Política de Certificación – Servicios Asociados A Sistemas De Información

Código: DYD-L-009

Fecha: Septiembre 2022

Versión: 001

Contenido

POLITICA DE CERTIFICACIÓN – SERVICIOS ASOCIADOS A SISTEMAS DE INFORMACIÓN

1. INTRODUCCIÓN

Este documento presenta una manifestación pública de la entidad de certificación digital abierta sobre las políticas y procedimientos específicos, normas y condiciones generales de los Servicios Asociados a Sistemas de Información los cuales contemplan los siguientes:

- Huella Biométrica Certificada
- Correo Electrónico Certificado
- Generación de Firmas Electrónicas Certificadas
- Generación de Firmas Digitales
- Digitalización Certificada con Fines Probatorios

Que presta la Sociedad Cameral de Certificación Digital Certicámara S.A.

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

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

1.1 Nombre e identificación del documento

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

Nombre	Políticas de Certificación – PC – Servicios Asociados a Sistemas de Información
Fecha de publicación	06/09/2022
Versión	001
Código	DYD-L-006
Ubicación	https://web.Certicámara.com/marco_legal

1.2 Alcance

Este documento establece las normas y reglas a seguir por la Entidad certificadora **Certicámara** para ofrecer los servicios de Huella Biométrica Certificada (Certihuella), Digitalización Certificada con Fines Probatorios, Correo Electrónico Certificado (Certimail),

Generación de firmas digitales, Generación de firma electrónicas certificadas (Clave Segura), tal como se encuentra establecido en el certificado de acreditación expedido por el Organismo Nacional de Acreditación ONAC en su página web https://onac.org.co/certificados/16-ECD-002.pdf

1.3 Procedimiento para la actualización o aprobación de la política

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

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

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

2. IDENTIFICACIÓN DE POLÍTICAS

2.1 Criterio de identificación de las políticas

Cada uno de los servicios prestados por Certicámara enmarcados dentro de esta política se identifica de acuerdo con su alcance, dada la naturaleza no cuenta con un identificador OID.

Los servicios enmarcados dentro de esta política están en la capacidad de utilizar los otros servicios acreditados para Certicámara.

2.2 Política de Huella Biométrica Certificada

2.2.1 Huella Biométrica Certificada

Servicio que permite realizar la verificación y validación de identidad de una persona a través de medios electrónicos, mediante el acceso y consulta de los patrones de su huella dactilar conocidos como minucia, frente a una fuente confiable como es la réplica II de la Base de Datos Biográfica y Biométrica de la Registraduría Nacional del Estado Civil (RNEC) contra la cual se realizará el cotejo de la huella, dando cumplimiento a la normativa vigente para la prestación de este servicio, los contratos comerciales, acuerdos comerciales y la promesa de valor ofrecida a los clientes. Para tal efecto, Certicámara es el aliado tecnológico/operador biométrico autorizado por la RNEC de acuerdo con el siguiente enlace https://wsp.registraduria.gov.co/biometria/operadores/listar/, que apoyará al suscriptor en

todos los aspectos relacionados con las tecnologías de la información para el proceso de autenticación biométrica de conformidad con lo previsto en la Resolución 5633 de 2016.

2.2.2 Principales características y funcionalidades del sistema de huella biométrica.

- Verificación de identidad de ciudadanos colombianos contra la réplica de la Base de Datos Biográfica y Biométrica de la RNEC.
- Posibilidad de hacer uso de las 10 huellas de las manos para verificar la identidad de un ciudadano colombiano.
- Conocer el estado de vigencia de la cédula.
- Conocer los datos biográficos públicos del ciudadano verificado:
    - Nombre completo.
    - Lugar y fecha de expedición de la cédula.
- Sitio web de gestión, en donde es posible:
    - Consultar la cantidad de verificaciones de identidad realizadas.
    - Llevar el registro de usuarios y equipos de cómputo que accederán al servicio.
- Posibilidad de integración con otros sistemas del cliente a través de Web Service.

2.2.3 Actividades ante la RNEC

A continuación, se indican las actividades que el solicitante habilitado por la normativa vigente prevista en el correspondiente a Huella Biométrica Certificada del Numeral relativo a “Referencias” del presente documento, para acceder y consultar la Base de Datos Biográfica y Biométrica de la Registraduría Nacional del Estado Civil (RNEC), debe llevar a cabo ante la RNEC con el fin de obtener aprobación para acceder y consultar la réplica de la Base de Datos Biográfica y Biométrica:

- Elevar Solicitud escrita a la RNEC con la intención de celebrar un contrato o convenio con esta última. Dicha solicitud debe encontrarse soportada en el estudio de necesidad que el solicitante elabore de conformidad con lo establecido en la Resolución 5633 de 2016.
- Presentación del modelo técnico y funcional a implementar.
- Revisión y análisis de la viabilidad técnica y jurídica de la solución a implementar por parte de la RNEC
- Revisión del software implementado
- Suscripción y legalización del contrato o convenio entre el solicitante y la RNEC

2.2.4 Notificación al solicitante por Certicámara de la activación del servicio

El SUSCRIPTOR sabrá sobre la emisión efectiva del certificado por medio de una notificación al mismo, mediante correo electrónico.

2.2.5 Forma en la que se acepta el servicio

Se considera que el servicio de huella biométrica certificada es aceptado por el solicitante desde el momento que se suscriba el contrato suscrito entre las partes.

2.3 Política de la digitalización certificada con fines probatorios

El servicio de digitalización certificada con fines probatorios es un proceso que consiste en otorgar autenticidad, integridad y no repudio a una imagen digital a través de un proceso reprográfico a un documento físico, mediante controles automatizados, los cuales permitirán mitigar riesgos de alteración de la información y suplantación de identidad, como son: la firma digital, el estampado cronológico y el cifrado de datos, mecanismos que permiten obtener un nuevo documento equivalente al documento físico original.

2.3.1 Administración de la política

Las políticas de administración del servicio están establecidas acorde a la política de seguridad vigente de **CERTICÁMARA**.

Ámbito de aplicación: La Digitalización Certificada con fines probatorios debe cumplir los siguientes propósitos:

- Autenticidad de la imagen digital
- Seguridad de documentos físicos y electrónicos

Límites de uso del servicio: El proceso de digitalización con fines probatorios se debe enmarcar en las condiciones establecidas por el Archivo General de la Nación dentro del protocolo de digitalización con fines probatorios.

2.3.2 Autenticación de la imagen digital

La autenticidad de la imagen digital tiene como alcance fundamental la conversión de un documento físico (Papel) a un documento electrónico a través de un proceso reprográfico (escáner) llamado digitalización con el objetivo de garantizar la existencia de un documento veraz, fiable, auténtico e íntegro tal y como el documento físico (papel) original.

2.3.3 Seguridad de documentos físicos y electrónicos

La Digitalización Certificada con fines probatorios, ofrece las siguientes garantías sobre el documento físico y electrónico:

- Evita la manipulación de los documentos físicos.
- Permite la adecuada conservación e integridad de los documentos físicos.

- Los documentos electrónicos obtenidos por este medio no pueden ser alterados ni modificados.
- Disponibilidad y portabilidad del documento electrónico.
- Reemplaza el documento físico en la ejecución de trámites
- Asegura la recuperación de los documentos mediante mecanismos de descripción apropiados.
- Preservación de los documentos en el tiempo, principalmente los de conservación total.

2.3.4 Alcance del servicio de digitalización certificada con fines probatorios

La Digitalización Certificada con fines probatorios garantiza la autenticidad de un documento electrónico obtenido mediante el uso de un proceso reprográfico (Digitalización a través de un escáner), el cual tiene la misma validez y garantía de un documento físico original, siempre y cuando el documento esté firmado digitalmente y estampado cronológicamente y que estos componentes de certificación sean emitidos por una Entidad de Certificación autorizada, soportado en la ley 527 de 1999, es un documento electrónico con atributos jurídicos que garantiza autenticidad, integridad y No repudiación de contenidos.

2.3.5 Principales Características de la digitalización certificada con fines probatorios

- El proceso de Digitalización Certificada con fines probatorios garantiza la fidelidad de la imagen del documento realizado en formato PDF/A
- Seguridad y garantía del documento electrónico, como un documento veraz, fiable, auténtico e íntegro, tal como el original.
- Cumplimiento de la normatividad
- Lineamiento con la política cero papel
- Conversión de diferentes formatos de documentos y mensajes de datos a PDF/A
- Integridad de los documentos firmados, minimizando el riesgo de alteración de los documentos electrónicos.
- Valor probatorio
- Equivalente funcional con documento físico
- Mitiga la pérdida de documentos
- Facilita la consulta de documentos

2.3.6 Elementos del proceso de digitalización certificada con fines probatorios

a) Documento físico
b) Equipo de Cómputo
c) Escáner
d) Certificado de firma digital
e) Estampas cronológicas.

2.3.7 Suscripción del contrato

El cliente firmará un contrato con **CERTICÁMARA S.A.,** con el fin de legalizar el proceso a ejecutar, el cual estará respaldado por una póliza de cumplimiento para ambas partes.

2.3.8 Organización de documentos

Los documentos físicos que van a ser sometidos al proceso de Digitalización Certificada con fines probatorios deben estar completamente organizados bajo todas las actividades inherentes a la organización cumpliendo la normatividad archivística vigente.

2.3.9 Ciclo de vida del proceso de digitalización certificada con fines probatorios y procedimientos de operación

El proyecto durará el tiempo que esté descrito en el contrato el cual debe ser coherente con el tiempo estimado en la propuesta técnica económica presentada al cliente.

2.3.10 Notificación al solicitante de la prestación del servicio de digitalización certificada con fines probatorios

Mediante cronograma aprobado por CERTICÁMARA y el solicitante, se realiza la activación del servicio que será legalizado mediante la suscripción del Contrato o de un acta de inicio entre las partes que forme parte integral del Contrato.

2.4 Política de correo electrónico certificado (certimail)

Plataforma de Correo electrónico certificado (Certimail), proporciona un servicio de notificación electrónica por e-mail, asegurando las características de trazabilidad e integridad. Para ello, el servicio permite certificar la recepción de los mensajes por medio del acuse de recibo, documento que se encuentra estampado cronológicamente. Este servicio cuenta con la misma validez jurídica y probatoria de un envío certificado por medios físicos, adicionalmente aporta seguridad jurídica, técnica e integra funcionalidades que optimizan la administración.

2.4.1 Ámbito de aplicación

Correo Electrónico Certificado emitido bajo esta política puede ser utilizado para los siguientes propósitos:

- Validar el envío correcto de un correo del remitente hacia un destinatario
- Validar la correcta entrega del correo a un destinario
- Saber la fecha y hora de la entrega

- Identificar si un corre ha sido alterado.

2.4.2 Auditoría digital de la comunicación electrónica

Servicio que permite demostrar la recepción del mensaje enviado, asegurando en todo momento las características de trazabilidad e integridad. Para ello, el servicio certifica por medio de un acuse de recibo, documento que se encuentra estampado cronológicamente.

2.4.3 Funcionalidades del servicio de correo electrónico certificado (Certimail)

Los correos electrónicos realizados mediante el proceso de correo electrónico certificado (Certimail) ofrecen la garantía de la integridad y la trazabilidad del mensaje de datos enviados por el emisor.

- Trazabilidad del mensaje: El servicio de correo electrónico certificado registra la cadena de custodia electrónica desde el momento en el que el mensaje de datos sale de la máquina del remitente hasta que es entregado al destinatario (Traza SMTP). La entrega del mensaje conocido como Acuse de Recibido o Acuse de Recibo contiene la totalidad de información relevante y la asocia al contenido del mensaje original, hora y fecha, cuenta de correo electrónico origen y cuenta de correo electrónico destinatario. El acuse de recibido se genera una vez se haya recopilado toda la información de la traza de todos los destinatarios.

- Integridad del acuse de recibido: Una vez se genere el documento de acuse de recibido se hace uso del servicio de estampado cronológico que cuenta con la hora legal Colombiana, el cual es enviado de manera adjunta al correo electrónico del emisor.

2.4.4 Principales características y funcionalidades del correo electrónico certificado (Certimail)

- Generación de notificación con respecto al envío del correo electrónico, el cual actúa como el registro que hace constar que el mensaje abandonó el servidor origen y está en camino hacia el destinatario, el cual será enviado al buzón del correo electrónico remitente. El tiempo promedio para la generación del acuse de envío es de 1 – 5 minutos.

- Generación de acuse de recibo certificado al correo electrónico del remitente el cual contiene la información sobre el estado de la entrega para cada destinatario. El tiempo promedio para la generación del acuse de recibo es de 1 – 360 minutos.

- El acuse de recibo se compone de:

    - Documento en formato PDF de la información de la recepción del mensaje de datos. Este documento es estampado cronológicamente en el momento de su generación, con la trazabilidad SMTP.

- Documento XML el cual lleva la cadena de custodia electrónica desde el momento en que el mensaje de datos sale de la máquina del remitente hasta que es entregado al destinatario (traza SMTP) o Protocolo simple de transferencia de correo.
- Documento HTML de la información del acuse de recepción con la trazabilidad SMTP.

- Posible notificación de apertura del correo electrónico por parte del receptor, de acuerdo con la configuración del servicio de correo del destinatario

- Permite visualizar los diferentes estados de entrega del correo electrónico hacia el receptor como parte de la información en el acuse de recibido:

  - Entregado y abierto (Delivered and Opened)
  - Entregado a Casillero de correo (Delivered to Mailbox)
  - Entregado a Servidor de correo (Delivered to Mail Server)
  - Falla externa en la entrega inicial (Delivery Failure)

- Permite visualizar los diferentes estados de falla de entrega del correo electrónico hacia el receptor como parte de la información en el acuse de recibido:

  - Casillero Lleno (Mailbox full)
  - Dirección Incorrecta (Bad address)
  - Email muy pesado (Email too large) para sistema de email del destinatario
  - Tipo de Archivo Prohibido (Attachment file type not accepted), ejemplo: Zip
  - Sistema del destinatario no disponible (Recipient's mail system down)

2.4.5 Emisión de correo electrónico certificado (Certimail)

- **Antes de comenzar**

El servicio de Certimail es utilizado sin necesidad de realizar instalación de software adicional, a su vez, permite interactuar con cualquier plataforma de correo electrónico de manera manual, automática, individual o masiva.

- **Características técnicas del correo electrónico certificado (Certimail)**

La arquitectura técnica de la plataforma del proveedor externo cuenta con controles físicos de seguridad, revisión de patentes, verificación de antecedentes del personal, evaluaciones y métricas de los recursos de la infraestructura en cuanto a: escalabilidad, rendimiento, seguridad, disponibilidad y capacidad de recuperación.

El proveedor por contrato debe cumplir la política de seguridad de información de Certicámara y llevar a cabo auditorías de cumplimiento y de temas relativos a seguridad de la información que considere pertinentes durante la ejecución del presente Contrato.

2.4.6 Proceso de correo electrónico certificado (Certimail)

- **Activación del servicio de correo electrónico certificado (Certimail)**

Para la activación del correo electrónico certificado, Certicámara le solicitará al responsable por parte del cliente los documentos necesarios establecidos al interior para su activación, tales como copia del documento de identidad, Registro Único Tributario, Orden de Compra / Contrato y demás que se consideren necesarios los cuales serán verificados de manera interna para constatar su validez y posterior activación del servicio.

- **Renovación de correo electrónico certificado (Certimail)**

CERTICÁMARA sí tiene contemplado el proceso de renovación de correo electrónico en el momento de terminar el cupo de correos certificados adquiridos, para lo cual se realiza comunicación con el cliente. Del mismo modo, en cuanto el contrato llega al final de su vigencia, se realiza comunicación con el cliente para su renovación o creación de un nuevo contrato.

- **Identificación y autenticación para solicitar finalización del servicio**

Se permite solicitar la finalización del servicio de correo electrónico certificado (Certimail) por medio de solicitud del cliente o vencimiento del contrato.

- **Ciclo de vida del correo electrónico certificado (Certimail) y procedimientos de operación**

La generación de correo electrónico certificado emitido por CERTICÁMARA tiene un periodo de vigencia según lo estipulado en el contrato en cuanto al cupo o la vigencia establecida.

- **Notificación al solicitante por CERTICÁMARA de la activación del servicio**

Mediante correo electrónico se informa al responsable la activación del Servicio de Correo electrónico certificado y por consiguiente, el solicitante acepta y reconoce que una vez reciba el citado correo electrónico, se entenderá entregado el Servicio de Correo electrónico certificado.

2.4.7 Aceptación del servicio

No se requiere confirmación de parte del responsable como aceptación del servicio recibido. Se considera que el Servicio de correo electrónico certificado es aceptado por el responsable desde el momento que solicita su activación, 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, se debe solicitar el ajuste respectivo.

2.5 Política de generación de firmas digitales

Ofrecer un componente de software, que contiene un conjunto de funciones, procedimientos y métodos programáticos con el objetivo de ejecutar una firma digital, verificar las firmas y/o estampar cronológicamente un conjunto de datos de acuerdo con las necesidades del cliente, aportando atributos de seguridad física, integridad, autenticidad y no repudio.

2.5.1 Ámbito de aplicación

- **Usos del certificado: e**l servicio de generación de firmas digitales entrega componentes que permiten firmar documentos haciendo uso de certificados digitales válidos, emitidos en conformidad a la política de certificados de firma digital.

- **Autenticación de identidad:** el componente entregado en el proceso de generación de firmas digitales provee herramientas al usuario que le permiten asegurar que una firma digital es creada con un certificado digital válido, para conservar las propiedades de integridad, autenticación y no repudio.

  En otras palabras, al hacer uso de un certificado digital válido se asegura la identidad del firmante como propietario de dicho certificado.

  Estos componentes permiten la creación de firmas digitales en los diferentes formatos mencionados previamente (CAdES, XAdES, PAdES), y la aplicación de estampado cronológico, haciendo uso de APIs y/o servicios técnicos para tal fin.

2.5.2 Funcionalidades del servicio de generación de firmas digitales certificadas

Las firmas digitales realizadas con componentes entregados con el servicio de generación de firmas digitales ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio.

- **Autenticidad del origen:** En un mensaje de datos, el suscriptor puede acreditar válidamente su identidad ante otra persona, demostrando la posesión de un documento firmado Digitalmente haciendo uso de un certificado válido emitido por una Entidad de Certificación Digital que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

- **Integridad del documento:** Existe la garantía de que el documento no fue alterado o modificado después de firmado por el suscriptor puesto que el resumen del documento es cifrado.

- **No repudio:** Evita que el emisor del documento firmado pueda negar o desconocer en un determinado momento la autoría o la integridad del documento, puesto que la firma aplicada con el certificado digital puede demostrar la identidad del emisor sin que este pueda repudiar.

2.5.3 Principales características y funcionalidades del sistema de generación de firmas digitales

Se pueden realizar las siguientes funcionalidades:

- El usuario puede seleccionar un documento para ser firmado.
- Firmar digitalmente documentos o archivos y almacenarlos en donde el cliente disponga.
- Permite la firma de documentos electrónicos con parámetros avanzados.
- La generación de firmas electrónicas certificadas verifica la integridad de los documentos firmados, minimizando el riesgo de alteración de los documentos electrónicos.
- Iniciar circuitos de firma digital de documentos, con uno o varios firmantes.
- Entrega de documentos o archivos asociados a una tarea de firma.
- Guarda la traza de los firmantes de un documento electrónico.
- Permite la integración con otros sistemas del cliente a través de Web Service y/o APIs de lenguaje de desarrollo.
- La generación de firmas electrónicas certificadas es personalizable en la medida en que el cliente lo requiera.

2.5.4 Emisión de generación de firmas digitales

- **Antes de comenzar:** Previo al uso de los componentes y adquisición del servicio, es necesario que el cliente cuente con un Certificado Digital en formato X509 v3, alineado con la política del servicio de Certificado de Firma Digital. Adicionalmente, en caso de requerir estampado, se debe contar con una suscripción vigente adquirida de acuerdo con la política de Estampado Cronológico TSA.

- **Características técnicas de generación de firmas digitales:** La entrega de componentes a través del servicio de generación de firmas digitales se realiza con las siguientes características:

  A partir de los resultados del proceso de preventa y la aceptación de una oferta se programa el acompañamiento a la entrega de un componente en modo estándar, o se inicia un proyecto para desarrollar personalizaciones.

  Una vez realizada la entrega, el cliente cuenta con soporte técnico durante el tiempo de vigencia del contrato, bajo el cual puede solicitar apoyo a la mesa de servicio de CERTICÁMARA S.A.

2.5.5 Políticas de administración de la generación de firmas digitales

Las políticas de administración están establecidos acorde con la política de seguridad de información vigente de CERTICÁMARA.

2.5.6 Periodos de retención de la información de generación de firmas digitales

Los periodos de retención de los documentos generados por componentes de este servicio están comprendidos en la política del cliente en su infraestructura o en las condiciones del contrato de cobro cuando se almacenan en la infraestructura de Certicámara.

2.5.7 Procedimientos de administración de generación de firmas digitales en caso de vencimiento de la suscripción del servicio

El componente entregado es vitalicio, y por lo tanto no requiere un procedimiento específico una vez se acabe el contrato de entrega.

- **Verificación de la firma:** Los componentes entregados permiten automatizar las siguientes actividades respecto a la funcionalidad de validación de firma:

1. Que la firma digital sea emitida por una Entidad de Certificación Digital (tercero de confianza) que garantice que esta firma sea asignada a la persona que corresponde utilizando mecanismos de verificación de identidad, de manera que se cumpla con un atributo de autenticidad, garantizando que los datos de creación de firma sean únicos al firmante.

2. Que la firma digital garantice la integridad del documento que se firma, y esto se puede lograr embebiendo la firma Digital como metadata dentro de una firma digital genérica, comúnmente a nombre de una razón social. Si el documento es alterado o modificado la firma digital se muestra inválida.

3. Se debe poder permitir que con cada firma, no se altere el contenido del documento y así se puedan incluir otras firmas sobre el mismo.

- **Servicios básicos y adicionales de la aplicación:** Servicios básicos de los componentes son los siguientes:
  - Componentes fiables para realizar procesos de firma digital en la organización.
  - El contenido del mensaje de datos no podrá ser alterado sin alterar las propiedades de la firma digital.
  - El emisor no podrá negar el conocimiento de un mensaje de datos y de los compromisos adquiridos a partir de éste
  - Garantiza que la información Digital no haya sido alterado ni modificado.
  - Permitir la consulta de propiedades de la firma digital y validez de la misma de un documento electrónico firmado.

- Aplicación de diferentes formatos de firma según el documento electrónico original (PAdES, XAdES, CAdES).
- Aplicación de estampado cronológico proveniente de un tercero confiable de hora legal válida TSA (Timestamp Authority).

2.5.8 Servicios adicionales

Solamente se contemplan variaciones sobre el servicio cuando se realizan personalizaciones para el cliente:

- Desarrollos hechos a la medida por solicitud del cliente que hagan uso del servicio de generación de firmas electrónicas certificadas.

En general todos los servicios adicionales tendrán un costo adicional que será establecido de acuerdo con la estimación de esfuerzo y tiempo sobre los requerimientos del suscriptor.

2.5.9 Proceso de generación de firmas digitales

- **Renovación de generación de firmas digitales:** CERTICÁMARA no tiene contemplado el proceso de renovación de componentes entregados a través del servicio de generación de firmas digitales, dado que se emite una licencia vitalicia sobre la versión el suscriptor desea obtener una nueva versión debe solicitar una nueva solicitud de servicio.
- **Ciclo de vida del servicio de generación de firmas digitales y procedimiento de operación:** En la operación del servicio se contemplan las versiones disponibles de cada componente, para ser entregadas bajo solicitud y compra a un usuario interesado. Una vez se realiza la compra se genera un proyecto que programa la entrega de un componente estándar, o a su vez se solicita al área de desarrollo las personalizaciones sobre el componente para ser entregado posteriormente al usuario bajo el mismo esquema de entrega estándar.

  En caso que los requerimientos del solicitante tengan condiciones especiales de infraestructura, se consulta con el área de TI una estimación que complemente las recomendaciones de instalación para el cliente. Una vez se realiza la entrega, el cliente configura el componente en su infraestructura y se da por cerrado el ciclo del servicio.

- **Notificación al solicitante por CERTICÁMARA de la activación del servicio:** El servicio se considera activo una vez se realiza la entrega a conformidad del componente en las instalaciones del cliente. Condiciones de posterior uso y soporte están por fuera del alcance del servicio aquí descrito.

- **Aceptación del servicio:** No se requiere confirmación por parte del responsable como aceptación del servicio recibido. Se considera que el servicio es aceptado por los responsables desde el momento que es entregado a conformidad.

2.6 Política de Generación de firmas electrónicas certificadas (clave segura)

Servicio que permite la generación de una Firma Electrónica Certificada (Clave Segura) como mecanismo de autenticación y firma electrónica, esto mediante un proceso de verificación y validación de identidad por medio de un cuestionario de Preguntas Reto, de acuerdo al Historial Financiero y Crediticio del Usuario. De igual forma, permite controlar el acceso en diversas webs o recursos tecnológicos, verificando la identidad de una persona con respecto a una fuente confiable.

2.6.1 Funcionalidades del servicio de generación de firmas electrónicas certificadas (Clave Segura)

La funcionalidad del servicio generación de firma electrónica certificada (Clave Segura) es validar la identidad de una persona natural, con el fin de generar en caso de ser exitoso una clave para realizar procesos de autenticación y firma electrónica de diversos documentos garantizando la autenticidad del origen, la integridad de los datos firmados y el no repudio.

- **Autenticidad del origen**: La autenticación se realiza a través del cuestionario de verificación de identidad. Para validar la identidad del solicitante, se mostrará en pantalla un cuestionario de verificación de identidad de acuerdo con el historial crediticio y financiero de la persona. Es como requisito aprobar la totalidad de las preguntas para poder continuar.

Estas preguntas son generadas de manera aleatoria por parte de centrales de riesgo, proveedores de preguntas reto o proveedor de mensajes de texto-OPT, así como diferentes bases de datos, tendrá una limitante de hasta 3 intentos erróneos diarios de tal manera que si no se aprueba en estos intentos el cuestionario, se bloqueará el servicio por 24 horas.

2.6.2 Principales características funcionales del servicio de generación de firma electrónica certificada (Clave Segura)

Funcionalidad para la emisión de una generación de firma electrónica certificada (Clave Segura)

A. Condiciones del servicio

Se mostrará en pantalla las condiciones globales del servicio, especificando que el proceso debe ser realizado directamente por el titular de la clave debido a que se verificará la identidad de la persona en un paso siguiente. Como medida de seguridad se solicitará la fecha de expedición del documento de identidad ingresado y si se desea hacer validación con segundo factor de autenticación a través de envío de un código OTP a través del número. El segundo factor de autenticación es opcional y sujeto a aprobación por el cliente.

B. Cuestionario de verificación de identidad

Para validar la identidad del solicitante, se mostrará en pantalla un cuestionario de verificación de identidad de acuerdo con el historial crediticio y financiero de la persona. Es requisito aprobar la totalidad de las preguntas para poder continuar. Estas preguntas son generadas de manera aleatoria por parte de centrales de riesgo, proveedores de mensajes de texto, tendrá una limitante de hasta 3 intentos erróneos diarios de tal manera que, si no se aprueba en estos intentos el cuestionario, se bloqueará el servicio por 24.

C. Definición y validación de la generación de firma electrónica certificada (Clave Segura)

Una vez aprobado el cuestionario de verificación de identidad, se solicitará que se defina una contraseña a la persona que está realizando el trámite o le llegará un mensaje de texto al número de celular registrado, cumpliendo algunas condiciones. Adicionalmente, el usuario podrá resolver dos preguntas de recordación, las cuales le servirán para recuperar la clave en caso de olvido.

D. Aceptación y firma de acuerdo

Antes finalizar el proceso, se solicitará al usuario que apruebe un acuerdo definido por la empresa que adquiera el servicio sobre el uso de esta clave generada.

E. Envío y notificación de la generación de firma electrónica certificada (Clave Segura)

Finalmente se notificará a la entidad el hash de la contraseña por medio del consumo de un servicio web expuesto por la entidad junto con los datos necesarios para la entrega de la información, esos datos se definen conforme las necesidades del cliente. Opcionalmente, se puede enviar un correo electrónico al solicitante con la notificación de la generación exitosa de la contraseña, sujeto a aprobación por el cliente.

2.6.3 Características de una contraseña segura

- Longitud de caracteres mínima (8)
- Una contraseña segura es aquella que otras personas no pueden determinar fácilmente adivinando o utilizando programas automáticos.
- Debe incluir números.
- Utilice una combinación de letras mayúsculas y minúsculas.
- Incluya caracteres especiales.
- No debe tener espacios en blanco.

2.6.4 Recomendaciones para la generación de firma electrónica certificada (Clave Segura)

El usuario debe tener en cuenta las siguientes recomendaciones adicionales para la generación de la Firma Electrónica Certificada (Clave Segura):

- No utilice información personal en la contraseña (como su nombre, fecha de nacimiento, etc.)
- No utilice patrones de teclado (qwerty) ni números en secuencia (1234).
- No utilice únicamente números, mayúsculas o minúsculas en su contraseña.
- No repita caracteres (1111111).
- No comunique la contraseña a nadie.
- Nunca anote su contraseña en papel para recordarla.
- No incluya nunca su contraseña en programas de mensajería, correo electrónico.
- No incluya palabras incluidas en los diccionarios.

2.6.5 Características Técnicas de la generación de firma electrónica certificada (Clave Segura)

Se genera con las siguientes características:

- Servicio de autenticación basada en la nube que se integra sin necesidad de adquirir hardware o software.
- Generación y utilización de claves de un solo uso (OTP One Time Password), opcional y sujeto a aprobación por el cliente.
- Cada operación de autenticación se realiza con una clave diferente que puede ser usada una única vez.
- Capacidad y facilidad de integrarse con diferentes aplicaciones de infraestructura empresarial
- Facilidad para habilitar y configurar el servicio.

El único medio de conexión al servicio de generación de firma electrónica certificada (Clave Segura) será por medio del envío de datos vía POST a una página web de autenticación, por lo tanto, se requiere que el aplicativo cliente sea una aplicación web.

- **Servicios Básicos y Adicionales de la Aplicación.**

Servicios básicos:

- El contenido del mensaje de datos no podrá ser conocido por ningún tercero no autorizado
- Confidencialidad permite garantizar que un mensaje de datos no pueda ser conocido sino por su emisor y los receptores deseados
- El emisor no podrá negar el conocimiento de un mensaje de datos y de los compromisos adquiridos a partir de éste
- Garantiza que el mensaje de datos o información digital no haya sido alterado ni modificado.
- Cuenta con una infraestructura tecnológica debidamente monitoreada y equipada con elementos de seguridad requeridos para garantizar una alta disponibilidad y confianza en los servicios ofrecidos a sus suscriptores, entidades y terceros de confianza.

2.6.6 Renovación del servicio de generación de firma electrónica certificada (Clave Segura)

Si el poseedor de este servicio desea la renovación, puede contactarse con CERTICÁMARA a través de correo electrónico, solicitud telefónica, visita comercial, con el fin de obtener una actualización de la oferta comercial.

2.6.7 Cancelación del Servicio de generación de Firma Electrónica Certificada (Clave Segura)

Se permite solicitar la cancelación del servicio de generación de firma Electrónica Certificada (Clave Segura) a las siguientes personas: - Al supervisor del contrato que haya sido designado por CERTICÁMARA, haciendo referencia a las causales de terminación de dicho contrato dentro de las relacionadas a continuación:

- Por mutuo acuerdo entre LAS PARTES
- Vencimiento servicio
- De manera unilateral por la parte cumplida, por incumplimiento de cualquiera de las obligaciones a cargo de la otra
- Por circunstancias de fuerza mayor o caso fortuito debidamente acreditadas que imposibiliten definitivamente la ejecución del servicio
- Por incurrir cualquiera de las partes o sus directivos en actividades de lavado de activos
- Por disolución y liquidación de alguna de LAS PARTES
- Las que establezca la ley

2.6.8 Ciclo de vida y procedimientos de operación

El servicio de generación de firma electrónica certificada (Clave Segura) prestado por CERTICÁMARA tiene un periodo de vigencia de acuerdo con lo especificado en el contrato generado entre CERTICÁMARA y el solicitante del servicio.

2.6.9 Notificación al solicitante por CERTICÁMARA de la activación del servicio

Mediante correo electrónico el director de proyecto le informa al solicitante la activación del servicio de generación de firma Electrónica Certificada (Clave Segura). Una vez realizada todas las pruebas funcionales y el paso a un ambiente productivo el director de proyecto le hace entrega al solicitante de información necesaria para acceder al servicio.

2.6.10 Aceptación del servicio

Se considera que el Servicio de Firma Electrónica Certificada (Clave Segura) es aceptado una vez se realiza el paso a producción del servicio.

3. USOS DE LOS CERTIFICADOS

3.1 Huella Biométrica Certificada

3.1.1 Usos permitidos del servicio de huella biométrica certificada

La verificación y validación de identidad con huella biométrica ante la RNEC en el ámbito de esta Política, puede utilizarse por el solicitante que se encuentre habilitado en virtud de la normativa vigente, con el fin de realizar la validación de identidad de ciudadanos colombianos con cédula de ciudadanía debidamente expedida y adicionalmente para aplicar firma electrónica certificada sobre el documento electrónico de Autorización de Tratamiento de Datos Personales (ATDP).

3.1.2 Límites de uso del servicio

La verificación de identidad con huella biométrica ante la RNEC no puede ser usada para fines contrarios a los previstos en normativa vigente.

3.1.3 Prohibiciones de uso del servicio de huella biométrica certificada (Certihuella)

La realización de operaciones no autorizadas según esta Política de verificación de identidad con huella biométrica ante la RNEC, por parte de solicitantes del servicio, eximirá a la Autoridad de Certificación CERTICÁMARA de cualquier responsabilidad por los usos prohibidos que a continuación se indican:

- ✓ Está totalmente prohibido recolectar, enrolar y almacenar huellas digitales o imágenes de éstas, o complementar bases de datos con la información consultada de la base de datos de la RNEC.
- ✓ Para el proceso de autenticación biométrica, la solución implementada no puede utilizar las imágenes de las huellas dactilares, excepto cuando medie en la solicitud una orden judicial o que dicho proceso haya sido verificado y avalado por la RNEC.
- ✓ De acuerdo con lo previsto en el Decreto 2241 de 1986 y ante la prohibición del tratamiento de imágenes de huellas dactilares, el solicitante y el operador biométrico no podrán realizar el ciclo de vida de la transacción biométrica mediante el uso de templates diferentes al ISO 19794-2 de manera cifrada que corresponde al autorizado para Certicámara como operador biométrico por la RNEC. Por último, no está permitido el almacenamiento del template en ninguna base de datos u otro tipo de almacenamiento.
- ✓ Se prohíbe el uso la Huella Biométrica en sistemas de control o sistemas intolerantes a fallos que puedan ocasionar daños personales o medioambientales.
- ✓ Se considera prohibida toda aquella acción que infrinja las disposiciones, obligaciones y requisitos estipulados en la presente Política de Certificación.

- ✓ Fines u operaciones ilegales e ilícitas bajo cualquier régimen legal del mundo.
- ✓ Cualquier práctica contraria al ordenamiento jurídico colombiano.
- ✓ Cualquier práctica contraria a los convenios internacionales suscritos por el Estado colombiano.
- ✓ Cualquier práctica contraria a las normas supranacionales.
- ✓ Cualquier práctica contraria a las buenas costumbres y prácticas comerciales.
- ✓ Cualquier uso en sistemas cuyo fallo pueda ocasionar: Muerte, lesiones a personas y perjuicios al medio ambiente.
- ✓ Como sistema de control para actividades de alto riesgo como son: Sistemas de navegación marítima, Sistemas de navegación de transporte terrestre, Sistemas de navegación aérea, Sistemas de control de tráfico aéreo, Sistemas de control de armas.

3.1.4 Términos y condiciones de uso

Estos términos son de obligatorio cumplimiento y aceptación para los solicitantes del servicio que se encuentren habilitados por la normativa vigente, para acceder y consultar la réplica de la Base de Datos Biográfica y Biométrica de la Registraduría Nacional del Estado Civil. Estos términos y condiciones, deberán ser cumplidos durante el término de prestación del servicio una vez el solicitante se convierta en suscriptor.

3.2 Correo Electrónico Certificado

3.2.1 Usos permitidos del correo electrónico certificado (Certimail)

El correo electrónico certificado (Certimail) puede ser usado por una persona natural o jurídica sin importar el cliente de correo que utilice. El uso del correo electrónico certificado no depende de un dispositivo por parte del receptor del mensaje de correo electrónico, posibilitando obtener garantías de la recepción distintas a las ofrecidas por el correo electrónico estándar. La plataforma CertiMail se ajusta a la necesidad de dar trazabilidad y garantía en la fecha y hora de generación del acuse de recibo, además de integrar información esencial dentro del acuse electrónico que posibilita total equivalencia al correo postal físico.

3.2.2 Límites de uso del correo electrónico certificado (Certimail)

El Correo electrónico Certificado no puede ser usado para fines contrarios a la normativa vigente.

3.2.3 Prohibiciones de uso de correo electrónico certificado (Certimail)

La realización de operaciones no autorizadas según esta Política, por parte de terceros o suscriptores del servicio eximirá a la Autoridad de Certificación CERTICÁMARA de cualquier responsabilidad por este uso prohibido.

- ✓ Las alteraciones sobre el correo electrónico certificado (Certimail) no están permitidas y el Correo Electrónico Certificado debe usarse tal y como fue suministrado por la Autoridad Certificadora CERTICÁMARA.
- ✓ Se considera prohibida toda aquella acción que infrinja las disposiciones, obligaciones y requisitos estipulados en la presente Política de Certificación.
- ✓ No es posible por parte de CERTICÁMARA emitir valoración alguna sobre el contenido de los documentos que son enviados por el suscriptor, por lo tanto, la responsabilidad del contenido del mensaje es responsabilidad única del suscriptor.
- ✓ Fines u operaciones ilícitas bajo cualquier régimen legal del mundo.
- ✓ Cualquier práctica contraria a los convenios internacionales suscritos por el Estado colombiano.
- ✓ Cualquier práctica contraria a las normas supranacionales.
- ✓ Cualquier práctica contraria a las buenas costumbres y prácticas comerciales.

3.3 Generación de Firmas Digitales

3.3.1 Usos permitidos de generación de firmas digitales

Las firmas digitales generadas en el ámbito de esta política de firma pueden utilizarse con cualquier tipo de documentos digitales de personas naturales o jurídicas, de acuerdo con las limitaciones de uso y restricciones derivadas de la Política de Certificación a la que está sometido el certificado digital utilizado en su creación, la presente Política de Firma y lo dispuesto por el ordenamiento jurídico vigente.

Garantiza la identidad y responsabilidad del autor de un documento o transacción Digital, así como permite comprobar la integridad del mismo, es decir que la información no ha sido alterada, aportando un atributo de seguridad jurídica adicional, como lo es la integridad de la información.

3.3.2 Límites de uso de los certificados

Las firmas digitales generadas a partir de los componentes entregado por el servicio de generación de firmas electrónicas certificadas no pueden ser usadas para fines contrarios a la legislación vigente.

3.3.3 Prohibiciones de uso de la generación de firmas digitales

La realización de operaciones no autorizadas según esta Política, por parte de terceros o suscriptores del servicio eximirá a la Autoridad de Certificación CERTICÁMARA de cualquier responsabilidad por este uso prohibido.

- ✓ No se permite el uso de componentes de firma de generación de firmas digitales para firmar otros certificados.
- ✓ Está prohibido utilizar la generación de firmas digitales para usos distintos a los estipulados en el apartado “Usos permitidos del certificado” y “Límites de uso de los certificados” de la presente Política.
- ✓ Cualquier alteración sobre los componentes de generación de firmas digitales no están permitidas y la generación de firmas digitales debe usarse tal y como fue suministrado por la Autoridad Certificadora CERTICÁMARA.
- ✓ Se prohíbe el uso de componentes de generación de firmas digitales en sistemas de control o sistemas que no toleran fallos que puedan ocasionar daños personales o medioambientales.
- ✓ Se considera prohibida toda aquella acción que infrinja las disposiciones, obligaciones y requisitos estipulados en la presente Política de Certificación.
- ✓ No es posible por parte de CERTICÁMARA emitir valoración alguna sobre el contenido de los documentos que firma el suscriptor, por lo tanto la responsabilidad del contenido del mensaje es responsabilidad única del signatario.
- ✓ Fines u operaciones ilícitas bajo cualquier régimen legal del mundo.
- ✓ Cualquier práctica contraria al ordenamiento jurídico colombiano.
- ✓ Cualquier práctica contraria a los convenios internacionales suscritos por el estado colombiano.
- ✓ Cualquier práctica contraria a las normas supranacionales.
- ✓ Cualquier práctica contraria a las buenas costumbres y prácticas comerciales.
- ✓ Cualquier uso en sistemas cuyo fallo pueda ocasionar: Muerte, Lesiones a personas y Perjuicios al medio ambiente.

Como sistema de control para actividades de alto riesgo como son: Sistemas de navegación marítima, Sistemas de navegación de transporte terrestre, Sistemas de navegación aérea, Sistemas de control de tráfico aéreo, Sistemas de control de armas.

3.4 Generación de Firmas Electrónica

3.4.1 Usos Permitidos de generación de firma electrónica certificada (Clave Segura)

El servicio de generación de firma electrónica certificada (Clave Segura) y verificación de identidad puede ser utilizado en cualquier portal transaccional que requiera validar la identidad de una persona natural para posteriormente realizar una firma electrónica.

Con esta firma se garantiza la identidad y responsabilidad del autor de un documento o transacción Digital, así como permite comprobar la integridad del mismo, es decir que la información no ha sido alterada, aportando un atributo de seguridad jurídica adicional, como lo es la integridad de la información.

3.4.2 Límites de uso de generación de firma electrónica certificada (Clave Segura)

La generación de firma electrónica certificada (Clave Segura) no puede ser usada para fines contrarios a la legislación vigente.

3.4.3 Prohibiciones de uso de la generación de firma electrónica certificada (Clave Segura)

La realización de operaciones no autorizadas según esta política de generación de firma electrónica certificada (Clave Segura), por parte de terceros o suscriptores del servicio eximirá a la Autoridad de Certificación CERTICÁMARA de cualquier responsabilidad por este uso prohibido.

- ✓ No se permite el uso de la generación de firma electrónica certificada (Clave Segura) de persona natural para firmar otros certificados.
- ✓ Está prohibido utilizar la generación de firma electrónica certificada (Clave Segura) para usos distintos a los estipulados en el apartado “Usos permitidos del certificado” y “Límites de uso de los certificados” de la presente política de generación de firma electrónica certificada (Clave Segura).
- ✓ Las alteraciones sobre la generación de firma electrónica certificada (Clave Segura) no están permitidas y la firma electrónica certificada (Clave Segura) debe usarse tal y como fue suministrado por la Autoridad Certificadora CERTICÁMARA.
- ✓ Se prohíbe el uso la generación de firma electrónica certificada (Clave Segura) en sistemas de control o sistemas intolerantes a fallos que puedan ocasionar daños personales o medioambientales.
- ✓ Se considera prohibida toda aquella acción que infrinja las disposiciones, obligaciones y requisitos estipulados en la presente Política de Certificación.
- ✓ No es posible por parte de CERTICÁMARA emitir valoración alguna sobre el contenido de los documentos que firma el suscriptor, por lo tanto la responsabilidad del contenido del mensaje es responsabilidad única del signatario.
- ✓ Fines u operaciones ilícitas bajo cualquier régimen legal del mundo.
- ✓ Cualquier práctica contraria a la legislación colombiana.
- ✓ Cualquier práctica contraria a los convenios internacionales suscritos por el estado colombiano.
- ✓ Cualquier práctica contraria a las normas supranacionales.
- ✓ Cualquier práctica contraria a las buenas costumbres y prácticas comerciales.
- ✓ Cualquier uso en sistemas cuyo fallo pueda ocasionar: Muerte, Lesiones a personas y Perjuicios al medio ambiente.
- ✓ Como sistema de control para actividades de alto riesgo como son: Sistemas de navegación marítima, Sistemas de navegación de transporte terrestre, Sistemas de navegación aérea, Sistemas de control de tráfico aéreo, Sistemas de control de armas.

4. OBLIGACIONES Y RESPONSABILIDADES DE LOS INTERVINIENTES

4.1 Obligaciones y responsabilidades 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.

4.2 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.

4.3 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.

4.4 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.

5. DERECHOS DE LOS INTERVINIENTES

5.1 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.

5.2 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.

6. CONFIDENCIALIDAD DE LA INFORMACIÓN

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

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

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

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

6.1 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.

6.2 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

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

7. TARIFAS DEL SERVICIO

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

7.1 Huella Biométrica Certificada

La tarifa que fija **Certicámara** para el servicio de **huella biométrica certificada (Certihuella)** se establece de acuerdo con las condiciones contractuales acordadas con los solicitantes del servicio, y será adecuadamente calculado y liquidado por **Certicámara** de

acuerdo con la volumetría de validación de identidad y firmas electrónicas que el cliente requiera, el precio base será:

Servicio	Cantidad	Valor Unitario Sin IVA
Validación de identidad	1	$ 910

7.2 Digitalización con Fines Probatorios

La tarifa que fija **Certicámara** para el servicio de **digitalización certificada con fines probatorios** se establece de acuerdo con las condiciones contractuales acordadas con los solicitantes del servicio y será adecuadamente calculado y liquidado por **Certicámara**. De acuerdo con la volumetría de documentos que el cliente requiera digitalizar, el precio base será:

Folio Digitalizado	Valor Unitario	Periodo
Folio digitalizado con fines probatorios	$500	Almacenamiento y conservación 1 año para consulta.

7.3 Correo Electrónico Certificado

El valor de la tarifa que fija **Certicámara** para el servicio de **correo electrónico certificado (Certimail)** se establece de acuerdo con las condiciones contractuales acordadas con los solicitantes del servicio y será adecuadamente calculado y liquidado por **Certicámara**. De acuerdo con la volumetría de correos electrónicos certificados que el cliente requiera los rangos de precios son:

Para rango de envío de entre 1 y 500 correos certificados mensuales:

PAQUETES	CUENTAS MÁXIMAS PERMITIDAS	VALOR TOTAL CUPO
HASTA 200 CERTIMAIL	3	$300,000.00
HASTA 500 CERTIMAIL	3	$675,000.00

Para rango superior a 500 correos certificados mensuales:

a. Modalidad pago mes vencido por consumos unitarios:

Rangos Mensuales				
RANGO INFERIOR	RANGO SUPERIOR	CUENTAS MÁXIMAS PERMITIDAS	VALOR UNITARIO	VALOR UNITARIO CON IVA
500	1,000	20	$ 1,185	$ 1,410.73
1,001	2,500	35	$ 1,138	$ 1,354.30
2,501	5,000	100	$ 1,043	$ 1,241.44
5,001	10,000	200	$ 983	$ 1,169.77
10,001	15,000	400	$ 965	$ 1,148.35
15,001	25,000	750	$ 911	$ 1,084.09
25,001	50,000	1000	$ 886	$ 1,054.34
50,001	75,000	1500	$ 867	$ 1,031.73
75,001	100,000	1500	$ 852	$ 1,013.88
100,001	125,000	1500	$ 833	$ 991.27
125,001	150,000	1500	$ 812	$ 966.28
150,001	200,000	1500	$ 791	$ 941.29

7.4 Generación de Firmas Digitales

La tarifa que fija **Certicámara** para el servicio de **generación de firmas digitales** se establece de acuerdo con las condiciones contractuales acordadas con los solicitantes del servicio y será adecuadamente calculado y liquidado por **Certicámara**, el precio base será:

Servicio	Cantidad	Valor Unitario Sin IVA
Generación de firmas digitales	1	$ 50,800,000

7.5 Generación de Firmas Electrónicas Certificadas

La tarifa que fija Certicámara para el servicio de generación de firma electrónica certificada (Clave Segura) se establece de acuerdo con las condiciones contractuales acordadas con los solicitantes del servicio y será adecuadamente calculado y liquidado por **Certicámara**. De acuerdo con la volumetría de verificación de identidad que el cliente requiera, el precio base será:

Servicio	Cantidad	Valor Unitario Sin IVA
Generación de Firma Electrónica Certificada (Clave Segura)	1	$ 3,970

- Los precios establecidos anteriormente no incluyen IVA.
- Las tarifas indicadas podrán variar según acuerdos comerciales especiales con entidades y suscriptores o por el desarrollo de campañas de promoción.

7.6 Políticas de Reembolso para Suscriptores

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

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

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

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

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 la Declaración de Prácticas de Certificación, 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.

El modelo de términos y condiciones para la suscripción que usa Certicámara en la prestación del servicio de certificado de estampado

9. NORMATIVIDAD ASOCIADA

9.1 Huella biométrica certificada (Certihuella)

- Numerales 1, 2, 4, 5, 6 y 9 del artículo 30 de la Ley 527 de 1999 modificado por el artículo 161 del Decreto Ley 019 de 2012.
- Artículo 17 de la Ley 527 de 1999
- Artículo 18 del Decreto Ley 019 de 2012
- Resolución 5633 de 2016 y anexos técnicos 1 y 2 de la Registraduría Nacional del Estado Civil y aquellas que la modifiquen, complementen o deroguen
- Ley 1581 de 2012
- Decreto 1377 de 2013
- RSA 2048, Entidad Final / RSA 4096, Root CA.
- FIPS PUB 180-4 Secure Hash Standard (SHS) 2015-08 - SHA 256
- RFC 5280: mayo 2008 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- RFC 3161 Agosto 2001
- ITU-T-X509: octubre 2019 - Tecnología de la información - Interconexión de sistemas abiertos - El directorio: Marcos para certificados de claves públicas y atributos;
- Decreto 4175 de 2011 del Ministerio de Comercio, Industria y Turismo - artículo 6 numeral 14

9.2 Digitalización certificada con fines probatorios

- Numeral 1, 5 y 9 del artículo 30 de la Ley 527 de 1999 modificado por el artículo 161 del Decreto Ley 019 de 2012.
- RSA 2048
- FIPS PUB 180-4 Secure Hash Standard (SHS) 2015-08 - SHA 256

- RFC 5280 Mayo 2008
- FIPS 140-2 Level 3 Mayo 2001
- ITU-T_X509 V3 Octubre 2012
- RFC 3161 Agosto 2001
- Decreto 4175 de 2011 del Ministerio de Comercio, Industria y Turismo - artículo 6 numeral 14

9.3 Correo Electrónico Certificado (Certimail)

- Numerales 2, 5 y 9 del artículo 30 de la Ley 527 de 1999 modificado por el artículo 161 del Decreto Ley 019 de 2012.
- Artículos 15, 16, 17, 18, 19, 20, 21, 22, 23, 24 y 25 de la Ley 527 de 1999.
- RSA 2048, Entidad Final / RSA 4096, Root CA.
- FIPS PUB 180-4 Secure Hash Standard (SHS) 2015-08 - SHA 256
- RFC 5280: mayo 2008 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- RFC 3161 Agosto 2001
- Decreto 4175 de 2011 del Ministerio de Comercio, Industria y Turismo - artículo 6 numeral 14

9.4 Generación de firmas digitales

- Numerales 4, 5, 6 y 9 del artículo 30 de la Ley 527 de 1999 modificado por el artículo 161 del Decreto Ley 019 de 2012.
- RSA 2048
- FIPS PUB 180-4 Secure Hash Standard (SHS) 2015-08 - SHA 256
- RFC 5280 Mayo 2008
- RFC 4523 Junio 2006
- RFC 3647 Noviembre 2003
- ETSI TS 102 042 Febrero 2013
- FIPS 140-2 Level 3 Mayo 2001
- ITU-T_X509 V3 Octubre 2012
- RFC 3161 Agosto 2001
- Decreto 4175 de 2011 del Ministerio de Comercio, Industria y Turismo - artículo 6 numeral 14

9.5 Firma electrónica certificada (Clave Segura)

- Numerales 1, 2, 3, 4, 6 y 9 del artículo 30 de la Ley 527 de 1999 modificado por el artículo 161 del Decreto Ley 019 de 2012.
- Artículo 17 de la Ley 527 de 1999
- Artículo 7 de la Ley 527 de 1999
- Decreto 2364 de 2012 compilado por el Decreto 1074 de 20158
- RSA 2048, Entidad Final / RSA 4096, Root CA.
- FIPS PUB 180-4 Secure Hash Standard (SHS) 2015-08 - SHA 256

- RFC 5280: mayo 2008 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- ITU-T-X509: octubre 2019 - Tecnología de la información - Interconexión de sistemas abiertos - El directorio: Marcos para certificados de claves públicas y atributos;
- ETSI TS 102 042 febrero 2013
- RFC 3647: noviembre 2003 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
- RFC 4523: junio 2006 - Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates.
- FIPS 140-2 Level 3 mayo 2001
- NTC-ISO 16175-1:2013
- UIT-T X.1251: septiembre 2019 Marco para el control por el usuario de la identidad digital;
- UIT-T X.1253: septiembre 2011 Directrices de seguridad para los sistemas de gestión de identidades;
- UIT-T X.1254: septiembre 2013 Marco de garantía de autenticación de entidad.

10. CONTROL DE CAMBIOS

Fecha	Razón de actualización
07/09/2022	• En el marco del cumplimiento de las disposiciones del capítulo 48 del DURSCIT, Artículo 2.2.2.48.3.1. Declaración de Prácticas de Certificación (DPC) y al estándar RFC 3647, se alinean los numerales con lo establecido en estos documentos y se crea el presente documento para dar mayor claridad al solicitante y suscriptor sobre las disposiciones, información, directrices, controles y demás aplicables para los demás servicios asociados, como son: Huella biométrica certificada, Digitalización certificada con fines probatorios, correo electrónico certificado (Certimail), Generación de firmas digitales, Generación de firmas electrónicas certificadas (clave segura). Teniendo en cuenta lo anterior, se asigna un nuevo código y versión del documento de acuerdo con la estructura de procesos de la organización.