certicámara.

Declaración de Prácticas de Certificación

Código: DYD-L-003

Fecha: enero 2024

Versión: 016

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Contenido

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

1. INTRODUCCIÓN

Este documento presenta la Declaración de Prácticas de Certificación (DPC), la cual consiste en una manifestación pública de la Entidad de Certificación Digital Abierta en donde se establecen normas y prácticas de la Autoridad de Certificación para la prestación de los servicios de certificación digital de conformidad con la Ley 527 de 1999, el Decreto 1074 de 2015 que compila al Decreto 333 de 2014, Decreto 620 de 2020, Ley 2106 de 2019, Ley 1581 de 2012, Ley 1898 de 2018 Artículo 13.10 y el Decreto Ley 019 de 2012, en especial las actividades del artículo 161, para los servicios acreditados de: Certificado de firma digital, Estampado Cronológico, Huella Biométrica Certificada, Digitalización Certificada Con Fines Probatorios, Correo Electrónico Certificado, Generación De Firmas Digitales, Generación De Firmas Electrónicas Certificadas que presta la Sociedad Cameral de Certificación Digital Certicámara S.A.

La DPC está dirigida a todas aquellas personas naturales o jurídicas, solicitantes, suscriptores, y en general a usuarios de los servicios de certificación digital y terceros que confíen en ellos como evidencias jurídicas y probatorias, en el ámbito que sean implementados.

El presente documento se encuentra construido de acuerdo con el 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 objetivo de prestar los servicios de certificación digital, siendo filial de la Cámara de Comercio de Bogotá.

Certicámara es una Entidad de Certificación Digital Abierta, que tiene como propósito fundamental ser el tercero de confianza de productos y servicios de seguridad en medios electrónicos, proporcionando las herramientas necesarias para que los empresarios y demás usuarios de Internet del país puedan realizar negocios electrónicos con seguridad jurídica**.**

Nombre	Sociedad Cameral de Certificación Digital Certicámara S.A.
NIT	830.084.433-7
Matricula mercantil	1079279
Certificado de existencia y representación legal	https://web.certicamara.com/nosotros
Domicilio principal	Bogotá

Dirección	Carrera 7 Nº 26-20 Pisos 18, 19 y 31
Teléfono (asuntos administrativos)	(601) 7452141
Correo Electrónico	info@certicamara.com
Teléfono (ventas, servicio al cliente y soporte técnico)	(601) 7442727 Opción 3
Línea gratuita nacional	018000181531 – No válido para celulares
Responsable de la recepción de las peticiones, consultas y reclamos de los suscriptores y usuarios	Subgerencia de Relacionamiento
Responsable de la revisión y aprobación de las respuestas a las peticiones, consultas y reclamos de los suscriptores y usuarios	Subgerente de Relacionamiento
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	15/01/2024
Versión	016
Código	DYD-L-003
Ubicación	https://web.Certicámara.com/marco_legal

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 las siguientes 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 2048 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 https://datatracker.ietf.org/doc/html/rfc3628 y el Protocolo TSP (Time-Stamp Protocol) en el RFC 3161 https://www.ietf.org/rfc/rfc3161.txt

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

- Proveedores de servicios

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.

Nombre:	Comunicación Celular S.A. Comcel S.A.
NIT:	800.153.993-7
Matricula 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
Matricula 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

Toda la información consignada dentro la presente **Declaración de Prácticas de Certificación (DPC) y Políticas de Certificación (PC)** es propiedad intelectual de Certicámara**,** por lo tanto, realiza su administración de acuerdo con los lineamientos definidos 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 Subgerente de producto e innovación.

Nombre	Anthony Molina Gamboa
Cargo	Subgerente de producto e innovación
Correo	info@certicamara.com
Teléfono	(601) 7452141

1.5.3 Procedimientos de aprobación de la DPC

La actualización de la Declaración de Prácticas de Certificación, se realizará cada vez que se requiera por cuestiones legales, reglamentarias y/o aplicables a los servicios acreditados.

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

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

1.6 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/ac_subordinada_online_certicamara_2016.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_legal

d) Para la verificación de estado de revocación de certificados OCSP

- WEB:
  http://ocsp.Certicamara.com

  http://ocsp.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 solo será de consulta y no podrá ser modificada por personas no autorizadas. La información pública solo será actualizada por el personal encargado de esta función que labora en Certicámara.

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	Pertenencia a Empresa / Entidad
1.3.6.1.4.1.23267.50.1.2	Representación de Empresa / Entidad
1.3.6.1.4.1.23267.50.1.3	Titular de Función Pública
1.3.6.1.4.1.23267.50.1.4	Profesional Titulado
1.3.6.1.4.1.23267.50.1.5	Persona Natural
1.3.6.1.4.1.23267.50.1.2	Persona Jurídica

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.

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.

3.2.2 Autenticación de la identidad de la organización o persona

Para la autenticación de la identidad de la organización o persona, el solicitante deberá suministrar los soportes requeridos para cada servicio acreditado. El solicitante deberá suministrar a Certicámara información veraz, suficiente y adecuada respecto a los requisitos exigidos.

3.2.3 Comprobación de las facultades de representación

La comprobación de las facultades de representación del solicitante ante Certicámara se realizará mediante el cruce con el Registro Único Empresarial y Social (RUES) o la comprobación de los documentos legales, establecidos en la normativa colombiana que lo califique y faculte como representante legal.

3.2.4 Mecanismos de validación de identidad

3.2.4.1 Verificación de identidad desde el portal web

Certicámara, como Entidad de Certificación Digital Abierta, realizará la comprobación de identidad por medio de su portal web, 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.

3.2.5 Información del suscriptor no verificada

Certicámara en su calidad de Entidad de Certificación Digital Abierta valida la información del solicitante que pueda ser respaldada con evidencias como soporte. Para aquella información que no se pueda contar con soporte tal como dirección física, correo electrónico y demás, se parte del principio de la buena fe del solicitante al momento de aportar la información.

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.

3.3 Identificación y autenticación para solicitudes de renovación de claves

Certicámara no contempla el proceso de renovación de certificados digitales bajo el mismo par de claves del suscriptor.

En caso de requerirse la renovación de un certificado previamente emitido, se deberá surtir el proceso de solicitud de emisión de un nuevo certificado el cual contendrá un nuevo par de claves.

3.4 Identificación y autenticación para solicitud de revocación

Certicámara validará la identidad del suscriptor que invoca la causal de revocación. Si la persona que expone dicha causal no es el suscriptor o en caso de serlo no puede identificarse satisfactoriamente, deberá dirigirse personalmente a las oficinas de Certicámara en horarios de oficina 08:00 a.m. – 05:00 p.m. de lunes a viernes, con la prueba de la existencia de la causal de revocación respectiva para los casos en que aplique, sin perjuicio de que Certicámara disponga de las medidas que se establezcan para la seguridad del Sistema de Certificación Digital. Se aclara que una vez se reciba la solicitud de revocación y se compruebe la veracidad de dicha solicitud, se procederá a la revocación del certificado, sin periodos de gracia para dichas revocaciones.

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

La documentación entregada por el solicitante, deberá encontrarse únicamente en idioma español o inglés, de conformidad con las políticas internas de Certicámara S.A. Aquellos documentos que se encuentren en un idioma diferente, deberán ser traducidos, a cualquiera de estos idiomas, mediante un traductor oficial avalado por el Ministerio de Relaciones Exteriores y será almacenada de acuerdo con las tablas de retención documental generadas por Certicámara. La información del solicitante no será publicada por Certicámara a no ser que se tenga su consentimiento explícito.

Los solicitantes que hacen uso y suscriben de manera electrónica el certificado de firma digital de CERTICÁMARA S.A. implica la aceptación plena, sin reservas y en su totalidad, de los Términos y Condiciones del servicio de certificación de firma digital de Certicámara S.A., las Declaraciones y Compromisos en materia de prevención de LA/FT/FPDAM Y C/ST, la Declaración de Prácticas de Certificación (DPC), la Política de certificación (PC) y de las políticas organizacionales de Certicámara S.A., publicados a través del sitio web de Certicámara S.A y que hacen parte integral del presente documento y en el contrato de prestación de servicios de certificación digital.

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

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

a) Haber leído en su integridad los Términos y Condiciones del servicio de certificación de firma digital de Certicámara S.A., las Declaraciones y Compromisos en materia

de prevención de LA/FT/FPDAM Y C/ST, la presente Declaración de Prácticas de Certificación (DPC) y la Política de certificación - certificado de firma digital (PC).

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

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

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

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

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

- Referencias comerciales de la empresa.
- Referencias personales del **solicitante**.
- Certificaciones bancarias.
- Licencia de conducción válida.
- Libreta militar.
- Documento de afiliación al régimen de seguridad social en salud.
- Documento de afiliación a la empresa administradora de riesgos profesionales.
- Otros documentos que permitan verificar la identidad o facultades del suscriptor o de la entidad, para la emisión de cualquiera de los tipos de certificados que emite Certicámara.

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

g) Consultará las bases de datos necesarias para dar cumplimiento al SAGRILAFT, previa aceptación del solicitante de las Declaraciones y Compromisos en materia de prevención del lavado de activos financiación del terrorismo, financiamiento de la proliferación de armas de destrucción masiva, corrupción y soborno trasnacional

publicadas en el sitio web de Certicámara S.A. y que hacen parte integral del presente documento.

h) Emitirá certificados de firma digital con vigencia máxima de dos (2) años.

i) Certicámara S.A. declinará la expedición de un certificado digital a un solicitante, cuando no se encuentre dentro del alcance de la acreditación que le fue otorgado por ONAC, por el incumplimiento de la ley y/o cuando a su juicio atente contra el buen nombre de la ECD. En este caso, no habrá lugar a la subsanación por parte del usuario.

j) Si Certicámara decide negar o declinar la solicitud de expedición del certificado de firma digital, lo notificará por correo electrónico al solicitante, indicando los motivos que la justifican.

k) Actualmente nos encontramos en el desarrollo de la infraestructura que permita la compatibilidad para la emisión de los certificados de firma digital para el sistema operativo Mac OS.

4.1.1 Quién puede presentar una solicitud de certificado

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

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

4.2 Emisión de certificados

4.2.1 Acciones de la CA durante la emisión del certificado

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

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

En la emisión de los certificados la CA Subordinada:

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

- Ningún certificado será emitido con un periodo de validez que se inicie con anterioridad de la fecha actual.

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

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

4.3 Entrega del certificado digital a los suscriptores por medio físico

4.3.1 Cubrimiento

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

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

4.3.2 Requisitos de entrega

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

4.3.3 Tiempo de gestión de entrega – Certificados Físicos

A nivel urbano y ciudades principales el tiempo de entrega desde la emisión del certificado hasta la entrega al solicitante, será aproximadamente de dos (2) días hábiles; ante la imposibilidad de ubicar al solicitante o tercero autorizado dicho término podrá ser de cinco (5) días hábiles.

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

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

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

4.3.4 Tiempo de descarga – Certificado Virtual

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

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

4.4 Aceptación del certificado

No se requiere confirmación de parte del suscriptor como aceptación del servicio recibido. Se considera que el servicio de certificado digital es aceptado desde el momento que solicita su expedición, por ello, si la información contenida en la comunicación de activación del servicio no corresponde al estado actual de la misma o no fue suministrada correctamente, el suscriptor deberá notificar a Certicámara por cualquiera de nuestros canales para los trámites pertinentes de corrección.

4.4.1 Publicación del certificado por la CA

El servidor de la autoridad de registro introducirá las llaves públicas de los certificados digitales emitidos por la autoridad de certificación subordinada en la estructura de directorio

LDAP (Lightweight Directory Access Protocol) de la PKI, en el momento que el certificado sea emitido.

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

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

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

4.5 Desistimiento

En el caso en donde el usuario haya realizado el pago de alguno de los servicios acreditados ofrecidos por Certicámara, y no haya finalizado el lleno de los requisitos documentales necesarios, este tendrá un término para completar la información de noventa (90) días posteriores a la fecha de solicitud del servicio.

En el caso que el solicitante no diligencie la información requerida, se entenderá como el desistimiento de la adquisición del servicio, teniendo como consecuencia la no devolución del dinero.

4.6 No devolución del dinero

En ningún caso, Certicámara estará obligada a devolver el dinero al solicitante, salvo en las excepciones previstas por la ley.

4.7 Uso de pares de claves y certificados

4.7.1 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.

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

Los terceros de buena fe sólo pueden depositar su confianza en los certificados para aquello que establece esta DPC, PC y la normativa.

Los terceros de buena fe pueden realizar operaciones de clave pública de manera satisfactoria confiando en el certificado emitido por la cadena de confianza. Así mismo,

deben tener la precaución y asumir la responsabilidad de verificar el estado del certificado utilizando los medios que se establecen en esta DPC.

4.8 Renovación del certificado

4.8.1 Tiempos para la renovación

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

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

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

Quién puede solicitar la renovación

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

4.8.2 Tramitación de solicitudes de renovación de certificados

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

4.6.4 Notificación de emisión de nuevo certificado al suscriptor

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

4.9 Renovación de llave de certificado

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

4.10 Modificación del certificado

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

4.11 Revocación y suspensión de certificados

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

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

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.

4.11.2 ¿Quién puede solicitar la revocación?

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

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

4.11.3 Procedimiento para solicitud de revocación

Certicámara ha dispuesto los siguientes medios para la recepción de solicitudes de revocación:

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

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

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

Certicámara validará la identidad del suscriptor que invoca la causal de revocación. Si la persona que expone dicha no es el suscriptor o en caso de serlo no puede identificarse satisfactoriamente, deberá dirigirse personalmente a las oficinas de Certicámara en horarios de oficina 08:00 a.m. – 05:00 p.m. de lunes a viernes, con la prueba de la existencia de la causal de revocación respectiva para los casos en que aplique, sin perjuicio de que Certicámara disponga de las medidas que se establezcan para la seguridad del Sistema de Certificación Digital. Se aclara que una vez se reciba la solicitud de revocación y se compruebe la veracidad de dicha solicitud, se procederá a la revocación del certificado, sin periodos de gracia para dichas revocaciones.

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

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 y http://ocsp.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.

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://solicitudes.certicamara.com/SSPS/solicitudes/RevocarCertificadoClienteCF.aspx

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

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

A continuación, el titular del contrato enviará esta solicitud al área de operaciones al correo revocaciones@certicamara.com, donde se debe indicar el certificado que debe ser objeto de la reposición así como la información correspondiente a la revocación respectiva. Con base en la información suministrada se procederá a realizar el control de los cupos de la entidad.

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.

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 y http://ocsp.Certicamara.co

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

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

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 y, 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 limite (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

Todas las operaciones críticas de la CA raíz y la CA Subordinada están protegidas físicamente con todas las medidas de seguridad necesarias para los elementos más críticos y con vigilancia durante las 24 horas al día, los 7 días a la semana. Estos sistemas están separados de otros de Certicámara, de forma que sólo el personal autorizado pueda acceder a ellos.

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 están ubicados los equipos cuentan con las condiciones de potencia y ventilación necesarias para evitar fallos de potencia u otras anomalías eléctricas o en los sistemas eléctricos.

El cableado de los equipos está protegido para evitar interceptaciones o daños y se han adoptado medidas especiales para evitar las pérdidas de información provocadas por la interrupción en el flujo de suministro eléctrico, conectando los componentes más críticos a UPS para asegurar un suministro continuo de energía eléctrica, con una potencia suficiente para mantener la red eléctrica durante los eventos de apagado controlado del sistema y para proteger a los equipos frente fluctuaciones eléctricas que los pudieran dañar.

Los sistemas de aire acondicionado, conservan las estancias de los equipos con las condiciones de humedad y temperatura adecuadas para el correcto funcionamiento y mantenimiento de los mismos.

5.1.4 Exposiciones al agua

La instalación de la CA Raíz y CA Subordinada, está protegida para evitar las exposiciones al agua de los mismos, mediante detectores de humedad, inundación y otros mecanismos de seguridad apropiados al medio.

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 CA Subordinada, cuentan con personal que por sus responsabilidades son sometidos a procedimientos de control especiales debido a que su actividad es esencial para el correcto funcionamiento de la entidad de certificación digital Certicámara S.A. Así tienen la consideración de roles de confianza:

Agente de la RA: Son los encargados de la revisión y validación la información contenida en los documentos remitidos por el solicitante para la emisión de un servicio de la ECD.

Agente de la CA: Son los encargados de la aprobación, activación y revocación de un servicio de la ECD.

Especialista de Infraestructura PKI/TSA: Responsable del funcionamiento de los sistemas que componen el sistema de la AC raíz y AC Subordinada, del hardware y del software base.

System Auditor: El Director de Planeación y Gestión es el responsable internamente del proceso de gestión de auditorías, donde se establecen 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 designado 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 encargados de cada uno de los roles cuentan con los permisos necesarios en el marco de sus funciones los cuales se autentican partiendo de algo que se sabe (credenciales de acceso a la plataforma), las cuales son personales e intransferibles

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

5.2.4 Roles que requieren separación de funciones

Las funciones del personal que ejecuta los roles correspondientes a la Autoridad de Registro (RA) y la Autoridad de Certificación (CA) se encuentran segregadas, de tal forma que se asegura la independencia e imparcialidad en sus actividades.

Teniendo en cuenta las funciones desempeñadas por la Autoridad de Registro (RA) y la Autoridad de Certificación (CA), y de conformidad con los Criterios Específicos de Acreditación – CEA, estas actividades son llevadas a cabo por el personal vinculado directamente por Certicámara S.A.

5.3 Controles de personal

5.3.1 Calificaciones, experiencia y requisitos de autorización

Los colaboradores de Certicámara que ejecuta actividades en la prestación de servicios digitales cuenta con un proceso de estudio de confiabilidad a través del cual se valida referencias, experiencia, antecedentes, visita domiciliaria, calificaciones, entre otros.

5.3.2 Procedimientos de verificación de antecedentes

Para la verificación de los antecedentes, Certicámara a través de una empresa especializada, realiza las consultas en listas definidas para el establecimiento de la idoneidad de un colaborador.

5.3.3 Requisitos de formación

Certicámara establece un plan de capacitación anual para sus colaboradores alineado con las necesidades de formación que se identifiquen en el marco de sus funciones, el cual podrá contemplar algunos de los siguientes aspectos:

- Aspectos legales relativos a la prestación de servicios de certificación.
- Seguridad de la información y protección de datos personales
- Características de los servicios acreditados a nivel operativo y técnico.
- Procedimientos de operación y administración.
- Continuidad del negocio
- Cambios tecnológicos del entorno
- Introducción de nuevas herramientas.
- Modificación de procedimientos operativos

5.3.4 Sanciones por acciones no autorizadas

Certicámara tiene establecido el procedimiento para realizar las investigaciones y tomar las medidas disciplinarias que apliquen en caso de que los colaboradores incumplan las directrices impartidas por la organización. En cualquier caso, si Certicámara sospecha de que algún empleado está efectuando una acción no autorizada, automáticamente suspenderá su permiso de acceso, con la posibilidad de despedido de la organización.

5.3.5 Requisitos del contratista independiente

Certicámara dispone de los soportes de contratación y del cumplimiento de los requisitos solicitados tanto administrativos como técnicos, para aquellos contratistas independientes que presten 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 auditoria es de 3 años, periodo 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 tiene establecido y probado el Plan de Continuidad y Contingencia del Negocio (BCP) que define las acciones a realizar, recursos a utilizar y personal a emplear, en el caso de producirse un desastre natural o un acontecimiento intencionado o accidental que inutilice o degrade los recursos y el servicio de certificado de firma digital acreditado por el ONAC, para garantizar la continuidad del servicio

El plan asegura que Certicámara pueda continuar prestando el servicio en situaciones adversas, después de identificar, evaluar, gestionar y minimizar cualquier tipo de riesgo.

A través del Análisis de Impacto al Negocio (BIA) se ha realizado la respectiva preparación, atención y respuesta ante las posibles situaciones adversas que se puedan presentar, así como las respectivas acciones a ejecutar, teniendo como referente la reducción de los impactos operativos a los que se hubiese expuesto Certicámara.

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 2048 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 2048 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 2048 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.

6.5.2 Calificación de seguridad informática

Actualmente Certicámara como parte de su enfoque organizacional se encuentra certificada bajo la Norma ISO/IEC 27001:2013 – Sistema de Gestión de Seguridad de la Información de acuerdo con el alcance publicado al interior del respectivo certificado.

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.

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 las siguientes normas:

- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, mayo 2008.
- ITU-T Recommendation X.509 (2012): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework
- ETSI TS 101 862 V1.3.3 (2006-01): Qualified Certificate Profile, 2006
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, March 2004 (prevaleciendo en caso de conflicto la TS 101 862)

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

De acuerdo con las definiciones del Organismo Nacional de Acreditación – ONAC en Colombia se tiene establecido un plan anual de auditorías, dentro de la cual se evalúan los diferentes servicios acreditados.

El sistema de acreditación de la AC raíz y AC Subordinada se someterá a una auditoría de tercera parte de forma anual, de acuerdo con el programa de auditorías definido por Certicámara. De esta manera se asegura la adecuación de su funcionamiento y operatividad con las estipulaciones incluidas en esta DPC.

Adicionalmente, Certicámara podrá establecer la realización de auditorías internas bajo su propio criterio o en cualquier momento, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de las claves.

Cada año se llevará a cabo una auditoría externa para evaluar el grado de conformidad con los principios y criterios de Web Trust para Autoridades de Certificación digital de AICPA/CICA.

8.2 Identidad/calificaciones del evaluador

Para el caso de 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 de ONAC y los definidos en los procesos internos para la contratación de terceros.

8.3 Relación del evaluador con la entidad evaluada

La relación entre el auditor y la entidad auditada se limitará estrictamente a los procesos e información requerida para la auditoría. Por lo tanto, la parte auditada (CA raíz o la entidad subordinada) no deberá tener ninguna relación, actual o planificada, financiera, legal, o de cualquier otra clase que pueda derivar en un conflicto de intereses con el auditor. En el caso de los auditores internos, estos no podrán tener relación funcional con el área objeto de la auditoría.

8.4 Temas cubiertos por la evaluación

Son objeto de auditoría todos los requisitos técnicos, funcionales y organizativos entre ellos:

- La DPC utilizada.
- Política de Seguridad de la Información.
- Administración de la AC Raíz y AC Subordinada.
- Consideraciones de Confidencialidad.
- Seguridad Física.
- Modelo de Respaldo.
- Plan de Continuidad del negocio.
- Personal Operativo.
- Los criterios específicos de acreditación de ONAC según el CEA vigente.

8.5 Acciones tomadas como resultado de una no conformidad

La identificación de cualquier no conformidad en las auditorías dará lugar a la aplicación del proceso de Gestión de acciones correctivas y preventivas internamente, con el fin de eliminar la causa raíz identificada. En el caso de una no conformidad crítica, Certicámara podrá determinar la suspensión temporal de las operaciones de la CA

raíz o de la CA Subordinada hasta que las deficiencias se corrijan, la revocación del certificado de la entidad, cambios en el personal, etc.

8.6 Comunicación de resultados

Todos los resultados de auditoría sean presentados al comité de presidencia, con el objetivo de determinar las acciones correctivas y preventivas que se consideren pertinentes.

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 los servicios de validación sobre el estado del certificado. Este servicio no tendrá ningún costo.

9.1.3 Política de reintegro

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

- Retracto del suscriptor: Derecho que tiene el suscriptor de devolver el producto que compró o el servicio que contrató, y solicitar la devolución del dinero pagado, sin dar explicaciones, antes de los 5 días hábiles contados a partir de la entrega del bien o de la celebración del contrato.
- Desistimiento del proceso de adquisición: El suscriptor solicita el reintegro cuando el certificado digital no ha sido emitido. En estos casos se habla de un desistimiento del proceso de adquisición, ya que aún no se ha entregado el bien.
- Reintegro por doble pago, pago en exceso, pago errado: El suscriptor hace el pago 2 veces de la misma factura o certificado digital, o pagó un poco más de lo que debía o realizó una consignación errada.
- Reintegro por Impuestos: En este caso el cliente pago un valor de algún impuesto que no debía pagar y por lo tanto se debe proceder con la devolución.
- 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 o simplemente el certificado no era el que este requería.

- Reintegro por incumplimiento al deber de información: Certicámara está obligada a suministrar información sobre sus productos que sea completa, clara y verdadera. Por lo tanto, en caso de incumpliendo al deber de información, Certicámara deberá proceder con la devolución del dinero independientemente del término en el que este se presente.
- Solicitud de reversión del pago de acuerdo con las causales establecidas en el Decreto 587 de 2016, para este caso podrá encontrar el formulario en la pestaña de reversión de pago.

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 7º) y el artículo 2.2.2.48.2.5 del Decreto 1074 de 2015 (que compila al Decreto 333 de 2014, artículo 9º), 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 https://web.certicamara.com/marco_legal , donde hallará la información actualizada de la póliza.

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 este, en su calidad de propietario de esta.

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 contengan datos relacionados con el salario del suscriptor.
- Toda la información que sea remitida a Certicámara y que haya sido etiquetada como “Confidencial” por el remitente.

9.3.2 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

Certicámara se compromete a salvaguardar la confidencialidad de la información y no ponerla a disposición ni revelarla a individuos no autorizados.

En materia de tratamiento de datos personales, Certicámara aplica el principio de confidencialidad a través del cual, para aquellos datos personales que no tienen la naturaleza de públicos, se garantiza la reserva de la información, realizando el suministro o comunicación solo en los casos autorizados por la ley.

9.3.4 Aviso y consentimiento para usar información privada

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

Adicional a lo anterior, previo a la adquisición de los servicios de certificación digital, Certicámara hace entrega de los términos y condiciones, los cuales hacen referencia también, a la existencia de la política y la forma de acceso a la misma.

Cuando sea aplicable, Certicámara generará avisos de privacidad informando a los titulares, el tratamiento y finalidades al que se someterán los datos, así como los derechos que le asisten al titular, para garantizar el cumplimiento al deber de informar al titular.

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 (s) certificado (s), 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 32º 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 términos y condiciones para la suscripción que usa Certicámara en la prestación del servicio de certificado digital se encuentra disponible en el siguiente enlace:

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

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

En el caso de los términos y condiciones anteriormente indicados, aplicara la cláusula compromisoria prevista en el presente documento, que incluye el procedimiento jurídico para la resolución de conflictos, y especifica la jurisdicción y ley aplicable en el caso en que alguna de las partes no tenga domicilio en el territorio colombiano.

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, con el fin de prevenir conflictos de interés en el contexto interno y externo organizacional. Por esta razón la organización, en cabeza de la Presidencia Ejecutiva, declara su compromiso de garantizar el cumplimiento de los requisitos de independencia, imparcialidad e integridad respecto a todos sus servicios, teniendo como principal mecanismo para garantizar la imparcialidad el proceso de gestión de la imparcialidad y la conformación del comité de imparcialidad.

La política se encuentra publicada en el siguiente enlace: https://web.certicamara.com/politicas

Certicámara ha identificado, analizado y evaluado los riesgos que pueden afectar la objetividad e imparcialidad de la prestación del servicio de certificación digital. Por esta razón se permite informar las acciones encaminadas con el fin de minimizar cualquiera situación que pueda poner en riesgos la objetividad e imparcialidad de la prestación de sus servicios:

Para prevenir riesgos con publicidad engañosa, nuestro portal WEB (https://web.certicamara.com/productos_y_servicios) está diseñado para que nuestros clientes y/o suscriptores puedan identificar claramente cuáles son nuestros productos y/o servicios acreditados ante el Organismo Nacional de Acreditación (ONAC).

Para prevenir riesgos en la contratación de servicios de Datacenter, nuestros proveedores que prestan este servicio son gestionados (selección, contratación y evaluación) de acuerdo con lo establecido en nuestro procedimiento de gestión de proveedores con el fin de asegurar el cumplimiento de los requisitos técnicos admisibles definidos en los criterios específicos de acreditación.

Las políticas y los procedimientos bajo los cuales opera Certicámara, así como la administración de éstos, no son discriminatorios. Certicámara no utiliza procedimientos que impidan o inhiban el acceso de los solicitantes a nuestros servicios.

Los servicios de certificación digital de Certicámara son accesibles a todos los solicitantes cuyas solicitudes estén dentro del alcance de su acreditación. Esto incluye la aplicación del principio de neutralidad tecnológica que se encuentra registrado en las definiciones y convenciones del presente documento.

El acceso a los servicios de certificación digital de Certicámara no dependen de alguna característica del solicitante o suscriptor diferente a las definidas en la Política de Certificación (PC), ni de la membresía de cualquier asociación o grupo, tampoco depende del número de certificaciones ya emitidas. No existen condiciones indebidas, sean financieras u otras.

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

Si usted o cualquier persona tiene alguna petición, queja, reclamo, sugerencia y/o felicitación frente a cualquiera de los servicios o actividades de Certicámara, puede acercarse a nuestra sede en Bogotá, generar su solicitud a través de nuestra página web, comunicarse con nuestra línea atención al cliente o escribir a nuestro correo electrónico.

- Dirección: Carrera 7 Nº 26-20 Pisos 18, 19 y 31
- Dirección de correo electrónico: certicamararesponde@certicamara.com
- Número de teléfono (ventas, servicio al cliente y soporte técnico): (601) 7442727 Opción 3
- Línea gratuita nacional 018000181531 – No valido para celulares
- Sistema de PQRSAF
- Responsable de atención: Subgerencia de Relacionamiento
- Responsable de revisión y aprobación: Subgerente de Relacionamiento

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

Certicámara brinda Soporte técnico a través de:

- Línea Gratuita Nacional: 018000181531 – No valido para celulares
- Línea Soporte Bogotá: (601) 7442727 Opción 2

La página www.certicamara.com brinda:

- Instructivos de instalación
- Soporte técnico en línea Vía Chat
- Soporte técnico vía correo electrónico: soporte.firmadigital@certicamara.com

Si se requieren explicaciones sobre la aplicación de la Declaración de Prácticas de Certificación (DPC) o alguna política de certificación (PC) definidas en este documento para un servicio de certificación digital específico, por favor dirigir su consulta a info@certicamara.com

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 RFC3647 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 Certificados Digitales
- PC Estampado Cronológico
- PC Servicios Asociados de Información

La cuales se encuentran disponibles en https://web.certicamara.com/marco_legal.

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. • 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.

Fecha	Razón de actualización
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 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

Fecha	Razón de actualización
	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. • 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.

Fecha	Razón de actualización
	• 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.
20/09/2021	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 ". • 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.

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Fecha	Razón de actualización
25/04/2022	• Se ajusta la redacción de la descripción de la política de Función Pública, de manera que se ofrezca un mayor entendimiento en la aplicación de la misma. • Se actualiza la política de persona natural, donde se incorpora lo relacionado con las directrices de persona jurídica de acuerdo con acreditación del servicio realizado. • Se incluyen los OID de la política de persona jurídica
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 • 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.

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Fecha	Razón de actualización
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. • 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.

Fecha	Razón de actualización
	• 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.