Política de Certificados de Viafirma Dominicana

Policy OID 1.3.6.1.4.1.27395.6.2.8.3

QUALIFIED CERTIFICATE FOR TSU

ÍNDICE

CONTROL DE DOCUMENTO

Título:	Política de Certificados de Viafirma Dominicana Policy OID 1.3.6.1.4.1.27395.6.2.8.3		
Asunto:	QUALIFIED CERTIFICATE FOR TSU		
Estado:	Aprobado		
Versión:	1.0		
Código:	CP-VIAFIRMA-DO-TSU-QSCD		29-03-2022
Idioma:	Castellano	**Revisión anterior:**	-
		Núm. Páginas:	57

CONTROL DE CAMBIOS Y VERSIONES		
Fecha	**Versión**	**Motivo del Cambio**
29-03-2022	1.0	Primera versión.

ACERCA DEL DOCUMENTO

Este documento, con nivel de seguridad público, es propiedad de Avansi SRL (**Viafirma Dominicana)**. Para más información contacte con:

Avenida Lope de Vega #19

Edificio PIISA A. Suite 102. Ensanche Naco

Santo Domingo, República Dominicana

Teléfono: + 1 809-682-3928

psc@viafirma.com

www.viafirma.do

1. INTRODUCCIÓN

1.1. Resumen

Avansi S.R.L., es la filial dominicana de Viafirma S.L., empresa española especializada en soluciones de firma digital.

Avansi arranca su actividad en la República Dominicana el 18 de julio de 2005. Al igual que su empresa matriz, Avansi se presenta como una empresa netamente de servicios, especializada en el segmento telemático de la administración para el ciudadano y en la firma digital.

Con este claro objetivo, en el año 2006, Avansi obtiene del **Instituto Dominicano de Telecomunicaciones (Indotel)** la distinción de ser **la primera Entidad de Certificación en la República Dominicana** capacitada legalmente para emitir certificados digitales según contempla la Ley 126-02 de Comercio Electrónico (Resolución Nº 166-06).

En la actualidad **Avansi** cuenta con dos líneas de negocio:

- Como Entidad de Certificación, **Avansi** está autorizada a prestar los servicios de emisión, administración, registro y conservación de certificados digitales. Asimismo está habilitada por el Indotel para constituir Unidades de Registro.

- Como filial de Viafirma España, está especializada en el desarrollo y comercialización para toda Latinoamérica de soluciones relacionadas con la firma digital y electrónica: identidad digital, autenticación, firma biométrica, movilidad, etc. Sus soluciones destacan por un elevadísimo nivel de seguridad y usabilidad y una enorme capacidad de adaptación a la necesidades específicas de sus clientes. Se comercializan bajo la marca Viafirma.

Tras Avansi S.R.L. se encuentra todo el equipo del grupo Viafirma, con más de 20 años de experiencia innovadora, cuyo lema es la FIRMA UNIVERSAL.

Avansi en la actualidad opera bajo la marca comercial Viafirma, registrada debidamente en la Oficina Nacional de la Propiedad Industrial de República Dominicana (ONAPI) desde el 6 de abril de 2021.

A lo largo de los siguientes capítulos de las presentes Políticas de Certificación nos referiremos a Åvansi como Viafirma, a todos los efectos como Prestador regulado.

1.2. Identificación del Documento

Este documento está estructurado acorde al RFC3647, con el nombre **QUALIFIED CERTIFICATE FOR TSU**, codificado con el código **CP-VIAFIRMA-DO-TSU-QSCD**, y disponible en la url https://cps.viafirma.do/.

Las presentes políticas de certificado están identificadas con el OID número **1.3.6.1.4.1.27395.6.2.8.3**.

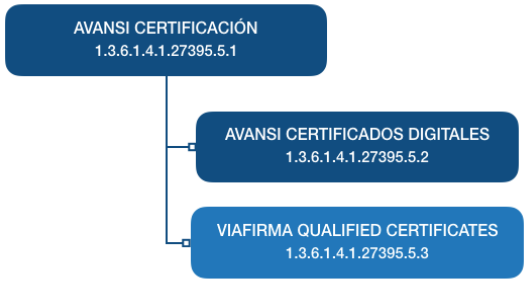
1.3. Participantes

Se consideran las siguientes partes intervinientes:

- **Avansi (Viafirma)**, Autoridad de Certificación (CA), que emite el certificado y actúa como Autoridad de Certificación autorizada por el INDOTEL, en adelante Prestador Cualificado de Servicios de Confianza o VIAFIRMA PCSC.
- **Suscriptor**: persona física 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

La Autoridad de Certificación de Viafirma que emite el certificado digital regulado en esta política es VIAFIRMA QUALIFIED CERTIFICATES, queda definida y regulada por su Autoridad de Certificación raíz AVANSI CERTIFICACIÓN.



1.3.2. Autoridades de Registro

El servicio ofrecido por la TSA de Viafirma no contempla la gestión de Autoridades de Registros para la emisión de certificado de sellos de tiempo (TSU). La generación del único Certificado de TSU se realiza mediante procedimiento único y no delegado en Autoridades de Registro. No obstante, en cada una de las Políticas de Certificados disponibles se definirá y regularán las Autoridades de Registro autorizadas.

1.3.3. Suscriptores

Será considerado suscriptor de un certificado TSU emitido por Viafirma TSA 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, incluyendo al menos el contrato de servicio y los términos y condiciones.
- Deben comprobar el estado de revocación del certificado utilizado para emitir el sello de tiempo.
- Deben disponer de sistemas de generación de sellos de tiempo adecuados a los estándares técnicos.
- Deben utilizar los sellos para los usos permitidos por la política.

1.3.4. Terceros que confían

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

a) Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.

b) 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.

c) 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

El uso de un certificado de TSU para la firma de sellos de tiempo.

1.4.2. Usos prohibidos del certificado

No se podrá usar un certificado de TSU para autenticar o cifrar.

1.5. Administración de Políticas

1.5.1. Autoridad de políticas

La autoridad de políticas está compuesta por roles de confianza de la compañía y debidamente registrados en acta.

1.5.2. Contacto de la autoridad de políticas

Avenida Lope de Vega #19
Edificio PIISA A. Suite 102. Ensanche Naco
Santo Domingo, República Dominicana
Teléfono: + 1 809-682-3928
psc@viafirma.com
www.viafirma.do

1.5.3. Persona que determina la idoneidad 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 modificado. 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 cambio que afecte a éstas será debidamente notificada tal y como se recoge en el capítulo 2.3 de las presentes políticas.

1.6. Definiciones y Acrónimos

- CA: Certificate Authority.
- CP: Certificate Policy.
- CPS: Certificate Practice Statement.
- eIDAS: electronic IDentification, Authentication and trust Services (Reglamento UE 910/2014).
- HSM: Hardware Security Module, módulo de seguridad hardware.
- INDOTEL: Instituto Dominicano de la Telecomunicaciones.
- ONAPI: Oficina Nacional de la Propiedad Industrial.
- NTP: Network Time Protocol.
- OID: Object identifier, identificador de objeto único.
- PKI: Public Key Infrastructure, iInfraestructura de clave pública.
- PSCC: Prestador de Servicios de Certificación Cualificada.
- VIAFIRMA PCSC: Prestador Cualificado de Servicios de Confianza.
- QSCD: Qualified Signature Creation Device.
- QTSP: Qualified Trust Services Provider (PSC cualificado).
- ROA: Real Instituto y Observatorio de la Armada.

- SGSI: Sistema de Gestión de la Seguridad de la Información.
- TSA: TimeStamp Authority, Autoridad de Sellado de Tiempo.
- TSP: TimeStamping 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 publicará las claves públicas de toda su cadena de confianza en el sitio web https://cps.viafirma.do/. Y de forma explícita en las siguientes direcciones:

Root-CA:

https://cps.viafirma.do/AVANSICERTIFICACION.crt

SubCA VIAFIRMA QUALIFIED CERTIFICATES:

https://cps.viafirma.do/VIAFIRMAQUALIFIEDCERTIFICATES.crt

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

http://crl.viafirma.do/rootca.crl

http://crl2.viafirma.do/rootca.crl

http://ocsp.viafirma.do

http://crl.viafirma.do/viafirmasub.crl

http://crl2.viafirma.do/viafirmasub.crl

2.2. Publicación de la información de certificación

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

https://cps.viafirma.do/CP-VIAFIRMA-DO-TSU-QSCD.pdf

2.3. Frecuencia de publicación

Cualquier versión que actualice la presente política de certificados será publicada en el sitio web https://cps.viafirma.do/ 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, los cambios en la presente política de certificado serán notificados acorde al procedimiento establecido por el correspondiente órgano regulador, INDOTEL.

En cuanto a la frecuencia de publicación de las CRLs de la presente Política de Certificados será de 96 horas.

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. IDENTIFICACION 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.

El distinguished name se incluye en el campo Common Name (CN) y se corresponde con el nombre de la Unidad de la Autoridad de Sello de tiempo autorizada por Viafirma Dominicana, por ejemplo, VIAFIRMA DO TSA. No tendrá que coincidir con un identificador único tipo CIF o similar.

3.1.2. Significado de los nombres

El nombre utilizado para identificar al certificado tendrá que ser semántico.

3.1.3. Seudónimos

No se permite el uso de seudónimos en los certificados emitidos bajo esta política.

3.1.4. Reglas para interpretar varios formatos de nombre

El nombre elegido para identificar a la TSA, y aque aparecerá en el Common Name del certificado de TSU, tendrá que ser semántico y estar asociado a la Organización a la que representa. En el contexto de la presente política de certificado el nombre utilizado para la identificación de la TSA será “VIAFIRMA DO TSA”.

3.1.5. Unicidad de nombres

En el propósito y alcance de la presente política no contempla emisiones masivas de certificados de TSU, por lo que el cumplimiento de unicidades de nombre no implicará mayores esfuerzos durante la fase de revisión previa a la emisión. Al mismo tiempo, la configuración del perfil de certificado incluye entre sus reglas la prohibición de emitir dos certificados con el mismo DN.

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 y/o Avansi, 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 oficiales:

En la República Dominicana:

ONAPI (Oficina Nacional de la Propiedad Intelectual)
Titular: Avansi, S.R.L.
Tipo de Registro: Nombre Comercial
Nombre comercial registrado: VIAFIRMA
Número de Registro: 625895

ONAPI (Oficina Nacional de la Propiedad Intelectual)

Titular: Avansi, S.R.L.
Tipo de Registro: Marca Mixta
Marca registrada: AVANSI
Número de Registro: 260513

ONAPI (Oficina Nacional de la Propiedad Intelectual)

Titular: Avansi, S.R.L.
Tipo de Registro: Marca Mixta
Marca registrada: VIAFIRMA

Número de Registro: 260514

En Europa:

EUIPO - European Union Intellectual Property Office

EUTM File Info **011204617**

https://euipo.europa.eu/eSearch/#details/trademarks/011204617

OEPM – Oficina Española de Patentes y Marcas:

Exp **M4026263**

http://consultas2.oepm.es/ceo/jsp/busqueda/consultaExterna.xhtml?numExp=M4026263

3.2. Validación de identidad inicial

3.2.1. Métodos de prueba de la posesión de la clave privada

No se contempla este procedimiento en la presente política. La emisión de un certificado de TSU se realizará mediante procedimientos internos.

3.2.2. Autenticación de la identidad de una organización

No se contempla este procedimiento en la presente política. La emisión de un certificado de TSU se realizará mediante procedimientos internos.

3.2.3. Autenticación de la identidad de un individuo

No se contempla este procedimiento en la presente política. La emisión de un certificado de TSU se realizará mediante procedimientos internos.

3.2.4. Información no verificada del suscriptor

No se contempla este procedimiento en la presente política. La emisión de un certificado de TSU se realizará mediante procedimientos internos.

3.2.5. Validación de la autoridad

No se contempla este procedimiento en la presente política. La emisión de un certificado de TSU se realizará mediante procedimientos internos.

3.2.6. Criterios de interoperabilidad

No se contempla este procedimiento en la presente política. La emisión de un certificado de TSU se realizará mediante procedimientos internos.

3.3. Identificación y autenticación para la renovación de certificados

3.3.1. Identificación y autenticación para la renovación de certificado vigente

No se contempla este procedimiento en la presente política. La emisión de un certificado de TSU se realizará mediante procedimientos internos.

3.3.2. Identificación y autenticación para la renovación un certificado caducado

No se contempla este procedimiento en la presente política. La emisión de un certificado de TSU se realizará mediante procedimientos internos.

3.4. Identificación y autenticación para solicitudes de revocación

El certificado de TSU regulado en la presente política es emitido a nombre de Viafirma Dominicana, por lo que no se contemplan solicitudes externas para la revocación del mismo. Se cuenta por tanto con un procedimiento interno, que prevé los distintos casos autorizados para poder revocar el certificado, y que serán llevados a cabo por miembros y roles de confianza de Viafirma Dominicana.

4. CICLO DE VIDA DEL CERTIFICADO Y REQUISITOS OPERACIONALES

4.1. Solicitud de Certificados

Viafirma QTSP no contempla la solicitud externa de certificados de TSU. La solicitud, emisión y gestión del mismo está destinada a uso interno acorde a los procedimientos internos de gestión del servicio cualificado de sello de tiempo.

4.1.1. Quién puede solicitar un certificado

No aplica.

4.1.2. Proceso de registro

No aplica.

4.2. Proceso de solicitud de un certificado

Viafirma QTSP no contempla la solicitud externa de certificados de TSU. La solicitud, emisión y gestión del mismo está destinada a uso interno acorde a los procedimientos internos de gestió del servicio cualificado de sello de tiempo.

4.2.1. Funciones de identificación y autenticación

No aplica.

4.2.2. Aprobación o rechazo de solicitudes

No aplica.

4.2.3. Plazos del proceso de solicitud

No aplica.

4.3. Emisión de certificados

4.3.1. Acciones de la CA durante la emisión de certificados

La CA 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

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

4.4. Aceptación del certificado

4.4.1. Hechos que constituyen la aceptación del certificado

La emisión del certificado de TSU regulado en la presente política se entenderá por aceptado tras la formalización de la ceremonia de creación de claves del certificado de TSA, en presencia de distintos roles de confianza autorizados por la Autoridad de Políticas.

4.4.2. Publicación del certificado por parte de la CA

La clave pública del certificado de TSU emitido por Viafirma QTSP quedará publicada en el sitio

web https://cps.viafirma.do, y en concreto en la siguiente dirección:

https://cps.viafirma.do/CP-VIAFIRMA-DO-TSU-QSCD.cer

4.4.3. Notificación de la emisión a otras entidades

La CA 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 por Viafirma QTSP podrá ser usada acorde al alcance y limitaciones para el que fueron emitidos, tal y como se recoge en los términos y uso del servicio

de sello de tiempo.

4.5.2. Confianza y uso de la clave pública

Será obligación de los terceros que confían en las claves públicas de la CA, 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

Al tratarse de un certificado de TSU, no sujeto al público en general, la renovación del certificado de TSU podrá inciarse según lo previsto en los procedimientos internos de Viafirma para la gestión de los servicios de confianza.

4.6.2. Quién puede solicitar la renovación

No se contempla la solicitud externa de certificados de TSU de esta CA.

4.6.3. Proceso de solicitudes de renovación

No se contempla la solicitud externa de certificados de TSU de esta CA.

4.6.4. Notificación de la renovación del certificado al suscriptor

No se contempla la solicitud externa de certificados de TSU de esta CA.

4.6.5. Hechos que constituyen la aceptación del certificado renovado

No se contempla la solicitud externa de certificados de TSU de esta CA.

4.6.6. Publicación del certificado renovado

La clave pública del certificado de TSU emitido por Viafirma QTSP quedará publicada en el sitio

web https://cps.viafirma.do, y en concreto en la siguiente dirección:

https://cps.viafirma.do/CP-VIAFIRMA-DO-TSU-QSCD.cer

4.6.7. Notificación de la renovación a otras entidades

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

4.7. Reemisión del Certificado

4.7.1. Circunstancias para la reemisión del certificado

VIAFIRMA PCSC 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 PCSC 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 PCSC 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 PCSC 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 PCSC 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 PCSC 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 PCSC 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 PCSC 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 PCSC 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 PCSC 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 PCSC 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 PCSC 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 PCSC 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 PCSC 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

Viafirma PCSC activará los procedimientos establecidos para la revocación de su certificado de TSU en caso de compromiso de claves, cambios significativos en los datos contenidos en el certificado, por ejemplo cambio de razón social, o bien, o ante un compromiso de algunos de los algoritmos utilizados para su generación.

4.9.2. Quién puede solicitar la revocación

No se contemplan solicitudes externas a Viafirma PCSC.

4.9.3. Proceso para la revocación del certificado

La renovación del certificado de TSU podrá inciarse según lo previsto en los procedimientos internos de Viafirma QTSP para la gestión de los servicios de confianza.

4.9.4. Período de gracia de la solicitud de revocación

VIAFIRMA PCSC 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

Al tratarse de un procedimiento interno de Viafirma QTSP, no sujeto a solicitudes externas, el proceso de revocación tendrá efecto inmediato.

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

Las distintas fuentes de verificación de certificados publicadas por VIAFIRMA PCSC 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 96 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 PCSC publica un servicio de validación online de sus certificados a través del protocolo OCSP y disponible en https://ocsp.viafirma.do/ocsp.

4.9.10. Requisitos para la comprobación online del estado de revocación

VIAFIRMA PCSC 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 PCSC podrán ser verificados a través de las distintas CRLs publicadas e informadas en sus respectivos certificados.

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 PCSC 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 PCSC no permite entre sus procedimientos la suspensión de certificados.

4.9.14. Quién puede solicitar la suspensión

VIAFIRMA PCSC no permite entre sus procedimientos la suspensión de certificados.

4.9.15. Procedimiento para la solicitud de suspensión

VIAFIRMA PCSC no permite entre sus procedimientos la suspensión de certificados.

4.9.16. Límites del período de suspensión

VIAFIRMA PCSC no permite entre sus procedimientos la suspensión de certificados.

4.10. Servicios para la comprobación del estado del certificado

4.10.1. Características operacionales

VIAFIRMA PCSC 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 Viairma Fortress.

4.10.2. Servicios disponibles

VIAFIRMA PCSC 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 Viairma Fortress.

4.10.3. Características opcionales

VIAFIRMA PCSC 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 Viairma Fortress.

4.11. Fin de la suscripción

Lo establecido en las Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

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 PCSC.

4.12.2. Prácticas de encapsulado y recuperación de recuperación de claves

Lo establecido en las Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5. INSTALACIÓN, GESTIÓN Y CONTROLES OPERACIONALES

5.1. Controles físicos

Lo establecido en las Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.1.1. Localización y construcción

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.1.2. Acceso físico

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.1.3. Alimentación eléctrica y aire acondicionado

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.1.4. Exposición al agua

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.1.5. Protección y prevención de incendios

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.1.6. Sistema de almacenamiento

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.1.7. Eliminación de residuos

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.1.8. Backup remoto

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.2. Controles procedimentales

5.2.1. Roles de confianza

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC, 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. 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 la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.2.3. Identificación y autenticación para cada rol

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.2.4. Roles que requieren separación de funciones

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.3. Controles personales

5.3.1. Requisitos de calificación, experiencia y autorización

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.3.2. Procedimientos de verificación de antecedentes

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.3.3. Requisitos de formación

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.3.4. Requisitos y frecuencia de formación

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.3.5. Frecuencia y secuencia de rotación de tareas

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.3.6. Sanciones por acciones no autorizadas

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.3.7. Requisitos para personal independiente

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.3.8. Documentación entregada al personal

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.4. Procedimientos para el registro de auditoría

5.4.1. Tipo de eventos registrados

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.4.2. Frecuencia del procesamiento de registros

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.4.3. Período de retención del registro de auditoría

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.4.4. Protección del registro de auditoría

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.4.5. Procedimiento del backup del registro de auditoría

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.4.6. Sistema de recolección de auditoría

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.4.7. Notificación de eventos

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.4.8. Evaluación de vulnerabilidades

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.5. Archivo de registros

5.5.1. Tipos de archivo de registros

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.5.2. Período de retención del archivo

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.5.3. Protección del archivo

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.5.4. Procedimientos para el backup del archivo

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.5.5. Requisitos para el sellado de tiempo del registro

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.5.6. Sistema de recolección del archivo

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.5.7. Procedimientos para obtener y verificar la información del archivo

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.6. Cambio 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. Procedimientos para la gestión de incidentes

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.7.2. Obsolescencia y deterioro

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.7.3. Procedimientos ante compromiso de clave de una entidad

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.7.4. Plan de continuidad de negocio ante desastres

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

5.8. Cese de la CA o RA

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

6. CONTROLES TÉCNICOS DE SEGURIDAD

6.1. Generación del par de claves y su instalación

6.1.1. Generación del par de claves

La generación del par de claves de un certificado de TSU, acorde a las presentes políticas, es llevada a cabo bajo un procedimiento denominado "Ceremonia de Claves", incluido entre los procedimientos internos de Viafirma PCSC.

6.1.2. Entrega de la clave privada al suscriptor

La clave privada del certificado es generada y almacenada en un módulo criptográfico (HSM) FIPS 140-2 Level 3 EAL4+ gestionado por VIAFIRMA PCSC.

6.1.3. Entrega de la clave pública al suscriptor

La clave pública del certificado emitido será publicada en el sitio web de VIAFIRMA PCSC 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 la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

6.1.5. Tamaño de las claves

Con carácter general, el tamaño de las claves generadas por VIAFIRMA PCSC 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 estarán asociados a la configuración definida en los CERTIFICATE PROFILE y END ENTITY PROFILES de la PKI de VIAFIRMA PCSC.

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 de TSU sujeto a la presente política, será Digital Signature y Non-Repudiation, además de la extensión "Time Stamping" (1.3.6.1.5.5.7.3.8).

6.2. Protección de clave privada y controles del módulo criptográfico

6.2.1. Controles y estándares del módulo criptográfico

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

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

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

6.2.3. Depósito de la clave privada

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

6.2.4. Backup de la clave privada

El backup de la clave privada del certificado coincide con lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

6.2.5. Archivo de la clave privada

El archivo de la clave privada del certificado coincide con lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

6.2.6. Importación de la clave privada al módulo criptográfico

La importación de la clave privada del certificado coincide con lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

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 la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

6.2.8. Método de activación de la clave privada

La activación de la clave privada del certificado coincide con lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

6.2.9. Método de desactivación de la clave privada

No se contemplan procedimientos de desactivación de claves.

6.2.10. Método de destrucción de la clave privada

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 dispositivo HSM.

6.2.11. Clasificación del módulo criptográfico

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

6.3. Otros aspectos sobre la gestión de par de claves

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. Periodos operativos de certificado y periodos de uso del par de claves

La validez de la clave pública del certificado de TSU será de 5 años, mientras que el valor operativo de su clave privada será de 3 años.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Los procedimientos de generación de datos para la activación se lleva a acabo acorde a los procedimientos definidos en sus respectivas ceremonias de clave y conforme con las normas ETSI EN 319 421.

Parte de estos datos de activación son generados individualmente por los distintos roles de confianza que participan en las ceremonias de creación y activación de claves.

6.4.2. Protección de los datos de activación

Los roles de confianza involucrados en la generación de datos para la activación de claves siguen un procedimiento interno de VIAFIRMA PCSC por el que se registra y audita el proceso de creación, almacenamiento y uso de los soportes que contienen los datos utilizados para la activación de claves.

Además, se cuenta con un depósito por duplicado, a cargo de más de un rol de confianza por si fuese necesario su uso en caso de fuerza mayor o indisponibilidad del custodio principal del dato.

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 la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

6.5.2. Clasificación de la seguridad

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

6.6. Ciclo de vida de los controles técnicos

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

6.7. Controles de seguridad de red

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

6.8. Sello de tiempo

Viafirma PCSC presta el servicio cualificado de sello de tiempo a través de su TSA y sus correspondientes certificados TSU emitidos bajo la presente política de certificado.

El servicio de sellado de tiempo se emite acorde a lo establecido en la norma ETSI EN 319 421 Anexo B, incorporando entre sus mecanismos de seguridad el control de desfase horario para asegurar que la desviación no supere los umbrales establecidos en la correspondiente políticas de sello de tiempo.

La validación de los sellos de tiempo firmados por certificados de la presente política pueden ser validados en las siguientes fuentes de validación:

- http://ocsp.viafirma.do
- http://crl.viafirma.do/viafirmasub.crl
- http://crl2.viafirma.do/viafirmasub.crl

También se cuenta con mecanismos de seguridad para el control y monitorización del consumo del servicio a través de credenciales seguras y bajo controles para evitar ataques de fuerza bruta.

La política de emisión del sellos cualificado de tiempo emitido por Viafirma QTSP queda identificada en el OID 0.4.0.2023.1.1 del sello.

La emisión de los sellos de tiempo cuenta con un desfase inferior a un segundo contemplado en ETSI EN 319 421. Para ello se utilizan fuentes de tiempo stratum 1, concretamente UTC(ROA), mediante protocolo NTP.

Todas las características técnicas del sellado de tiempo quedan definidas y publicadas en los Términos y Condiciones TSA Viafirma disponible en el sitio https://qtsp.viafirma.com y en concreto en la siguiente dirección: https://cps.viafirma.do/TERMS-VIAFIRMA-DO-TSU-QSCD.pdf.

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

El perfil asociado al certificado de TSU regulado en la presente política cuenta con las siguientes extensiones:

Subject Name	
Country	*<DO>*
Organization	*<ORGANIZATION NAME>*
Organizational Unit	*<OU NAME>*
Common Name	*<TSA NAME>*
Other Name	*<VATDO>*

7.1.3. Identificador (OID) del algoritmo de firma

SHA-256 with RSA Encryption (1.2.840.113549.1.1.11).

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

Extension	Certificate Policies (2.5.29.32)
Critical NO	
Policy ID #1	(0.4.0.194112.1.2)
Policy ID #2	(1.3.6.1.4.1.27395.6.2.8.3)

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 PCSC, y debidamente informada en el OID 2.5.29.31 "CRL Number" de la estructura de la CRL.

7.2.2. CRL y extensiones

Extensiones disponibles acorde al estándar X.509 CRL Number (2.5.29.31) y Authority Key Identifier (2.5.29.35).

7.3. Certificado OCSP

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

7.3.1. Certificado utilizado para firmar el OCSP que valida el certificado de la SUBCA

Disponible en:

https://cps.viafirma.do/AVANSICERTIFICACION.pem

AVANSI CERTIFICACION

Subject Name
- Country or Region DO
- Locality DISTRITO NACIONAL - REPUBLICA DOMINICANA
- Organisation AVANSI S.R.L. - RNC 130222509
- Common Name AVANSI CERTIFICACION

Issuer Name
- Country or Region DO
- Locality DISTRITO NACIONAL - REPUBLICA DOMINICANA
- Organisation AVANSI S.R.L. - RNC 130222509
- Common Name AVANSI CERTIFICACION

Serial Number 3655751313016107516
Version 3
Signature Algorithm SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
- Parameters None

Not Valid Before Wednesday, 16 May 2012 at 10:48:31 Central European Summer Time
Not Valid After Friday, 16 May 2042 at 10:48:31 Central European Summer Time

Public Key Info
- Algorithm RSA Encryption (1.2.840.113549.1.1.1)
- Parameters None
- Public Key 512 bytes: C1 DD 5E 9C E0 B4 3F 50

DD A6 16 1E 80 E4 7D 7F 31 21 BF B1 3B 3B BB 23 76 1D E9 6F 0D DF 5B A0 F4 87 3D 8A FA 31 CB 43 DE 3C
CF 33 60 CB FF 15 3B 0D EB A0 F8 2F 11 0C E2 94 C9 CC 6A 84 33 4B F7 A2 C4 1A 14 D4 E9 7D D0 37 A0 1C A1
2A 32 07 EC 37 09 22 E9 76 6E 84 09 A8 E6 BA 27 56 8B 56 B6 DF 91 EC 20 12 49 42 89 1B 36 AC 0F 9F 6A D6
DD 87 CE EE 42 A6 5A D8 D9 BD 96 80 48 28 2A D7 3A F9 C0 48 36 B4 DE 46 77 3F AF 56 31 2D 37 89 C8 B7
B8 7E DC 3D DC D9 64 21 A4 7F 8E 60 84 0C 6F 76 6D 7B 3C 24 F4 65 E5 7C BE 9E 22 AE CE 1C F4 11 68 2E 97
3C B3 86 26 4E 49 F6 18 6A 74 24 BD F3 C7 E3 80 42 37 67 D0 5E 80 0F 25 7D D4 D3 73 85 12 06 76 53 45 B1

50 E3 45 F8 64 4C 91 81 CD 9E CA 26 09 4B F7 D9 88 9D F3 1E 38 C5 95 88 EC 9C CD F3 AB A0 4B 0B 83 A2 82 C9 18 4A 49 A3 60 F1 23 3A 6C 0E 8E C5 A0 A2 F5 51 43 A0 5E ED 24 FA E8 0B B0 63 B7 CB 93 C5 E6 5E 41 41 4A 7A 7E AA FE 96 A3 F2 C6 55 F8 02 2C C2 A5 1C 51 F0 D6 E8 9E 24 15 58 82 DB 1A A5 87 FE 33 F1 D0 69 DA DB F1 03 83 DD 1C 7C 90 C8 F8 2B 2D 4A 27 C0 68 99 28 04 A1 02 DD 1B FE D7 69 05 4E 70 71 0D 8C 01 D6 DF 1B E8 1D 1C 8C A8 3C BA 7A 61 D5 24 F2 7F D3 17 5A 9C C4 24 3F 63 34 96 B0 3F 61 36 D8 83 1B EF EE F7 B8 10 F4 30 C9 AB 1F 40 41 BD A0 98 DB 9A CE B1 F2 77 C3 CF 39 8E D4 88 3A 36 D5 EC DE BB D6 03 69 FE 73 FE FB CF 1A 7E E8 20 44 AD 79 A5 E1 FF AC 20 BE 11 F8 25 21 BE A1 D4 4B 10 8D B2 AD E3 E9 25 BF FE D8 06 B1 EC 13 F5 49 21 D3 99 3D CB 8E 82 6B BC 1F 04 91 92 74 51 51 E7 DD 12 5E 1D 0C 93 64 3A CF 7F B5 52 6F 8B 6E EC 1E DE 00 BE CC E1 D6 93 F1 D2 4D 18 2E EF

Exponent 65537

Key Size 4.096 bits

Key Usage Verify

Signature512 bytes: 1C 65 58 00 92 3E 66 8F

29 C1 74 07 65 F9 3E 73 2C BE B4 8C 8D 6A 69 E1 BA AB 6B E2 1D C9 90 B4 0A F9 96 7D 92 CF FD CD 8D 58 DF 79 0F 3B E8 84 87 7E 13 D7 BD A3 0D 3F 5A 91 93 06 89 9C E9 96 BC 10 D6 3E 04 FC F2 F3 B1 A1 FF 24 A5 B9 C3 F3 0D AB A9 CA 32 41 36 EC 78 32 74 AC FA 29 34 2C B1 38 7B FA EC A4 30 65 8A 25 C5 F5 DE AC 5A DC FC 89 FB EC 70 11 9B 9B 56 D4 6A A8 CD 5D 49 85 4B A7 06 45 AF 64 F2 7F 65 B7 FA B2 F6 E6 A2 93 65 CA 4B 41 25 9B 2B 06 A5 92 B9 85 37 42 97 78 84 A3 96 92 80 67 65 80 38 43 B3 8A 1C B2 20 BE 80 20 E0 56 57 66 3F F5 FD BF 49 3A C7 96 83 D6 74 AB B3 EE 30 E5 54 76 11 67 CE 98 54 A6 D2 04 23 F5 AA A8 02 CF 3A 53 30 B1 08 1A 24 71 A2 8A 26 48 33 50 0A A8 C5 B6 72 1C 3D E3 18 EE E8 11 21 9F 46 98 F8 BE FB 42 C7 F5 34 D4 7D 61 97 15 4B 8F 16 1C 35 B7 E2 F1 3E E2 D8 A3 9F C8 BD A7 B8 3D 97 24 61 A9 81 B4 6D C3 98 33 2F AE EC 2E 0D 14 64 CD 2C FE 21 4D AE 81 DD 60 46 78 36 44 78 10 DB EC C1 DB FF 3D EE C0 A8 7F 26 2F 34 44 02 C7 F1 9D 5F C1 48 39 37 50 6F EF 69 E2 77 34 05 FC D1 0A 0F F0 19 A1 CE D7 BB 01 D8 A0 71 DE D6 5E 57 12 36 80 DF AE 35 FF 5D 6F 0E 64 DA 6D EE 43 C9 16 55 21 15 1C 97 5A 33 E2 50 D7 CE B3 62 B8 C6 A7 B2 33 84 3B C8 45 BD A6 03 FB A5 C3 26 7E A0 EA 21 79 B1 5C DC BF 23 53 D9 F7 C7 1A 14 91 26 CC 65 48 95 E2 E0 AD 54 CC 2E D4 AD 58 98 78 AC A2 CE 49 37 98 C9 12 71 BB FF 3F ED 6B 50 4A 0F CE 2A FF C4 DA 7E 7B 6F B9 1E 76 CF EE E8 DC 0B D5 55 36 37 A8 60 70 9F 70 28 86 4D B0 A0 D0 50 7C 22 78 8A 9C 84 3A 39 2C D4 28 54 C9 0B 10 B6 6E 4F BD 60 A3 84 DA 1A 97 82 F2 F0 7B

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 1

Extension Subject Key Identifier (2.5.29.14)

Critical NO

Key ID 15 38 05 14 6F 12 69 93 C8 2A E7 BA 5B A6 F9 C7 A2 31 A4 FB

Extension Certificate Policies (2.5.29.32)

Critical NO

Policy ID #1 (1.3.6.1.4.1.27395.5.1)

Qualifier ID #1 Certification Practice Statement (1.3.6.1.5.5.7.2.1)

CPS URI http://cps.avansi.com.do

Fingerprints

SHA-256 68 20 B7 51 4B 24 38 C2 4A E3 B5 DD B6 97 C0 8F BD 57 0C 20 5D 47 EA 07 3D 5D DF C6 17 D3 24 CB

SHA-1 77 8C 7A 2F 8B 77 25 71 6C C7 FF FE D3 3B 58 A4 93 F5 0F 59

7.3.2. Certificado utilizado para firmar el OCSP que valida el certificado regulado esta política

Disponible en:

https://cps.viafirma.do/OCSP_VIAFIRMA_QUALIFIED_CERTIFICATES.pem

OCSP VIAFIRMA QUALIFIED CERTIFICATES

Subject Name
- Country or Region DO
- Organisation AVANSI SRL
- Organisational Unit VIAFIRMA DOMINICANA
- Serial Number RNC 130222509
- Common Name OCSP VIAFIRMA QUALIFIED CERTIFICATES

Issuer Name
- Country or Region DO
- Organisation AVANSI SRL
- Organisational Unit VIAFIRMA DOMINICANA
- Serial Number RNC 130222509
- Common Name VIAFIRMA QUALIFIED CERTIFICATES

Serial Number 53 3F 4E DE F4 AB 30 62 24 3F 28 0D E7 8F B3 9F 6E 35 3C 95
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
- Parameters None

Not Valid Before Monday, 10 May 2021 at 09:56:38 Central European Summer Time
Not Valid After Wednesday, 10 May 2023 at 09:56:38 Central European Summer Time

Public Key Info
- Algorithm RSA Encryption (1.2.840.113549.1.1.1)
- Parameters None
- Public Key 256 bytes: C2 AB 96 FC C8 1D 3E 03

D5 D0 DA 58 CE 0A 27 E5 5C 45 D6 A1 F8 70 96 A5 20 B9 3F 45 5D 9A CF 3B 0C BC 47 B8 DB 88 7F 62 B3 BF 19 B5 CF 85 5D 41 A7 DC 72 73 2B 5A BD 42 A5 75 C5 8A 64 99 C2 4A 91 1B 74 AA B9 40 3B 27 DE 51 77 91 17 DA 79 0C 4C 01 CE F8 F9 D7 85 01 92 2D 1F C5 2A 0C D9 EC BF 60 40 F2 D1 60 2F 52 EA F8 BF A3 21 5F 8C B9 0E B9 F0 BE 32 64 39 99 41 7D 03 58 F4 21 D4 08 06 1A 3A 43 E6 FD BD 1C 58 46 18 4F 4D C3 DC C0 D3 B0 A7 6A 3E A4 77 C6 F5 3D 0D 6B 3D 21 6D F4 73 B5 73 60 C4 EC F3 DD AA C6 C4 7D 88 F0 FD 20 1F A6 8E 18 01 FD 40 66 92 91 50 FB 9D C6 A3 5E 1E 71 AF 86 42 27 A1 87 D1 9F 61 68 34 DA 3C A2 80 AE F2 9A 60 9C 9A D1 0D 16 D8 DA 8A 2E 69 91 A2 AD CC 7F C8 0F CD 7B 30 5D 96 1C 58 D1 07 D4 5D F9 B2 47 69 1E 65 BE 47 25 30 E1 F1 8D 6A 6F

- Exponent 65537
- Key Size 2.048 bits
- Key Usage Verify

Signature 512 bytes: 17 F3 CD DF 2D 0D BA E1

C3 E0 FF D3 8B 7E 74 18 DE CE D2 50 19 6C A7 EA 4D 14 C2 4E C7 4C BF 58 B7 CC D3 88 28 AB 53 07 5B A4 17 24
B7 6D 9B 97 80 DD EE B9 54 56 C7 4F BE A3 CA 16 10 B6 CA 2D 79 88 E3 09 A3 7F B0 83 2E 72 39 BB 95 E9 4F BC
10 2A 4F EA 56 DD A2 2F 3F 16 F1 25 0A BB E4 D3 BC F7 18 CA 61 94 C6 EF 15 A6 04 CA 2D 28 A6 FB D8 FE 15 62
CF 81 44 CE 4F CC F7 26 EF 5C 62 15 B2 64 DD 8E 5C 6A 3C 7E 02 FD BA AD 71 7C A6 80 08 C7 AA F1 F0 6B A9 BB
AB 24 5D D3 26 E2 50 F9 55 FB E9 8C 49 8A F3 A2 38 E2 91 47 93 44 5F 54 79 A1 D3 86 E5 88 29 D9 76 FF F6 93 DD
73 AD 53 1F 05 E6 D3 4C 83 42 87 D9 60 C2 25 34 F0 69 55 B1 52 D7 F4 83 E6 06 72 D8 F3 EF C6 FD 8E 06 86 D5 96
EF 65 2E 11 4D B6 1C 1A 53 AE AE BC D0 D2 CC 19 97 20 6F BD DF BC 54 24 D3 7C 02 F5 21 D7 6E C6 4D 41 F4 74
AB 33 8A 56 0B 4F 21 A8 15 F1 63 EF 77 2E D7 D3 49 01 2E D8 B8 6A 23 C7 A5 96 5D 90 19 2F 5B 72 66 E7 3E A1 10
D5 92 15 61 17 B5 E3 D0 EB C5 0B 9C 63 B6 16 52 5C 89 2B 2F 53 06 1E BD EE A3 A8 56 20 B0 F0 25 1B E2 63 C4 ED
5A 32 28 9E 74 BE 08 31 EA F0 E9 05 28 5E 9D 2C 1F E8 1E AC 1A 3E 87 A2 7B 7D 9F 85 E5 2D 0E 3F 49 1F 99 CF E0
A2 1A 9E 0A 4B 72 2F EF 23 26 84 31 FC 42 AC 43 FB 56 A3 9B 5F 6E 1C FA E0 BB 8C A1 69 B7 0F FE 8F CA A2 79 B5
DB 73 38 AF EE A6 93 68 15 81 B7 59 71 6C 04 90 BE 69 1D B7 FE D0 A0 01 28 F9 D2 70 C8 6C 12 C6 69 7D DA C6
CA F1 28 B9 35 4E A4 DA 72 AB 93 BD B9 75 51 BA AB 72 A6 B4 8D DF 86 D9 54 C9 99 60 EF BD 2E C4 3F E4 C2 E8
89 7A 5A 41 FA 26 92 DD 9E 37 D0 87 F1 79 AB DD 8F 68 46 9B 26 96 CF 15 03 56 D4 3A 77 24

Extension Key Usage (2.5.29.15)
- Critical YES
- Usage Digital Signature

Extension Basic Constraints (2.5.29.19)
- Critical YES
- Certificate Authority NO

Extension Extended Key Usage (2.5.29.37)
- Critical NO
- Purpose #1 OCSP Signing (1.3.6.1.5.5.7.3.9)

Extension Subject Key Identifier (2.5.29.14)
- Critical NO
- Key ID 91 B2 C5 D2 2E B2 15 84 91 40 AA F8 66 66 7A 04 B9 76 10 B1

Extension Authority Key Identifier (2.5.29.35)
- Critical NO
- Key ID 92 C1 FC F0 DC E7 8A 73 E3 BA C5 41 95 85 D2 C5 2E 02 C0 AD

Extension OCSP No Revocation Check (1.3.6.1.5.5.7.48.1.5)
- Critical NO
- Data 05 00

Fingerprints
- SHA-256 66 CE FD 72 67 F7 AC 08 93 35 3F D4 6B AA E4 9C 76 49 B5 89 F0 2B C6 F0 7E 16 2D E8 A1 09 71 46
- SHA-1 B0 FB C3 66 B6 DA FF 14 00 87 B1 C6 AC DE 1E 9C EB 41 C5 2F

8. AUDITORÍAS

8.1. Frecuencia o circunstancias de la auditoría

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

8.2. Identidad y cualificación del auditor

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

8.3. Relación del auditor con el prestador

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

8.4. Temas tratados en la auditoría

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

8.5. Acciones a realizar como resultado de una deficiencia

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

8.6. Comunicación de resultados

Lo establecido en la Declaración de Prácticas de Certificación de Viafirma QTSP.

9. OTROS ASUNTOS LEGALES

9.1. Tarifas

9.1.1. Tarifa para la emisión y renovación de certificados

VIAFIRMA PCSC 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://www.viafirma.do.

9.1.2. Tarifa de acceso al certificado

VIAFIRMA PCSC 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://www.viafirma.do.

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 PCSC . Su uso es gratuito.

9.1.4. Tarifa para otros servicios

VIAFIRMA PCSC 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://cps.viafirma.do/, o bien, pueden ser consultados a través del formulario de contacto que se establece en la misma página.

9.1.5. Política de reembolsos

VIAFIRMA PCSC 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://cps.viafirma.do/.

9.2. Responsabilidad financiera

Lo establecido en las Declaración de Prácticas de Certificación de VIAFIRMA PCSC.

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 PCSC.

9.3.2. Alcance excluido de la información confidencial

Lo establecido en las Declaración de Prácticas de Certificación de VIAFIRMA PCSC .

9.3.3. Responsabilidad para la protección de la información confidencial

Lo establecido en las Declaración de Prácticas de Certificación de VIAFIRMA PCSC .

9.4. Privacidad de la información personal

9.4.1. Plan de privacidad

Lo establecido en las Declaración de Prácticas de Certificación de VIAFIRMA PCSC .

9.4.2. Información con tratamiento privado

Lo establecido en las Declaración de Prácticas de Certificación de VIAFIRMA PCSC .

9.4.3. Información no considerada con tratamiento privado

Lo establecido en las Declaración de Prácticas de Certificación de VIAFIRMA PCSC .

9.4.4. Responsabilidad para la protección de la información privada

Lo establecido en las Declaración de Prácticas de Certificación de VIAFIRMA PCSC .

9.4.5. Consentimiento de uso de la información privada

Lo establecido en las Declaración de Prácticas de Certificación de VIAFIRMA PCSC .

9.4.6. Divulgación de conformidad con procesos judiciales o administrativos

Lo establecido en las Declaración de Prácticas de Certificación de VIAFIRMA PCSC .

9.4.7. Otras casos para la divulgación de información

Lo establecido en las Declaración de Prácticas de Certificación de VIAFIRMA PCSC .

9.5. Derechos de propiedad intelectual

Lo establecido en las Declaración de Prácticas de Certificación de VIAFIRMA PCSC .

9.6. Obligaciones y Responsabilidad

9.6.1. Obligaciones de la CA

Lo establecido en las CPS de VIAFIRMA PCSC.

9.6.2. Obligaciones de la RA

Bajo la presente política no se contempla el uso de autoridades de registro.

9.6.3. Obligaciones del suscriptor

El suscriptor de cualquier certificado digital emitido por el PCSC 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 limites 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 PCSC:

a) 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.

b) Verificar la validez de los certificados en el momento de realizar o verificar cualquier operación basada en los mismos.

c) Asumir su responsabilidad en la correcta verificación de las firmas electrónicas.

d) Asumir su responsabilidad en la comprobación de la validez, revocación o caducidad de los certificados en que confía.

e) 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 PCSC no establece obligaciones a otras entidades participantes.

9.7. Renuncias de la garantía

VIAFIRMA PCSC 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 PCSC, 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 RA, 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

VIAFIRMA PCSC cuenta con un seguro de responsabilidad civil ajustado a los límites y condiciones establecidas por la actual normativa, y depositado en el organismo regulador INDOTEL.

9.10. Términos de uso y duración

9.10.1. Términos de uso

VIAFIRMA PCSC 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://www.viafirma.do.

9.10.2. 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 de forma explícita, y de forma general para el perfil de certificado regulado en esta política.

9.10.3. Supervivencia tras fin de la duración

VIAFIRMA PCSC 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 PCSC 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 PCSC tiene previsto en los contratos formalizados con los suscriptores, 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 PCSC se rigen por la normativa dominicana vigente emanada del órgano regulador (INDOTEL), así como la legislación específica civil, mercantil y de protección de datos aplicable. En concreto, en relación a la protección de datos, será de aplicación la Resolución 055-06 del INDOTEL que aprueba la Norma sobre Protección de Datos de Carácter Personal por los Sujetos Regulados.

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 Santo Domingo de Guzmán, República Dominicana.

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

9.14. Normativa aplicable

El presente documento se ha realizado considerando, al menos, la siguiente normativa aplicable:

- Ley 126-02 sobre Comercio Electrónico Documentos y Firma Digital de República Dominicana, así como los Decretos Reglamentarios y Normas Complementarias que la desarrollan.

- Resolución 055-06 del INDOTEL que aprueba la Norma sobre Protección de Datos de Carácter Personal por los Sujetos Regulados.

- Resolución 071-19 del INDOTEL, que actúa como:

    - Norma Complementaria por la que se establece la equivalencia regulatoria del Sistema Dominicano de Infraestructura de Claves Públicas y de Confianza con los Marcos Regulatorios Internacionales de Servicios de Confianza.

    - Norma Complementaria sobre los Procedimientos de Autorización y Acreditación.

Del mismo modo, se han considerando los siguientes estándares tecnológicos:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers.

- ETSI TS 102 573: Policy requirements for trust service providers signing and/or storing data objects

- ETSI TS 119 511: Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques

- ETSIEN 319 402: General Policy Requirements for Trust Service Providers.

- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

- ETSI EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

- ETSI EN 319 412: Certificate Profiles.

- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles.
- RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs).

9.15. Cumplimiento de la normativa aplicable

VIAFIRMA PCSC declara que las presentes CPS y sus correspondientes políticas de certificados cumplen con lo dispuesto en la normativa aplicable y en concreto a lo dispuesto en Resolución 071-19 del INDOTEL.

9.16. Otras disposiciones

No se definen otras disposiciones adicionales.

9.17. Otras provisiones

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

a) La PC (política de certificado o servicio explícita)
b) La CPS,
c) Límites de uso y condiciones del servicio explícitamente contratado