certicámara.

# Política de Certificación – Servicios Asociados a Sistemas De Información

**Código:** DYD-L-009

**Fecha:** Agosto de 2025

**Versión:** 006

certicámara.

| | |
|---|---|
| **Código:** | DYD-L-009 |
| **Fecha:** | 05/08/2025 |
| **Versión:** | 006 |
| **Etiquetado:** | PÚBLICO |

# POLÍTICA DE CERTIFICACIÓN – SERVICIOS ASOCIADOS A SISTEMAS DE INFORMACIÓN

**Contenido**

# POLÍTICA DE CERTIFICACIÓN – SERVICIOS ASOCIADOS A SISTEMAS DE INFORMACIÓN

## 1. INTRODUCCIÓN

La presente Política de Certificación (PC) constituye la manifestación pública de la Entidad de Certificación Digital Abierta, en la cual se establecen las normas y prácticas adoptadas para los Servicios Asociados a Sistemas de Información ofrecidos por la Sociedad Cameral de Certificación Digital Certicámara S.A. Estos servicios incluyen:

- Huella Biométrica Certificada
- Correo Electrónico Certificado
- Generación de Firmas Electrónicas Certificadas
- Generación de Firmas Digitales

La presente **Política de Certificación (PC)** se ha elaborado siguiendo las recomendaciones de los estándares internacionales RFC 3647, RFC 3628 y RFC 3161. Adicionalmente, cumple con la legislación colombiana vigente, específicamente la Ley 527 de 1999, el Decreto Ley 019 de 2012, el Decreto 333 de 2014, y cualquier reglamento que los modifique o complemente.

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

### *1.1 Nombre e identificación del documento*

Certicámara para la prestación de los servicios mencionados en el numeral anterior, establece la siguiente información para el presente documento.

| | |
|---|---|
| **Nombre** | Política de Certificación – Servicios Asociados a Sistemas de Información |
| **Fecha de publicación** | 05/08/2025 |
| **Versión** | 006 |
| **Código** | DYD-L-006 |
| **Ubicación** | https://web.certicamara.com/marco-normativo |

### *1.2 Alcance*

Este documento establece las normas y reglas a seguir por la Entidad certificadora **Certicámara** para ofrecer los servicios de Huella Biométrica Certificada (Certihuella),

Correo Electrónico Certificado (Certimail), Generación de firmas digitales (Ws Sign), 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 y aprobación de la política*

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

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

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

## 2. IDENTIFICACIÓN DE POLÍTICAS

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

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

### *2.1 Política de Huella Biométrica Certificada*

*2.1.1 Ámbito de aplicación*

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 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 se ha acreditado como operador de autenticación de identidad digital ante la RNEC como lo confirma el siguiente enlace https://wsp.registraduria.gov.co/biometria/operadores/listar .

Certicámara apoyará al suscriptor en todos los aspectos relacionados con el proceso de autenticación biométrica de conformidad con lo previsto en la Resolución 27145 de 2023.

*2.1.2 Principales características y funcionalidades*

- 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.

*2.1.3 Requisitos para la expedición*

El solicitante debe adjuntar los siguientes documentos:

1. Registro Único Tributario (RUT): Será responsabilidad del suscriptor actualizar la información de domicilio (dirección, municipio, y departamento) en el RUT. Las personas con domicilio fuera de Colombia que no se encuentren registrados ante la DIAN deberán adjuntar el documento que haga las veces de residente fiscal en su país y el mismo se deberá validar con la Dirección de Asuntos Legales y Contractuales quienes darán concepto para la emisión.
2. Documento de identificación del representante legal: Cédula de ciudadanía, Pasaporte, Documento de identificación de venezolanos o Cédula de extranjería.
3. Documento que acredita la existencia y representación legal de la empresa o entidad: Para empresas o entidades registradas en cámara de comercio se requiere Certificado de existencia y representación legal no mayor a 30 días y para empresas o entidades no registradas en cámara de comercio Certificado expedido por un organismo de control, tales como: Superintendencia financiera, Superintendencia de industria y comercio, Ministerio de educación, Alcaldías, entre otras.

4. Autorización de la RNEC para acceder a la réplica de la base de datos: Notificación de convenio o contrato establecido entre RNEC y el cliente para acceder a la base de datos réplica.
5. Contrato, orden de compra o soporte de pago.

Certicámara se reserva el derecho de solicitar documentos adicionales a los mencionados 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.

*2.1.4 Actividades ante la RNEC*

A continuación, se indican las actividades que el solicitante autorizado por la normativa vigente para la utilización del servicio de Huella Biométrica Certificada, para acceder y consultar la Base de Datos Biográfica y Biométrica de la Registraduría Nacional del Estado Civil (RNEC) y las cuales debe llevar a cabo.

- Elevar una 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 27145 de 2023.
- 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.

*2.1.5 Activación del servicio*

El SUSCRIPTOR sabrá sobre la activación efectiva del servicio por medio de una notificación mediante correo electrónico, una vez se haya validado la completitud de los requisitos definidos para este servicio.

*2.1.6 Ciclo de vida del servicio y procedimientos de operación*

El servicio de huella biométrica certificada prestado por Certicámara tendrá una vigencia que dependerá del tiempo establecido en el contrato o el número de transacciones acordadas.

*2.1.7 Aceptación del servicio*

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

*2.1.8 Renovación del servicio*

Para la renovación del servicio se procederá de acuerdo con las condiciones contractuales pactadas en la prestación del servicio y en caso de requerirse se solicitarán los documentos actualizados al cliente.

*2.1.9 Finalización (revocación) del servicio*

La solicitud de finalización (revocación) del servicio de huella biométrica certificada deberá ser realizada por el supervisor o representante legal por parte del cliente, quien deberá tener en cuenta las causales de terminación estipuladas en la prestación del servicio y que se enlistan a continuación:

- Por mutuo acuerdo entre LAS PARTES.
- Revocación de la autorización de la RNEC.
- De manera unilateral por la parte cumplida, por incumplimiento de cualquiera de las obligaciones a cargo de la otra.
- Solicitud del cliente. El cliente solicita la terminación anticipada del servicio.
- 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.

## *2.2 Política de correo electrónico certificado (certimail)*

*2.2.1 Ámbito de aplicación*

La 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 posee estampado cronológico. Este servicio cuenta con la misma validez jurídica y probatoria de un envío certificado por medios físicos.

El 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 destinatario.
- Conocer la fecha y hora de la entrega.
- Identificar si un correo ha sido alterado.

*2.2.2 Principales características y funcionalidades*

Los correos electrónicos enviados mediante el proceso de correo electrónico certificado (Certimail) ofrecen la garantía de integridad y 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 del servidor del remitente hasta que es entregado al servidor del destinatario (SMTP). La entrega del mensaje conocido como 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 recibo se genera una vez se haya recopilado toda la información de la traza de todos los destinatarios.

- Integridad del acuse de recibo: Una vez se genere el documento de acuse de recibo se hace uso del servicio de estampado cronológico que cuenta con la hora legal colombiana avalada por el Instituto Nacional de Metrología de Colombia, el cual es enviado de manera adjunta al correo electrónico del emisor.

- Generación de notificación de envío: Actúa como registro para hacer constar que el mensaje abandonó el servidor de origen y está en camino hacia el servidor del destinatario. Será enviado al buzón del correo electrónico del remitente el tiempo promedio para la generación del acuse de envío es de 1 a 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 a 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 del servidor del remitente hasta que es entregado al servidor del destinatario.
    - Documento HTML de la información del acuse de recepción con la trazabilidad SMTP.

- Acuse de apertura: Notificación entregada por parte del correo electrónico del receptor, en la que consta la apertura del mensaje entregado. La generación del acuse de apertura dependerá de 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 recibo:

- 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)

*2.2.3 Requisitos para la expedición*

El solicitante debe adjuntar los siguientes documentos:

1. Registro Único Tributario (RUT): Será responsabilidad del suscriptor actualizar la información de domicilio (dirección, municipio, y departamento) en el RUT. Las personas con domicilio fuera de Colombia que no se encuentren registrados ante la DIAN deberán adjuntar el documento que haga las veces de residente fiscal en su país y el mismo se deberá validar con la Dirección de Asuntos Legales y Contractuales quienes darán concepto para la emisión.
2. Documento de identificación: Cédula de ciudadanía, Pasaporte, Documento de identificación de venezolanos oCédula de extranjería.
3. Documento que acredita la existencia y representación legal de la empresa o entidad: Para empresas o entidades registradas en cámara de comercio se requiere Certificado de existencia y representación legal no mayor a 30 días y para empresas o entidades no registradas en cámara de comercio Certificado expedido por un organismo de control, tales como: Superintendencia financiera, Superintendencia de industria y comercio, Ministerio de educación, Alcaldías, entre otras. Para consorcios y uniones temporales el documento que acredita la existencia y representación legal es el acta de conformación consorcial o unión temporal.
4. Contrato, orden de compra o soporte de pago, de acuerdo con la solicitud.

Certicámara se reserva el derecho de solicitar documentos adicionales a los mencionados 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.

*2.2.4 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.

2.2.5 *Activación del servicio*

El SUSCRIPTOR sabrá sobre la activación efectiva del servicio por medio de una notificación mediante correo electrónico, una vez se haya validado la completitud de los requisitos definidos para este servicio.

*2.2.6 Ciclo de vida del servicio y procedimientos de operación*

El servicio de correo electrónico certificado emitido por Certicámara tendrá una vigencia que dependerá del tiempo establecido en el contrato o el número de transacciones acordadas.

*2.2.7 Aceptación del servicio*

Se considera que el servicio de correo electrónico certificado es aceptado por el responsable desde el momento que solicita su activación.

*2.2.8 Renovación del servicio*

Para la renovación del servicio se procederá de acuerdo con las condiciones contractuales pactadas en la prestación del servicio y en caso de requerirse se solicitarán los documentos actualizados al cliente.

*2.2.9 Finalización (revocación) del servicio*

La solicitud de finalización (revocación) del servicio de correo electrónico certificado (Certimail) deberá ser realizada por el supervisor o representante legal por parte del cliente, quien deberá tener en cuenta las causales de terminación estipuladas en la prestación del servicio y que se enlistan a continuación:

- Vencimiento del plan. El vencimiento se da cuando la vigencia del plan finaliza.

- Unidades del plan agotadas. El total de unidades adquiridas en el plan se agotan antes del periodo de tiempo acordado.
- Solicitud del cliente. El cliente solicita la terminación anticipada del servicio.
- Por mutuo acuerdo entre LAS PARTES.
- 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.

### *2.3 Política de generación de firmas digitales (Wssign)*

*2.3.1 Ámbito de aplicación*

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 integridad, autenticidad y no repudio.

El servicio de generación de firmas digitales es un componente que permite firmar documentos haciendo uso de certificados digitales válidos previamente generados y emitidos en conformidad con alguna de las políticas vigentes.

*2.3.2 Principales características y funcionalidades*

Las firmas digitales emitidas con el componente entregado con el servicio de generación de firmas digitales ofrecen los medios de respaldo para 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.

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, según se requiera.
- 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 de acuerdo con las políticas configuradas.
- Entrega 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.
- Es personalizable en la medida en que el cliente lo requiera.

*2.3.3 Autenticación de identidad*

El componente entregado 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.

Este componente permite 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.

*2.3.4 Requisitos para la expedición*

El solicitante debe adjuntar los siguientes documentos:

1. Registro Único Tributario (RUT): Será responsabilidad del suscriptor actualizar la información de domicilio (dirección, municipio, y departamento) en el RUT. Las personas con domicilio fuera de Colombia que no se encuentren registrados ante la DIAN deberán adjuntar el documento que haga las veces de residente fiscal en su país y el mismo se deberá validar con la Dirección de Asuntos Legales y Contractuales quienes darán concepto para la emisión.
2. Documento de identificación: Cédula de ciudadanía, Pasaporte, Documento de identificación de venezolanos o Cédula de extranjería.
3. Documento que acredita la existencia y representación legal de la empresa o entidad: Para empresas o entidades registradas en cámara de comercio se

requiere Certificado de existencia y representación legal no mayor a 30 días y para empresas o entidades no registradas en cámara de comercio Certificado expedido por un organismo de control, tales como: Superintendencia financiera, Superintendencia de industria y comercio, Ministerio de educación, Alcaldías, entre otras. Para consorcios y uniones temporales el documento que acredita la existencia y representación legal es el acta de conformación consorcial o unión temporal.

4. Contrato, orden de compra o soporte de pago, de acuerdo con la solicitud.

Certicámara se reserva el derecho de solicitar documentos adicionales a los mencionados 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.

*2.3.5 Emisión de generación de firmas digitales*

- **Antes de comenzar:** Previo al uso de componente 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.

- **Características técnicas de generación de firmas digitales:** La entrega del componente se realiza con las siguientes características:

  A partir de los resultados del proceso de preventa y la aceptación de la oferta, se programa el acompañamiento para la entrega del componente en modo estándar, o se inicia la implementación para desarrollar las personalizaciones acordadas

  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.

*2.3.6 Periodos de retención de la información*

Los periodos de retención de los documentos generados por el componente 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.

*2.3.7 Renovación de generación de firmas digitales:*

CERTICÁMARA no tiene contemplado el proceso de renovación del componente 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. En caso de que el cliente no cancele el valor del soporte técnico no tendrá derecho a actualizaciones y atención de novedades sobre la versión adquirida.

*2.3.8 Activación del servicio*

El servicio se considera activo una vez se realiza la entrega del componente para que el cliente haga el despliegue en su infraestructura. Condiciones de posterior uso y soporte están por fuera del alcance del servicio aquí descrito.

*2.3.9 Ciclo de vida del servicio del servicio 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 activa el proceso de implementación que realiza el acompañamiento y 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.

*2.3.10 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.

*2.3.11 Procedimientos de administración del servicio en caso de vencimiento (revocación / renovación) de la suscripción del servicio*

El componente es entregado bajo una licencia de uso. Bajo esta premisa, el soporte deberá ser solicitado y pagado por el cliente.

- **Verificación de la firma:** El componente entregado permite 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:** 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 alterada ni modificada.
  - 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).
  - Opcionalmente la aplicación puede integrarse con estampado cronológico proveniente de un tercero confiable de hora legal válida TSA (Timestamp Authority) así como con otros protocolos de firma.

*2.3.12 Servicios adicionales*

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

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.

**2.4 Política de Generación de firmas electrónicas certificadas (clave segura)**

*2.4.1 Ámbito de aplicación*

Las firmas electrónicas certificadas son un conjunto de Plataformas web tipo SaaS que tiene como objetivo mitigar la suplantación y ayudar a prevenir el fraude en las empresas mediante servicios de validación de identidad.

Dentro de los mecanismos de validación de identidad disponibles están:

- Cuestionario de Preguntas Reto
- One time password (OTP)
- One time password (OTP) verificado

- Biometría facial

*2.4.2 Principales características y funcionalidades*

La funcionalidad del servicio de 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, la firma electrónica de diversos documentos, garantizando la autenticidad del origen y la integridad de los datos firmados.

- **Autenticidad del origen**: La autenticación de la identidad del solicitante se podrá realizar por uno o varios de los siguientes métodos:

- Cuestionario de preguntas reto: Servicio que permite identificar a una persona a través de la validación de la información que el mercado conoce de él, a través de la contestación de preguntas aleatorias del historial crediticio, financiero y sociodemográfico. Para aprobar la validación, el usuario debe contestar correctamente las preguntas y no haber superado los límites de fallo de consultas 3 diarias, 6 semanales y 10 mensuales del buró de crédito.

  De sobrepasar el límite de intentos permitidos, la persona será bloqueada para realizar más consultas durante un tiempo fijo de 1 día por el Buró crediticio, con el fin de disminuir el riesgo de fraude a través de reintento.

- One time password (OTP): Servicio de validación de identidad a través de la confirmación de un código numérico aleatorio de 4 dígitos que se envía mediante SMS al número de línea telefónica móvil proporcionado por el usuario durante la transacción. Este código numérico es de un solo uso (es decir, no permite ser usado para otra autenticación) y posee una vigencia temporal de 1 minuto para que el usuario le proporcione la respuesta. En caso de vencimiento del tiempo se debe solicitar otro.
- One time password (OTP) verificado: Servicio de validación de identidad apoyado por fuentes confiables el cual busca identificar si la persona posee acceso a la línea celular conocida por el buró de crédito para el tipo y número de documento indicado. Este servicio al igual que OTP, solicita confirmación de un código numérico aleatorio de 4 dígitos que se envía mediante SMS al número de línea telefónica móvil que el mercado conoce de ese número de documento. Este código numérico es de un solo uso (es decir, no permite ser usado para otra autenticación) y posee una vigencia temporal de 5 minutos para que el usuario lo proporcione. En caso de vencimiento del tiempo se debe solicitar otro.
- Biometría facial: Servicio tipo SaaS mediante el cual se realiza una identificación de la persona a través de la captura de su rostro en vivo y la comparación con una fotografía de referencia de un documento de identidad. En el caso que el rostro cumpla con la prueba de vida y la captura de este coincida con la imagen extraída del documento de identidad, se da como correcta la validación de identidad.

- Biometría dactilar: Servicio que se integra con el componente de captura de huella para realizar la validación de la identidad de una persona a través de la huella capturada cumpliendo los criterios de uso y servicio definidos por la Registraduría Nacional de Colombia. Para ello, el cliente deberá cumplir con los permisos de consulta de datos biométricos y cumplir con sus lineamientos de seguridad de la información, infraestructura tecnología y dispositivos de captura homologados.

- **Firma del documento**: Como resultado del proceso de validación de identidad se obtendrá si la validación fue exitosa o fallida. Para la firma solamente se deberá tomar la validación exitosa y de acuerdo con las necesidades específicas de cada cliente, se podrá utilizar como un dato electrónico para incrustarlo en el documento a ser firmado.

El servicio provisto es tipo SaaS (Software como Servicio) en la cual el cliente no requiere hacer un despliegue en su infraestructura dado que el aseguramiento de la misma estará bajo responsabilidad de Certicámara.

Bajo el esquema del servicio, el cliente tendrá derecho a la utilización de un portal transaccional donde podrá hacer uso de los servicios a través de una interfaz web. Asimismo, se dispone de servicios tipo API REST para la integración con sistemas de información en caso de ser necesario.

*2.4.3 Características técnicas de la generación de firma electrónica certificada (Clave Segura)*

Se genera con las siguientes características:

- Servicio web que requiere autenticación y un dato electrónico de validación de identidad para ejecutar el firmado de documentos en formato PDF
- 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.

Los medios de conexión al servicio de generación de firma electrónica certificada (Clave Segura) será por medio de los métodos de consumo del API y el Front.

- **Servicios Básicos de la Aplicación.**

Servicios básicos:

- El contenido del mensaje de datos no podrá ser conocido por ningún tercero no autorizado

- Permite garantizar que un mensaje de datos no pueda ser conocido sino por su emisor y los receptores deseados
- 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.

*2.4.4 Requisitos para la expedición*

El solicitante debe adjuntar los siguientes documentos:

1. Registro Único Tributario (RUT): Será responsabilidad del suscriptor actualizar la información de domicilio (dirección, municipio, y departamento) en el RUT. Las personas con domicilio fuera de Colombia que no se encuentren registrados ante la DIAN deberán adjuntar el documento que haga las veces de residente fiscal en su país y el mismo se deberá validar con la Dirección de Asuntos Legales y Contractuales quienes darán concepto para la emisión.
2. Documento de identificación: Cédula de ciudadanía, Pasaporte, Documento de identificación de venezolanos o Cédula de extranjería.
3. Documento que acredita la existencia y representación legal de la empresa o entidad: Para empresas o entidades registradas en cámara de comercio se requiere Certificado de existencia y representación legal no mayor a 30 días y para empresas o entidades no registradas en cámara de comercio Certificado expedido por un organismo de control, tales como: Superintendencia financiera, Superintendencia de industria y comercio, Ministerio de educación, Alcaldías, entre otras. Para consorcios y uniones temporales el documento que acredita la existencia y representación legal es el acta de conformación consorcial o unión temporal.
4. Contrato, orden de compra o soporte de pago, de acuerdo con la solicitud.

Certicámara se reserva el derecho de solicitar documentos adicionales a los mencionados 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.

*2.4.5 Activación del servicio*

El SUSCRIPTOR sabrá sobre la activación efectiva del servicio por medio de una notificación mediante correo electrónico, una vez se haya validado la completitud de los requisitos definidos para este servicio.

*2.4.6 Ciclo de vida del servicio 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 u orden de compra generado.

*2.4.7 Aceptación del servicio*

Se considera que el Servicio de Firma Electrónica Certificada (Clave Segura) es aceptado una vez finalizan las pruebas en el ambiente diseñado para tal fin y se solicita por parte de cliente el paso a producción del servicio.

*2.4.8 Renovación del servicio*

Para la renovación del servicio se procederá de acuerdo con las condiciones contractuales pactadas en la prestación del servicio y en caso de requerirse se solicitarán los documentos actualizados al cliente.

*2.4.9 Finalización (renovación) del servicio*

La solicitud de finalización (revocación) del servicio de generación de firma Electrónica Certificada (Clave Segura) deberá ser realizada por el supervisor o representante legal por parte del cliente quien deberá tener en cuenta las causales de terminación estipuladas en el contrato firmado y que se enlistan 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.

## 3. USOS DE LOS CERTIFICADOS

### *3.1 Huella Biométrica Certificada*

*3.1.1 Usos permitidos del servicio*

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 autorizado en virtud de la normativa vigente, con el fin de:

- Realizar la validación de identidad de ciudadanos colombianos con cédula de ciudadanía y firmar electrónicamente documento 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 la normativa vigente.

*3.1.3 Prohibiciones de uso del servicio*

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. No está permitido el almacenamiento del template en ninguna base de datos u otro tipo de almacenamiento.
- ✓ Se prohíbe el uso de 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 el presente documento.
- ✓ 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 servicio*

El correo electrónico certificado (Certimail) puede ser usado por una persona natural o jurídica sin importar el tipo 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. 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 servicio*

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

*3.2.3 Prohibiciones de uso del servicio*

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, por lo cual, el correo electrónico certificado deberá 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 del servicio*

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 seguridad jurídica e integridad de la información.

*3.3.2 Límites de uso del servicio*

Las firmas digitales generadas a partir del componente 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 del servicio*

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 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 Electrónicas Certificada*

*3.4.1 Usos permitidos del servicio*

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, en caso de ser necesario

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 del servicio*

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 del servicio*

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 tolerantes 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 los servicios asociados para los fines establecidos y de acuerdo con los condicionamientos establecidos en el contrato u orden de compra celebrado con él de manera individual y la 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. Asegurarse de que toda la información entregada a Certicámara se encuentre actualizada.

c. Informar inmediatamente a Certicámara acerca de cualquier situación que pueda afectar la confiabilidad de la prestación del servicio asociado.
d. 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 servicios asociados.
e. Cualquier otra que se derive de la normativa vigente, del contenido de la Declaración de Prácticas de Certificación o de la Política de Certificación.
f. Abstenerse de monitorear, alterar, realizar ingeniería inversa o interferir en cualquier otra forma la prestación de servicios de certificación digital.
g. Abstenerse de utilizar los servicios aquí descritos en situaciones que puedan ocasionar mala reputación y perjuicios a Certicámara.
h. 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.
i. Cumplir con el manual de uso del logo establecido por parte de Certicámara.
j. 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.
k. Las demás establecidas en el artículo 39 de la Ley 527 de 1999.

### *4.3 Obligaciones y responsabilidades de la parte que confía*

Los servicios asociados a sistemas de información de Certicámara comprenden la utilización de un conjunto de elementos integrados en torno a la prestación de un servicio tanto a los suscriptores como a terceros. Cuando una tercera persona confía en uno de los servicios asociados, 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 Prácticas de Certificación. Esa tercera persona se convierte en un interviniente del Sistema, en calidad de parte confiante, y por ello asume las obligaciones que se establecen a continuación:

a) Aceptar y reconocer a los servicios asociados solamente el uso que se permite darles de conformidad con lo establecido en la sección de Uso.
b) Conocer con detenimiento y cumplir en todo momento con la Declaración de Prácticas de Certificación.
c) Informar a Certicámara de cualquier irregularidad o sospecha de la misma que se presente en la utilización de los servicios asociados.

d) Abstenerse de monitorear, alterar, realizar ingeniería reversa o interferir en cualquier otra forma la prestación de servicios asociados.

### *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 Práctica de Certificación y los requerimientos del marco normativo colombiano vigente.

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 de Colombia.

## 5 DERECHOS DE LOS INTERVINIENTES

### *5.1 Derechos del solicitante*

Los solicitantes de los servicios 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 Certicámara tendrán los siguientes derechos:

a) Poder utilizar de manera adecuada el servicio asociado adquirido.
b) Informar a los terceros confiantes que Certicámara es su ECD que presta el servicio adquirido.
c) Solicitar la finalización del servicio 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 asociados 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 las actividades dentro de Certicámara. En este caso los empleados y/o consultores son informados sobre las obligaciones de confidencialidad.

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

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

### *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 contenga datos relacionados 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

### *6.3 Responsabilidad de proteger la información confidencial*

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

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

- Implementar y mantener estrictas políticas y procedimientos de seguridad de la información que cumplan con los estándares nacionales e internacionales, incluyendo los requisitos de la ONAC y la legislación vigente en materia de protección de datos.
- Capacitar continuamente a todo nuestro personal sobre las mejores prácticas en seguridad de la información, la importancia de la confidencialidad y sus responsabilidades individuales en la protección de los datos.
- Utilizar tecnologías y sistemas de seguridad robustos y actualizados, incluyendo cifrado de datos, controles de acceso estrictos, sistemas de detección de intrusiones y mecanismos de respaldo y recuperación de información.
- Limitar el acceso a la información confidencial únicamente al personal autorizado que requiera dicha información para el desempeño de sus funciones. Todo acceso es monitoreado y registrado.
- Establecer acuerdos de confidencialidad con todos nuestros empleados, contratistas y terceros que puedan tener acceso a información sensible.
- Gestionar de forma segura y responsable la información de las claves privadas de los suscriptores, asegurando su protección contra el acceso no autorizado, la divulgación, la alteración o la destrucción.
- Notificar de manera oportuna a las autoridades competentes y a los afectados sobre cualquier incidente de seguridad que comprometa la confidencialidad, integridad o disponibilidad de la información, de acuerdo con los marcos regulatorios aplicables.
- Realizar auditorías internas y externas de forma regular para evaluar la efectividad de nuestros controles de seguridad y asegurar el cumplimiento continuo con nuestras políticas y los requisitos regulatorios.

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

### *6.4 Tratamiento de Datos personales*

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

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

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

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

### *6.5 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.

## 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 |
|---|---|---|
| Validación de identidad | 1 | $ 1015 |

- 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.

### *7.2 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 50 correos certificados mensuales:

| Paquetes | Cuentas máximas permitidas | Valor total cupo anual |
|---|---|---|
| Certimail 365 | 1 | $670.000 |

Para rango superior a 100 correos certificados mensuales:

a. Modalidad pago mes vencido por consumos unitarios:

| Planes Corporativos | Frecuencia de Recarga | # de Cuentas | Unidades Disponibles | Valor Anual |
|---|---|---|---|---|
| Certimail Compartido 100 mensual | Mensual | 3 | 100 | $1.100.000 |
| Certimail Compartido 500 mensual | Mensual | 10 | 500 | $5.100.000 |
| CertImail Compartido 1K mensual | Mensual | 25 | 1000 | $9.800.000 |
| Certimail Compartido 3K mensual | Mensual | 50 | 3000 | $27.800.000 |
| Certimail Compartido 5K mensual | Mensual | 75 | 5000 | $45.100.000 |
| Certimail Compartido 10K mensual | Mensual | 100 | 10.000 | $84.150.000 |
| Certimail Compartido 20K mensual | Mensual | 150 | 20.000 | $158.750.000 |
| Certimail Compartido 50K mensual | Mensual | 200 | 50.000 | $369.850.000 |
| Certimail Compartido Anual 2K | Anual | 5 | 2.000 | $1.870.000 |
| Certimail Compartido Anual 5k | Anual | 10 | 5.000 | $4.350.000 |
| Certimail Compartido 10K anual | Anual | 25 | 10.000 | $7.950.000 |
| Certimail Compartido 20K Anual | Anual | 35 | 20.000 | $15.100.000 |
| Certimail Compartido 50K anual | Anual | 200 | 50.000 | $33.450.000 |
| Certimail Compartido 150K anual | Anual | 750 | 150.000 | $92.680.000 |

- 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.

### *7.3 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 |
|---|---|---|
| Generación de firmas digitales | 1 | $ 57.800.000 |

- 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.

### *7.4 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 calculada y liquidada por **Certicámara**. De acuerdo con la volumetría de verificación de identidad que el cliente requiera, el precio base será:

| Servicio | Cantidad | Valor Unitario |
|---|---|---|
| Generación de Firma Electrónica Certificada (Clave Segura) | 1 | $ 9,970 |

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

Para la prestación de los servicios asociados a sistemas de información, Certicámara y el suscriptor firmarán un documento legal donde se establezcan las condiciones particulares de cada servicio.

## 9 NORMATIVIDAD ASOCIADA

Los documentos normativos o técnicos que los servicios descritos en el alcance de este documento y acreditados por el ONAC dan cumplimiento, se encuentran descritos en el certificado publicado en https://onac.org.co/directorio-de-acreditados/

## 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. |
| 21/07/2023 | Se realizan los siguientes cambios al documento:<br>• Eliminación del numeral *"7.6 Políticas de reembolso para suscriptores"*, dado que estas condiciones se tienen establecidas en la ***Declaración de Prácticas de Certificación*** transversales para todos los productos.<br>• Actualización de las tarifas para los servicios correo electrónico certificado y generación de firmas electrónicas certificadas. |
| 15/01/2024 | • Actualización de las tarifas para los servicios asociados a sistemas de información año 2024. |
| 18/03/2024 | Se realizan los siguientes cambios al documento:<br>• Eliminación de todo lo relacionado con el servicio de Digitalización certificada con fines probatorios, dado que es un servicio que se retira de la acreditación.<br>• Actualización integral de los links de acuerdo con los cambios en la página web.<br>• Actualización de la Resolución 27145 de 2023 asociada al servicio de huella biométrica certificada.<br>• Ajuste en la redacción de la política de correo electrónico certificado, generación de firmas digitales y generación de firmas electrónicas certificadas para mayor claridad. |

# POLÍTICA DE CERTIFICACIÓN – SERVICIOS ASOCIADOS A SISTEMAS DE INFORMACIÓN

| Fecha | Razón de actualización |
|---|---|
| | • Claridad que las obligaciones y responsabilidades del suscriptor aplican para todos los servicios que hacen parte de este documento.<br>• Actualización de la normatividad aplicada a cada servicio. |
| 26/04/2024 | Se realizan los siguientes cambios al documento:<br>• Inclusión de los requisitos para la prestación del servicio de huella biométrica certificada, correo electrónico certificado, generación de firmas digitales, generación de firmas electrónicas certificadas.<br>• Aclaración de las causales de finalización (revocación) de los servicios de: huella biométrica certificada, correo electrónico certificado y generación de firmas digitales. |
| 05/08/2025 | Se realizan los siguientes cambios al documento:<br>• Ajuste del procedimiento de aprobación de los cambios en la PC.<br>• Ajuste integral de redacciones para dar mayor claridad y precisión en la información.<br>• Eliminación de la línea nacional gratuita.<br>• Actualización de las tarifas. |