Política de certificado

Facturación Electrónica (Persona Natural y Persona Jurídica) emitido en PKCS10

ECD-CP-FE-PKCS10

ÍNDICE

CONTROL DE DOCUMENTO

Título	Política de Certificado de Facturación Electrónica en QSCD		
Código	ECD-CP-FE-QSCD		
Versión	1.0	**Fecha Versión Actual**	10/11/2025
Fecha Creación	10/11/2025	**Fecha Aprobación**	10/11/2025
Revisado por	Benito Galán	**Aprobado por**	Mamen Maya
Tipología información	Pública		

Control de Cambios y Versiones		
Fecha	**Versión**	**Motivo del Cambio**
10/10/2024	1.0	Primera versión.

Acerca del documento

Este documento es propiedad de Viafirma Colombia, identificada con los siguientes datos de contacto:

Viafirma Colombia

NIT - 901465419-6

Carrera 72 # 81 B 13 Edificio Connecta 80 Torre Fura

111021 Bogotá, D.C. - Colombia

administracioncolombia@viafirma.com

Viafirma Colombia es una sucursal comercial del grupo Viafirma.

Marcas registradas

Todas las marcas, nombres comerciales o signos distintivos de cualquier clase que aparecen en las páginas de Viafirma, y en especial los escritos doctrinales o publicaciones de la misma son propiedad de Viafirma o, en su caso, de terceros que han autorizado su uso, sin que pueda entenderse que el uso o acceso a dichos Contenidos atribuya al Usuario derecho alguno sobre las citadas marcas, nombres comerciales y/o signos distintivos, y sin que puedan entenderse cedidos al Usuario, ninguno de los derechos de explotación que existen o puedan existir sobre dichos Contenidos.

La utilización no autorizada de dichos contenidos, así como la lesión de los derechos de Propiedad Intelectual o Industrial de Viafirma o de terceros incluidos en la Página que hayan cedido contenidos dará lugar a las responsabilidades legalmente establecidas. La marca VIAFIRMA cuenta con los correspondientes registros europeos y españoles con los siguientes números de depósito:

República de Colombia - Superintendencia de Industria y Comercio

SIPI (Oficina Virtual de Propiedad Industrial)

- Resolución #64688
- Expediente #SD2019/0048570

Registro de marca VIAFIRMA (Mixta) en clasificación internacional de Niza Edición No. 11.

EUIPO - European Union Intellectual Property Office

- EUTM File Info 011204617

OEPM - Oficina Española de Patentes y Marcas

- Exp. M4026263

1. INTRODUCCIÓN

1.1 Resumen

Viafirma S.L. es una compañía española especializada en el desarrollo de sistemas de información de firma electrónica, con CIF B91052142, ubicada en España, en la ciudad de Tomares (Sevilla), Edificio CENTRIS, Glorieta Fernando Quiñones s/n, Planta Baja, Módulo 8 (código postal 41940).

Viafirma Colombia es una sucursal comercial de Viafirma, S.L., identificada con NIT 901465419-6, y ubicada en la Carrera 72 # 81 B 13 Edificio Connecta 80 Torre Fura, en Bogotá, D.C. - Colombia.

Viafirma se constituye como ECD (Entidad de Certificación Digital) en Colombia, recogiendo en el presente documento la política del certificado de Sello Electrónico utilizado para la expedición de sellos electrónicos cualificados, así como los aspectos más relevantes y procedimientos definidos para la gestión del servicio.

1.2 Identificación del documento

Este documento está estructurado acorde al **RFC 3647**, con el nombre Política de Certificados de Viafirma Sello Electrónico CO, codificado con el código ECD-CP-ESEAL-VIAFIRMA, y disponible en la siguiente URL de acceso público:

- https://ecd.viafirma.com/docs/ECD-CP FE-QSCD.pdf

Las presentes políticas de certificado están identificadas con el siguiente identificador OID:

- Policy ID: **1.3.6.1.4.1.34253.7.8 FACTURACIÓN ELECTRÓNICA EN QSCD**

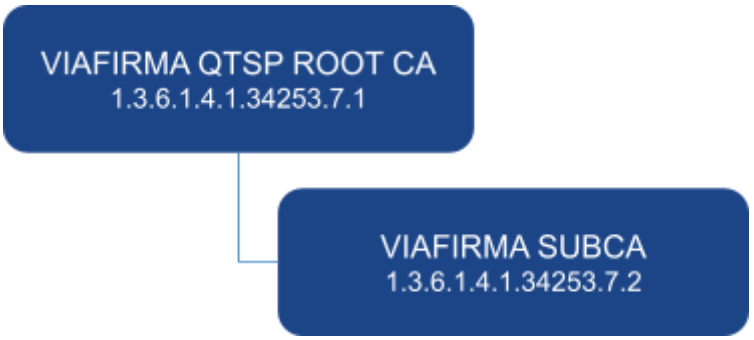
1.3 Participantes

Se consideran las siguientes partes intervinientes:

- **Viafirma**, Autoridad de Certificación (CA), que emite el certificado y actúa como Autoridad de Certificación autorizada por el ONAC, en adelante Entidad de Certificación Digital o VIAFIRMA COLOMBIA ECD.
- **Suscriptor**: persona jurídica que adquiere el certificado digital proporcionado por Viafirma, mediante un acuerdo comercial.
- **Terceras partes** que confían en los certificados digitales emitidos por Viafirma.

1.3.1 Autoridad de certificación

Viafirma ECD queda definida y regulada en la presente política de certificados por su Autoridad de Certificación raíz VIAFIRMA QTSP ROOT CA, que firma a una CA subordinada, y desde la que se emiten y firman los distintos perfiles de certificados.



La presente política se corresponde al perfil de certificado con **OID 1.3.6.1.4.1.34253.7.8** dependiente de la jerarquía descrita anteriormente.

1.3.2 Autoridad de registro

Entidad que actúa conforme esta Política de Certificados y, en su caso, mediante acuerdo suscrito con la CA VIAFIRMA, y cuyas funciones son la gestión de las solicitudes, identificación y registro de los solicitantes del Certificado, así como aquellas otras actividades previstas en las Prácticas de Certificación de la CA.

Para la presente Política de Certificados, la RA será cualquiera de las sedes autorizadas por la CA VIAFIRMA.

1.3.3 Suscriptores

Será considerado suscriptor de un certificado digital emitido bajo esta política el titular del certificado para el que es emitido, constatado en el DN y Common Name del mismo.

Será obligación de los suscriptores los siguientes términos y condiciones:

- Deben respetar y cumplir lo plasmado en el presente documento y en los documentos que regulan la relación comercial con VIAFIRMA ECD, incluyendo al menos el contrato de servicio y los términos y condiciones.

- Deben utilizar los certificados digitales para los usos permitidos por su respectiva política.

1.3.4 Terceros que confían

Será obligación de los Terceros que confían cumplir con lo dispuesto por la normativa vigente y además:

- Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.
- Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confían, y aceptar sujetarse a las mismas.

- No aceptar certificados digitales para fines no contemplados en la presente Política de Certificación.

1.4 Uso del certificado

1.4.1 Usos apropiados del certificado

Los certificados para emisor de factura electrónica son emitidos a personas naturales o personas jurídicas, acreditan la identidad del titular y su condición como Facturador Electrónico en la firma de documentos electrónicos garantizando la autenticidad del emisor de la comunicación, el no repudio del origen y la integridad del contenido, así como el cumplimiento de la resolución de la DIAN

1.4.2 Usos prohibidos del certificado

Los certificados no podrán ser utilizados para propósitos distintos a los autorizados en estas Políticas o en las Prácticas de Certificación (CPS) de Viafirma.

1.5 Administración de políticas

1.5.1 Autoridad de políticas

La autoridad de políticas de Viafirma ECD está compuesta por los roles de confianza incluidos en el comité de seguridad, definido en el procedimiento específico “PE-02 - Comité de Seguridad” de la compañía.

1.5.2 Contacto de la autoridad de políticas

VIAFIRMA COLOMBIA
NIT: 901465419-6
Carrera 72 # 81 B 13 Edificio Connecta 80 Torre Fura
Bogotá, D.C. - Colombia
ecd@viafirma.com

1.5.3 Personas que determinan la autoridad de las políticas

Los cambios y actualizaciones de las presentes Políticas de Certificado serán revisadas y aprobadas por la Autoridad de Políticas.

1.5.4 Procedimiento de aprobación de las políticas

Cualquier elemento de esta política es susceptible de ser modificada. Todos los cambios autorizados serán inmediatamente publicados en la web pública junto al histórico de versiones anteriores. Los terceros que confían afectados pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los 15 días siguientes a la publicación.

Cualquier acción tomada como resultado de unos comentarios queda a la discreción de la autoridad de políticas.

La aprobación de políticas o cualquier cambios que afecten a éstas serán debidamente notificadas tal y como se recoge en el capítulo 2.3 de las presentes políticas.

1.6 Definiciones y acrónimos

- CA: Autoridad de Certificación.
- CEA: criterios específicos de acreditación de ECD en Colombia.
- ECD: Entidad de Certificación Digital.
- eIDAS : Electronic IDentification, Authentication and trust Services (Reglamento UE 2024/1183).
- HSM: Hardware Security Module, módulo de seguridad hardware.
- INM: Instituto Nacional de Metrología de Colombia.
- NTP: Network Time Protocol.
- OID: Object identifier, identificador de objeto único.
- ONAC: Organismo Nacional de Acreditación de Colombia.
- PKI: Public Key Infrastructure, infraestructura de clave pública.
- PSC: Prestador de Servicios de Confianza.
- QTSP: Qualified Trust Services Provider (PSC cualificado).
- SGSI: Sistema de Gestión de la Seguridad de la Información.

- TSA: Time Stamp Authority, Autoridad de Sellado de Tiempo.
- TSP: Time Stamping Protocol, protocolo de sellado de tiempo.
- TSP: Trust Services Provider, correspondencia en inglés a PSC.
- TST: TimeStamping Token, token de sellado de tiempo.
- TSU: TimeStamping Unit, Unidad de Sellado de Tiempo.
- UTC: Coordinated Universal Time.

2. PUBLICACIÓN Y REPOSITORIO DE CERTIFICADOS

2.1 Repositorios

Viafirma ECD publicará las claves públicas de toda su cadena de confianza en el sitio web https://ecd.viafirma.com. Y de forma explícita en las siguientes direcciones:

- https://ecd.viafirma.com/tsp/rootca.crt
- https://ecd.viafirma.com/tsp/subca.crt

Las fuentes de verificación de certificados revocados para esta política serán las siguientes:

- http://ecd.viafirma.com/tsp/tsa_subca.crl
- http://ecd1.viafirma.com/tsp/tsa_subca.crl
- http://ecd.viafirma.com/ocsp

2.2 Publicación de la información de certificación

La presente política de certificado estará publicada en el sitio web https://ecd.viafirma.com. Y de forma explícita en la siguiente dirección:

- https://ecd.viafirma.com/docs/ECD-CP-PJ-QSCD.pdf

2.3 Frecuencia de publicación

Cualquier versión que actualice la presente política de certificados será publicada en el sitio web https://ecd.viafirma.com manteniendo el histórico de versiones anteriores. El intervalo máximo establecido para la revisión de las presentes políticas es de seis meses a contar desde la fecha de su última publicación.

Al mismo tiempo, cuando sea necesario por implicar cambios en los servicios prestados, los cambios en la presente política de certificado serán notificados acorde al procedimiento establecido por el correspondiente órgano regulador.

En cuanto a la frecuencia de publicación de las CRLs de la presente Política de Certificados será de 12 horas, y con un vencimiento de 96 horas (4d).

Al mismo tiempo, se expone un servicio de validación online, basado en el protocolo OCSP (RFC6960), que ofrece el estado en tiempo real.

2.4 Control de acceso a los repositorios

El acceso a la información será gratuito y estará a disposición de los Firmantes/Suscriptores y terceros que confían. El acceso se hará mediante protocolo HTTP, tanto para el acceso a las CRLs como al servicio OCSP.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 Uso de nombres

3.1.1. Tipo de nombres

Todos los suscriptores de certificados requieren un nombre distintivo (distinguished name) conforme con el estándar X.509.

Para la presente política el Subject DN estará formado por los siguientes atributos:

Country (C),
Organization Name (O),
Organization Unit (OU),
Common Name (CN),
serialNumber (SN),
Name (NAME),
User ID (UID),
Locality Name (L),
DN Qualifier

3.1.2 Significado de los nombres

En el contexto de la presente política los nombres de los atributos incluidos se corresponden al siguiente significado:

- Country (C), valor CO para Colombia.
- Organization Name (O), nombre de la organización.
- Organization Unit (OU), departamento de la organización.
- Common Name (CN), concatenación de los atributos O + OU.
- serialNumber (SN), identificación legal de la organización, por ejemplo NIT.
- Name (NAME), nombre completo del representante de la organización.
- User ID (UID), identificación del representante legal de la organización, por ejemplo cédula.
- Locality Name (L), ubicación de la organización, normalmente ciudad, por ejemplo, Bogotá.
- DN Qualifier, valor fijo "CERTIFICADO DIGITAL DE PERSONA JURIDICA EMITIDO EN DISPOSITIVO SEGURO DE CREACION DE FIRMA QSCD".

  Y adicionalmente:

- RFC 822 Name {email address} = para la presente política estará asociado al email asociado al organismo o departamento de la organización, el cual será validado durante el proceso de activación del certificado.

3.1.3 Seudónimos

Viafirma ECD no permite el uso de seudónimos en los certificados que emite.

3.1.4 Reglas para interpretar varios formatos de nombres

El nombre utilizado para identificar al certificado tendrá que coincidir con el documento de identificación vigente que se utilizó para la acreditación, por ejemplo, el NIT de la organización o la cédula del representante autorizado a tramitar la solicitud.

3.1.5 Unicidad de nombres

La configuración habilitada en esta CA para la emisión de certificados incluye mecanismos que impiden la emisión de un mismo Subject DN para distintos suscriptores.

3.1.6 Reconocimiento, autenticación y función de las marcas registradas

Todas las marcas, nombres comerciales o signos distintivos de cualquier clase que aparecen en las páginas de Viafirma ECD, y en especial los escritos doctrinales o publicaciones de la misma son propiedad de Viafirma o, en su caso, de terceros que han autorizado su uso, sin que pueda entenderse que el uso o acceso a dichos Contenidos atribuya al Usuario derecho alguno sobre las citadas marcas, nombres comerciales y/o signos distintivos, y sin que puedan entenderse cedidos al Usuario, ninguno de los derechos de explotación que existen o puedan existir sobre dichos Contenidos.

La utilización no autorizada de dichos contenidos, así como la lesión de los derechos de Propiedad Intelectual o Industrial de Viafirma o de terceros incluidos en la Página que hayan cedido contenidos dará lugar a las responsabilidades legalmente establecidas.

La marca VIAFIRMA cuenta con los correspondientes registros:

República de Colombia - Superintendencia de Industria y Comercio

- SIPI (Oficina Virtual de Propiedad Industrial)
- Resolución #64688
- Expediente #SD2019/0048570
- Registro de marca VIAFIRMA (Mixta) clasificación internacional de Niza Edición No. 11.

EUIPO - European Union Intellectual Property Office:

- EUTM File Info 011204617
- Consulta registro EUIPO

OEPM - Oficina Española de Patentes y Marcas:

- Exp M4026263
- Consulta registro OEPM

3.2 Validación de identidad inicial

3.2.1 Métodos de prueba de la posesión de la clave privada

La presente política define el uso de un certificado digital cuya clave privada reside en un dispositivo seguro centralizado (QSCD), y cuyo uso está protegido por diversos factores de protección por parte de su titular. La correcta autenticación de dichos factores de protección supone la prueba de que su titular es quien hace uso de la clave privada. En resumen, este método evidencia el control de la clave privada pero no la posesión.

El certificado también puede ser emitido en formato PKCS#10. En este modelo, es el suscriptor quien tiene la responsabilidad de generar su propio par de llaves (pública y privada). El suscriptor sólo comparte la llave pública con la Entidad de Certificación Digital (ECD) para que esta la firme. Una vez firmado, el suscriptor se encarga, y bajo su exclusiva custodia, de ensamblar el certificado final.

Para los usos automatizados previstos para este perfil de certificado "Sello Electrónico / E-Seal", el uso estará protegido por un identificador único asociado a unas credenciales nominales bajo el control del suscriptor.

3.2.2. Autenticación de la identidad de una organización

Para acreditar que la organización vinculada al certificado solicitado existe, será necesario adjuntar un documento vigente que deje constancia de esa existencia así como de su NIT y razón social. Para ello, se exigirá a las organizaciones de naturaleza privada, copia del Registro Mercantil vigente (con fecha de expiración posterior a la fecha de solicitud y emisión del certificado digital).

Para aquellos casos en los que las organizaciones no tienen obligación de estar inscritas en el Registro Mercantil, será necesario presentar un documento similar, emitido por el ente regulador de dicha organización (por ejemplo, certificación de inscripción en la base de datos de dicha institución reguladora, indicando fecha de inscripción, estado actual como activo, fecha de dicha certificación y periodo de validez de la misma, así como firma y sello de la entidad emisora del documento).

3.2.3 Autenticación de la identidad de un individuo

La presente política autoriza la acreditación remota y presencial en los siguientes términos y modalidades:

Remota Automática: basado en un proceso automatizado en el que se guía al usuario a través de una serie de pasos que permiten a un software de verificación de identidades validar los siguientes aspectos del suscriptor:

Que el documento de identificación presentado, cédula o pasaporte, se corresponde al formato documental autorizado y vigente mediante la validación técnica de elementos de seguridad incorporados en cada uno de los documentos admitidos.

- Que los datos extraídos del documento de identificación presentados coinciden con los datos presentados en la solicitud del certificado: nombre, apellidos y número de cédula o pasaporte.

- Que durante la prueba de vida, consistente en hacer movimientos delante de la cámara de un dispositivo electrónico, permiten al sistema descartar intentos de suplantación de identidad mediante superposición de imágenes o fotos a la cámara.

- Que durante la grabación del vídeo, se capturan adecuadamente los rasgos faciales necesarios para realizar una verificación facial tomando como patrón la foto extraída del documento de identidad presentado, cédula o pasaporte, previamente validado.

- Que la validación del número de cédula realizada de forma online a través del servicio ofrecido por la Registraduría de Colombia, ha sido satisfactoria.

Remota Asistida: basado en un proceso a distancia, consistente en una conferencia web, previamente coordinada a través de cita previa con los registradores autorizados, y en la que el suscriptor presenta la documentación a la cámara y sigue las instrucciones del registrador, basadas éstas en una serie de preguntas y respuestas de control.

Presencial: las dos modalidades de "acreditación remota" descritas más arriba podrán coexistir con las acreditaciones presenciales, llevadas a cabo por los registradores autorizados por la CA, de forma presencial.

En las tres modalidades de acreditación se preservan las evidencias obtenidas durante el procedimiento técnico a modo de valor probatorio en caso necesario.

3.2.4 Información no verificada del suscriptor

Para la presente política, además de la información y documentación susceptible de ser verificada sin asistencia (documento de identidad: cédula o pasaporte), es requerida otra documentación que será verificada antes de emitir el certificado, en concreto, esta documentación es:

- Copia de Registro Mercantil por Certificado de Existencia y Representación Legal (CERL) que aplica en Colombia con una antigüedad no superior a seis meses.

- Carta de Autorización Legalizada de la empresa en la que conste que el suscriptor está autorizado para firmar a nombre de la empresa, pues el representante legal se encuentra en el CERL.

3.2.5 Validación de la autoridad

Las autoridades de registro autorizadas cuentan con mecanismos de validación y autenticación de suscriptores para cada una de las tres modalidades permitidas por la presente política, en particular:

Remota Automática: el sistema permitirá completar un proceso 100% de forma desatendida, sin la participación de registradores autorizados. Para estos casos, los registradores cuentan con mecanismos de auditoría, para revisión y control, pero en una fase post-emisión de la fase de acreditación, y de la revisión necesaria de la documentación corporativa aportada, antes de la emisión del certificado.

Remota Asistida: en caso de que la validación del suscriptor requiera la participación de un registrador autorizado, el sistema audita qué registrador participó en el proceso, y se encargará de validar la documentación presentada por los medios disponibles en el sistema de video-acreditación asistida.

Presencial: de igual forma que en el caso anterior, la participación del registrador autorizado quedará auditado en el sistema, y en este caso se ocupará de validar presencialmente la documentación presentada por el suscriptor.

3.2.6 Criterios de interoperabilidad

Para la presente política se han establecido los medios técnicos y operacionales que garanticen la interoperabilidad con los siguientes servicios.

- Para la validación de identidad: para los procesos de verificación remota automática se cuenta con la integración de los servicios de la Registraduría de Colombia, para la comprobación del número de cédula.
- Para la firma electrónica del contrato: mediante firma OTP remitido a la cuenta de correo electrónico asociadas a la solicitud.

3.3. Identificación y autenticación para la renovación de certificados

3.3.1 Identificación y autenticación para la renovación de certificados vigentes

Bajo la presente política se permite la identificación del suscriptor para la renovación de su certificado digital con su certificado digital, siempre y cuando éste esté vigente, es decir, no esté caducado ni revocado.

La solicitud de renovación podrá hacerse en cualquier momento desde la fecha de su emisión hasta la fecha de su vencimiento.

También se permite para la renovación de certificados vigentes, la identificación mediante los mecanismos ya previstos para la primera emisión y descritos en el capítulo 3.2 de la presente política.

Para la presente política, basada en la emisión centralizada del certificado, el suscriptor podrá solicitar la renovación de su certificado desde la gestión ofrecida por el propio sistema, denominado Viafirma Fortress, y cuya funcionalidad requiere de autenticación previa del suscriptor.

3.3.2 Identificación y autenticación para la renovación de certificados caducados

No se permite la renovación de certificados ya caducados. Si el certificado ya estuviera caducado, el suscriptor deberá iniciar el proceso de nueva adquisición, y podrá optar por alguno de los mecanismos de validación de identidad inicial previstos en el capítulo 3.2 de la presente política.

3.4 Identificación y autenticación para solicitudes de revocación

Solo se permite revocar un certificado que esté vigente, no pudiendo solicitar la revocación de un certificado caducado o revocado.

Para la presente política, basada en la emisión centralizada del certificado, el suscriptor podrá revocar su certificado desde la plataforma de gestión ofrecida por el propio sistema, denominado Viafirma Fortress, y cuya funcionalidad requiere de autenticación previa del suscriptor.

4. CICLO DE VIDA DEL CERTIFICADO Y REQUISITOS OPERACIONALES

4.1 Solicitud de certificados

Viafirma ECD cuenta con una solución web desarrollada y gestionada por Viafirma, denominada Viafirma Fortress, y que permite la gestión de todo el Ciclo de Vida del Certificado centralizado de forma plenamente online, y sobre esta solución están basados los requisitos operacionales descritos a continuación.

4.1.1 Quién puede solicitar un certificado

En la presente política la solicitud del certificado puede hacerla cualquier persona natural que pueda ser identificado mediante un documento de identidad, que puede ser cédula o pasaporte, y que pueda justificar que ostenta la representación legal y poderes de firma en nombre de alguna institución de naturaleza pública o privada.

4.1.2 Proceso de registro

Para las solicitudes de certificados en la presente política, la emisión del certificado implica obligatoriamente el registro de una solicitud de certificado, a instancia del propio suscriptor, consistente en el llenado de una serie de datos expuestos en un formulario web. Dichos datos incluyen nombre, apellidos, número de documento de identidad, dirección de correo electrónico, teléfono, razón social y NIT de la empresa o institución de la que forma parte y departamento entro otros campos requeridos para la solicitud.

El sistema de centralización de certificados de Viafirma configura y activa sus credenciales de gestión así como los distintos factores de autenticación con los que se protegerá el uso de su certificado. Este registro supone un paso obligatorio previo a la activación del certificado digital centralizado.

4.2 Proceso de solicitud de un certificado

4.2.1 Funciones de identificación y autenticación

Los certificados emitidos bajo esta política permiten hasta tres tipos de identificación y autenticación, tal y como se describen en el capítulo 3.2.3 "Autenticación de la identidad de un individuo".

4.2.2 Aprobación o rechazo de solicitudes

La aprobación o rechazo de solicitudes podrá estar asociada principalmente a dos casos:

- No superar el proceso de pago, si procede, en cada uno de los mecanismos previstos.
- No superar la validación de la documentación y/o identificación del individuo alguna de las tres modalidades de solicitudes descritas en el capítulo 3.2.3:
    - **Solicitudes semiautomáticas:** este perfil permite una solicitud y verificación de identidad 100% online, si bien, su aprobación y finalización no será automática, ya que requiere el análisis de cierta documentación por parte de los registradores. Si durante el proceso automático algunos de los mecanismos de validación de la documentación y/o identificación del invididuo no supera los umbrales y requisitos exigidos, la solicitud será rechazada de forma automática. Llegado a este punto de rechazo, el solicitante podrá optar por: (1) reintentar el proceso automático, (2) solicitar el proceso asistido.
    - **Solicitudes asistidas:** para los casos en los que la verificación de identidad iniciada mediante procedimiento automático haya sido rechazada, el solicitante podrá intentarlo mediante una solicitud asistida, y donde un registrador contactará con el solicitante para proceder a una vídeo-acreditación asistida. Si durante el proceso de vídeo-acreditación el registrador encargado del proceso considera que no tiene suficientes garantías para verificar la documentación y/o identificación del individuo, el proceso de solicitud podrá (1) ser rechazado o (2) emplazado a realizar una solicitud presencial.

- **Solicitudes presenciales:** el proceso de solicitud presencial queda delegado a la responsabilidad y criterio del registrador encargado para la aprobación o rechazo y en función de la documentación presentada.

4.2.3 PLazos del proceso de solicitud

No aplica

4.3 Emisión del certificado

4.3.1 Acciones de la CA durante la emisión de certificados

Viafirma ECD se reserva las acciones necesarias derivadas de los eventos generados durante cualquier fase del ciclo de vida de una emisión de certificado.

4.3.2 Notificaciones a suscriptores por parte de la CA durante la emisión de certificados

A partir de los datos facilitados y autorizados a Viafirma ECD, el suscriptor podrá ser notificado a lo largo del ciclo de vida del proceso de emisión del certificado.

4.4 Aceptación del certificado

4.4.1 Hechos que constituyen la aceptación del certificado

La emisión del certificado regulado en la presente política se entenderá por aceptada si tras la emisión del certificado, el suscriptor no contacta con la RA o la CA para informar de algún error en los datos del mismo. El plazo de contacto para estos fines se establecerá contractualmente.

4.4.2 Publicación del certificado por parte de la CA

La clave pública del certificado emitido estará a disposición la RA autorizada quien permitirá su consulta mediante el acceso a https://ecd.viafirma.com/ra.

4.4.3 Notificación de la emisión a otras entidades

Viafirma ECD no establece entre sus procedimientos la notificación a otras entidades de la emisión de un nuevo certificado.

4.5 Uso del certificado

4.5.1 Uso de clave privada del suscriptor

La clave privada de los certificados emitidos podrá ser usada por una entidad legal (como una empresa o una organización) para demostrar la autenticidad de documentos electrónicos, asegurando a los destinatarios que el documento proviene realmente de esa entidad.

4.5.2 Confianza y uso de la clave pública

Será obligación de los terceros que confían en las claves públicas de Viafirma ECD cumplir con lo dispuesto en la normativa. También será obligación de éstos la verificación de la validez de los certificados en el momento de realizar cualquier operación basada en el uso de los mismos. De igual forma deberán conocer y sujetarse a las garantías, límites y responsabilidades aplicables en cada caso.

4.6 Renovación de certificados

4.6.1 Situaciones para la renovación de certificados

Este perfil de certificado podrá ser renovado en el período comprendido entre la fecha de su emisión y la fecha de su caducidad, siempre que no haya sido revocado antes de la fecha de caducidad. Una vez superada la fecha de caducidad, el certificado no podrá

ser renovado. Para que sea renovado, no basta con que la solicitud de renovación se haga antes de la fecha de caducidad, sino que la emisión del nuevo certificado (es decir, la culminación del proceso de renovación) debe producirse antes de la fecha de caducidad del certificado que se quiere renovar.

4.6.2 Quién puede solicitar la renovación

La solicitud de este perfil de certificado únicamente podrá realizarla el propio interesado, es decir, el titular del mismo, siempre que no se hayan producido cambios respecto a su solicitud inicial.

4.6.3 Proceso de solicitudes de renovación

Para iniciar una solicitud de renovación se habilitarán los mismos procedimientos descritos en el capítulo 4.2 “Proceso de solicitud de un certificado”.

4.6.4 Notificación de la renovación del certificado al suscriptor

El suscriptor podrá ser notificado por cualquiera de los medios previstos, email y/o SMS, como mecanismo de validación o seguimiento del proceso de renovación.

4.6.5 Hechos que constituyen la aceptación del certificado renovado

La renovación se entenderá por aceptada tras completar el proceso de activación del nuevo certificado renovado y si tras la emisión del nuevo certificado, el suscriptor no contacta con la RA o la CA para informar de algún error en los datos del mismo. El plazo de contacto para estos fines se establecerá contractualmente.

.

4.6.6 Publicación del certificado renovado

La clave pública del certificado emitido estará a disposición la RA autorizada quien permitirá su consulta mediante el acceso a https://ecd.viafirma.com/ra.

4.6.7 Notificación de la renovación a otras entidades

Viafirma ECD no establece entre sus procedimientos la notificación a otras entidades de la renovación de un certificado.

4.7 Reemisión del certificado

4.7.1 Circunstancias para la reemisión del certificado

Viafirma ECD no permite la reemisión entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.7.2 Quién puede solicitar la reemisión del certificado

Viafirma ECD no permite la reemisión entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.7.3 Procedimiento para las solicitudes de reemisión del certificado

Viafirma ECD no permite la reemisión entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.7.4 Notificación al suscriptor del nuevo certificado reemitido

Viafirma ECD no permite la reemisión entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.7.5 Hechos que constituyen la aceptación del certificado reemitido

Viafirma ECD no permite la reemisión entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.7.6 Publicación por parte de la CA del certificado reemitido

Viafirma ECD no permite la reemisión entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.7.7 Publicación por parte de la CA del certificado reemitido a otras entidades

Viafirma ECD no permite la reemisión entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.8 Modificación del certificado

4.8.1 Circunstancias para la modificación del certificado

Viafirma ECD no permite la modificación de los datos de un certificado ya emitido entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.8.2 Quién puede solicitar la modificación del certificado

Viafirma ECD no permite la modificación de los datos de un certificado ya emitido entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.8.3 Proceso de solicitud de modificación del certificado

Viafirma ECD no permite la modificación de los datos de un certificado ya emitido entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.8.4 Notificación de la modificación del certificado

Viafirma ECD no permite la modificación de los datos de un certificado ya emitido entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.8.5 Hechos que constituyen la aceptación del certificado modificado

Viafirma ECD no permite la modificación de los datos de un certificado ya emitido entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.8.6 Publicación por parte de la CA de la modificación del certificado

Viafirma ECD no permite la modificación de los datos de un certificado ya emitido entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.8.7 Notificación de la modificación del certificado por parte de la CA a otras entidades

Viafirma ECD no permite la modificación de los datos de un certificado ya emitido entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.9 Revocación y suspensión de certificados

4.9.1 Situaciones para la revocación del certificado

Entre las situaciones contempladas para la revocación de este perfil de certificado serán las siguientes:

- Compromiso de claves: Para Certificados emitidos bajo la la presente política se considera compromiso de claves al hecho de sospechar o tener evidencias de la desvelación de la contraseña de uso de la clave privada del certificado y/o de algunos de los factores de protección configurados para la protección del uso del certificado centralizado: contraseña, PIN o incluso el uso no autorizado de la cuenta de email y/o celular utilizados para el envío de los códigos de un solo uso OTP.
- Cambios significativos en los datos contenidos en el certificado, por ejemplo, nombre de la organización.
- Compromiso de algunos de los algoritmos utilizados para su generación.

- Cualquier motivación particular que lleve al suscriptor querer revocar su certificado.

4.9.2 Quién puede solicitar la revocación del certificado

La revocación de un certificado podrá solicitarse por el suscriptor, por un representante de la organización (justificando documentalmente su relación con la organización), o por la propia CA. Todas las solicitudes serán en todo caso autenticadas.

4.9.3 Proceso para la revocación del certificado

Para iniciar una solicitud de revocación se habilitarán los mismos procedimientos descritos en el capítulo 4.2 “Proceso de solicitud de un certificado”.

- Autoridad de Registro: accediendo al sistema centralizado desde el que se solicitó y activó, Viafirma Fortress, en las opciones disponibles para solicitar la revocación del certificado.

- Notificando por email la solicitud de revocación al equipo de registradores: el suscriptor puede escribir un correo desde la misma cuenta de correo con la que fue creado su certificado digital, remitiéndose a ecd@viafirma.com, en el cual solicite su revocación. La empresa o institución también podrá remitir dicho email adjuntando un documento que justifique las condiciones necesarias para proceder con la revocación (retirada de los poderes de firma, cambio de cargo, desvinculación de la empresa, etc.). El equipo de registradores se encargará de revocar el certificado y el suscriptor será notificado de que la renovación ha sido realizada. El equipo de registradores se encargará de revocar el certificado y el suscriptor será notificado de que la revocación ha sido realizada.

4.9.4 Período de gracia de la solicitud de revocación

Viafirma ECD no contempla período de gracia durante el proceso de revocación. Una vez completado el proceso de revocación tendrá efecto inmediato.

4.9.5 Período en el que la CA debe procesar la solicitud de revocación

Si la solicitud de revocación fue realizada por el titular desde la propia herramienta de centralización de certificados Viafirma Fortress, la revocación tendrá efecto inmediato.

Si la solicitud se hace a través de un email enviado a ecd@viafirma.com, la revocación se llevará a cabo durante el horario laboral de ese mismo día (de 9:00am a 5:00pm), siempre que ese mismo día no sea fin de semana o festivo. Si es fin de semana o festivo, se hará durante el próximo día laborable.

4.9.6 Requisitos de verificación de la revocación por las partes que confían

Las distintas fuentes de verificación de certificados publicadas por Viafirma ECD podrán ser consultadas gratuitamente por los terceros que confían, siendo éstos responsables de verificar la autenticidad de la fuente.

4.9.7 Frecuencia de emisión de la CRL

Las CRLs sujetas a la presente política cuentan con una frecuencia de emisión y publicación de 12 horas.

4.9.8 Latencia máxima de la CRL

Las CRLs sujetas a la presente política cuentan con una carencia máxima de 4 días.

4.9.9 Comprobación online del estado de la revocación

Viafirma ECD publica un servicio de validación online de sus certificados a través del protocolo OCSP publicado en la siguiente dirección:

http://ecd.viafirma.com/ocsp

4.9.10 Requisitos para la comprobación online del estado de revocación

Viafirma ECD no define requisitos particulares para el uso de este servicio más allá de las recomendaciones citadas en la RFC6960 .

4.9.11 Otras formas de comprobación del estado de revocación

Además del servicio OCSP los certificados emitidos por Viafirma ECD podrán ser verificados a través de las distintas CRLs publicadas e informadas en sus respectivos certificados.

Y para los certificados emitidos bajo la la presente política, el propio suscriptor podrá comprobar el estado de su certificado (revocado o no), desde el sistema de centralización de certificados Viafirma Fortress, accediendo con sus credenciales.

4.9.12 Requisitos especiales para la reemisión de certificados por compromiso de claves

Viafirma ECD no permite entre sus procedimientos la reemisión de certificados. En caso de compromiso de claves éstos deberán ser revocados, y el suscriptor tendrá que completar un proceso de nueva emisión.

4.9.13 Circunstancias para la suspensión

Viafirma ECD no permite entre sus procedimientos la suspensión de certificados.

4.9.14 Quién puede solicitar la suspensión

Viafirma ECD no permite entre sus procedimientos la suspensión de certificados.

4.9.15 Procedimiento para la solicitud de suspensión

Viafirma ECD no permite entre sus procedimientos la suspensión de certificados.

4.9.16 Límites del período de suspensión

Viafirma ECD no permite entre sus procedimientos la suspensión de certificados.

4.10 Servicios para el estado del certificado

4.10.1 Características operacionales

Viafirma ECD no ofrece servicios adicionales para la comprobación del estado del certificado distintos a la comprobación de la CRL y/o OCSP descritos en capítulos anteriores, o su consulta desde la propia cuenta del usuario en el sistema de centralización de certificados Viafirma Fortress para los certificados emitidos bajo la política la presente política.

4.10.2 Servicios disponibles

Viafirma ECD no ofrece servicios adicionales para la comprobación del estado del certificado distintos a la comprobación de la CRL y/o OCSP descritos en capítulos anteriores, o su consulta desde la propia cuenta del usuario en el sistema de centralización de certificados Viafirma Fortress para los certificados emitidos bajo la política la presente política.

4.10.3 Características opcionales

Viafirma ECD no ofrece servicios adicionales para la comprobación del estado del certificado distintos a la comprobación de la CRL y/o OCSP descritos en capítulos anteriores, o su consulta desde la propia cuenta del usuario en el sistema de centralización de certificados Viafirma Fortress para los certificados emitidos bajo la la presente política.

4.11 Fin de la suscripción

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

4.12 Depósito de claves y recuperación

4.12.1 Prácticas para el depósito y recuperación de claves

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

4.12.2 Prácticas de encapsulado y recuperación de recuperación de claves

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5. INSTALACIÓN, GESTIÓN Y CONTROLES OPERACIONALES

5.1 Controles físicos

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.1.1. Localización y construcción

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.1.2 Acceso físico

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.1.3 Alimentación eléctrica y aire acondicionado

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.1.4 Exposición al agua

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.1.5 Protección y prevención de incendios

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.1.6 Sistema de almacenamiento

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.1.7 Eliminación de residuos

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.1.8 Backup remoto

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.2 Controles procedimentales

5.2.1 Roles de confianza

Lo establecido en la Declaración de Prácticas de Certificación de Viafirma ECD, y de forma específica para la gestión del Servicio Cualificado de Servicios de Confianza, se cuentan con los siguientes roles de confianza:

Se dispone de un número de personal suficiente con conocimiento experto en la gestión de Certificados Digitales, Sellos de Tiempo y toda la gestión relacionada con el ciclo de vida de los servicios asociados por una Autoridad de Certificación y Autoridad de Sellado de Tiempo.

Para ello se definen una serie de roles y responsabilidades encajadas en el organigrama organizacional de la compañía e identificados en el equipo designado para la gestión de la Seguridad de Viafirma ECD. En algún caso, se amplían las responsabilidades de roles existentes en el apartado anterior, y en otro, se crean nuevos roles. Los roles no implican unívocamente cargos: una persona puede ostentar más de un rol, si bien se han tenido en cuenta las incompatibilidades y restricciones recogidas en las buenas prácticas y estándares como RFC3647.

La norma especifica cuatro nuevos roles:

- Security Officer
- System Administrator
- System Operator
- System Auditor

5.2.2 Número de personas requeridas por tarea

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.2.3 Identificación y autenticación para cada rol

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.2.4 Roles que requieren separación de funciones

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.3 Controles personales

5.3.1 Requisitos de calificación, experiencia y autorización

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.3.2 Procedimiento de verificación de antecedentes

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.3.3 Requisitos de formación

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.3.4 Requisitos y frecuencia de formación

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.3.5 Frecuencia y secuencia de rotación de tareas

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.3.6 Sanciones por acciones no autorizadas

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.3.7 Requisitos para personal independiente

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.3.8 Documentación entregada al personal

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.4 Procedimiento para el registro de auditoría

5.4.1 Tipo de eventos registrados

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.4.2 Frecuencia del procesamiento de registros

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.4.3 Período de retención del registro de auditoría

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.4.4 Protección del registro de auditoría

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.4.5 Procedimiento del backup del registro de auditoría

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.4.6 Sistema de recolección de auditoría

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.4.7 Notificación de eventos

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.4.8 Evaluación de vulnerabilidades

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.5 Archivo de registros

5.5.1 Tipos de archivos de registros

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.5.2 Período de retención del archivo

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.5.3 Protección del archivo

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.5.4 Procedimiento para el backup del archivo

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.5.5 Requisitos para el sellado de tiempo del registro

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.5.6 Sistema de recolección del archivo

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.5.7 Procedimiento para obtener y verificar la información del archivo

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.6 Cambio de clave

No se contempla el cambio de claves para la presente política de certificados.

5.7 Recuperación en caso de compromiso de la clave o desastre

5.7.1 Procedimiento para la gestión de incidentes

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.7.2 Obsolescencia y deterioro

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.7.3 Procedimientos ante compromiso de clave de una entidad

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.7.4 Plan de continuidad de negocio ante desastres

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

5.8 Cese de la CA o RA

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

6. CONTROLES TÉCNICOS DE SEGURIDAD

6.1 Generación del par de clave y su instalación

6.1.1 Generación del par de clave

Bajo la presente política, las claves del certificado son generadas en el sistema centralizado de certificados, Viafirma Fortress. La clave privada no permite ser exportada.

6.1.2 Entrega de la clave privada al suscriptor

Bajo la presente política,, la clave privada del certificado es generada y almacenada en un módulo criptográfico (HSM) FIPS 140-2 Level 3 EAL4+ gestionado por Viafirma, y por tanto no es entregada al suscriptor.

6.1.3 Entrega de la clave pública al suscriptor

La clave pública del certificado emitido será publicada en el sitio web de Viafirma tal y como se define en el capítulo 2.2 de la presente política de certificados.

6.1.4 Entrega de la clave pública de la CA a los terceros que confían

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

6.1.5 Tamaño de las claves

Con carácter general, el tamaño de las claves generadas por Viafirma serán de 2048 bits para los certificados finales y de 4096 bits para los certificados de entidades intermedias y raíz de su jerarquía. En el caso del certificado regulado en la presente política de certificados, el tamaño será de 2048 bits.

6.1.6 Control de calidad de los parámetros de generación de la clave pública

Los parámetros utilizados para la generación del certificado regulado en la presente política serán definidos como parte del procedimiento de ceremonia de claves y aprobados por Viafirma ECD.

6.1.7 Propósito de uso de la clave

Las directrices para el uso de clave en los certificados de las entidades intermedias y raíz de su jerarquía serán Key Cert Sign y CRL Sign. Para el caso de los certificados finales, como el certificado sujeto a la presente política, será Digital Signature, Non-Repudiation Encrypt y Key Encipherment.

6.2 Protección de clave privada y controles del módulo criptográfico

6.2.1 Controles y estándares del módulo criptográfico

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

6.2.2 Control dual n de m para el uso de la clave privada

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

6.2.3 Depósito de la clave privada

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

6.2.4 Backup de la clave privada

Lo establecido para el procedimiento de respaldo del HSM principal con el que se gestionan las claves privadas de la presente política.

6.2.5 Archivo de la clave privada

No aplica para la presente política.

6.2.6 Importación de la clave privada al módulo criptográfico

La clave privada del certificado generado bajo la presente política no permite su importación en el módulo criptográfico, ésta es generada en el módulo criptográfico y no permite su exportación.

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

El almacenamiento de la clave privada del certificado coincide con lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

6.2.8 Método de activación de la clave privada

Para la presente política, la clave privada generada en el módulo criptográfico no será activada hasta que su titular haya finalizado la activación de los factores de protección de uso de su clave en el sistema centralizado Viafirma Fortress.

6.2.9 Método de desactivación de la clave privada

El sistema centralizado Viafirma Fortress ofrece al suscriptor varias opciones relativas al ciclo de vida de sus certificados, entre ellas, la desactivación.

6.2.10 Método de destrucción de la clave privada

Para la presente política, el suscriptor dispone de un método en la herramienta de centralización de certificados Viafirma Fortress para eliminar su certificado digital. Esta acción supone la eliminación de la clave privada custodiada por el módulo criptográfico.

6.2.11 Clasificación del módulo criptográfico

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

6.3 Otros aspectos sobre la gestión de par de clave

6.3.1 Archivo de la clave pública

No se contempla procedimiento para la publicación de claves públicas de la raíz, sus subordinadas o del certificado cuando éstas han caducado. No obstante esta información está disponible en el sistema que gestiona la PKI a partir del histórico de claves públicas registradas por el sistema, incluyendo claves que hayan sido renovadas o revocadas.

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

La validez de la clave pública del certificado será de 2 años (730 días).

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

Para la presente política, y tras la decisión por parte de la CA de aprobar la generación del certificado solicitado desde el sistema centralizado Viafirma Fortress, los datos de activación estarán vinculados al suscriptor, debiendo activar los distintos factores de protección de uso de la clave privada.

6.4.2 Protección de los datos de activación

Para la presente política, el suscriptor cuenta con mecanismos para la protección y gestión de los factores de protección del uso de su clave privada en el sistema centralizado Viafirma Fortress.

6.4.3 Otros aspectos de los datos de activación

No se han definido otros aspectos relevantes para este punto.

6.5 Controles de seguridad informática

6.5.1 Requisitos técnicos de los controles de seguridad

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

6.5.2 Clasificación de la seguridad

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

6.6 Ciclo de vida de los controles técnicos

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

6.7 Controles de seguridad de red

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

6.8 Sello de tiempo

Lo establecido en la Declaración de Prácticas de Certificación de Viafirma ECD y en concreto en las políticas del perfil de certificado emitido para el sello de tiempo.

7. CERTIFICADOS, CRL,OCSP Y PERFILES

7.1 Perfil de certificado

7.1.1 Número de versión

Perfil asociado a la versión 3 del estándar X.509.

7.1.2 Extensiones del certificado

Non-Critical Extensions

None

```
Authority Information Access (AIA)      1.3.6.1.5.5.7.1.1

Authority Information Access [1]:
       Access Method: CA Issuers (1.3.6.1.5.5.7.48.2)
       Access Location:
       URI: http://ecd.viafirma.com/tsp/subca.crt
Authority Information Access [2]:
       Access Method: OCSP (1.3.6.1.5.5.7.48.1)
       Access Location:
       URI: http://ecd.viafirma.com/ocsp

Authority Key Identifier (AKI)   2.5.29.35

       Key Identifier:
              0x4AC8 0204 1843 C2BD 7F03 90B8 8FF7 13C8 DCBE BE26

Certificate Policies (CP)  2.5.29.32

       Certificate Policy [1]:
              PolicyIdentifier: 0.4.0.194112.1.3
       Certificate Policy [2]:
              PolicyIdentifier: 1.3.6.1.4.1.34253.7.7
              Policy Qualifier Information [2.1]:
              PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1)
              CPS Pointer: http://ecd.viafirma.com/cps
```

CRL Distribution Points (CDP) **2.5.29.31**

CRL Distribution Point [1]:
Distribution Point Name:
Full Name:
URI: http://ecd.viafirma.com/tsp/tsa_subca.crl
CRL Distribution Point [2]:
Distribution Point Name:
Full Name:
URI: http://ecd1.viafirma.com/tsp/tsa_subca.crl

Extended Key Usage (EKU) **2.5.29.37**

TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)
E-mail Protection (1.3.6.1.5.5.7.3.4)

QC Statements **1.3.6.1.5.5.7.1.3**

QC Statement [1]:
QC Compliance
QC Statement [2]:
QC Secure Signature Creation Device
QC Statement [3]:
0.4.0.194112.1.3 EMITIDO POR LA ECD VIAFIRMA EN COLOMBIA CON CODIGO DE ACREDITACION ONAC 24-ECD-001

Subject Alternative Name (SAN) **2.5.29.17**

RFC 822 Name: {EMAIL}

Subject Key Identifier (SKI) **2.5.29.14**

Key Identifier:
0xC8C4 A406 58F2 796E 48FF D5AC 2D9F 2BB9 ADB4 27D8

Critical Extensions

None

Basic Constraints 2.5.29.19

Subject is not a CA
Path Length Constraint: None

Key Usage (KU) 2.5.29.15

Digital Signature
Non-Repudiation
Key Encipherment

7.1.3 Identificador (OID) del algoritmo de firma

None

Signature Algorithm SHA-256 with RSA Encryption
(1.2.840.113549.1.1.11)
Parameters None

7.1.4 Uso de nombres

Lo establecido en el capítulo 3.1.

7.1.5 Restricciones de nombres

No se permiten DN duplicados.

7.1.6 Identificador de política de certificado

```
None
Non-Critical Extension

Certificate Policies (CP)  2.5.29.32

       Certificate Policy [1]:
              PolicyIdentifier: 0.4.0.194112.1.3
       Certificate Policy [2]:
              PolicyIdentifier: 1.3.6.1.4.1.34253.7.7
              Policy Qualifier Information [2.1]:
              PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1)
              CPS Pointer: http://ecd.viafirma.com/cps
```

7.1.7 Uso de la extensión de política de restricciones

No se hacen uso de Policies Constraints.

7.1.8 Sintaxis y semántica de la política de calificadores

No se contempla.

7.1.9 Semántica del procedimiento para las extensiones críticas del certificado

No se contempla.

7.2 Perfil de la CRL

7.2.1 Número de versión

Número secuencial de cada CRL emitida y publicada por Viafirma ECD, y debidamente informada en el OID 2.5.29.20 “CRL Number” de la estructura de la CRL.

7.2.2 CRL y extensiones

Extensiones disponibles acorde al estándar X.509 CRL Number (2.5.29.20) y Authority Key Identifier (2.5.29.32).

7.3 Certificado OCSP

Se cuenta con dos servicios OCSP, uno para validar el certificado correspondiente a este perfil, emitido por la SUBCA y otro servicio OCSP para validar el certificado de la SUBCA. Ambos servicios OCSP están firmados por los siguientes Certificados.

La respuesta OCSP en la que se comprueba la validez del certificado asociado a la presente política, y publicado en http://ecd.viafirma.com/ocsp, está firmada con el siguiente certificado:

```
None
VIAFIRMA TSA SUB CA

Subject Name
    Country         ES
    Organization    VIAFIRMA SOCIEDAD LIMITADA
    Organizational Unit    VIAFIRMA QTSP
    Serial Number          VATES-B91052142
    Common Name            VIAFIRMA TSA SUB CA

Issuer Name
    Country         ES
    Organization           VIAFIRMA SOCIEDAD LIMITADA
    Organizational Unit    VIAFIRMA QTSP
    Serial Number          VATES-B91052142
    Common Name            VIAFIRMA QTSP ROOT CA

Serial Number       42 D7 40 76 6F AB 99 18 26 D4 9B 0B 3A 23 84 3C 2B
02 69 92
Version                    3
Signature Algorithm SHA-256 with RSA Encryption ( 1.2.840.113549.1.1.11
)
    Parameters             none
```

```
Not Valid Before    Thursday, 17 October 2019 at 14:25:49 Central
European Summer Time
Not Valid After     Monday, 17 October 2039 at 14:25:49 Central European
Summer Time

Public Key Info
    Algorithm RSA Encryption ( 1.2.840.113549.1.1.1 )
    Parameters      none
    Public Key      512 bytes : CD 52 FF 1F 3B E5 3D 39
BE DC 2A E8 2B C7 17 81 AF 00 57 49 A1 91 77 C5 9A C4 00 95 BD B8 4E 7B
D5 97 70 B6 5F 6F F7 62 66 A5 1E 1B 18 7F 4A 5D 7B D2 76 95 83 CC ED 67
BD 51 40 47 9C 1F 7E 8E 81 8B 22 62 FB EC FF EF 92 BC D9 AF 7C 8D 8A 83
25 36 29 18 FB 1C 44 F1 90 AD 74 EB C1 30 92 EF 5C 0D 37 8A 56 A7 FD CF
65 81 35 BD DE 95 E7 06 D0 61 3B E6 19 D5 48 2A 6A D5 A5 F6 F7 63 BA 5A
4E 6E AF 33 85 CA 98 71 42 56 C0 CE 45 25 28 A3 4E 8E E0 90 77 E7 CC 45
E2 CD 53 E4 7E 5E DF 07 79 C4 26 39 EF 7A DE 78 21 54 84 5A FB 4C 03 60
DB C1 A7 BC BC 09 CC CD 5C 83 90 37 42 A1 70 EE 27 F6 7B 13 4E 5A 6C DE
9F DF F1 0E 3B 61 1B 99 77 CC 70 A9 70 2F 16 B0 A0 20 26 56 DD 68 38 8C
69 E2 26 D8 DE AF 88 4E 54 3E 4E 56 4F 00 19 B0 DC 28 AF A0 95 6C 65 B4
2B 11 DD 8E FB 85 E2 B4 33 B8 32 D2 7D 0B 08 71 F7 BE 53 29 49 1C 49 FE
59 71 A0 1B 04 32 3C 90 2C 2E 3A BD F1 24 9C F4 34 FF 0B 32 3D 14 4B 00
6D 6A 9B 99 5E 78 A7 05 65 C5 1D AB 73 9C 48 D6 03 1C 8D 94 8F A0 97 61
E4 EF 9B 4F 6F 24 CD B0 F5 36 03 37 ED E4 BA B7 27 D7 93 35 23 F3 AE D8
F5 7A 6F D9 AD 5F 94 80 2D AA 5C 33 B3 79 8F 47 0A 0B A6 64 D5 4D 59 2C
C2 0C 82 F2 B1 A6 D0 BA F5 FD 80 4D FB 58 19 45 5A 1A 5F BC B4 B3 7C AC
BE 4B 8A E0 30 79 DC 94 B7 3D AB 8A A6 C0 E8 97 FF 03 D1 47 04 06 9D 8A
DF 10 C9 33 FC B6 E7 1D DA B5 46 65 E8 D4 27 A6 52 C5 4D 72 FA AF F1 9D
60 F9 BF A3 C7 91 3B 96 C7 5A 96 2E 2F 2B 7A 3C 9A 18 A6 86 FA B4 06 E5
8B 4E 61 D4 CE BE 96 23 F9 00 32 19 BB 9E A2 89 E8 75 64 0C D7 63 49 8F
50 D4 96 A4 F9 F7 FA 45 D4 C9 F7 B6 55 A6 1A CB 93 6A CD E6 74 30 3A BF
    Exponent  65537
    Key Size  4096 bits
    Key Usage Verify

Signature     512 bytes : 9A 17 F7 DE 5A 05 E2 55
94 BF 31 E3 98 01 39 BD D3 60 05 C9 0C 69 BB 8A F3 5A E7 A9 97 26 11 4D
E0 A0 0E 7A 21 BB D9 F8 F8 34 0F 20 37 9F 66 78 8D A2 91 1F 41 6A 38 39
9B 7B 9A 4B 4C 73 9A 95 D4 A7 5E 1E AC 98 6E C7 61 07 5F C3 1E 85 1F 22
2A 0D CF 08 15 0F 48 47 5B 65 CA FF 28 3A A0 22 70 C6 78 A8 F2 BF 29 FA
E9 69 B9 F4 37 18 9F FE AA 0F 3C B5 A4 8F B0 5B 48 7B 52 CA 73 91 3C 21
96 AA 4B 65 BE D4 F7 11 D8 6C E5 9B F8 30 39 86 4E DF 2F 19 B3 2F 78 6C
68 0A 8B 9B C4 6C 6C F0 D8 2B 5B FD 89 E2 7F 42 42 C3 A9 82 DF E3 AD 64
71 F2 28 E5 21 8A 06 AD 1E 0B 24 3D 18 28 23 2E 80 C5 DE 2C 2C 50 1D FE
CE B3 B2 14 61 A8 84 08 32 BB 7B 4D 9D D0 30 9A 53 21 89 B0 97 66 26 E8
ED EC 70 60 2A 42 61 DF 90 1E E7 21 CE 49 E1 09 94 FE 6E CC A9 96 DC 50
8A 31 DE FF 06 33 F7 4A B5 54 34 3D B9 A2 26 8F F5 A5 69 32 18 C2 B4 F8
A8 6E 6A 5B 93 C0 0D E9 06 B0 3D D6 1C 05 52 A4 C2 27 03 68 A5 35 5D B2
F5 45 A6 84 FA 8A 6A 65 3C 7D 90 B1 13 3E 32 BA C7 08 6F 45 70 C8 F6 23
```

```
73 12 D9 63 C9 CE DC 7E 45 0F C3 15 2E 6C 64 47 78 9E A3 1E 32 AB 4D 39
85 7A C1 4F 7D 8A 5B FC F4 DB 94 C6 02 01 DE 64 62 3B 44 6F 20 22 13 39
26 86 2C 45 EC 85 82 E9 E1 E5 8F EA C8 C8 94 8D 7A 80 EC 84 5C E0 FB 09
F7 39 6D 49 6E 83 16 AC 32 93 C6 ED FC 27 E4 A9 07 47 8F EF 47 7F 28 F2
99 92 63 9D 7E 6B AC E7 CA 69 C2 CF 4F DC 4E 16 4A 47 B1 13 81 A8 68 E8
49 85 D2 64 20 31 89 26 97 89 00 94 F5 6A 72 E6 24 E0 71 98 52 32 53 06
A1 9F 13 9E D5 B2 71 B8 C8 8D D2 9E B7 30 F1 D5 71 34 F9 CE FF 26 7C 05
F0 B0 80 97 DA 79 F7 D7 59 F6 3B 66 5A 31 A8 C0 47 93 70 7D E0 1A FC 5D

Extension     Key Usage ( 2.5.29.15 )
    Critical  YES
    Usage     Key Cert Sign, CRL Sign

Extension     Basic Constraints ( 2.5.29.19 )
    Critical  YES
    Certificate Authority  YES
    Path Length Constraint 0

Extension     Subject Key Identifier ( 2.5.29.14 )
    Critical  NO
    Key ID    4A C8 02 04 18 43 C2 BD 7F 03 90 B8 8F F7 13 C8 DC BE BE
26

Extension     Authority Key Identifier ( 2.5.29.35 )
    Critical  NO
    Key ID    73 A0 A2 20 9D 0C C2 10 56 6D 9A 7D 17 F7 F5 63 61 12 67
11

Extension     Certificate Policies ( 2.5.29.32 )
    Critical  NO
    Policy ID #1     ( 1.3.6.1.4.1.34253.7.2 )
    Qualifier ID #1 Certification Practice Statement ( 1.3.6.1.5.5.7.2.1
)
        CPS URI      http://qtsp.viafirma.com/cps

Extension     CRL Distribution Points ( 2.5.29.31 )
    Critical  NO
    URI       http://qtsp.viafirma.com/tsp/root_ca.crl
    URI       http://qtsp1.viafirma.com/tsp/root_ca.crl

Extension     Certificate Authority Information Access (
1.3.6.1.5.5.7.1.1 )
    Critical  NO
    Method #1 CA Issuers ( 1.3.6.1.5.5.7.48.2 )
        URI   http://qtsp.viafirma.com/tsp/rootca.crt
    Method #2 Online Certificate Status Protocol ( 1.3.6.1.5.5.7.48.1 )
        URI   http://qtsp.viafirma.com/ocsp
```

```
Fingerprints
    SHA-256   45 13 96 84 F6 2A 6D 70 A5 B8 B2 45 6B 9F 1D 63 CF 5A 57
20 12 3F 48 FA C1 C1 6B EB BE 3E 4E 24
    SHA-1     58 A2 40 64 73 EB C0 B2 29 4D 8B 64 50 02 EA 87 98 58 3C
29
```

8. AUDITORÍAS

8.1 Frecuencia o circunstancias de la auditoría

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

8.2 Identidad y cualificación del auditor

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

8.3 Relación del auditor con el prestador

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

8.4 Temas tratados en la auditoría

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

8.5 Acciones a realizar como resultado de una deficiencia

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

8.6 Comunicación de resultados

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

9. OTROS ASUNTOS LEGALES

9.1 Tarifas

9.1.1 Tarifa para la emisión y renovación de certificados

Viafirma ECD establece en sus límites de uso las condiciones de uso de los distintos servicios de confianza prestados. Todos ellos serán informados en el Texto Divulgativo asociado a cada servicio y publicado en la página oficial https://ecd.viafirma.com.

9.1.2 Tarifa de acceso al certificado

Viafirma ECD establece en sus límites de uso las condiciones de uso de los distintos servicios de confianza prestados. Todos ellos serán informados en el Texto Divulgativo asociado a cada servicio y publicado en la página oficial https://ecd.viafirma.com.

9.1.3 Tarifa de acceso a OCSP o CRL

No se establecen tarifas o costes adicionales para el acceso a las fuentes de verificación OCSP o CRL publicadas por Viafirma ECD. Su uso es gratuito.

9.1.4 Tarifa para otros servicios

Viafirma ECD establece en sus límites de uso las condiciones de uso de los distintos servicios de confianza prestados. Todos ellos serán informados en el Texto Divulgativo asociado a cada servicio y publicado en la página oficial https://ecd.viafirma.com.

9.1.5 Política de reembolsos

Viafirma ECD establece en sus límites de uso las condiciones de uso de los distintos servicios de confianza prestados. Todos ellos serán informados en el Texto Divulgativo asociado a cada servicio y publicado en la página oficial https://ecd.viafirma.com.

9.2 Responsabilidad financiera

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

9.3 Confidencialidad de la información comercial

9.3.1 Alcance de la información confidencial

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

9.3.2 Alcance excluido de la información confidencial

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

9.3.3 Responsabilidad para la protección de la información confidencial

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

9.4 Privacidad de la información personal

9.4.1 Plan de privacidad

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

9.4.2 Información con tratamiento privado

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

9.4.3 Información no considerada con tratamiento privado

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

9.4.4 Responsabilidad para la protección de la información privada

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

9.4.5 Consentimiento de uso de la información privada

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

9.4.6 Divulgación de conformidad con procesos judiciales o administrativos

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

9.4.7 Otras casos para la divulgación de información

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

9.5 Derechos de propiedad intelectual

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma.

9.6 Obligaciones y Responsabilidad

9.6.1 Obligaciones de la CA

La Entidad de Certificación VIAFIRMA ECD actuando bajo estas Políticas de Certificación está obligada a cumplir con lo dispuesto por la normativa vigente, y además a:

a. Respetar lo dispuesto en estas Políticas.

b. Proteger sus claves privadas de forma segura.

c. Emitir Certificados conforme a estas Políticas y a los estándares de aplicación.

d. Emitir Certificados según la información que obra en su poder y libres de errores de entrada de datos.

e. Emitir Certificados cuyo contenido mínimo sea el definido por la normativa vigente para los Certificados Digitales.

f. Revocar los Certificados según lo dispuesto en estas Políticas y publicar las mencionadas revocaciones en su correspondiente CRL y/o OCSP.

g. Informar a los Firmantes/Suscriptores de la revocación de sus Certificados, en tiempo y forma de acuerdo con la legislación vigente.

h. Publicar estas Políticas y las Prácticas correspondientes en su página web.

i. Informar sobre las modificaciones de estas Políticas y de su Declaración de Prácticas de Certificación a los Suscriptores y Unidades de Registro que estén vinculadas a ella.

j. Generar y custodiar la clave privada o los datos de creación de firma del Firmante/Suscriptor para la centralización del Certificado.

k. Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia, en su caso.

l. Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndose ante pérdida, destrucción o falsificación.

m. Conservar la información sobre el Certificado emitido por el período mínimo exigido por la normativa vigente.

9.6.2 Obligaciones de la RA

La Unidad de Registro Viafirma actuando bajo estas Políticas de Certificación está obligada a cumplir con lo dispuesto por la normativa vigente, y además a:

a. Recibir las solicitudes de emisión, renovación o revocación de Certificados Digitales;

b. Validar la identidad y los datos suministrados por EL SUSCRIPTOR, al momento de recibir su solicitud;

c. Recibir de VIAFIRMA ECD el Certificado Digital y proceder con la notificación de su disponibilidad a favor de EL SUSCRIPTOR, conforme las condiciones definidas en las PC, una vez verificada su identidad;

d. Tramitar las solicitudes de revocación de Certificados lo antes posible;

e. Comunicar a EL SUSCRIPTOR la revocación de su Certificado de Firma Digital cuando ésta se produzca;

f. Mantener actualizada la base de datos de Certificados emitidos, renovados, en vigor, caducados y revocados;

g. Todas las obligaciones puestas a su cargo como Unidad De Registro especificadas en las PC para cada tipo de Certificado, en la Declaración de Prácticas de Certificación del Prestador Cualificado de Servicios de Confianza, así como de la legislación y normativa vigente.

9.6.3 Obligaciones del suscriptor

El suscriptor de cualquier certificado digital emitido por el ECD o la RA, deberá cumplir con lo establecido en estas Políticas de Certificación y en la normativa vigente:

a. Hacer uso del certificado acorde a los límites y condiciones regulados en la presente política de certificados.

b. Poner todos los medios a su alcance para la protección y uso adecuado de la clave privada del certificado.

c. Solicitar inmediatamente la revocación del certificado ante la sospecha de un compromiso de clave.

d. No hacer uso del certificado cuando éste ha caducado o ha sido revocado.

9.6.4 Obligaciones de los terceros que confían

Es obligación de los terceros que confían en los certificados y servicios prestados por Viafirma ECD:

- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y su correspondiente política de certificado.
- Verificar la validez de los certificados en el momento de realizar o verificar cualquier operación basada en los mismos.
- Asumir su responsabilidad en la correcta verificación de las firmas digitales
- Asumir su responsabilidad en la comprobación de la validez, revocación o suspensión de los certificados en que confía.
- Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

9.6.5 Obligaciones de otras entidades

Viafirma ECD no establece obligaciones a otras entidades participantes.

9.7 Renuncias de la garantía

Viafirma ECD podrá renunciar aquellas garantías de los servicios que estuvieran asociados a las obligaciones definidas en el marco regulatorio vigente para los

prestadores de confianza, en concreto aquellas que pudieran estar adaptadas a un propósito particular o mercantil.

9.8 Límites de responsabilidad

- Daños y perjuicios en los usos que puedan realizarse de los certificados o sellos de tiempo de Viafirma ECD, ya sean estos por culpa de los interesados o por defectos de origen de los elementos.
- Hechos acontecidos por usos no acordes con las presentes CPS, en casos de desastres naturales, atentado terrorista, huelga, fuerza mayor (incidencias en servicios eléctricos o redes telemáticas o de comunicaciones), así como en los supuestos que se trate de acciones constitutivas de delito o falta que afecten a sus infraestructuras prestadoras, salvo que hubiera mediado culpa grave de la entidad.
- Usos indebidos, fraudulentos, en ausencia de convenio o contrato suscrito con Viafirma ECD, en caso de extralimitación del uso o de omisiones del suscriptor.
- Los algoritmos criptográficos ni de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si se ha procedido con la diligencia debida de acuerdo al estado actual de la técnica, y conforme a los documentos publicados y la normativa vigente.
- Problemáticas asociadas al incumplimiento por parte de los suscriptores de las condiciones de contratación (por ejemplo, impagos).

9.9 Indemnizaciones

Las cuantías que en concepto de daños y perjuicios debiera satisfacer por imperativo judicial Viafirma a los suscriptores en defecto de regulación específica en los contratos o convenios, se limitan a un máximo de 13 MILLONES DE PESOS COLOMBIANOS (COP 13,000.000).

9.10 Términos de uso y duración

9.1.0.1 Términos de uso

Viafirma ECD establece en sus límites de uso las condiciones de uso de los distintos servicios de confianza prestados. Todos ellos serán informados en el Texto Divulgativo asociado a cada servicio y publicado en la página oficial https://ecd.viafirma.com.

9.1.0.2 Duración

La duración estará sujeta al tipo de servicio contratado en cada caso, y definido por tanto en los términos y condiciones de cada uno de ellos.

9.1.0.3 Supervivencia tras fin de la duración

Viafirma ECD establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, cláusulas de supervivencia, en virtud de la que ciertas reglas continúan vigentes después de la finalización de la relación jurídica reguladora del servicio entre las partes.

9.11 Avisos y comunicaciones individuales a los participantes

Viafirma ECD podrá hacer uso de notificaciones y comunicaciones realizadas de forma individual a las partes involucradas en el servicio prestado, en especial a los suscriptores, donde podrán ser notificados de forma automática ante eventos asociados a caducidades, renovaciones, etc.

9.12 Resolución de Conflictos

9.12.1 Procedimiento de conflictos

Viafirma ECD tiene previsto el uso de mecanismos jurídicos mediante los que se articule su relación con los suscriptores del servicio, los procedimientos de mediación, arbitraje

y resolución de conflictos que se consideren oportunos, todo ello sin perjuicio de la legislación de procedimiento administrativo aplicable.

9.12.2 Mecanismo y período de notificación

Se mantendrán de forma preferente los mismos canales elegidos por las partes afectadas en el conflicto.

9.12.3 Circunstancias por las que un OID puede ser modificado

No se contempla.

9.13 Disposiciones para la resolución de disputas

Las relaciones entre los suscriptores y Viafirma ECD se rigen por la normativa colombiana vigente, así como la legislación específica civil, mercantil y de protección de datos que sea aplicable.

En el caso de conflictos surgidos en relación con los servicios de prestador de confianza, las partes tratarán una resolución amistosa. En el caso de no ser posible, las partes se someten a la jurisdicción exclusiva de los tribunales de España en la ciudad de Sevilla.

De igual forma, en los Términos y condiciones del servicio de confianza expresamente contratado o consumido estarán publicados en el sitio web https://ecd.viafirma.com.

9.14 Normativa aplicable

El presente documento se ha realizado considerando, al menos, con el cumplimiento de los requisitos establecidos por la Ley 527 de 1999 de Firmas Digitales en Colombia, para los criterios específicos de acreditación de entidades de certificación digital recogidos en CEA-3.0-07. Del mismo modo, se han considerando los siguientes estándares tecnológicos:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers.
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 422: Time-stamping protocol and timestamp token profiles.
- RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs).
- RFC 3126 Electronic Signature Formats for long term electronic signatures.
- RFC 5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification.
- Protocolo ANSI ASC X9.95.
- ETSI TS 101 861 V1.2.1 Time stamping profile.
- Hora oficial de Colombia, provista por el Instituto Nacional de Meteorología.
- Los servidores se mantienen actualizados con la escala de tiempo internacional UTC, mediante sincronización a través del protocolo NTP v4, conforme al Instituto nacional de metrología (INM), y debe tener otro punto de sincronización ya sea por coordenadas establecidas en la plataforma.
- ETSI TS (EN) 102 023 Policy requirements for time-stamping authorities.

9.15 Cumplimiento de la normativa aplicable

Viafirma ECD declara que la presente política de certificado cumple con lo dispuesto en Ley 527 de 1999 de Firmas Digitales en Colombia, y de forma específica los requisitos específicamente definidos en los capítulos 10.5.2 “Requisitos generales para las ECD” y 10.9.1 “estándares y prácticas no admisibles” recogidos en el CEA-3.0-07.

9.16 Otras disposiciones

- Reglamento (UE) 2024/1183, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (eIDAS).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

9.17 Otras provisiones

Dando cobertura a cualquier eventualidad que haga colisionar algunas de las disposiciones definidas en la documentación reguladas por la presente pol´litica, se tendrá en consideración como criterio de prioridad el siguiente orden de documentos.

- La PC (política de certificado o servicio explícita),
- La DPC (declaración de prácticas de certificación - CPS en inglés),
- Límites de uso y condiciones del servicio explícitamente contratado.