Política de Certificados de DGA RA

Policy OID 1.3.6.1.4.1.34253.7.4.40.2

CLOUD QUALIFIED CERTIFICATE FOR NATURAL PERSON WITH PRIVATE KEY GENERATED IN QUALIFIED ELECTRONIC SIGNATURE/SEAL CREATION DEVICE (QSCD)

PERSONA FÍSICA PARA LA ACTIVIDAD ADUANERA

v.2

ÍNDICE

1. INTRODUCCIÓN 11
1.1. Resumen 11
1.2. Identificación del Documento 11
1.3. Participantes 12
1.3.1. Autoridad de Certificación 12
1.3.2. Autoridades de Registro 13
1.3.3. Suscriptores 13
1.3.4. Terceros que confían 14
1.4. Uso del Certificado 14
1.4.1. Usos apropiados del certificado 14
1.4.2. Usos prohibidos del certificado 14
1.5. Administración de Políticas 15
1.5.1. Autoridad de políticas 15
1.5.2. Contacto de la autoridad de políticas 15
1.5.3. Persona que determina la idoneidad de las políticas 15
1.5.4. Procedimiento de aprobación de las políticas 15
1.6. Definiciones y Acrónimos 15

2. PUBLICACIÓN Y REPOSITORIO DE CERTIFICADOS 18
2.1. Repositorios 18
2.2. Publicación de la información de certificación 18
2.3. Frecuencia de publicación 19
2.4. Control de acceso a los repositorios 19

3. IDENTIFICACION Y AUTENTICACIÓN 20
3.1. Uso de nombres 20
3.1.1. Tipo de Nombres 20
3.1.2. Significado de los nombres 20
3.1.3. Seudónimos 21
3.1.4. Reglas para interpretar varios formatos de nombre 21
3.1.5. Unicidad de nombres 21
3.1.6. Reconocimiento, autenticación y función de las marcas registradas 21
3.2. Validación de identidad inicial 23
3.2.1. Métodos de prueba de la posesión de la clave privada 23
3.2.2. Autenticación de la identidad de una organización 23
3.2.3. Autenticación de la identidad de un individuo 23

3.2.4. Información no verificada del suscriptor 24
3.2.5. Validación de la autoridad 24
3.2.6. Criterios de interoperabilidad 25
3.3. Identificación y autenticación para la renovación de certificados 25
3.3.1. Identificación y autenticación para la renovación de certificado vigente 25
3.3.2. Identificación y autenticación para la renovación un certificado caducado 26
3.4. Identificación y autenticación para solicitudes de revocación 26

4. CICLO DE VIDA DEL CERTIFICADO Y REQUISITOS OPERACIONALES 27
4.1. Solicitud de Certificados 27
4.1.1. Quién puede solicitar un certificado 27
4.1.2. Proceso de registro 27
4.2. Proceso de solicitud de un certificado 27
4.2.1. Funciones de identificación y autenticación 28
4.2.2. Aprobación o rechazo de solicitudes 28
4.2.3. Plazos del proceso de solicitud 29
4.3. Emisión de certificados 29
4.3.1. Acciones de la CA durante la emisión de certificados 29
4.3.2. Notificaciones a suscriptores por parte de la CA durante la emisión de certificados . 29
4.4. Aceptación del certificado 29
4.4.1. Hechos que constituyen la aceptación del certificado 29
4.4.2. Publicación del certificado por parte de la CA 30
4.4.3. Notificación de la emisión a otras entidades 30
4.5. Uso del certificado 30
4.5.1. Uso de clave privada del suscriptor 30
4.5.2. Confianza y uso de la clave pública 30
4.6. Renovación de certificados 30
4.6.1. Situaciones para la renovación de certificados 30
4.6.2. Quién puede solicitar la renovación 31
4.6.3. Proceso de solicitudes de renovación 31
4.6.4. Notificación de la renovación del certificado al suscriptor 31
4.6.5. Hechos que constituyen la aceptación del certificado renovado 31
4.6.6. Publicación del certificado renovado 31
4.6.7. Notificación de la renovación a otras entidades 31
4.7. Reemisión del Certificado 32
4.7.1. Circunstancias para la reemisión del certificado 32
4.7.2. Quién puede solicitar la reemisión del certificado 32
4.7.3. Procedimiento para las solicitudes de reemisión del certificado 32
4.7.4. Notificación al suscriptor del nuevo certificado reemitido 32
4.7.5. Hechos que constituyen la aceptación del certificado reemitido 32
4.7.6. Publicación por parte de la CA del certificado reemitido 32

4.7.7. Publicación por parte de la CA del certificado reemitido a otras entidades 33
4.8. Modificación del certificado 33
4.8.1. Circunstancias para la modificación del certificado 33
4.8.2. Quién puede solicitar la modificación del certificado 33
4.8.3. Proceso de solicitud de modificación del certificado 33
4.8.4. Notificación de la modificación del certificado 33
4.8.5. Hechos que constituyen la aceptación del certificado modificado 33
4.8.6. Publicación por parte de la CA de la modificación del certificado 33
4.8.7. Notificación de la modificación del certificado por parte de la CA a otras entidades .. 34
4.9. Revocación y suspensión de certificados 34
4.9.1. Situaciones para la revocación 34
4.9.2. Quién puede solicitar la revocación 34
4.9.3. Proceso para la revocación del certificado 34
4.9.4. Período de gracia de la solicitud de revocación 35
4.9.5. Período en el que la CA debe procesar la solicitud de revocación 35
4.9.6. Requisitos de verificación de la revocación por las partes que confían 35
4.9.7. Frecuencia de emisión de la CRL 35
4.9.8. Latencia máxima de la CRL 36
4.9.9. Comprobación online del estado de la revocación 36
4.9.10. Requisitos para la comprobación online del estado de revocación 36
4.9.11. Otras formas de comprobación del estado de revocación 36
4.9.12. Requisitos especiales para la reemisión de certificados por compromiso de claves . 36
4.9.13. Circunstancias para la suspensión 36
4.9.14. Quién puede solicitar la suspensión 36
4.9.15. Procedimiento para la solicitud de suspensión 37
4.9.16. Límites del período de suspensión 37
4.10. Servicios para la comprobación del estado del certificado 37
4.10.1. Características operacionales 37
4.10.2. Servicios disponibles 37
4.10.3. Características opcionales 37
4.11. Fin de la suscripción 37
4.12. Depósito de claves y recuperación 37
4.12.1. Prácticas para el depósito y recuperación de claves 37
4.12.2. Prácticas de encapsulado y recuperación de recuperación de claves 38

5. INSTALACIÓN, GESTIÓN Y CONTROLES OPERACIONALES 39
5.1. Controles físicos 39
5.1.1. Localización y construcción 39
5.1.2. Acceso físico 39
5.1.3. Alimentación eléctrica y aire acondicionado 39
5.1.4. Exposición al agua 39
5.1.5. Protección y prevención de incendios 39

5.1.6. Sistema de almacenamiento 39
5.1.7. Eliminación de residuos 39
5.1.8. Backup remoto 39
5.2. Controles procedimentales 40
5.2.1. Roles de confianza 40
5.2.2. Número de personas requeridas por tarea 40
5.2.3. Identificación y autenticación para cada rol 40
5.2.4. Roles que requieren separación de funciones 40
5.3. Controles personales 41
5.3.1. Requisitos de calificación, experiencia y autorización 41
5.3.2. Procedimientos de verificación de antecedentes 41
5.3.3. Requisitos de formación 41
5.3.4. Requisitos y frecuencia de formación 41
5.3.5. Frecuencia y secuencia de rotación de tareas 41
5.3.6. Sanciones por acciones no autorizadas 41
5.3.7. Requisitos para personal independiente 41
5.3.8. Documentación entregada al personal 41
5.4. Procedimientos para el registro de auditoría 41
5.4.1. Tipo de eventos registrados 41
5.4.2. Frecuencia del procesamiento de registros 42
5.4.3. Período de retención del registro de auditoría 42
5.4.4. Protección del registro de auditoría 42
5.4.5. Procedimiento del backup del registro de auditoría 42
5.4.6. Sistema de recolección de auditoría 42
5.4.7. Notificación de eventos 42
5.4.8. Evaluación de vulnerabilidades 42
5.5. Archivo de registros 42
5.5.1. Tipos de archivo de registros 42
5.5.2. Período de retención del archivo 42
5.5.3. Protección del archivo 43
5.5.4. Procedimientos para el backup del archivo 43
5.5.5. Requisitos para el sellado de tiempo del registro 43
5.5.6. Sistema de recolección del archivo 43
5.5.7. Procedimientos para obtener y verificar la información del archivo 43
5.6. Cambio clave 43
5.7. Recuperación en caso de compromiso de la clave o desastre 43
5.7.1. Procedimientos para la gestión de incidentes 43
5.7.2. Obsolescencia y deterioro 43
5.7.3. Procedimientos ante compromiso de clave de una entidad 44
5.7.4. Plan de continuidad de negocio ante desastres 44
5.8. Cese de la CA o RA 44

6. CONTROLES TÉCNICOS DE SEGURIDAD 45
6.1. Generación del par de claves y su instalación 45
6.1.1. Generación del par de claves 45
6.1.2. Entrega de la clave privada al suscriptor 45
6.1.3. Entrega de la clave pública al suscriptor 45
6.1.4. Entrega de la clave pública de la CA a los terceros que confían 45
6.1.5. Tamaño de las claves 45
6.1.6. Control de calidad de los parámetros de generación de la clave pública 45
6.1.7. Propósito de uso de la clave 46
6.2. Protección de clave privada y controles del módulo criptográfico 46
6.2.1. Controles y estándares del módulo criptográfico 46
6.2.2. Control dual n de m para el uso de la clave privada 46
6.2.3. Depósito de la clave privada 46
6.2.4. Backup de la clave privada 46
6.2.5. Archivo de la clave privada 46
6.2.6. Importación de la clave privada al módulo criptográfico 46
6.2.7. Almacenamiento de la clave privada en el módulo criptográfico 47
6.2.8. Método de activación de la clave privada 47
6.2.9. Método de desactivación de la clave privada 47
6.2.10. Método de destrucción de la clave privada 47
6.2.11. Clasificación del módulo criptográfico 47
6.3. Otros aspectos sobre la gestión de par de claves 47
6.3.1. Archivo de la clave pública 47
6.3.2. Periodos operativos de certificado y periodos de uso del par de claves 47
6.4. Datos de activación 48
6.4.1. Generación e instalación de datos de activación 48
6.4.2. Protección de los datos de activación 48
6.4.3. Otros aspectos de los datos de activación 48
6.5. Controles de seguridad informática 48
6.5.1. Requisitos técnicos de los controles de seguridad 48
6.5.2. Clasificación de la seguridad 48
6.6. Ciclo de vida de los controles técnicos 48
6.7. Controles de seguridad de red 49
6.8. Sello de tiempo 49

7. CERTIFICADOS, CRL, OCSP Y PERFILES 50
7.1. Perfil de certificado 50
7.1.1. Número de versión 50
7.1.2. Extensiones del certificado 50
7.1.3. Identificador (OID) del algoritmo de firma 52
7.1.4. Uso de nombres 53

7.1.5. Restricciones de nombres 53
7.1.6. Identificador de política de certificado 53
7.1.7. Uso de la extensión de política de restricciones 53
7.1.8. Sintaxis y semántica de la política de calificadores 54
7.1.9. Semántica del procedimiento para las extensiones críticas del certificado 54
7.2. Perfil de la CRL 54
7.2.1. Número de versión 54
7.2.2. CRL y extensiones 54
7.3. Certificado OCSP 55
7.3.1. Certificado utilizado para firmar el OCSP que valida el certificado de la SUBCA 55
7.3.2. Certificado utilizado para firmar el OCSP que valida el certificado regulado esta política 55

8. AUDITORÍAS 57
8.1. Frecuencia o circunstancias de la auditoría 57
8.2. Identidad y cualificación del auditor 57
8.3. Relación del auditor con el prestador 57
8.4. Temas tratados en la auditoría 57
8.5. Acciones a realizar como resultado de una deficiencia 57
8.6. Comunicación de resultados 57

9. OTROS ASUNTOS LEGALES 58
9.1. Tarifas 58
9.1.1. Tarifa para la emisión y renovación de certificados 58
9.1.2. Tarifa de acceso al certificado 58
9.1.3. Tarifa de acceso a OCSP o CRL 58
9.1.4. Tarifa para otros servicios 58
9.1.5. Política de reembolsos 58
9.2. Responsabilidad financiera 58
9.3. Confidencialidad de la información comercial 59
9.3.1. Alcance de la información confidencial 59
9.3.2. Alcance excluido de la información confidencial 59
9.3.3. Responsabilidad para la protección de la información confidencial 59
9.4. Privacidad de la información personal 59
9.4.1. Plan de privacidad 59
9.4.2. Información con tratamiento privado 59
9.4.3. Información no considerada con tratamiento privado 59
9.4.4. Responsabilidad para la protección de la información privada 59
9.4.5. Consentimiento de uso de la información privada 59
9.4.6. Divulgación de conformidad con procesos judiciales o administrativos 60
9.4.7. Otras casos para la divulgación de información 60

9.5. Derechos de propiedad intelectual 60
9.6. Obligaciones y Responsabilidad 60
9.6.1. Obligaciones de la CA 60
9.6.2. Obligaciones de la RA 61
9.6.3. Obligaciones del suscriptor 61
9.6.4. Obligaciones de los terceros que confían 62
9.6.5. Obligaciones de otras entidades 62
9.7. Renuncias de la garantía 62
9.8. Límites de responsabilidad 62
9.9. Indemnizaciones 63
9.10. Términos de uso y duración 63
9.10.1. Términos de uso 63
9.10.2. Duración 63
9.10.3. Supervivencia tras fin de la duración 63
9.11. Avisos y comunicaciones individuales a los participantes 64
9.12. Resolución de Conflictos 64
9.12.1. Procedimiento de conflictos 64
9.12.2. Mecanismo y período de notificación 64
9.12.3. Circunstancias por las que un OID puede ser modificado 64
9.13. Disposiciones para la resolución de disputas 64
9.14. Normativa aplicable 65
9.15. Cumplimiento de la normativa aplicable 66
9.16. Otras disposiciones 66
9.17. Otras provisiones 66

CONTROL DE DOCUMENTO

Título:	Política de Certificados de Viafirma Dominicana Policy OID 1.3.6.1.4.1.34253.7.4.40.2		
Asunto:	CLOUD QUALIFIED CERTIFICATE FOR NATURAL PERSON WITH PRIVATE KEY GENERATED IN QUALIFIED ELECTRONIC SIGNATURE/SEAL CREATION DEVICE (QSCD) PERSONA FÍSICA PARA LA ACTIVIDAD ADUANERA		
Estado:	Aprobado		
Versión:	v.2		
Código:	CP-DGA-PFAA-QSCD	**Última revisión**	13-10-2021
Idioma:	Castellano	**Revisión anterior:**	07-10-2021
		Núm. Páginas:	66

CONTROL DE CAMBIOS Y VERSIONES		
Fecha	**Versión**	**Motivo del Cambio**
06-09-2021	1.0	Primera versión.
22-09-2021	1.1	Corrección de las OIDs de la CRL
07-10-2021	1.2	Adaptación del atributo del certificado “Serial Number” a la ETSI EN 319 412-1 V1.1.1 (2016-02)
13-10-2021	2.0	Actualización de una nueva jerarquía de certificados, que conlleva sustitución de: • Nueva CA: de “Root-CA: AVANSI CERTIFICATION” a “VIAFIRMA QSTP ROOT CA”. • Nueva SubCA: de “Sub-CA (2021): VIAFIRMA QUALIFIED CERTIFICATES” a “Sub-CA (2023): VIAFIRMA QUALIFIED CERTIFICATES”- • Policiy OID de este perfil de certificado: de “1.3.6.1.4.1.27395.6.2.40.2” a “1.3.6.1.4.1.34253.7.4.40.2”. • CRLs y OCSP de los certificados.

ACERCA DEL DOCUMENTO

Este documento, con nivel de seguridad público, es propiedad de la Dirección General de Aduanas de República Dominicana (DGA). Para más información contacte con:

Avenida Abraham Lincoln #1101
Santo Domingo, República Dominicana
Teléfono: + 1 809-547-7070
firmasdigitales@aduanas.gob.do
www.aduanas.gob.do

1. INTRODUCCIÓN

1.1. Resumen

La Dirección General de Aduanas de República Dominicana (DGA) es una entidad de naturaleza pública, adscrita al Ministerio de Hacienda de República Dominicana, encargada de, entre otras cosas, gestionar y regular todos los trámites aduaneros realizados en el país (importación, exportación, etc.).

Desde el año 2018, y con el objetivo de que los contribuyentes puedan gestionar sus trámites aduaneros online pero con las mayores garantías legales desde las plataformas habilitadas para ello (SIGA, VUCE, o cualquier otra), la DGA decidió constituirse como Entidad de Registro (RA por sus siglas en inglés), para proporcionar certificados digitales a sus contribuyentes y que estos puedan autenticarse con estos certificados en estas plataformas, así como firmar los documentos que tengan disponibles para firmar. Del mismo modo, la DGA hace uso de certificados de firma centralizada, almacenados en un HSM (Hardware Security Module).

Con este claro objetivo, en ese mismo año, la DGA obtiene del **Instituto Dominicano de Telecomunicaciones (Indotel)** la autorización para operar como Autoidad de Registo (RA) o Unidad de Registro, dependiente de la **Entidad de Certificación de avansi, en la República Dominicana**, capacitada legalmente desde entonces para emitir certificados digitales según contempla la Ley 126-02 de Comercio Electrónico y la Resolución de indotel Nº025-11 que aprueba la Norma de Aplicación de la Ley 126-02 a los Procedimientos Aduaneros (Resolución Nº 008-18).

Desde entonces, DGA RA ha formado parte de la cadena de confianza de certificados emitidos por AVANSI CA, y ahora de su actual SubCA "VIAFIRMA QUALFIED CERTIFICATES", y además, hace uso del resto de soluciones de software de la marca Viafirma.

Por este motivo, a lo largo del documento se mencionará Viafirma, como proveedor de sitios web e infraestructura necesaria para que la DGA pueda proveer este tipo de servicios de firma y certificación digital a sus clientes y empleados.

1.2. Identificación del Documento

Este documento está estructurado acorde al RFC3647, con el nombre **CLOUD QUALIFIED CERTIFICATE FOR NATURAL PERSON WITH PRIVATE KEY GENERATED IN QUALIFIED ELECTRONIC SIGNATURE/SEAL CREATION DEVICE (QSCD) PERSONA FÍSICA PARA LA ACTIVIDAD ADUANERA**, codificado con el código **CP-DGA-PFAA-QSCD**, y disponible en la url https://cps.viafirma.do/.

Las presentes políticas de certificado están identificadas con el OID número **1.3.6.1.4.1.34253.7.4.40.2**.

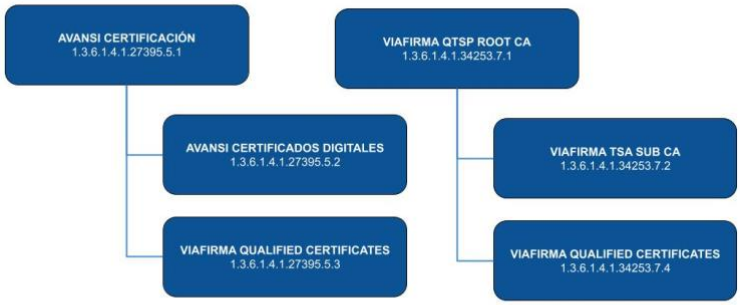
1.3. Participantes

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 VIAFIRMA QTSP ROOT CA.



- **La CA AVANSI CERTIFICACIÓN** es la CA Root de la que dependen dos CA´s subordinadas y desde las que se emiten los distintos perfiles de certificados finales, incluyendo el perfil de TSU desde el que se firman los sellos de tiempo.

- **La CA SUBORDINADA AVANSI CERTIFICADOS DIGITALES:** esta CA subordinada AVANSI CERTIFICADOS DIGITALES no emite certificados desde el pasado 11 de Septiembre de 2021, acorde a la normativa vigente, quedando activa para fines de validación de los certificados emitidos con dicha CA subordinada con fecha anterior al 11 de Septiembre de 2021 con estado activo, es decir, no han caducado y no han sido revocados.

- **La CA SUBORDINADA VIAFIRMA QUALIFIED CERTIFICATES** emite perfiles de certificados desde el 11 de Septiembre de 2021, y será sustituida a partir de 2023 por la CA homóloga dependiente de la ROOT VIAFIRMA QTSP ROOT CA.

- **La CA VIAFIRMA QTSP ROOT CA** es la CA ROOT desde la que cuelga una CA subordinada diseñada para la emisión de perfiles de certificados TSU con los que se firman sellos de tiempo y otra CA subordinada con la que se emiten perfiles de certificados cualificados.

- **La CA subordinada VIAFIRMA TSA SUB CA** opera desde 2019 para la emisión de perfiles de certificados TSU para la emisión de sellos cualificados de tiempo.

- **La CA subordinada VIAFIRMA QUALIFIED CERTIFICATES** opera desde 2023 para la emisión de perfiles de certificados digitales cualificados asociados a la jerarquía VIAFIRMA QTSP ROOT CA con OID de Política de CA 1.3.6.1.4.1.34253.7.4.

1.3.2. Autoridades de Registro

Entidad que actúa conforme esta Política de Certificados y, en su caso, mediante acuerdo suscrito con la CA Avansi (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 Avansi (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 Avansi (Viafirma), 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:

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 Certificado emitido bajo la presente Política permite identificar a una persona física en aquellas gestiones que realice por cuenta propia en el ámbito de la Actividad Aduanera. El Certificado emitido bajo esta Política puede ser utilizado con los siguientes propósitos:

- Integridad del documento firmado
- No repudio
- Autenticación
- Cifrado

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

1.5.2. Contacto de la autoridad de políticas

Avenida Abraham Lincoln #1101

Santo Domingo, República Dominicana

Teléfono: + 1 809-547-7070

firmasdigitales@aduanas.gob.do

www.aduanas.gob.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.
- DGA: Dirección General de Aduanas.
- 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 Creacion 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/viafirmaqtsproot.crt

SubCA VIAFIRMA QUALIFIED CERTIFICATES:

https://cps.viafirma.do/viafirmaqtspsubca008.crt

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

http://crl.viafirma.do/viafirmaqtsproot.crl

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

http://crl.viafirma.do/viafirmaqtspsubca008.crl

http://crl2.viafirma.do/viafirmaqtspsubca008.crl

http://ocsp.viafirma.do/ocsp008

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-DGA-PFAA-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.

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

{DN Qualifier} + { Common Name} + {Serial Number} + {Given Name} + {Surname} + {Organization Unit} + {DN_CUSTOM1} {Country}

+

Other subject attributes: {RFC 822 Name (email address)}

3.1.2. Significado de los nombres

En el contexto de la presente política el nombre corresponderá a la persona física, correspondiente a la figura del suscriptor y titular del certificado emitido, según se describe a continuación:

C = {country} para esta política "DO" como valor fijo, correspondiente a República Dominicana

SURNAME = para la presente política estará asociado al apellido o apellidos acreditadps por el suscriptor durante la emisión.

GIVENNAME = para la presente política estará asociado al nombre o nombres acreditados por el suscriptor durante la emisión.

SERIALNUMBER = para la presente política estará asociado al número de cédula o pasaporte acreditado por el suscriptor durante la emisión y tendrá la estructura [{identityType}{countryCode}-{number}}]

{IndentityType} será un campo con tres caracteres, que se representan con IDC (Cédula de Identidad) o PAS (Pasaporte).

{CountryCode} será el código país del documento de identidad, que se representará según la normativa ISO 3166.

{Number} se corresponderá con el número del documento de identidad.

CN = {common-name} para la presente política estará compuesto de forma automática por la suma del {GIVENNAME} + {SURNAME}.

OU = {Organization Unit} para la presente política estará asociado a la nacionalidad del suscriptor.

DN_CUSTOM1 = para esta política "1.3.6.1.4.1.27395.8.1" como valor fijo, correspondiente al Perfil de Certificado de Persona Física para la Actividad Aduanera.

DN Qualifier = para la presente política tendrá como valor "CLOUD QUALIFIED CERTIFICATE FOR NATURAL PERSON WITH PRIVATE KEY GENERATED IN QUALIFIED ELECTRONIC

SIGNATURE/SEAL CREATION DEVICE (QSCD) PERSONA FÍSICA PARA LA ACTIVIDAD ADUANERA".

Other subject attributes: {RFC 822 Name (email address)} = para la presente política estará asociado al email del suscriptor, el cual será validado durante el proceso de activación del certificado.

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 utilizado para identificar al certificado tendrá que coincidir con el documento de identificación vigente que se utilizó para la acreditación, por ejemplo la Cédula de Identidad y Electoral, o pasaporte.

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 y/o Avansi y la DGA, y en especial los escritos doctrinales o publicaciones de la misma son propiedad de Viafirma, y la DGA 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, la DGA 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

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 al control de la clave privada pero no la posesión.

3.2.2. Autenticación de la identidad de una organización

No aplica para la presente política que solo define el uso de certificados de individuales de persona física sin ningún tipo de asociación o vinculación a una organización.

3.2.3. Autenticación de la identidad de un individuo

La presente política autoriza la video-acreditación en las dos modalidades actualmente soportadas por Viafirma, y que se describen a continuación.

Automática: basado en un proceso automátizado 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 extraidos del documento de identificación presentado 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 imagenes 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 extraida 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 Junta Central Electoral (JCE), ha sido satisfactoria.

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 eviencias 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 una Carta de solicitud de Emisión de Certificado Digital, dirigida al Director General de Aduanas.

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:

Semi-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 a emisión.

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:
    - validación online del número de cédula electoral a través de los servicios web ofrecidos por la Junta Central Electoral (JCE) de la República Dominicana.
    - Servicios para la verificación de documentos de identidad (cédulas o pasaportes), prueba de vida y reconomiento facial ofrecidos por el prestador MatiLock, Inc. (San Francisco, CA – EEUU).
- Para la firma electrónica del contrato:
    - Verificación OTP y captura de otras evidencias electrónicas realizadas en remoto a través de la herramienta Viafirma Documents, solución desarrollada y gestionada por Viafirma.
- Para la centralización del certificado:
    - Comunicación securizada, activación de cuenta del usuario, y activación de los factores de protección de claves gestionada por Viafirma Fortress, solución desarrollada y gestionada por Viafirma.
- Para el pago en línea:
    - Integración con la pasarela de pago AZUL, desarrollada y gestionada por el Banco Popular Dominicano.

3.3. Identificación y autenticación para la renovación de certificados

3.3.1. Identificación y autenticación para la renovación de certificado vigente

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, revocado, que podrá solicitar 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 un certificado caducado

No se permite la renovación de certificados ya caducados. Si el certificado ya estuviera caducado, el suscriptor deberá iniciar el proceso 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 permtie 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 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

La DGA cuenta con una solución desarrollada y gestionada por Viafirma, denominada Viafirma RA, que permite la gestión de todo el Ciclo de Vida del Certificado, y sobre esta solución están basados los requisitos operacionales descritos a continuación.

Al mismo tiempo, este perfil de certificado permite ser solicitado desde Viafirma Fortress, la herramienta autorizada para la centralización de certificados.

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.

4.1.2. Proceso de registro

Para la presente política la emisión del certificado implica obligatoriamente el registro de una cuenta de usuario en Viafirma Fortress, el sistema de centralización de certificados de Viafirma. Durante este registro el suscriptor configura y activa sus credenciales de gestión así como los distintos factores de autenticación con los que se protegará 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

La solicitud de certificados emitidos bajo la presente política puede originarse desde varios puntos autorizados:

- Autoridad de Registro: accediendo a la herramienta Viafirma RA, publicada en la dirección web https://ra.viafirma.do y siguiendo los pasos del asistente asociado al perfil del certificado deseado.

- Sistema Centralizado: si el usuario ya cuenta con una cuenta de usuario en el sistema de centralización de certificados de Viafirma, podrá solicitar desde aquí un nuevo certificado asociado a esta política, siguiendo de igual forma los pasos propuestos por el asistente.

- Solicitudes Masivas Autorizadas: para proyectos ad-hoc autorizados por Viafirma, se habilitarán interfaces web previamente integradas con Viafirma que facilitarán la gestión de solicitudes cuando éstas corresponden a un proyecto o campaña específica.

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 inviduo alguna de las tres modalidades de solicitudes descritas en el capítulo 3.2.3:

    - Solicitudes semi-automáticas: 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 solicitud iniciada mediante un 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 inviduo, 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

El proceso de solicitud asociado a este perfil, y todas las fases previstas de su ciclo de vida hasta su emisión y centralización, permite ser tramitado 100% oline, incluyendo pago, validación de documentación, verificación del invididuo y firma del contrato, de forma que si no hay inconvenientes en el proceso de solicitud, éste puede completarse en el mismo día de la solicitud, sin perjuicio de que el propio suscriptor no haya aportado la documetación requerida paa el proceso, corregido algún campo que estuviera erróneo, o cuaquier otra circunstancia ajena al control de la CA o la RA.

Para los procesos de solicitud asociados a procedimientos asistidos o presenciales, los plazos vendrán determinados por la disponibilidad de equipo de registradores asociados a la Autoridad de Registro que recibió la solicitud, contando con que dicho equipo ejecutará acciones pendientes de su parte en horario de 9:00am a 5:30pm de lunes a viernes excepto festivos en República Dominicana. El tiempo de finalización de una solicitud dependerá de la diligencia con la que el suscriptor cumpla con los pasos que debe realizar durante el poceso, incluida la confirmación de una fecha para la acreditación, si fuera necesario hacerla de manera asistida o presencial.

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 regulado en la presente política se entenderá por aceptada tras completar el proceso de activación del certificado, realizado éste mediante la herramienta de centralización Viafirma Fortress.

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://ra.viafirma.do.

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 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.

El suscriptor deberá proteger el uso de la clave privada con algunos de los factores de protección definidos en la herramienta de centralización Viafirma Fortress (como OTP). Sin dicha protección la clave privada no podrá ser usada.

La clave privada centralizada no podrá ser usada cuando ésta haya caducado o haya sido revocada. El sistema de centralización de certificados Viafirma Fortress no permite su uso si se dan alguna de estas condiciones.

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

Este perfil de certificado podrá ser renovado en el período comprendido entre la fecha de su emisión y la fecha de su 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 fechade 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.

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

4.6.5. Hechos que constituyen la aceptación del certificado renovado

La renovación del certificado regulado en la presente política se entenderá por aceptada tras completar el proceso de activación del nuevo certificado renovado, realizado ésto mediante la herramienta de centralización Viafirma Fortress.

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://ra.viafirma.do.

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

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

- Compromiso de claves: al tatarse de un certificado centralizado, la clave privada no está en posesión de su tiular, por tanto, se considera compromiso de claves al hecho de sospechar o tener evidencias de la desvelación de alguno 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, en este caso, nombre, apellidos, email o número de cédula o pasaporte.

- 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

La revocación de un certificado podrá solicitarse únicamente por el suscriptor 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 revocaión se habilitarán los mismos procedimientos descritos en el capítulo 4.2 “Proceso de solicitud de un certificado”.

- Autoridad de Registro: accediendo a la herramienta Viafirma RA, publicada en la dirección web https://ra.viafirma.do, será posible solicitar la revocación del certificado siempre que

el suscriptor disponga de un código de revocación que se le habrá facilitado por email en la comunicación que se le confirmó que hizo su solicitud correctamente.

- Sistema Centralizado: si el usuario ya cuenta con una cuenta de usuario en el sistema de centralización de certificados de Viafirma, podrá solicitar desde aquí la revocación de su certificado digital, siguiendo los pasos propuestos por el asistente.

- 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, remitiéndolo a firmasdigitales@aduanas.gob.do en el cual solicite su revocación. 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 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

Si la solicitud de revocación fue realizada por el titular desde la propia herramienta de centralización de certificados Viafirma Fortress, o bien desde la página de la Autoridad de Registro (https://ra.viafirma.do), la revocación tendrá efecto inmediato.

Si la solicitud se hace a través de un email enviado a firmasdigitales@aduanas.gob.do, la revocación se llevará a cabo durante el horario laboral de ese mismo día (de 9:00am a 5:30pm), siempre que ese mismo día no sea fin de semana o festivo. Si es fin de semana o festivo, se hará durante el próimo 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 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

Para la presente política lass claves del certificado son generadas en el sistema centralizado de certificados, Viafirma Fortress.

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 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 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 de TSU 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 será de 1 año (365 días).

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

Lo establecido en la Declaración de Prácticas de Certificación de VIAFIRMA PCSC y en concreto en las políticas del perfil de certificado emitido para el 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

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

Subject Name	
DN Qualifier	*CLOUD QUALIFIED CERTIFICATE FOR NATURAL PERSON WITH PRIVATE KEY GENERATED IN QUALIFIED ELECTRONIC SIGNATURE/SEAL CREATION DEVICE (QSCD) PERSONA FÍSICA PARA LA ACTIVIDAD ADUANERA*
Common Name	*<GIVEN NAME + SURNAME>*
Serial Number	*<TIPO DE DOCUMENTO DE IDENTIDAD + CÓDIGO PAÍS + NÚMERO DE CÉDULA O PASAPORTE>*
Given Name	*<NOMBRE DE LA PERSONA NATURAL>*
Surname	*<APELLIDO O APELLIDOS DE LA PERSONA NATURAL>*
Organization Unit	*<NACIONALIDAD DE LA PERSONA NATURAL>*
Country or Region	*DO*
Issuer Name	
Country or Region	*DO*
Organisation	*AVANSI SRL*
Organisational Unit	*VIAFIRMA DOMINICANA*
Serial Number	*RNC 130222509*
Common Name	*VIAFIRMA QUALIFIED CERTIFICATES*
Serial Number	<SERIAL NUMBER>
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	None
Not Valid Before	<FECHA INICIO>

Not Valid After	<FECHA INICIO + 1 AÑO >
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	None
Public Key	256 bytes: <PUBLIC KEY>
Exponent	65537
Key Size	2.048 bits
Key Usage	Encrypt, Verify, Wrap, Derive
Signature	512 bytes: <SIGNATURE>
Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Digital Signature, Non-Repudiation, Key Encipherment
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Client Authentication (1.3.6.1.5.5.7.3.2)
Purpose #2	Email Protection (1.3.6.1.5.5.7.3.4)
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	52 2B 34 5C E2 C0 90 A5 EB E9 F7 D6 D5 4E 8E D1 49 42 67 17
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	04 6E 4B 7C B9 DC 3D 9D 39 A1 2F 48 8B 26 26 E5 BD 5E 4E E0
Extension	Subject Alternative Name (2.5.29.17)
Critical	NO

RFC 822 Name <EMAIL DEL TITULAR>

Extension Certificate Policies (2.5.29.32)
Critical NO
Policy ID #1 (0.4.0.194112.1.2)
Policy ID #2 (1.3.6.1.4.1.34253.7.4.40.2)
Qualifier ID #1 Certification Practice Statement (1.3.6.1.5.5.7.2.1)
CPS URI http://cps.viafirma.do
Qualifier ID #2 User Notice (1.3.6.1.5.5.7.2.2)
User Notice CLOUD QUALIFIED CERTIFICATE FOR NATURAL PERSON WITH PRIVATE KEY GENERATED IN QUALIFIED ELECTRONIC SIGNATURE/SEAL CREATION DEVICE (QSCD)

Extension CRL Distribution Points (2.5.29.31)
Critical NO
URI http://crl.viafirma.do/viafirmaqtsproot.crl
URI http://crl2.viafirma.do/viafirmaqtsproot.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 https://cps.viafirma.do/viafirmaqtspsubca008.crt
Method #2 Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
URI http://ocsp.viafirma.do/ocsp008

Other Field Qualified Certificate Statements (1.3.6.1.5.5.7.1.3)
Data 30 14 30 08 06 06 04 00 8E 46 01 01 30 08 06 06 04 00 8E 46 01 04

Fingerprints
SHA-256 49 2A A0 F9 6E 6A 77 AB 74 55 1D 14 20 1C 67 D7 ED 1E 65 02 DD 4B CF 7D 0E 86 F1 52 AD 5D 5A 06
SHA-1 7D F7 48 6D AF DA 16 08 9B 6C A8 38 51 EA 9F A0 DD C8 AD 31

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 (1.3.6.1.4.1.27395.6.2.4.2)

Qualifier ID #1 User Notice (1.3.6.1.5.5.7.2.2)

User Notice CLOUD QUALIFIED CERTIFICATE FOR NATURAL PERSON WITH PRIVATE KEY GENERATED IN QUALIFIED ELECTRONIC SIGNATURE/SEAL CREATION DEVICE (QSCD)

Qualifier ID #2 Certification Practice Statement (1.3.6.1.5.5.7.2.1)

CPS URI http://cps.viafirma.do

Extension Certificate Policies (2.5.29.32)

Critical NO

Policy ID #1 (0.4.0.194112.1.2)

Policy ID #2 (1.3.6.1.4.1.34253.7.4.40.2)

Qualifier ID #1 Certification Practices Statement (1.3.6.1.5.5.7.2.1)

CPS URI http://cps.viafirma.do

Qualifier ID #2 User Notice (1.3.6.1.5.5.7.2.2)

User Notice CLOUD QUALIFIED CERTIFICATE FOR NATURAL PERSON WITH PRIVATE KEY GENERATED IN QUALIFIED ELECTRONIC SIGNATURE/SEAL CREATION DEVICE (QSCD)

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 2.5.29.20 "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 (2.5.29.35).

7.3. Certificado OCSP

Se cuenta con un certificado OCSP para validar el certificado regulado en la presente política, firmado éste por la SUBCA VIAFIRMA QUALIFIED CERTIFICATES.

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

No aplica.

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

Disponible en:

https://cps.viafirma.do/CA008_VIAFIRMAQUALIFIEDCERTIFICATES_OCSP_SIGNER.cer

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
Valid From:	5 October 2023 at 12:29:47 Central European Summer Time
Valid Until:	5 October 2033 at 12:29:47 Central European Summer Time
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	OCSP Signing (1.3.6.1.5.5.7.3.9)

Public Key

-----BEGIN CERTIFICATE-----
MIIFITCCAwmgAwIBAgIUEb6Y1/ZsJ8HApd/C4zPJO3p71S8wDQYJKoZIhvcNAQEL
BQAwgYIxCzAJBgNVBAYTAkRPMRMwEQYDVQQKDApBVkFOU0kgU1JMMRwwGgYDVQQL
DBNWSUFGSVJNQSBET01JTklDQU5BMRYwFAYDVQQFEw1STkMgMTMwMjIyNTA5MSgw
JgYDVQQDDB9WSUFGSVJNQSBRVUFMSUZJRUQgQ0VSVElGSUNBVEVTMB4XDTIzMDUx
MDEwMjk0N1oXDTMzMDUxMDEwMjk0N1owgYcxCzAJBgNVBAYTAkRPMRMwEQYDVQQK
DApBVkFOU0kgU1JMMRwwGgYDVQQLDBNWSUFGSVJNQSBET01JTklDQU5BMRYwFAYD
VQQFEw1STkMgMTMwMjIyNTA5MS0wKwYDVQQDDCRPQ1NQIFZJQUZJUk1BIFFVQUxJ
RklFRCBDRVJUSUZJQ0FURVMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQDCq5b8yB0+A9XQ2ljOCiflXEXWofhwlqUguT9FXZrPOwy8R7jbiH9is78Ztc+F
XUGn3HJzK1q9QqV1xYpkmcJKkRt0qrlAOyfeUXeRF9p5DEwBzvj514UBki0fxSoM
2ey/YEDy0WAvUur4v6MhX4y5DrnwvjJkOZlBfQNY9CHUCAYaOkPm/b0cWEYYT03D
3MDTsKdqPqR3xvU9DWs9IW30c7VzYMTs892qxsR9iPD9IB+mjhgB/UBmkpFQ+53G
o14eca+GQiehh9GfYWg02jyigK7ymmCcmtENFtjaii5pkaKtzH/ID817MF2WHFjR
B9Rd+bJHaR5lvkclMOHxjWpvAgMBAAGjgYcwgYQwHQYDVR0OBBYEFJGyxdIushWE
kUCq+GZmegS5dhCxMAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgwFoAUksH88NzninPj
usVBlYXSxS4CwK0wDwYJKwYBBQUHMAEFBAIFADAOBgNVHQ8BAf8EBAMCB4AwEwYD
VR0lBAwwCgYIKwYBBQUHAwkwDQYJKoZIhvcNAQELBQADggIBAA1J5bTVEVHBeBBr
5dP52l19/qwmVhO1GIiNLTcS0YjF4sJPi7wW4Mg5BQ7VbeUdt2XduwUIdg1se3kQ
RiCD21X5Gg1DtPW4zx/DeLQz6ImDIAx4izs3U6LfbBadL4iirvWgiQAlqQfjCllv
NQ4BCN3HEeXu0qLLR/pFlYuNpi+dEx1lNK0lSe+l7voMYDv5hmYyls2JJ41ZC3fI
gp6j173X4XJ1c7RSR/+tn8YT37yWQE+PQ/VsxoiZ5dOqoQbdHdFYi9WGCNEwqNAE
cciveVieQviZ1ORkWrt8gQCNpWYN8rGmvnwKvSaLIvf/3X0daEhAiHb2LeILDn5T
5Fij3YII5ecHL3wPBu8fLHFfKceRBtJV0QvWDxnC31oAgkN6vWGZOCApnTUrOGU9
o3TWkeOrIx1AXLtjDGByfFHkjTJaN2FU1Ked+GfOOhHmb4f7zhYYRAM3z5L8CGXM
tGLRwtaTe7oDAzuRgCssoV/cGUrqMtAuuzuM+nm/yCYtLqlzAhM19nYfNrgZOtPg
C3RbDlommc4tYRASeOlvIXdfB72Z8yFgPWOtsFTzLv8T8jnJrZA0Zb7NUXH2bMJf
BIgEATUKrI+bYjuxqLyeVHcZG7wqqhx9cYMYdWanucIw5IL/HZ8ySxf06tS9GdW5
O2+LISDIlgWNDqzhuW3F8Dwj6plg
-----END CERTIFICATE-----

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

La Entidad de Certificación VIAFIRMA PCSC 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, protegiéndolas 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 DGA 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 PCSC 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 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, la duración estipulada será de un máximo de un (1) año.

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 Nº025-11 del INDOTEL, que aprueba la Norma de Aplicación de la Ley 126-02 a los Procedimientos Aduaneros
- 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 y en la Resolución Nº025-11 del INDOTEL, que aprueba la Norma de Aplicación de la Ley 126-02 a los Procedimientos Aduaneros

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 DPC
c) Límites de uso y condiciones del servicio explícitamente contratado