandonado y Certicámara procederá al bloqueo definitivo del enlace. En tal caso, si desea obtener el certificado de firma digital, deberá iniciar un nuevo proceso de solicitud, lo cual generará un costo según las tarifas de Certicámara.

4.4 Aceptación del certificado

No se exige una confirmación por parte del suscriptor como aceptación del servicio recibido. Se entiende que el servicio de certificado de firma digital es aceptado a partir del momento en que se solicita su expedición. En consecuencia, si la información

contenida en la comunicación de activación del servicio no se ajusta a su estado actual o no fue proporcionada correctamente, el suscriptor deberá informar a Certicámara a través de cualquiera de los canales de atención disponibles para llevar a cabo los trámites de corrección pertinentes en caso que apliquen.

4.4.1 Publicación del certificado por la CA

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

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

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

Certicámara dispone de un repositorio de certificados digitales LDAP, a través del cual entidades, organismos gubernamentales, empresas del sector privado y demás partes interesadas tienen la posibilidad de consultar la emisión de los certificados. Este repositorio se encuentra accesible en la siguiente dirección web: https://ar.Certicámara.com:8443/Search/. La información se publica en este repositorio una vez que el certificado ha sido emitido.

4.5 Desistimiento

En caso de que el usuario haya efectuado el pago por alguno de los servicios ofrecidos por Certicámara, pero no haya completado la entrega de la totalidad de los requisitos documentales exigidos, se establece un plazo de noventa (90) días calendario a partir de la fecha de solicitud del servicio para que dicha información sea debidamente suministrada.

Si el solicitante no completa la información requerida dentro del término estipulado, se entenderá que existe un desistimiento de la adquisición del servicio. Como consecuencia, los valores cancelados por el servicio no serán objeto de devolución.

4.6 No devolución del dinero

Certicámara no estará obligada a devolver el dinero al solicitante en ningún caso, excepto cuando la ley lo exija expresamente.

4.7 Uso de pares de claves y certificados

4.7.1 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.

4.7.2 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.

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

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

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

4.8 Renovación del certificado

4.8.1 Tiempos para la renovación

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

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

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

4.8.2 ¿Quién puede solicitar la renovación?

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

4.8.3 Tramitación de solicitudes de renovación de certificados

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

4.8.4 Notificación de emisión de nuevo certificado al suscriptor

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

4.9 Renovación de llave de certificado

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

4.10 Modificación del certificado

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

4.11 Revocación de certificados

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

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

4.11.1 Causales para la revocación

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

a) Por compromiso de la seguridad en cualquier motivo, modo, situación o circunstancia.

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

4.11.2 ¿Quién puede solicitar la revocación?

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

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

4.11.3 Procedimiento para solicitud de revocación

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

- **Telefónicamente:** Llamando a la línea de atención (601) 7442727, de 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.
- **En línea:** A través de la página web de Certicámara, registrando la solicitud en la siguiente URL: https://ventadigital.certicamara.com/revocar-certificado

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

Certicámara validará la identidad del suscriptor que invoca la causal de revocación. Si la persona que expone dicha no es el suscriptor o en caso de serlo no puede identificarse satisfactoriamente, podrá dirigirse personalmente a las oficinas de Certicámara en horarios de oficina 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.

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

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

4.11.4 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.

4.11.5 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.

4.11.6 Disponibilidad de verificación de estado/revocación en línea

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

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

4.11.7 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, http://ocsp.certicamara.co y http://ocsp4096.certicamara.co

4.11.8 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.

4.12 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.
- Se realizará la reposición del certificado de firma digital por el tiempo faltante de este.

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

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

- El suscriptor deberá generar la solicitud en la página web de Certicámara: https://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 4.2 de la presente Declaración de Prácticas 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://ventadigital.certicamara.com/revocar-certificado

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.

4.12.1 Causales para la Reposición

Para cada una de las causales expuestas a continuación, se realizará un análisis interno por parte de esta compañía y se determinará la procedencia de la reposición, de conformidad con el procedimiento definido.

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

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

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

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

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

4.13 Características de los certificados

4.13.1 Características operativas

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

Un cliente de OCSP envía una petición sobre el estado del certificado a la AV, la cual, tras consultar su Base de Datos, ofrece una respuesta sobre el estado del certificado vía

HTTP por medio de las direcciones http://ocsp.Certicamara.com, http://ocsp.Certicamara.co y http://ocsp4096.certicamara.co.

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

http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara.crl
http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_2014.crl
http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica.crl

http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_2014.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

4.13.2 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%.

4.13.3 Funciones opcionales

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

4.14 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.

4.15 Custodia y recuperación de llaves

4.15.1 Política y prácticas de custodia y recuperación de llaves

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

5. CONTROLES DE INSTALACIONES, GESTIÓN Y OPERACIÓN

5.1 Controles físicos

5.1.1 Ubicación y construcción del sitio

La totalidad de las operaciones críticas de la CA raíz y la CA Subordinada se encuentran resguardadas físicamente mediante la implementación de rigurosas medidas de seguridad y un esquema de vigilancia ininterrumpida las 24 horas del día, los 7 días de la semana. Dichos sistemas operan de manera independiente de otros sistemas de Certicámara, restringiendo el acceso exclusivamente al personal debidamente autorizado.

5.1.2 Acceso físico

Certicámara cuenta con servicios y tecnologías que complementan los controles de acceso físico tanto a sus racks como a sus Datacenter, donde normalmente deben pasar como mínimo tres (03) controles.

Los Centros de Proceso de Datos de la AC raíz y la AC Subordinada cumplen los siguientes requisitos físicos:

- Circuito cerrado de televisión en las áreas críticas o de acceso restringido.
- Control de acceso basado en biometría, llaves
- Autorizaciones a través de sistemas
- Sistemas de protección y prevención de incendios: detectores, extintores, formación del personal para actuar ante incendios, etc.
- Las instalaciones se encuentran alejadas de salidas de humos.
- Capturas en video y/o fotografías

5.1.3 Energía y aire acondicionado

Las instalaciones donde se encuentran ubicados los equipos cumplen con las condiciones de potencia y ventilación requeridas para prevenir interrupciones en el suministro eléctrico u otras anomalías de naturaleza eléctrica.

El cableado de los equipos se encuentra protegido para evitar interceptaciones o daños físicos. Adicionalmente, se han adoptado medidas específicas para mitigar la pérdida de información ocasionada por la interrupción del flujo de suministro eléctrico, mediante la conexión de los componentes esenciales a sistemas UPS que garantizan una alimentación eléctrica continua con la capacidad suficiente para sostener la red eléctrica durante los procedimientos de apagado controlado del sistema y para salvaguardar los equipos ante fluctuaciones eléctricas que pudieran comprometer su integridad.

Los sistemas de acondicionamiento de aire mantienen los espacios donde se encuentran los equipos con los niveles de humedad y temperatura óptimos para su adecuado funcionamiento y conservación.

5.1.4 Exposiciones al agua

Las instalaciones de la CA Raíz y la CA Subordinada se encuentran protegidas para prevenir la exposición al agua, a través de la implementación de detectores de humedad e inundación y otros mecanismos de seguridad adecuados al entorno.

5.1.5 Prevención y protección contra incendios

La instalación de la CA Raíz y CA Subordinada, cuenta con sistema de detección y extinción inteligentes. Está conformado por:

- Panel de control inteligente.
- Boquillas de extensión en el techo.
- Detectores de incendios en el techo y techo falso.
- Sistema de alarma que activa los detectores de incendios.

5.1.6 Almacenamiento de medios

La información relacionada a la infraestructura de la CA raíz y CA Subordinada se almacenan de forma segura en armarios ignífugos y cajas fuertes, según la clasificación de la información en ellos contenida.

Esta información se encuentra alojada en sitios con diferente ubicación, con el fin de minimizar riesgos asociados.

5.1.7 Eliminación de residuos

Todo residuo que se genere de la operación de los servicios de certificación digital, son tratados de acuerdo con la normatividad aplicable para contribuir con el medio ambiente y garantizar la seguridad de la información.

5.1.8 Copia de seguridad fuera del sitio

Todas las copias de seguridad son almacenadas en entidades distantes a la CA Raíz y CA Subordinada. Estas dependencias están protegidas con medios y mecanismos de seguridad, apegadas a buenas prácticas internacionales de seguridad.

5.2 Controles de procedimiento

5.2.1 Roles de confianza

La CA Raíz y la CA Subordinada cuentan con personal que, debido a sus responsabilidades esenciales para el funcionamiento de Certicámara S.A., son sometidos a procedimientos de control especiales y considerados roles de confianza:

- **Agente de la RA:** Responsables de la revisión y validación de la información en los documentos del solicitante para la emisión de servicios de la ECD.
- **Agente de la CA:** Responsables de la aprobación, activación y revocación de servicios de la ECD.
- **Especialista de Infraestructura PKI/TSA:** Responsable del funcionamiento de los sistemas (hardware y software base) de la AC raíz y AC Subordinada.
- **System Auditor:** El Director de Mejoramiento Continuo es internamente el responsable del proceso de gestión de auditorías, estableciendo las directrices para evaluar el cumplimiento de los requisitos aplicables a través de un tercero especializado.

5.2.2 Número de personas requeridas por tarea

Como medida de seguridad, se han asignado colaboradores a los diferentes roles, garantizando la debida segregación de funciones, independencia e imparcialidad en sus actuaciones dentro de los servicios acreditados.

5.2.3 Identificación y autenticación para cada rol

Los colaboradores asignados a cada rol cuentan con los permisos necesarios para sus funciones, los cuales se autentican mediante credenciales de acceso personales e intransferibles a la plataforma.

La autenticación se complementa con las autorizaciones correspondientes para acceder a activos de información específicos del sistema de Certicámara.

5.2.4 Roles que requieren separación de funciones

Las responsabilidades del personal que desempeña los roles correspondientes a la Autoridad de Registro (RA) y la Autoridad de Certificación (CA) se encuentran debidamente segregadas, garantizando así la independencia e imparcialidad en el desarrollo de sus funciones.

En consideración de las funciones inherentes a la Autoridad de Registro (RA) y la Autoridad de Certificación (CA), y en concordancia con los Criterios Específicos de Acreditación – CEA, estas actividades son llevadas a cabo por personal que mantiene un vínculo laboral directo con Certicámara S.A.

5.3 Controles de personal

5.3.1 Calificaciones, experiencia y requisitos de autorización

Certicámara implementa un proceso de estudio de confiabilidad para los colaboradores que desempeñan actividades en la prestación de servicios digitales. Este proceso comprende la validación de referencias, experiencia laboral, antecedentes, visita domiciliaria y calificaciones, entre otros criterios de evaluación.

5.3.2 Procedimientos de verificación de antecedentes

En el proceso de verificación de antecedentes, Certicámara recurre a una empresa especializada para realizar consultas en listas definidas, con el objetivo de determinar la idoneidad de sus colaboradores.

5.3.3 Requisitos de formación

Certicámara implementa un plan de capacitación anual para sus colaboradores, diseñado en función de las necesidades formativas identificadas en el marco de sus responsabilidades. Este plan podrá contemplar, entre otros, los siguientes temas:

- Marco legal relativo a la prestación de servicios de certificación.
- Seguridad de la información y protección de datos personales.
- Características operativas y técnicas de los servicios acreditados.
- Procedimientos de operación y administración.
- Continuidad del negocio.
- Evolución tecnológica del entorno.
- Implementación de nuevas herramientas.
- Modificación de procedimientos operativos.

5.3.4 Sanciones por acciones no autorizadas

Certicámara ha establecido un procedimiento para llevar a cabo investigaciones y aplicar las sanciones disciplinarias que correspondan en caso de que sus colaboradores contravengan las directrices impartidas por la organización. Ante la sospecha por parte de Certicámara de que algún empleado esté ejecutando una acción no autorizada, se procederá a la suspensión automática de su permiso de acceso, con la posibilidad de la terminación de su contrato laboral.

5.3.5 Requisitos del contratista independiente

Certicámara mantiene los soportes de contratación y la documentación que acredita el cumplimiento de los requisitos tanto administrativos como técnicos por parte de los contratistas independientes que proveen el servicio de data center.

5.3.6 Documentación suministrada al personal

Certicámara pondrá a disposición de todo el personal la documentación relacionada con las funciones asociadas al cargo que desempeña, las políticas y prácticas que rigen dichos procesos y la documentación de seguridad.

5.4 Procedimientos de registro de auditoría (Logs)

Certicámara cuenta con una herramienta de análisis de logs, que permite monitorear los registros de auditoría transaccional y de seguridad y a su vez emite alertas automáticas, con el fin de identificar oportunamente fallas o eventos de riesgos que requieran remediaciones. Así mismo, custodia su registro por un periodo mínimo de tres (3) años que se hayan generado en los sistemas durante este periodo de tiempo.

5.4.1 Tipos de eventos registrados

Certicámara contempla el registro de los siguientes eventos:

- Advertencia: Indica que una acción realizada al interior de los sistemas involucrados presenta una situación anormal, pero que no necesariamente es un fallo.
- Informativo: Indica que una acción realizada al interior de los sistemas involucrados en la prestación de los servicios acreditados se ha finalizado de manera correcta.
- Error: Indica que una acción realizada al interior de los sistemas involucrados presenta un comportamiento inesperado que trae como consecuencia la no finalización esperada de la acción.

5.4.2 Frecuencia de procesamiento del registro

La frecuencia en el procesamiento de los registros se realiza de manera permanente asegurando que la información derivada de las acciones al interior de los sistemas de información involucrados se salvaguarde.

5.4.3 Período de retención para el registro de auditoría

Se tiene definido que el periodo de retención para los diferentes registros de auditoría es de tres (3) años, período después del cual y de acuerdo con las directrices dadas se puede proceder a la destrucción de los mismos.

5.4.4 Protección del registro de auditoría

Los registros derivados de las acciones realizadas en los sistemas de información serán salvaguardados en una copia dentro de las instalaciones de Certicámara y otra por fuera asegurando siempre tener una copia disponible para la consulta de la información en caso de que sea necesario.

5.4.5 Evaluaciones de vulnerabilidad

Se realizan pruebas de seguridad que contemplan análisis de riesgos, escaneo de vulnerabilidades y ethical hacking al menos una vez al año. Las cuales son contratadas por un tercero especializado que cumpla con los requisitos de aseguramiento definidos en los criterios específicos de acreditación de ONAC e internos por la compañía.

5.5 Archivo de registros

5.5.1 Tipos de registros archivados

Para los servicios de certificados de firma digital la documentación estará definida en el sistema de información de acuerdo con cada tipo de política. Para los demás servicios acreditados se visualizarán en las respectivas políticas de certificación.

5.5.2 Periodo de conservación del archivo

El periodo de conservación de los documentos estará acorde al artículo 38 ley 527 de 1999, a las tablas de retención documental de Certicámara y a la regulación vigente.

5.5.3 Protección del archivo

Las medidas de seguridad definidas están destinadas a proteger los archivos de accesos (internos o externos) no autorizados, de modo que sólo ciertas personas pueden consultar, modificar o eliminar los archivos. Los archivos son almacenados aplicando medidas de seguridad física y lógica para protegerlos.

5.5.4 Procedimientos de copia de seguridad de archivos

Se realizan copias de los ficheros que componen los archivos a retener de acuerdo con las políticas de backup definidas. La copia se genera y se almacena en un sitio seguro dentro del centro de datos principal de la CA Subordinada, el cual cumple con las condiciones ambientales y físicas de seguridad.

5.5.5 Procedimientos para obtener y verificar información de archivo

Los eventos registrados están protegidos mediante técnicas criptográficas, de forma que nadie salvo las propias aplicaciones de visualización y gestión de eventos pueda acceder a ellos. Sólo el personal autorizado tiene acceso a los archivos físicos de soportes y archivos informáticos, para llevar a cabo verificaciones de integridad u otras.

5.6 Cambio de clave

Las claves de los certificados emitidos por CA Raíz dejarán de tener validez en el mismo momento en que lo haga su certificado autofirmado. Una vez expirado la CA Raíz generará un nuevo par de claves que auto firma para generar el nuevo certificado raíz. Certicámara, notificará al auditor externo y/o ente de acreditación establecido por la normatividad vigente al momento de efectuar el cambio de clave, con el fin de determinar las condiciones técnicas, procedimentales y de ley que sean aplicables para este procedimiento antes de su ejecución, para garantizar que se dará cumplimiento a las normas aplicables al proceso desde el punto de vista de seguridad. Para tal fin, Certicámara presentará el documento denominado Ceremonia de cambio de clave que será redactado y ajustado para su presentación con antelación a la fecha propuesta para el cambio de llaves.

5.7 Compromiso y recuperación ante desastres

Certicámara S.A. planifica y prepara la Continuidad de Negocio para tener la capacidad de seguir operando durante eventos de emergencia o cualquier evento que provoque una interrupción o mal funcionamiento, para ello identifica y gestiona los riesgos que podrían tener impacto en la continuidad de negocio y toma medidas frente a su materialización, propendiendo por el cumplimiento de los requisitos legales, regulatorios, reglamentarios, estatutarios y contractuales de nuestras partes interesadas relacionados a la continuidad del negocio.

Certicámara S.A. establece y aplica directrices, lineamientos y compromisos, con el fin de responder rápidamente a una interrupción o eventos disruptivos, gestionando adecuadamente los riesgos y realizando pruebas que consideren procesos, proveedores, servicios y actividades críticas.

5.7.1 Procedimientos de manejo de incidentes y compromisos

Certicámara ha definido el procedimiento para la gestión de incidentes que permite asegurar la continuidad de la operación, la prevención y la reacción oportuna ante posibles fallas en la operación normal de los servicios, garantizando un mínimo de interrupciones en la prestación y disponibilidad de las plataformas.

El plan de continuidad del negocio asegura que Certicámara pueda continuar prestando el servicio en situaciones adversas, después de identificar, evaluar, gestionar y minimizar cualquier tipo de eventos de riesgo, donde se contemplan como mínimo los siguientes:

- Cuando la seguridad de la clave privada de la entidad de certificación se ha visto comprometida.
- Cuando el sistema de seguridad de la entidad de certificación ha sido vulnerado.
- Cuando se presenten fallas en el sistema de la entidad de certificación que comprometan la prestación del servicio.
- Cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratado por el suscriptor.

Certicámara propenderá por el seguimiento de las recomendaciones dadas por:

https://csrc.nist.gov/projects/hash-functions

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-57pt3r1.pdf

5.7.2 Capacidades de continuidad del negocio después de un desastre

Las capacidades de continuidad del negocio de Certicámara se encuentran definidas en el plan de continuidad del negocio, donde se establecen los recursos necesarios para su ejecución.

5.8 Cese de actividades

Conforme con lo dispuesto en el artículo 163 del Decreto Ley 019 del 2012 que modifica el artículo 34 de la Ley 527 de 1999, las ECD acreditadas por ONAC "*pueden cesar en el ejercicio de actividades, siempre y cuando garanticen la continuidad del servicio de certificación digital a quienes ya lo hayan contratado, directamente o a través de terceros, sin costos adicionales a los servicios ya cancelados*". En consecuencia, de lo anterior, Certicámara informará de la cesación de los servicios a ONAC, con una antelación de 30 días, según lo establecido en el capítulo 48 del DURSCIT, Artículo 2.2.2.48.3.8. Cesación de actividades.

Por consiguiente, Certicámara ha definido un plan de continuidad y contingencia de negocio para todos los servicios que se encuentren acreditados, asegurando la continuidad en alta disponibilidad de la infraestructura prestada y garantizando la adecuada cesación en sus actividades como ECD.

Certicámara informará el cese mediante el envío de un correo electrónico dirigido a todos los suscriptores que tengan vigente los servicios acreditados y mediante dos avisos publicados en diarios o medios de amplia circulación nacional, con un intervalo de 15 días, sobre:

i. La terminación de su actividad o actividades y la fecha precisa de cesación.
ii. Las consecuencias jurídicas de la cesación respecto a los servicios acreditados
iii. La posibilidad de que un suscriptor obtenga el reembolso equivalente al valor del tiempo de vigencia restante sobre el servicio contratado.
iv. La autorización emitida por ONAC para que la ECD pueda cesar el servicio, y si es el caso, el operador de la CRL responsable de la publicación de los certificados emitidos por la ECD, hasta cuando expire el último de ellos.
v. Cualquier otra obligación que establezca la ley

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

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

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1 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.

El procedimiento de generación de las claves para las CA Subordinadas acreditadas ante Certicámara es idéntico, en su propio HSM.

6.1.1 Entrega de llave privada al suscriptor

El algoritmo que se utiliza para la generación del par de llaves de los suscriptores es RSA no inferior a 4096 bits usando como función criptográfica de resumen o hash, el denominado SHA256. Los suscriptores pueden utilizar los siguientes medios para generar sus certificados digitales y custodiarlos:

- Dispositivos de hardware token USB para generar su llave privada, los cuales cumplen con el estándar FIPS 140-2 Nivel 3.
- Token Virtual, utilizando los HSM (Hardware Security Module) de Certicámara.
- PKCS#10, cuando el suscriptor crea previamente sus propias claves y solicita a Certicámara firmar el certificado digital, la solicitud debe garantizar:
    - Tamaño de claves mínimo 4096 bits.
    - La solicitud debe enviarse en formato PKCS#10.

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

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

Para conocer el nivel de riesgos asociados de los dispositivos criptográficos, se puede consultar el documento NIST.FIPS.140-2.pdf

6.1.2 Entrega de clave pública al emisor del certificado

Las claves públicas generadas por la entidad final bajo su responsabilidad se envían a Certicámara como parte de una solicitud de certificado. csr que se solicita firmar por la CA subordinada.

6.1.3 Entrega de clave pública de la CA a partes de confianza

La llave pública de cualquier suscriptor de Certicámara estará permanentemente disponible en el directorio activo para la consulta de las partes de confianza que así lo requieran

6.1.4 Tamaños de clave

- Para los certificados de la CA Raíz se emplea algoritmo RSA con tamaño de 4096 bits
- Para los certificados de la CA Subordinada se emplea el algoritmo RSA con tamaño de 4096 bits.
- Para los certificados de entidad final se emplea el algoritmo RSA con tamaño mínimo de las llaves de 2048 bits.

6.1.5 Propósitos de uso de clave (según el campo de uso de clave X.509 v3)

Sólo se puede utilizar la clave privada y el certificado para los usos autorizados en esta DPC y PC. Certicámara emite certificados con los campos de uso de clave privada limitados a firma de certificados y firma de CRL.

Los usos previstos para las llaves de los certificados de la CA son:

- Firma de Certificados
- Firma CRL sin conexión
- Firma de lista de revocación de certificados (CRL)

Los usos previstos para las llaves de los certificados de entidad final son:

- Firma digital

- Sin repudio
- Cifrado de la clave
- Cifrado de datos
- Acuerdo de clave.
- Uso mejorado de claves:
- Autenticación del suscriptor (OID 1.3.6.1.5.5.7.3.2)- Aplica para todos los certificados.
- Correo seguro (OID 1.3.6.1.5.5.7.3.4) – Aplica para todos los certificados
- Autenticación del servidor (1.3.6.1.5.5.7.3.1) – Aplica para los certificados de Representación de Empresa / Entidad y Persona Jurídica

6.2 Protección de clave privada e ingeniería de módulos criptográficos

La clave privada de la CA Raíz, es protegida por un esquema de seguridad generada por un dispositivo criptográfico. Con la finalidad de mantener el resguardo de las claves privadas del certificado auto firmado, la clave privada nunca se encuentra descifrada fuera del HSM.

Las copias de seguridad mantienen el secreto de la clave privada de la misma forma en que se resguarda la clave privada original.

6.2.1 Estándares y controles del módulo criptográfico

El HSM que utiliza la CA Raíz, para generar sus claves es certificado FIPS 140-2 Nivel 3.

La clave pública ha sido almacenada en formato electrónico firmado, de modo que están protegidas de fallos electrónicos y/o problemas con la potencia eléctrica.

Por lo tanto, la puesta en marcha de una CA implica las siguientes tareas:

- Inicialización del estado del módulo HSM.
- Creación de las tarjetas de administración y de operador.
- Generación de las claves de la AC. Z<A

6.2.2 Clave privada (K de N) control multipersona

La CA Raíz, genera su par de claves utilizando un módulo de hardware criptográfico (HSM). La autenticación contra el HSM requiere de al menos 2 de 3 operadores. Este procedimiento sigue el esquema K de N, con el modo no persistente del dispositivo criptográfico. En este modo es necesario garantizar la conexión física del último juego de tarjetas en el lector del HSM, para abrir la clave privada de la CA Raíz.

6.2.3 Custodia de la clave privada

La clave privada de la CA raíz y CA Subordinada se encuentra alojada en un dispositivo criptográfico. El mismo 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 de seguridad.

El resto de las claves privadas de operadores y administradores se encuentran contenidas en smartcards criptográficas en poder de los administradores de cada entidad, la llave privada de Certicámara no es conservada en fideicomiso por un tercero.

6.2.4 Copia de seguridad de clave privada

Las copias de seguridad de la clave privada se realiza de acuerdo con los lineamientos de seguridad y recomendaciones indicadas por el fabricante del software de la PKI, dentro de los lineamientos de seguridad se describe el uso de dispositivos criptográficos que cumplan FIPS 140-2 nivel 3, un juego de tarjetas que cumplan el requisito k/n para su protección, y por lo menos se requiere la colaboración del especialista de infraestructura PKI/TSA, custodio de material criptográfico y personal designado desde la Gerencia de Operaciones y Tecnología.

6.2.5 Archivo de claves privadas

Las copias de backup de las claves privadas estarán bajo custodia de forma cifrada en el centro de cómputo alterno. Las copias de backup de las claves privadas se realizan en archivos seguros ignífugos.

6.2.6 Almacenamiento de claves privadas en módulo criptográfico

Las claves privadas se crean dentro del módulo criptográfico en el momento en que este se inicializa, posteriormente la clave privada generada dentro del HSM es exportada en forma cifrada.

6.2.7 Método de activación de clave privada

El único método de activación para la clave privada consiste en la utilización de las tarjetas inteligentes para repartir el acceso en distintas personas y roles. Explícitamente la única combinación para activar la clave privada requiere dos de tres administradores del HSM, tres de ocho operadores del HSM y un administrador del Sistema Operativo de la aplicación.

6.2.8 Método de desactivación de clave privada

Un administrador del sistema operativo puede proceder a la desactivación de la clave privada de la CA raíz y CA Subordinada. Después de haber sido activada por la combinación descrita en el apartado anterior el operador puede proceder a la desactivación mediante la detención de la aplicación de la Autoridad de Certificación.

6.2.9 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.

6.2.10 Calificación del módulo criptográfico

La CA raíz y CA Subordinada utilizan módulos criptográficos hardware y software disponibles comercialmente desarrollados por terceros. La CA raíz y CA Subordinada únicamente utiliza módulos criptográficos con certificación FIPS 140-2 Level 3 (nShield Edge, nShield Connect 500, nShield Connect 1500+, nShield Connect 6000+).

6.3 Otros aspectos de la gestión de pares de claves

6.3.1 Archivo de claves públicas

La clave pública de la CA Raíz y CA Subordinada, es archivada según el formato estándar PKCS#7, por un período de 20 años**.**

6.3.2 Períodos operativos del certificado y períodos de uso del par de claves

El par de claves de la CA raíz tendrá una validez hasta el sábado, 24 de mayo de 2031. Por otro lado, los periodos de operación de los certificados serán de diez años.

El par de claves de la CA subordinada tendrá una validez hasta el sábado, 24 de mayo de 2031. Por otro lado, los periodos de operación de los certificados serán de diez años.

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

Los datos de activación de la CA raíz y CA Subordinada se deben generar y almacenar en tarjetas inteligentes. Su protección se garantiza mediante un PIN en posesión de personal autorizado.

6.4.2 Protección de datos de activación

Sólo el personal autorizado posee las tarjetas criptográficas con capacidad de activación de las claves privadas de la CA, así mismo conocen los PINs necesarios para su utilización.

- La clave personal de acceso (PIN) es confidencial, personal e intransferible y es el parámetro que protege las llaves privadas permitiendo la utilización de los certificados de CA raíz y CA Subordinada; por lo tanto, deben tenerse en cuenta unas normas de seguridad para su custodia y uso:
- No debe enviarse ni comunicarse el PIN a ninguna persona.
- Los operadores y administradores deben cambiar el PIN cuando sospechen que es conocido por otra persona.
- Se recomienda cambiar el PIN periódicamente.

6.5 Controles de seguridad informática

6.5.1 Requisitos técnicos específicos de seguridad informática

Para la respectiva prestación del servicio se tiene establecido una serie de controles técnicos, que propenden por su buen funcionamiento garantizando su adecuado funcionamiento. Entre los aspectos que se tiene en cuenta son:

- Configuración del equipo
- Configuración de las aplicaciones
- Configuración del usuario
- Aplicación de los perfiles para el acceso a la red
- Información sobre el sistema de seguridad para proteger la información que se recopila con el fin de expedir certificados.

6.5.2 Calificación de seguridad informática

Actualmente Certicámara como parte de su enfoque organizacional se encuentra certificada bajo la Norma ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información de acuerdo con el alcance definido en el certificado, el cual se encuentra disponible en la página web de Certicámara.

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles de desarrollo del sistema

Los requisitos de seguridad para el desarrollo de sistemas para la CA raíz y la ENTIDAD SUBORDINADA son exigibles.

Se debe realizar un análisis de diseño de seguridad durante las fases de diseño y especificación de nuevos requisitos de cualquier componente que se va a utilizar en las aplicaciones de la CA raíz y CA Subordinada. Esto con la finalidad de garantizar que los sistemas involucrados sean seguros.

La infraestructura tecnológica de la CA raíz y CA Subordinada debe estar dotada de entornos de desarrollo y producción claramente diferenciados e independientes. Debe utilizarse procedimientos de control de cambio para las nuevas versiones y actualizaciones.

6.6.2 Controles de gestión de la seguridad

Certicámara, mantiene un inventario de todos los activos informáticos y realiza una clasificación de estos de acuerdo con sus necesidades de protección; las pautas para ella serán dictadas por los resultados del análisis de riesgos efectuado.

La configuración de los sistemas se debe auditar de forma periódica y realizar un seguimiento del crecimiento de necesidad de recursos de acuerdo con la demanda.

6.6.3 Controles de seguridad del ciclo de vida

Durante todo el ciclo de vida se debe implementar controles de seguridad que permitan instrumentar y auditar cada fase de los sistemas de la CA raíz y CA Subordinada.

6.7 Controles de seguridad de la red

La infraestructura tecnológica de la CA raíz y CA Subordinada posee una red con todos los mecanismos de seguridad necesarios para garantizar un servicio fiable e íntegro. Se utiliza cortafuegos o intercambio de datos cifrados entre redes para garantizar integridad. Por otro lado, se utilizan tecnologías de renuncias y alta disponibilidad para garantizar un funcionamiento confiable y de alto rendimiento. Adicionalmente la infraestructura debe ser auditada periódicamente por personas internas y externas de Certicámara.

6.8 Sellado de tiempo

La sincronización de los relojes de la CA y la RA se realiza con base en la Hora Legal de La República de Colombia, tomada directamente de los patrones de referencia del Instituto Nacional de Metrología –INM, de Colombia, de acuerdo con lo establecido en el artículo 14 del Decreto 4175 de 2011, modificado por el Decreto 62 de 2021.

7. PERFILES DE CERTIFICADO, CRL Y OCSP

7.1 Perfil de certificado

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

7.1.1 Número(s) de versión

Los certificados expedidos por Certicámara se encuentran conformes con el estándar X. 509 v3.

7.1.2 Extensiones de certificado

Las extensiones de los certificados de la CA Raíz y CA Subordinada permiten codificar información adicional en los certificados.

Las extensiones estándar X.509 definen los siguientes campos:

- SubjectKeyIdentifier
- AuthorityKeyIdentifier
- BasicConstraints. Marcada como crítica
- Certificate Policies. Marcada como crítica

- KeyUsage. Marcada como crítica
- CRLDistributionPoint. Marcada como crítica
- SubjectAlternativeName. Marcada como crítica
- AuthorityInformationAccess

Los siguientes son los campos de los certificados que se emiten a los suscriptores:

- Fecha y hora de firmado
- Nombre del documento
- Asunto
- Entidad Certificadora
- Serial del Certificado
- Thumbprint
- Certificado válido desde
- Certificado válido hasta

7.1.3 Identificadores de objetos de algoritmo

- OID del algoritmo de firma SHA256withRSAEncryption 1.2.840.113549.1.1.11
- OID del algoritmo de la llave pública RSAEncryption 1.2.840.113549.1.1.1

7.1.4 Formas de nombre

Los certificados emitidos por Certicámara cuentan con un DN, en formato X. 500, los nombres del emisor y titular del certificado en los campos emisor (issuer) y sujeto (subject).

7.1.5 Restricciones de nombre

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

7.1.6 Identificador de objeto de política de certificados

La AC raíz tiene definida una política de asignación de OID's dentro de su árbol privado de numeración.

7.1.7 Sintaxis y semántica de calificadores de políticas

La sintaxis y semántica su descripción se encuentra al interior de los certificados digitales generados, dentro de la sección directivas del certificado, donde se muestra una URL donde se encuentra publicada la DPC de Certicámara.

7.2 Perfil de lista de revocación de certificados

7.2.1 Número(s) de versión

La AC Subordinada, emite las CRLs con formato X. 509.

7.2.2 CRL y extensiones de entrada de CRL

Las extensiones de las CRL emitidas por la AC Raíz, son las definidas de acuerdo con el RFC 5280, es decir:

- Authority Key Identifier
- CRL Number
- Issuing Distribution Point

7.3 Perfil OCSP

El estado de validez de un certificado en particular emitido a un suscriptor podrá ser verificado el uso del protocolo en línea de estado de los certificados OCSP, el cual se encuentra implementado acorde a lo establecido en el RFC 6960.

7.3.1 Número(s) de versión

Se utiliza la versión 1 del protocolo OCSP, según lo establecido en el RFC 6960.

7.3.2 Extensiones OCSP

De acuerdo con el funcionamiento de la generación de los certificados digitales, no se tiene establecido el uso de extensiones OCSP

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

8.1 Frecuencia o circunstancias de la evaluación

En concordancia con las definiciones del Organismo Nacional de Acreditación de Colombia – ONAC, Certicámara ha establecido un programa anual de auditorías para la evaluación de sus diversos servicios acreditados.

El sistema de acreditación de la AC raíz y la AC Subordinada será objeto de una auditoría de tercera parte con una periodicidad anual, en conformidad con el programa de auditorías definido por Certicámara. Este proceso garantiza la adecuación de su funcionamiento y operatividad a las disposiciones contenidas en la presente DPC.

Adicionalmente, Certicámara se reserva el derecho de realizar auditorías internas bajo su propio criterio o en cualquier momento en que exista sospecha de incumplimiento de alguna medida de seguridad o ante un posible compromiso de las claves.

Asimismo, se efectuará anualmente una auditoría externa para evaluar el nivel de conformidad con los principios y criterios de Webtrust para Autoridades de Certificación digital de AICPA/CICA.

8.2 Identidad/calificaciones del evaluador

En el caso de la auditoría de tercera parte, la firma auditora deberá cumplir con los requisitos mínimos de aseguramiento estipulados en los criterios específicos de acreditación que el ONAC ha publicado en su página web, además de aquellos definidos en los procedimientos internos de Certicámara para la contratación de terceros.

8.3 Relación del evaluador con la entidad evaluada

La interacción entre el auditor y la entidad sujeta a auditoría se circunscribirá estrictamente a los procesos y la información requerida para la realización de la auditoría. En consecuencia, la parte auditada (ya sea la CA raíz o la entidad subordinada) no deberá mantener ninguna relación de carácter financiero, legal o de cualquier otra índole, bien sea actual o proyectada, que pueda derivar en un conflicto de intereses con el auditor. Respecto a los auditores internos, se exigirá la ausencia de cualquier relación funcional con el área objeto de la auditoría.

8.4 Acciones tomadas como resultado de una no conformidad

La identificación de cualquier no conformidad durante las auditorías activará el proceso interno de gestión de acciones de mejoramiento, cuyo objetivo es la eliminación de la causa raíz detectada. En el supuesto de una no conformidad crítica, Certicámara estará facultada para determinar la suspensión temporal de las operaciones de la CA raíz o de la CA Subordinada hasta que las deficiencias sean subsanadas en el menor plazo posible.

8.5 Comunicación de resultados

La totalidad de los resultados de auditoría son presentados al comité de presidencia con el fin de determinar las acciones correctivas y de mejora que deban implementarse.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 Tarifas

9.1.1 Tarifas de emisión o renovación de certificados

Las tarifas establecidas por parte de Certicámara para cada uno de los servicios que se encuentran acreditados se encuentran definidas en cada una de las políticas de certificación publicadas en la página web.

9.1.2 Tarifas de acceso a la información de revocación o estado

Certicámara no considera dentro de sus políticas tarifarias el cobro por el acceso a la información de revocación o estado de los servicios relacionados con el certificado. Tanto la consulta como la revocación no tendrán ningún costo.

9.1.3 Política de reintegro

Los suscriptores podrán solicitar el reintegro del dinero a través del sitio web de Certicámara S.A. sección PQRSAF https://web.certicamara.com/soporte/Sistema-de-PQRSAF en los siguientes casos:

- Desistimiento del proceso de adquisición: Derecho ejercido por el suscriptor cuando el certificado digital no ha sido emitido. En estos casos se habla de un desistimiento en el curso del proceso de adquisición hasta antes de la descarga del certificado digital o la entrega del token físico. El suscriptor o usuario cliente cuenta con un término máximo de noventa (90) días.

- Retracto del suscriptor: Procede cuando se ejerce dentro de los 5 días hábiles contados a partir de la entrega del bien, la prestación del servicio o la celebración del contrato. La procedencia del mismo se evaluará en consideración a las características específicas del producto o servicio adquirido.

  Los suscriptores que adquieran certificados de firma digital emitidos por Certicámara S.A. mediante mecanismos no tradicionales o a distancia (incluidos canales electrónicos, telefónicos o virtuales), podrán ejercer su derecho de retracto dentro de los cinco (5) días hábiles siguientes a la celebración del contrato, siempre que el servicio no haya comenzado a ejecutarse.

  Dado que los certificados de firma digital constituyen servicios personalizados, asociados de forma exclusiva al titular, y cuya ejecución se perfecciona con la emisión o descarga del certificado, el derecho de retracto no procederá una vez iniciado el proceso técnico de activación del certificado.

  Por lo tanto, el derecho de retracto sólo será procedente si: i) Se ejerce dentro del término legal de cinco (5) días hábiles desde la contratación, y ii) El certificado no ha sido emitido, descargado, activado ni vinculado al usuario.

- Reversión del pago: Derecho ejercido en casos de fraude, operación no solicitada, producto defectuoso, producto adquirido no sea recibido y producto no conforme, dentro de los 5 días hábiles .

- Reintegro por doble pago, pago en exceso, pago errado: Solicitud que hace el suscriptor cuando se realiza un pago dos (2) veces sobre la misma factura o certificado digital, o cuando se pagó un poco más de lo que debido o se realizó una consignación errada. El suscriptor o usuario cliente cuenta con un término máximo de noventa (90) días.

- Reintegro por Impuestos: En este caso el cliente pagó un valor de algún impuesto que no debía pagar y por lo tanto se debe proceder con la devolución. El suscriptor o usuario cuenta con un término máximo de noventa (90) días.

- Reintegro por incompatibilidad: En estos casos el cliente solicita la devolución del dinero porque el certificado digital no es compatible con su equipo o su

sistema. El suscriptor o usuario cuenta con un término máximo de noventa (90)días siempre y cuando no haya sido descargada la firma digital.

- Reintegro por incumplimiento al deber de información: Sucede en los casos en que medie sanciones o multas por incumplimiento a este deber siempre que medie decisión judicial o administrativa en cuyos casos se deberá proceder con la devolución del dinero independientemente del término en el que este se presente.

9.2 Responsabilidad financiera

9.2.1 Cobertura de seguro

De acuerdo con lo establecido en numeral 5 del artículo 2.2.2.48.2.3 del Decreto 1074 de 2015 (que compila al Decreto 333 de 2014, artículo 7°) y el artículo 2.2.2.48.2.5 del Decreto 1074 de 2015 (que compila al Decreto 333 de 2014, artículo 9°), Certicámara ha suscrito una póliza de seguro con una entidad aseguradora autorizada de acuerdo con la legislación colombiana, que ampara los perjuicios contractuales y extracontractuales de los suscriptores y terceros de buena fe exenta de culpa derivados de errores y omisiones, o de actos de mala fe de los administradores, representantes legales o empleados de Certicámara en el desarrollo de sus actividades.

b) La cuantía asegurada es de 7.500 SMMLV por evento.

c) Las condiciones generales de la póliza se pueden consultar en la página web en la siguiente sección: https://web.certicamara.com/marco-normativo/poliza-de-garantias.

9.3 Confidencialidad de la información

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

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

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

La información confidencial del suscriptor de servicios de certificación digital podrá ser expuesta por solicitud de éste, en su calidad de propietario de esta. Cuando se exige a la ECD, por ley o autorización en las disposiciones contractuales, la divulgación de información confidencial, el suscriptor o la persona implicada debe, a menos que lo prohíba la ley, ser notificada de la información suministrada.

9.3.1 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 contenga datos relacionados del suscriptor.
- Toda la información que sea remitida a Certicámara y que haya sido etiquetada como "Confidencial" por el remitente.
- La información acerca del suscriptor obtenida en fuentes ajenas al mismo (por ejemplo, de un reclamante o de los reguladores) debe ser tratada como confidencial, excepto cuando la misma sea de carácter público.

9.3.2 Información fuera del alcance de la información confidencial

Se considera información no confidencial:

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

9.3.3 Responsabilidad de proteger la información confidencial

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

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

- Implementar y mantener estrictas políticas y procedimientos de seguridad de la información que cumplan con los estándares nacionales e internacionales, incluyendo los requisitos de la ONAC y la legislación vigente en materia de protección de datos.
- Capacitar continuamente a todo nuestro personal sobre las mejores prácticas en seguridad de la información, la importancia de la confidencialidad y sus responsabilidades individuales en la protección de los datos.
- Utilizar tecnologías y sistemas de seguridad robustos y actualizados, incluyendo cifrado de datos, controles de acceso estrictos, sistemas de detección de intrusiones y mecanismos de respaldo y recuperación de información.

- Limitar el acceso a la información confidencial únicamente al personal autorizado que requiera dicha información para el desempeño de sus funciones. Todo acceso es monitoreado y registrado.
- Establecer acuerdos de confidencialidad con todos nuestros empleados, contratistas y terceros que puedan tener acceso a información sensible.
- Gestionar de forma segura y responsable la información de las claves privadas de los suscriptores, asegurando su protección contra el acceso no autorizado, la divulgación, la alteración o la destrucción.
- Notificar de manera oportuna a las autoridades competentes y a los afectados sobre cualquier incidente de seguridad que comprometa la confidencialidad, integridad o disponibilidad de la información, de acuerdo con los marcos regulatorios aplicables.
- Realizar auditorías internas y externas de forma regular para evaluar la efectividad de nuestros controles de seguridad y asegurar el cumplimiento continuo con nuestras políticas y los requisitos regulatorios.

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

9.3.4 Tratamiento de Datos personales

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

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

- Recolectar los datos personales únicamente cuando sea necesario y pertinente para la prestación de sus servicios de certificación digital, la verificación de identidad, la emisión, renovación, suspensión o revocación de certificados, y el cumplimiento de nuestras obligaciones legales y contractuales.
- Informar a los titulares de los datos sobre la finalidad específica para la cual sus datos serán recolectados y tratados, obteniendo su consentimiento previo, expreso e informado, a menos que la ley exija o permita lo contrario.
- Utilizar los datos personales exclusivamente para las finalidades informadas y autorizadas, absteniéndose de utilizarlos para propósitos distintos a los establecidos en su política de tratamiento de datos personales, autorizaciones o aviso de privacidad dispuestos al momento de la recolección.
- Garantizar la veracidad, actualización y completitud de la información que reposa en nuestras bases de datos, implementando los mecanismos necesarios para que los titulares puedan actualizar o rectificar sus datos.

- Implementar medidas técnicas, humanas y administrativas rigurosas para salvaguardar la seguridad de los datos personales, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Permitir el acceso de los titulares a sus datos personales y a la información sobre el tratamiento de los mismos, así como facilitar el ejercicio de sus derechos a conocer, actualizar, rectificar y suprimir sus datos, y a revocar la autorización otorgada.
- Mantener la confidencialidad de los datos personales, incluso después de finalizada la relación con el titular, salvo en los casos en que la información sea requerida por una autoridad judicial o administrativa en ejercicio de sus funciones legales.
- No transferir ni comunicar datos personales a terceros sin la autorización expresa del titular, salvo en los casos que la ley lo permita o lo exija para el cumplimiento de una función legal o contractual.

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

9.3.5 Revelación en virtud de un proceso judicial o administrativo

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

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

9.4 Derechos de propiedad intelectual

El suscriptor deberá respetar y atender la normativa en materia de propiedad intelectual, que incluye tanto a la propiedad industrial como a Derechos de Autor. Para tal efecto, atenderá lo dispuesto en el Código de Comercio, la Decisión 486 de 2000, la Decisión 351 de 1993 y demás normas complementarias a estas materias.

Por medio de la presente disposición se establece que toda la información contenida en la Declaración de Prácticas de Certificación –DPC pertenece única y exclusivamente a la Sociedad Cameral de Certificación Digital Certicámara S.A.,de tal forma que esta se reserva todos los derechos relacionados con la propiedad intelectual del presente documento (DPC), incluyendo la información, técnicas, modelos, políticas internas, procesos y procedimientos, de acuerdo con la normativa nacional e internacional relacionada con la materia.

9.5 Obligaciones y responsabilidades de los intervinientes

9.5.1 Obligaciones y deberes de Certicámara

Certicámara tiene las siguientes obligaciones en la prestación de sus servicios:

a) Implementar y mantener los sistemas de seguridad que resulten razonables en función del servicio prestado y en general la infraestructura necesaria para la prestación del servicio de Certificación Digital.
b) Cumplir con la Declaración de Prácticas de Certificación (DPC), Políticas de Certificación (PC) y con los acuerdos realizados con los suscriptores.
c) Informar al suscriptor las características de la prestación del servicio, los límites de responsabilidad, y las obligaciones que asume como interviniente en el proceso de certificación digital. En particular Certicámara deberá informar al suscriptor o terceras personas que lo soliciten, sobre el tiempo y recursos computacionales requeridos para validar la firma digital que se efectúa con los certificados de firma que expide a sus suscriptores.
d) Comprobar directamente o a través de las Entidades de Registro debidamente acreditadas ante Certicámara, la información definida en esta Declaración de Prácticas de Certificación como verificable para la expedición de certificados digitales.
e) Abstenerse de acceder o almacenar la clave privada del suscriptor.
f) Conservar por sí mismo o por interpuesta persona la custodia del soporte físico del certificado digital hasta la entrega efectiva del mismo al suscriptor (si aplica).
g) Permitir y facilitar la realización de las auditorías por parte del Organismo Nacional de Acreditación de Colombia.
h) Expedir certificados digitales de conformidad con lo establecido en la sección de procedimiento de expedición de certificados digitales de esta Declaración de Prácticas de Certificación, y las especificaciones acordadas por el suscriptor en el contrato de suscripción.
i) Publicar los certificados digitales expedidos y llevar el Registro de Certificados Emitidos.
j) Informar al Organismo Nacional de Acreditación de Colombia la ocurrencia de cualquier evento establecido en la Declaración de Prácticas de Certificación, que comprometa la prestación del servicio.
k) Informar al Organismo Nacional de Acreditación de Colombia la introducción de nuevos requisitos o cambios en la infraestructura PKI que puedan afectar la prestación del servicio.
l) Notificar al suscriptor cualquier cambio de estado de su certificado digital, explicando las razones de las decisiones tomadas de acuerdo con lo establecido en la Declaración de Prácticas de Certificación.
m) Mantener el control y confidencialidad de su clave privada y establecer las seguridades razonables para que no se divulgue o comprometa.
n) Procurar diligentemente la prestación permanente e ininterrumpida de los servicios de certificación digital.

o) Permitir el acceso de los suscriptores, de las partes confiantes y de terceros a esta Declaración de Prácticas de Certificación y al repositorio de la Entidad de Certificación.
p) Actualizar la Base de datos de certificados digitales revocados en los términos establecidos en esta Declaración de Prácticas de Certificación y efectuar los avisos y publicaciones que se establezcan por ley en ésta.
q) Revocar los certificados digitales que se requiera de conformidad con lo establecido en la sección 4.7 de esta Declaración de Prácticas de Certificación.
r) Informar al suscriptor, dentro de las 24 horas siguientes, la revocación de su certificado digital de acuerdo con la normatividad vigente.
s) Remover a los administradores o representantes que resulten incursos en las causales establecidas en el literal c del artículo 29 de la Ley 527 de 1999.
t) Disponer de una línea telefónica de atención a suscriptores y terceros, que permita las consultas y la pronta solicitud de revocación de certificados por los suscriptores.
u) Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas y certificados digitales emitidos y en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración.
v) Conservar física o electrónicamente la documentación que respalda los certificados digitales emitidos, por el término previsto en la ley para los papeles de los comerciantes y tomar las medidas necesarias para garantizar la integridad y la confidencialidad que le sean propias.
w) Atender las peticiones, quejas y reclamos hechas por los suscriptores, de conformidad con lo establecido en esta Declaración de Prácticas de Certificación.
x) Otorgar la información suministrada por el suscriptor el tratamiento que se establece en la sección de solicitud de certificados de esta Declaración de Prácticas de Certificación.
y) Cumplir con los Criterios Específicos de Acreditación CEA 3.0-7 publicado en la página WEB de ONAC.
z) Advertir, sobre las medidas de seguridad que deben observar los suscriptores de firmas y certificados digitales para la utilización de estos mecanismos.
aa) Certicámara sin discriminación alguna prestará el servicio de certificación digital a cualquier solicitante que cumpla con los requisitos establecidos en esta DPC y normas legales vigentes., sin embargo, Certicámara pude declinar la solicitud de certificación digital al solicitante o suscriptor cuando se evidencie participación en actividades ilícitas.
bb) Cumplir con lo dispuesto en la Ley Estatutaria 1581 de 2012 sobre Protección de Datos Personales y su normativa de desarrollo, los datos personales proporcionados se tratarán de acuerdo con los procedimientos que Certicámara S.A. ha definido para tal fin y con la finalidad de emitir un servicio de Certificación Digital o servicios conexos a éste.
cc) Notificar al suscriptor anticipadamente acerca de las actividades de subcontratación con el fin de brindarle la oportunidad de objetar de

conformidad con la normatividad colombiana vigente, para ello Certicámara dispone en su página web un sistema de recepción de Peticiones, quejas, reclamos, sugerencias y apelaciones PQRSA.

dd) Los proveedores críticos contratados para la prestación del servicio de datacenter, cumplen con los requisitos mínimos establecidos en el documento de Criterios Específicos de Acreditación CEA 3.0-7 publicado en la página WEB de ONAC. Para tal efecto se les hará extensivo el cumplimiento de los requisitos descritos en los Criterios Específicos de Acreditación CEA 3.0-7 publicado por el ONAC cuando ello corresponda.

ee) Las demás que establece la Ley 527 de 1999 en su artículo 32° y el Decreto 1074 de 2015 (que compila al Decreto 333 de 2014) en su artículo 2.2.2.48.3.6

El cumplimiento de todas o parte de las obligaciones o procedimientos de expedición de certificados digitales o de la prestación en general del servicio de certificación digital podrá ser realizado en forma directa por Certicámara o a través de sus Entidades de Registro.

CERTICÁMARA NO TIENE OBLIGACIONES ADICIONALES A LAS PREVISTAS EN ESTE ACÁPITE SALVO AQUELLAS PREVISTA EN LA NORMATIVA VIGENTE, NI DEBERÁ ENTENDERSE QUE EXISTEN OBLIGACIONES IMPLÍCITAS ADICIONALES A LAS EXPRESAMENTE CONSAGRADAS EN ESTA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN.

9.5.2 Obligaciones y deberes del solicitante

Los solicitantes de los servicios de certificación de Certicámara tendrán las siguientes obligaciones y responsabilidades:

a) Suministrar la información requerida de acuerdo con el servicio de certificación digital solicitado.

9.5.3 Obligaciones y responsabilidades del suscriptor

El suscriptor tiene las siguientes obligaciones frente a Certicámara y terceras personas:

a) Utilizar la clave privada y el certificado digital emitido tan sólo para los fines establecidos y de acuerdo con los condicionamientos establecidos en el contrato celebrado con él de manera individual y en esta Declaración de Prácticas de Certificación y la política de certificación correspondiente. Será responsabilidad del suscriptor el uso indebido que éste o terceros hagan del mismo.

b) Utilizar la clave privada y el certificado digital para firmar mensajes de datos, explicando a las partes confiantes bajo qué calidad se está firmando (ya sea como persona natural o como persona natural vinculada a una cualidad determinada al momento de la emisión del certificado digital), siempre y cuando el sistema de información de la parte confiante no verifique la cualidad en la que esté actuando el suscriptor. El mensaje de datos o documento electrónico que el suscriptor firma con su certificado digital será el que determinará el contexto de

la calidad en la que firma el suscriptor, y si éste está utilizando o no la cualidad asociada al certificado digital (si aplica).

c) Responder por la custodia de la clave privada y de su soporte físico (si aplica) evitando su pérdida, revelación, modificación o uso no autorizado. Especialmente, el suscriptor deberá abstenerse, sin importar la circunstancia, de anotar en el soporte físico del certificado digital el código de activación o las claves privadas, ni tampoco en cualquier otro documento que el suscriptor conserve o transporte consigo o con el soporte físico.

d) Solicitar la revocación del certificado digital que le ha sido entregado cuando se cumpla alguno de los supuestos previstos para la revocación de los certificados digitales.

e) Abstenerse en toda circunstancia de revelar la clave privada o el código de activación del certificado digital, así como abstenerse de delegar su uso a terceras personas.

f) Asegurarse de que toda la información contenida en el certificado digital es cierta y notificar inmediatamente a Certicámara en caso de que se haya incluido cualquier información incorrecta o inexacta o en caso de que por alguna circunstancia posterior la información del certificado digital no corresponda con la realidad. Asimismo, deberá comunicar de manera inmediata el cambio o variación que haya sufrido cualquiera de los datos que aportó para adquirir el certificado digital, aunque éstos no estuvieran incluidos en el propio certificado digital.

g) Informar inmediatamente a Certicámara acerca de cualquier situación que pueda afectar la confiabilidad del certificado digital, e iniciar el procedimiento de revocación del certificado digital cuando sea necesario. Especialmente, deberá notificar de inmediato la pérdida, robo o falsificación del soporte físico y cualquier intento de realizar estos actos sobre el mismo, así como el conocimiento por otras personas del código de activación o de las claves privadas, solicitando la revocación del certificado digital de conformidad con el procedimiento que se establece en la Declaración de Prácticas de Certificación.

h) Destruir el soporte físico cuando así lo exija Certicámara, cuando haya sido sustituido por otro con los mismos fines o cuando termine el periodo del servicio adquirido del certificado digital con Certicámara, siguiendo en todo caso las instrucciones de Certicámara.

i) Devolver el soporte físico del certificado digital cuando así lo exija Certicámara.

j) Respetar los derechos de propiedad intelectual (Propiedad Industrial y Derechos de Autor) de Certicámara y de terceras personas en la solicitud y en el uso de los certificados digitales. Certicámara no incluirá información en el certificado digital cuya inclusión pueda constituir de alguna forma la violación de los derechos de propiedad intelectual o industrial de Certicámara y de terceras personas.

k) Cualquier otra que se derive de la normativa vigente, del contenido de esta Declaración de Prácticas de Certificación o de la Política de Certificación.

l) Abstenerse de monitorear, alterar, realizar ingeniería inversa o interferir en cualquier otra forma la prestación de servicios de certificación digital.

m) Abstenerse de utilizar el certificado digital en situaciones que puedan ocasionar mala reputación y perjuicios a Certicámara.
n) Abstenerse de usar el nombre de la ECD y de la marca de certificación o en todo el material publicitario que contenga alguna referencia al servicio de certificación digital prestado por Certicámara inmediatamente después de su cancelación o terminación y emprender las acciones exigidas por el servicio de certificación digital y cualquier otra medida que se requiera.
o) Cumplir con el manual de uso del logo establecido por parte de Certicámara.
p) Cumplir los requisitos que establezca el servicio de certificación digital en relación con el uso de marcas en la prestación de los servicios y en consecuencia respetar los derechos marcarios que se encuentren en cabeza de Certicámara.
q) Las demás establecidas en el artículo 39 de la Ley 527 de 1999

EL SUSCRIPTOR PODRÁ UTILIZAR SU CERTIFICADO PARA: (I) IDENTIFICARSE COMO PERSONA NATURAL, O (II) ASOCIAR SU IDENTIFICACIÓN PERSONAL A UNA CUALIDAD ESPECÍFICA VERIFICADA POR CERTICÁMARA AL MOMENTO DE EMISIÓN DEL CERTIFICADO DIGITAL (SI APLICA). LA UTILIZACIÓN DEL CERTIFICADO DIGITAL EN UNO U OTRO CASO DEPENDERÁ DIRECTAMENTE DEL CONTEXTO EN EL QUE SE ESTÉ UTILIZANDO EL CERTIFICADO DIGITAL Y DE SI EL SISTEMA DE INFORMACIÓN DE LA PARTE CONFIANTE PUEDE O NO VERIFICAR LA IDENTIFICACIÓN DEL SUSCRIPTOR.

SERÁ EL DOCUMENTO ELECTRÓNICO O MENSAJE DE DATOS QUE EL SUSCRIPTOR FIRMA DIGITALMENTE, EL QUE OFRECERÁ EL CONTEXTO DENTRO DEL CUAL EL SUSCRIPTOR HACE USO DEL CERTIFICADO Y SI ESTE UTILIZA O NO LA CUALIDAD ASOCIADA AL CERTIFICADO DIGITAL.

9.5.4 Obligaciones y responsabilidades de la parte que confía

El Sistema de Certificación Digital de Certicámara comprende la utilización de un conjunto de elementos integrados en torno a la prestación de un servicio tanto a los suscriptores como aquellos que utilizan y confían en los certificados digitales emitidos por Certicámara. Cuando una tercera persona confía en un certificado digital, está aceptando utilizar dicho sistema en su integridad y por tanto acepta regirse por las normas establecidas para el mismo, las cuales se encuentran contenidas esencial pero no exclusivamente en esta Declaración de Prácticas de Certificación. Esa tercera persona se convierte en un interviniente del Sistema de Certificación Digital, en calidad de parte confiante, y por ello asume las obligaciones que se establecen a continuación:

a) Verificar la confiabilidad de la firma digital y del certificado digital, revisando especialmente que éste no se encuentre en la base de datos de certificados digitales revocados de Certicámara disponible en el sitio de Internet o en las oficinas de Certicámara. La confiabilidad de la firma digital y del certificado digital deberá en todo caso ceñirse a lo establecido en la sección de Confiabilidad de las firmas y los certificados digitales.
b) Aceptar y reconocer a los certificados digitales solamente el uso que se permite darles de conformidad con lo establecido en la sección de Uso de los certificados digitales.

c) Conocer con detenimiento y cumplir en todo momento con la Declaración de Prácticas de Certificación en la utilización de las firmas y los certificados digitales de Certicámara. En especial la parte confiante deberá tener presente y actuar en todo momento de acuerdo con las limitaciones de responsabilidad y garantías que ofrece Certicámara.
d) Informar a Certicámara de cualquier irregularidad o sospecha de la misma que se presente en la utilización del Sistema de Certificación Digital.
e) Abstenerse de monitorear, alterar, realizar ingeniería reversa o interferir en cualquier otra forma la prestación de servicios de certificación digital.

9.5.5 Obligaciones de los contratistas

En caso de que Certicámara contrate de forma externa servicios o productos, relacionados con las actividades acreditadas en el alcance, se hará extensible el cumplimiento de los requisitos establecido en el CEA 3.0-7, con base en la naturaleza del servicio contratado, la presente Declaración de Prácticas de Certificación y los requerimientos del marco normativo colombiano vigente según su función contratada para los certificados digitales.

Certicámara determinará si la entidad externa de aprobación proporciona los niveles de cumplimiento, según lo establecido contractualmente, sin perjuicio de las normas de mayor jerarquía vigentes a nivel legal, técnico, operativo y procedimental para el proceso de aprobación, las cuales estarán disponibles para su estudio y contraste en los sistemas de gestión de Certicámara, los cuales permiten establecer el acceso según su clasificación de confidencialidad, y en todo caso se encontrarán disponibles para la recepción de auditorías de tercera parte y por el Organismo Nacional de Acreditación.

9.6 Límites de responsabilidad

a) Las obligaciones enumeradas en la sección de obligaciones de Certicámara son de medio y no de resultado. Ello significa que Certicámara utilizará su conocimiento y experiencia en la prestación del servicio de certificación digital, y responderá profesionalmente por la culpa leve en sus actuaciones como Entidad de Certificación Digital. Certicámara no puede asegurar que la actividad de certificación tenga un resultado determinado. Certicámara sólo responderá por aquellos errores que, ocurridos, hubieran podido evitarse por su diligencia profesional.
b) Los daños producidos o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del **suscriptor**, de la **parte confiante** o de ambos, correrán por cuenta de éstos, así como todo perjuicio que se ocasione por el uso indebido de los **certificados digitales** o las violaciones a sus limitaciones de uso establecidas en el mismo, en la sección de Uso de los certificados digitales o en cualquier otro documento que regule el **Sistema de Certificación Digital**. Aunado a lo anterior, en el caso de los suscriptores se tendrá en cuenta lo que la normativa vigente establece en términos de responsabilidad de los suscriptores.
c) Certicámara no responderá por los perjuicios ocasionados por el incumplimiento de sus obligaciones por casos de fuerza mayor, caso fortuito o, en general, cualquier circunstancia sobre la que no se pueda tener un control razonable,

incluyendo pero sin limitarse a los siguientes: los desastres naturales, las alteraciones de orden público, el corte de suministro eléctrico y/o telefónico, los virus informáticos, las deficiencias en los servicios de telecomunicaciones (Internet, canales de comunicación, etc.) o el compromiso de las claves asimétricas derivado del riesgo tecnológico imprevisible.

d) Independientemente de la causa u origen de su responsabilidad, Certicámara fija como cuantía máxima para la indemnización de perjuicios por los daños ocasionados por certificado digital emitido, de acuerdo lo fijado en la póliza de responsabilidad civil profesional. En consecuencia, Certicámara solo indemnizará a las personas perjudicadas por un certificado digital emitido por ésta, independientemente del número de veces que el mismo se haya utilizado o del número de perjudicados por dichos usos. En caso de que existan varios perjudicados, el monto máximo indemnizable se distribuirá a prorrata entre ellos. Si habiéndose distribuido la indemnización, surgieren nuevos perjudicados, estos deberán dirigirse contra las personas ya indemnizadas para efectos de obtener a prorrata su indemnización.
e) Certicámara solo responderá por los perjuicios que se ocasionen por la utilización de los servicios de certificación digital dentro del año siguiente a la expiración o revocación del certificado digital. Certicámara no ofrece ningún tipo de garantía que no esté expresamente estipulada en esta Declaración de Prácticas de Certificación, ni responderá por evento que no esté expresamente contemplado en este acápite.
f) Será responsable de conformidad con lo previsto en los artículos 16 y 19 del Decreto 333 de 2014 compilado por el Decreto 1074 de 2015
g) En caso de que las leyes aplicables al servicio de certificación digital establezcan la imposibilidad de limitar la responsabilidad en alguno de los aspectos aquí descritos o que se describen en esta **Declaración de Prácticas de Certificación**, se dará a estas cláusulas el mayor alcance que la ley permita darles en cuanto a la limitación de la responsabilidad de Certicámara.

9.7 Derechos de los intervinientes

9.7.1 Derechos del solicitante

Los solicitantes de los servicios de certificación de Certicámara tendrán los siguientes derechos:

a) Que sea atendida su solicitud de acuerdo con los tiempos definidos por la entidad.
b) Que sea cumplida lo establecido en las políticas de certificación
c) Recibir la atención para solucionar dudas o inquietudes frente al servicio de certificación digital.

9.7.2 Derechos del suscriptor

Los suscriptores de los servicios de certificación de Certicámara tendrán los siguientes derechos:

a) Poder utilizar de manera adecuada el servicio de certificación digital adquirido.

b) Informar a los terceros confiantes que Certicámara es su ECD que presta el servicio adquirido.
c) Solicitar la revocación del servicio de certificación digital cuando lo requiera.
d) Solicitar la rectificación y/o revocación de la información de acuerdo con la política de tratamiento de datos personales.
e) Recibir soporte de o de los servicios de certificación digital de acuerdo con los términos y condiciones establecidos entre las partes.
f) A retractarse de la adquisición de los servicios de certificación, siempre que cumpla con los requisitos establecidos en la ley 1480 de 2011.
g) A revertir el pago cuando se trate de uno de los eventos determinados en el decreto 587 de 2016.

9.8 Exclusión de garantías

Certicámara no se hará responsable por

a) La veracidad de la información entregada por el suscriptor o solicitante.
b) Delitos Informáticos sufridos por el suscriptor
c) El uso fraudulento de los servicios certificados o CRLs
d) Por daños y perjuicios originados por la interpretación errónea de la Declaración de Prácticas de Certificación (DPC).
e) Por el incumplimiento de las obligaciones del suscriptor o solicitante.
f) Por el contenido de los mensajes o documentos en los cuales se utilicen los servicios de certificación digital.
g) Por caso fortuito o fuerza mayor.
h) Por el uso de los certificados cuando exceda lo dispuesto en la normativa vigente, en la DPC y PCs.

9.9 Minutas de contratos

El modelo de contrato que usa Certicámara para la prestación del servicio de certificado de firma digital está conformado por dos (2) documentos, los cuales se encuentran disponibles en los siguientes enlaces:

- Términos y condiciones del servicio de certificación de firma digital Certicámara S.A.
- Condiciones generales de contratación del servicio de certificación de firma digital de Certicámara S.A.

Por otra parte, el modelo de contrato que usa Certicámara para la prestación de los demás servicios acreditados, está conformado por dos (2) documentos, los cuales se encuentran disponibles en los siguientes enlaces:

- Términos y condiciones de productos, servicios y/o soluciones de Certicámara S.A.
- Condiciones generales de contratación de productos, servicios y/o soluciones de Certicámara S.A.

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

9.10 Política de manejo de otros servicios

No aplica.

9.11 Imparcialidad y no discriminación

Certicámara reconoce la importancia de salvaguardar la imparcialidad e independencia para prevenir conflictos de interés tanto internos como externos. Por ello, la Presidencia declara su compromiso de garantizar el cumplimiento de los requisitos de independencia, imparcialidad e integridad en todos sus servicios. El principal mecanismo para asegurar la imparcialidad es el proceso de gestión de la imparcialidad y la conformación del comité de imparcialidad.

La política de imparcialidad está disponible en: https://web.certicamara.com/politicas

Certicámara ha llevado a cabo un exhaustivo proceso de identificación, análisis y evaluación de los riesgos susceptibles de comprometer la objetividad e imparcialidad en la prestación de su servicio de certificación digital. En consecuencia, se informa sobre las acciones implementadas con el propósito de minimizar cualquier circunstancia que pudiera poner en riesgo la objetividad e imparcialidad en la provisión de sus servicios:

- Con el fin de prevenir riesgos asociados a publicidad engañosa, su portal web ha sido cuidadosamente diseñado para asegurar que sus clientes y/o suscriptores puedan discernir con claridad cuáles son sus productos y/o servicios que cuentan con la acreditación del Organismo Nacional de Acreditación de Colombia (ONAC).
- Para mitigar riesgos en la contratación de servicios de Datacenter, los proveedores que suministran este servicio son gestionados integralmente (desde la selección y contratación hasta la evaluación de su desempeño) en estricta observancia de su procedimiento de gestión de proveedores, asegurando así el cumplimiento de los requisitos técnicos admisibles definidos en los criterios específicos de acreditación.
- Las políticas y los procedimientos que rigen la operación de Certicámara, así como su administración, se aplican de manera no discriminatoria. Certicámara se abstiene de utilizar procedimientos que puedan obstaculizar o restringir el acceso de los solicitantes a sus servicios.

Los servicios de certificación digital ofrecidos por Certicámara son accesibles a todos aquellos solicitantes cuyas peticiones se enmarquen dentro del alcance de su acreditación, aplicando de manera consistente el principio de neutralidad tecnológica, el

cual se encuentra debidamente consignado en las definiciones y convenciones del presente documento.

El acceso a los servicios de certificación digital de Certicámara no está condicionado por ninguna característica particular del solicitante o suscriptor que no sean aquellas expresamente definidas en la Política de Certificación (PC), ni por la pertenencia a asociación o grupo alguno, ni tampoco por el número de certificaciones previamente emitidas. No existen condiciones indebidas, ya sean de índole financiera o de otra naturaleza.

9.12 Política de Peticiones, quejas, reclamos, sugerencias y felicitaciones

Certicámara establece los lineamientos, procesos y canales de comunicación para la recepción, gestión, seguimiento y respuesta oportuna a las Peticiones, Quejas, Reclamos, Sugerencias y Felicitaciones presentadas por los clientes, usuarios y la demás partes interesadas. De esta manera, se garantiza la mejora continua de los servicios y productos, así como la satisfacción de todos los grupos de interés.

Para lo anterior se han dispuestos los siguientes canales para radicar una PQRSF:

- **Presencialmente:** En nuestra sede de Bogotá, Carrera 7 N° 26-20 Piso 18
- **Correo electrónico:** certicamararesponde@certicamara.com
- **Línea telefónica (ventas, servicio al cliente y soporte técnico):** (601) 7442727
- **Sistema PQRSAF:** Disponible en la página web.

El procedimiento para la atención de Peticiones, Quejas, Reclamos, Solicitudes y Felicitaciones se encuentra enmarcado de la siguiente manera:

9.13 Disposiciones de resolución de disputas

Todas las diferencias que se presenten entre las partes con ocasión de la celebración del contrato, durante su ejecución o por su interpretación , serán resueltas entre el Titular del Certificado Digital y Certicámara S.A. en primera instancia, por la vía de la conciliación, transacción o amigable composición, para lo cual, la parte inconforme remitirá comunicación escrita debidamente sustentada a la otra PARTE, quien evaluará los motivos de inconformidad y enviará respuesta dentro de los cinco (5) días hábiles a la fecha de su recibo (será responsabilidad de la parte que envía la comunicación asegurarse de que la otra parte reciba la comunicación enviada teniendo en cuenta parámetros de seguridad y de integridad de la información).

Si después del término antes señalado, transcurren quince (15) días y la(s) diferencia(s) persista(n), ésta(s) será(n) resueltas por un Tribunal de Arbitramento independientemente de la nacionalidad del titular del Certificado Digital, que se sujetará a las normas vigentes sobre la materia y se regirá especialmente, por las siguientes reglas:

a) El Tribunal estará integrado por un (1) árbitro designado por LAS PARTES de común acuerdo. Si esto no es posible, se delega su nombramiento al Director del Centro de Arbitraje y Conciliación que establezca Certicámara S.A. Al momento

de aceptar su designación, el árbitro deberá manifestar por escrito a LAS PARTES su independencia e imparcialidad para actuar como árbitro de la controversia.

b) El árbitro deberá ser abogado colombiano, inscrito en las listas de árbitros del Centro de Arbitraje y Conciliación.

c) La organización interna del Tribunal se sujetará a las reglas previstas para el efecto por el Centro de Arbitraje y Conciliación, en lo no regulado en la presente cláusula.

d) El Tribunal funcionará en la ciudad de Bogotá, en el Centro de Arbitraje y Conciliación.

e) El Tribunal decidirá en derecho y su fallo tendrá efectos de cosa juzgada material de última instancia y, en consecuencia, será final y obligatorio para LAS PARTES.

f) Los costos que se causen con ocasión de la convocatoria del Tribunal estarán a cargo de la PARTE vencida.

g) La normatividad aplicable será la colombiana**.**

9.14 Ley aplicable

Desde Certicámara se ha identificado la siguiente normatividad que se encuentra dentro del alcance de la prestación de los servicios acreditados en cumplimiento de:

- Decreto Único del Sector Comercio, Industria y Turismo - DURSCIT, 1074 de 2015
- Ley 527 de 1999
- Decreto 019 de 2012
- Decreto 620 de 2020
- Ley 2106 de 2019
- Ley 1581 de 2012
- Ley 1898 de 2018
- Decreto 333 de 2014
- Ley 1341 de 2009
- Decreto 1595 de 2015

- **Actividad 1.** Emisión de certificados en relación con las firmas digitales de personas naturales o jurídicas.
- **Actividad 2.** Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.
- **Actividad 3.** Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999.
- **Actividad 4.** Ofrecer o facilitar los servicios de generación de los datos de creación de las firmas digitales certificadas.

- **Actividad 6.** Ofrecer o facilitar los servicios de generación de datos de creación de las firmas electrónicas.
- **Actividad 9.** Cualquier otra actividad relacionada con la creación, uso o utilización de firmas digitales y electrónicas."

9.15 Políticas de certificación

La interrelación entre esta DPC y las Políticas de Certificación aplicable a los diferentes tipos de servicios de certificación se fundamenta en que:

- La presente DPC se estructura con base a las recomendaciones del RFC 3647 y establece las prácticas adoptadas por Certicámara para la prestación de los servicios acreditados por ONAC y contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los certificados, además sobre la relación de confianza entre Solicitante, Suscriptor, Responsable, Proveedores, Terceros de buena fe y la ECD.
- Las Políticas de Certificación establecen los procedimientos y requisitos particulares aplicables a los servicios de Certificación prestados por Certicámara. En cada una de las Políticas de Certificación se definen los requisitos para la solicitud del servicio, responsabilidades, condiciones comerciales y en general las condiciones particulares para cada uno de los servicios de certificación.

Certicámara detalla los requisitos aplicables a cada uno de los servicios en las siguientes Políticas de Certificación:

- PC Certificado de Firma Digital
- PC Estampado Cronológico
- PC Servicios Asociados de Información

La cuales se encuentran disponibles en https://web.certicamara.com/marco-normativo

10. CONTROL DE CAMBIOS

Fecha	Razón de actualización
12/09/2019	Se realizan los siguientes ajustes al documento: • Se actualizan los nombres de los cargos y áreas de acuerdo con la estructura organizacional vigente. • Se actualizan las URL´s. • De acuerdo con el nuevo modelo de operación, el responsable de mantener actualizada la DPC en la página web es el Director Gestión de Producto. Así mismo, los responsables de revisar y aprobar los cambios a la declaración de prácticas de certificación es el Gerente Comercial y de Mercadeo y el Director de Gestión de Producto.

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Fecha	Razón de actualización
	• Se alinean las responsabilidades y roles de confianza definidos por la organización para la administración y control de la infraestructura de la PKI. • En el numeral de "Análisis de vulnerabilidades", se aclara que son gestionadas por un tercero que cumpla con los criterios específicos de acreditación del ONAC a través de la Gerencia Administrativa y Financiera. • En el numeral "Auditores", se aclara que, para auditoría de tercera parte, la empresa auditora debe cumplir con los requisitos mínimos de aseguramiento establecidos en los criterios específicos de acreditación publicados en la página web del ONAC. • Se actualiza la tabla de tarifas por tipo de certificado. • Se actualizan los datos de las instalaciones físicas de Certicámara. • Se actualiza a nivel general la gestión de logs que realiza la organización para su monitoreo y control. • Se alinean los requisitos para cada tipo de certificado con lo definido internamente por la organización. • Cambia de código y versión de acuerdo con la estructura documental.
11/06/2020	Se realizan los siguientes ajustes al documento: • Se actualizan los cargos responsables de realizar los ajustes, la revisión y aprobación de las declaraciones de prácticas de certificación, de acuerdo con los cambios en la estructura organizacional. Así mismo, el responsable de su publicación en la página web. • Se incluyen los roles que requieren segregación de funciones y los requerimientos de contratistas independientes.
30/06/2020	Se realizan las siguientes actualizaciones al documento: • Aclaración que las políticas de certificación (PC) se encuentran inmersas en los capítulos de este documento de Declaración de Prácticas de Certificación (DPC), con el objetivo de facilitar el manejo y consulta de la información para las partes interesadas. • Para la actualización y/o modificación de la Declaración de Prácticas de Certificación (DPC), se realizará a través del procedimiento establecido por Certicámara, el cual contempla una primera etapa de revisión de los cambios y/o ajustes donde se analizan en conjunto los impactos

Fecha	Razón de actualización
	con los involucrados de cada gerencia. Posteriormente, son presentados al Presidente Ejecutivo para su aprobación.
02/09/2020	Se realizan los siguientes ajustes al documento: • Aclaración sobre los mecanismos para la entrega de los certificados digitales, descritos en el numeral 6.1.8. Generación del par de llaves de los suscriptores. A partir de lo anterior, se desactiva la Declaración de prácticas de certificación de Servicios firma centralizada, dado que se unifica con este documento. • Requisitos para la solicitud de expedición para cada política de certificación, en cuanto al documento de identificación del suscriptor.
22/10/2020	Se actualiza el documento, en los siguientes aspectos: • Palabras claves y su definición, para un mejor entendimiento del documento. • Para ciudadanos colombianos mayores de edad, se requiere adjuntar la copia de la cédula de ciudadanía en la solicitud para todas las políticas de certificación mencionadas. • En el numeral 1.2 "*La Sociedad Cameral de Certificación Digital Certicámara S.A*", se incluyen los datos de identificación de la empresa y el responsable de las Peticiones, Consultas y Reclamos de los suscriptores y usuarios. • Para modificación/actualización de la información contenida en los certificados, se ajusta la redacción para dar claridad al suscriptor de los pasos que debe seguir al respecto. • Como parte del numeral 10 de "*Políticas de Manejo de los Certificados Digitales*" que expide Certicámara, se aclara que los certificados emitidos podrán tener una vigencia máxima de 2 años de acuerdo con lo establecido en el CEA-4.1.10. • Se adiciona numeral "Modelo y Minutas de Contrato".
27/10/2020	Se actualiza el documento, en los siguientes aspectos: • Modificación del nombre del edificio donde se encuentra ubicado Certicámara • Inclusión del procedimiento para la atención de PQRSAF.

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Fecha	Razón de actualización
	• Inclusión del link para consultar el certificado de existencia y representación legal de la ECD y los DataCenter. • Inclusión de la información de identificación relacionada con los DataCenter. • Ajuste del vínculo del certificado de acreditación de la ECD. • Documentos y actividades de referencia de entidades de certificación que se encuentran en el alcance del servicio.
22/02/2021	Se actualiza el documento, en los siguientes aspectos: • Cambio de razón social del Datcenter Bt Latam por SENCINET LATAM COLOMBIA S.A. • En el glosario, se incluye la definición de Autoridad de Registro (RA) y se ajusta la de Estampado Cronológico (Time Stamping) • Redacción de lo relacionado con el plan de continuidad de negocio para mayor claridad. • Ajuste en las políticas de los tipos de certificados digitales • Inclusión del Anexo 1 donde se describe la información disponible en los diferentes certificados digitales. • Actualización de tarifas.
22/09/2021	Se actualiza el documento, en los siguientes aspectos: • Indicativo y número de contacto para temas administrativos de Certicámara. • En el numeral 1.5.1 Autoridad de Certificación AC Raíz y Certificadoras subordinadas, se incluye el serial y el hash del certificado de la CA raíz y la Subordinada respectivamente. • En el numeral 4.1 Solicitud de certificados, se incluye que Certicámara consultará las bases de datos necesarias para dar cumplimiento a SAGRILAFT. • En el numeral 4.6.1 Uso de clave CA Raíz y Subordinada, se actualizan los usos de la clave conforme con los declarados en el certificado digital. • Aclaración “Certicámara anualmente para asegurar la construcción de las llaves, tomara las recomendaciones dadas por: https://csrc.nist.gov/projects/hash-functions ”.

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Fecha	Razón de actualización
	• Actualización de tarifa para certificados digitales en token físico con vigencia a dos (2) años. • Ajuste en las etapas y canales de comunicación en el Procedimiento para la atención de Peticiones, Quejas, Reclamos, Sugerencias, Apelaciones y Felicitaciones. • En el anexo 1 – Certificados digitales, se elimina de los OID´S Email Address (E). • Actualización de nombres de cargos responsables de acuerdo con la nueva estructura organizacional. • Ajuste en la redacción para que la información sea más clara de cara al usuario y suscriptor.
12/05/2022	Se realizan los siguientes cambios al documento: • Redacción de la descripción de la política de Función Pública, de manera que se ofrezca un mayor entendimiento en la aplicación de esta. • En la política de persona natural, se incorpora lo relacionado con las directrices de persona jurídica de acuerdo con la acreditación del servicio por parte de ONAC. • Inclusión de los OID de la política de persona jurídica • Actualización de las tarifas para el 2022.
01/09/2022	• 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 ajusta la redacción para dar mayor claridad al solicitante y suscriptor sobre las disposiciones, información, directrices, controles y demás aplicables a los servicios acreditados ante el Organismo Nacional de Acreditación de Colombia ONAC. A partir de lo anterior, se define una DPC transversal y unas políticas de certificación (PC) independientes para los servicios: Certificado de firma digital, estampado cronológico y servicios asociados los cuales están publicados en la página web en la misma sección.
22/09/2022	En el numeral 1.1 *Identificación de la entidad de certificación digital,* se actualizan los cargos responsables de: • Recepción de las peticiones, consultas y reclamos de los suscriptores y usuarios

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Fecha	Razón de actualización
	• Revisión y aprobación de las respuestas a las peticiones, consultas y reclamos de los suscriptores y usuarios.
29/09/2022	En el numeral 4.9.6 *Disponibilidad de verificación de estado/revocación en línea*, se incluye que Certicámara cuenta con el histórico de certificados revocados desde el inicio de la prestación del servicio.
16/02/2023	Se incluye el numeral 4.10 para la definición de la reposición de los certificados de firma digital, donde se aclara que se debe generar un nuevo certificado y las condiciones que debe tener en cuenta el suscriptor para su gestión.
21/07/2023	Se actualiza el documento, en los siguientes aspectos: • Inclusión de los numerales: "*4.5 Desistimiento" y "4.6 no devolución de dinero"*, con el fin de dar a conocer a los solicitantes y suscriptores las condiciones que deben tener en cuenta para cada uno de estos temas. • Actualización de las URL de los nuevos puntos de distribución 4026 para la lista de certificados revocados CRL.
18/09/2023	Se actualiza el documento, en los siguientes aspectos: • Inclusión de las definiciones: Declinación de la solicitud, negación de la solicitud y recomendación para la decisión. • Actualización de los conceptos declinación y negación de la solicitud en el numeral *"4.1 Solicitud del certificado"*. Así mismo, se da claridad del idioma de los documentos entregados por el solicitante. • En el numeral "*4.12.1 Causales para la reposición*" se da claridad frente a las directrices a tener en cuenta para la gestión de este tipo de solicitudes. • Aclaración en el numeral "*5.2.4 Roles que requieren separación de funciones*" respecto a las funciones que desempeña la Autoridad de Registro (RA) y Autoridad de Certificación (CA) de conformidad con los Criterios Específicos de Acreditación – CEA, son llevadas a cabo por el personal vinculado directamente por Certicámara S.A. • Inclusión en el numeral *"9.1.3 Política de reintegro"* del canal autorizado para solicitar el reintegro y reversión del pago a través del sitio web de Certicámara S.A. sección PQRSAF o pestaña reversión de pago.

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Fecha	Razón de actualización
	• En el numeral *"9.11 Imparcialidad y no discriminación"* se da claridad sobre las políticas y los procedimientos relacionados con la no discriminación y la aplicación del principio de neutralidad tecnológica.
15/01/2024	Se realizan los siguientes cambios al documento: • En el numeral *"1.3.5 Otros participantes, proveedores de servicios", se a*ctualizan los proveedores para la prestación del servicio de Datacenter. • En el numeral *"3.2 Mecanismos de validación de identidad",* se incluye la verificación de identidad desde el portal web cuando el solicitante radica su solicitud. • Inclusión en el numeral "*4.1 Solicitud del certificado*" la aceptación plena, sin reservas y en su totalidad de los Términos y Condiciones del servicio, así como 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. • Aclaración en el numeral *"4.8.1 Tiempos para la renovación"* que la emisión de un nuevo certificado digital implica de manera previa la aceptación de Términos y Condiciones del servicio, 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.
18/03/2024	Se realizan los siguientes cambios en el documento: • Eliminación del servicio de Digitalización certificada con fines probatorios del alcance de los servicios acreditados. • En el numeral 4.1 solicitud de certificado, se aclara que la validación de la identidad hace parte de los requisitos que debe cumplir el suscriptor. • Actualización de los links de acuerdo con los cambios en la página web.
26/04/2024	• Aclaración de las condiciones generales de contratación de los servicios de certificación digital en el numeral *9.9 Minutas de contratos*.

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Fecha	Razón de actualización
09/09/2024	Se realizan los siguientes cambios al documento: • Actualización de los tiempos de gestión de entrega de los certificados digitales en medio físico. • Aclaración sobre la reposición en caso de error imputable a Certicámara. • Ajuste de los canales de atención para soporte técnico. • Actualización de la longitud de clave 4096 bits en la emisión de certificados digitales. • Inclusión de la causal de revocación por terminación del contrato laboral o vínculo contractual del suscriptor. • Inclusión de las políticas: Certificado digital persona natural PKCS#10 y Certificado digital persona jurídica PKCS#10
05/08/2025	Se realizan los siguientes cambios al documento: • Ajuste integral de redacciones para dar mayor claridad y precisión en la información. • Actualización del cargo y área responsable de atención de PQRSAF, así como el procedimiento a seguir. • Ajuste del procedimiento de aprobación de los cambios en la DPC. • Ajuste de las condiciones de Tiempo de descarga • Inclusión que el procedimiento de revocación del certificado digital no genera costo alguno. • Claridad de las condiciones a tener en cuenta para el reintegro por retracto. • Eliminación de la línea nacional gratuita. • Actualización de enlaces.
26/09/2025	Se realizan los siguientes cambios al documento: • Actualización de los datos de persona de contacto en el numeral 1.5.2. • Ajuste del lineamiento para restablecer la contraseña de token virtual, el cual no genera costo hasta diez solicitudes.