Política de Certificados de OGTIC CA

Policy OID 1.3.6.1.4.1.49353.6.3.0

SOFTWARE QUALIFIED CERTIFICATE FOR

PUBLIC EMPLOYEE

v.1

ÍNDICE

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

2. PUBLICACIÓN Y REPOSITORIO DE CERTIFICADOS 17
   2.1. Repositorios 17
   2.2. Publicación de la información de certificación 17
   2.3. Frecuencia de publicación 17
   2.4. Control de acceso a los repositorios 18

3. IDENTIFICACION Y AUTENTICACIÓN 19
   3.1. Uso de nombres 19
      3.1.1. Tipo de Nombres 19
      3.1.2. Significado de los nombres 19
      3.1.3. Seudónimos 20
      3.1.4. Reglas para interpretar varios formatos de nombre 20
      3.1.5. Unicidad de nombres 20
      3.1.6. Reconocimiento, autenticación y función de las marcas registradas 20
   3.2. Validación de identidad inicial 20
      3.2.1. Métodos de prueba de la posesión de la clave privada 20

3.2.2. Autenticación de la identidad de una organización 21
3.2.3. Autenticación de la identidad de un individuo 21
3.2.4. Información no verificada del suscriptor 22
3.2.5. Validación de la autoridad 22
3.2.6. Criterios de interoperabilidad 23
3.3. Identificación y autenticación para la renovación de certificados 23
3.3.1. Identificación y autenticación para la renovación de certificado vigente 23
3.3.2. Identificación y autenticación para la renovación un certificado caducado 24
3.4. Identificación y autenticación para solicitudes de revocación 24

4. CICLO DE VIDA DEL CERTIFICADO Y REQUISITOS OPERACIONALES 25
4.1. Solicitud de Certificados 25
4.1.1. Quién puede solicitar un certificado 25
4.1.2. Proceso de registro 25
4.2. Proceso de solicitud de un certificado 25
4.2.1. Funciones de identificación y autenticación 25
4.2.2. Aprobación o rechazo de solicitudes 26
4.2.3. Plazos del proceso de solicitud 26
4.3. Emisión de certificados 27
4.3.1. Acciones de la CA durante la emisión de certificados 27
4.3.2. Notificaciones a suscriptores por parte de la CA durante la emisión de certificados 27
4.4. Aceptación del certificado 27
4.4.1. Hechos que constituyen la aceptación del certificado 27
4.4.2. Publicación del certificado por parte de la CA 27
4.4.3. Notificación de la emisión a otras entidades 27
4.5. Uso del certificado 28
4.5.1. Uso de clave privada del suscriptor 28
4.5.2. Confianza y uso de la clave pública 28
4.6. Renovación de certificados 28
4.6.1. Situaciones para la renovación de certificados 28
4.6.2. Quién puede solicitar la renovación 28
4.6.3. Proceso de solicitudes de renovación 29
4.6.4. Notificación de la renovación del certificado al suscriptor 29
4.6.5. Hechos que constituyen la aceptación del certificado renovado 29
4.6.6. Publicación del certificado renovado 29
4.6.7. Notificación de la renovación a otras entidades 29
4.7. Reemisión del Certificado 29
4.7.1. Circunstancias para la reemisión del certificado 29
4.7.2. Quién puede solicitar la reemisión del certificado 29

4.7.3. Procedimiento para las solicitudes de reemisión del certificado 30
4.7.4. Notificación al suscriptor del nuevo certificado reemitido 30
4.7.5. Hechos que constituyen la aceptación del certificado reemitido 30
4.7.6. Publicación por parte de la CA del certificado reemitido 30
4.7.7. Publicación por parte de la CA del certificado reemitido a otras entidades 30
4.8. Modificación del certificado 30
4.8.1. Circunstancias para la modificación del certificado 30
4.8.2. Quién puede solicitar la modificación del certificado 30
4.8.3. Proceso de solicitud de modificación del certificado 31
4.8.4. Notificación de la modificación del certificado 31
4.8.5. Hechos que constituyen la aceptación del certificado modificado 31
4.8.6. Publicación por parte de la CA de la modificación del certificado 31
4.8.7. Notificación de la modificación del certificado por parte de la CA a otras entidades 31
4.9. Revocación y suspensión de certificados 31
4.9.1. Situaciones para la revocación 31
4.9.2. Quién puede solicitar la revocación 32
4.9.3. Proceso para la revocación del certificado 32
4.9.4. Período de gracia de la solicitud de revocación 32
4.9.5. Período en el que la CA debe procesar la solicitud de revocación 33
4.9.6. Requisitos de verificación de la revocación por las partes que confían 33
4.9.7. Frecuencia de emisión de la CRL 33
4.9.8. Latencia máxima de la CRL 33
4.9.9. Comprobación online del estado de la revocación 33
4.9.10. Requisitos para la comprobación online del estado de revocación 33
4.9.11. Otras formas de comprobación del estado de revocación 34
4.9.12. Requisitos especiales para la reemisión de certificados por compromiso de claves 34
4.9.13. Circunstancias para la suspensión 34
4.9.14. Quién puede solicitar la suspensión 34
4.9.15. Procedimiento para la solicitud de suspensión 34
4.9.16. Límites del período de suspensión 34
4.10. Servicios para la comprobación del estado del certificado 34
4.10.1. Características operacionales 34
4.10.2. Servicios disponibles 35
4.10.3. Características opcionales 35
4.11. Fin de la suscripción 35
4.12. Depósito de claves y recuperación 35
4.12.1. Prácticas para el depósito y recuperación de claves 35
4.12.2. Prácticas de encapsulado y recuperación de recuperación de claves 35

5. INSTALACIÓN, GESTIÓN Y CONTROLES OPERACIONALES 36

5.1. Controles físicos 36
5.1.1. Localización y construcción 36
5.1.2. Acceso físico 36
5.1.3. Alimentación eléctrica y aire acondicionado 36
5.1.4. Exposición al agua 36
5.1.5. Protección y prevención de incendios 36
5.1.6. Sistema de almacenamiento 36
5.1.7. Eliminación de residuos 36
5.1.8. Backup remoto 36
5.2. Controles procedimentales 37
5.2.1. Roles de confianza 37
5.2.2. Número de personas requeridas por tarea 37
5.2.3. Identificación y autenticación para cada rol 37
5.2.4. Roles que requieren separación de funciones 38
5.3. Controles personales 38
5.3.1. Requisitos de calificación, experiencia y autorización 38
5.3.2. Procedimientos de verificación de antecedentes 38
5.3.3. Requisitos de formación 38
5.3.4. Requisitos y frecuencia de formación 38
5.3.5. Frecuencia y secuencia de rotación de tareas 38
5.3.6. Sanciones por acciones no autorizadas 38
5.3.7. Requisitos para personal independiente 38
5.3.8. Documentación entregada al personal 38
5.4. Procedimientos para el registro de auditoría 39
5.4.1. Tipo de eventos registrados 39
5.4.2. Frecuencia del procesamiento de registros 39
5.4.3. Período de retención del registro de auditoría 39
5.4.4. Protección del registro de auditoría 39
5.4.5. Procedimiento del backup del registro de auditoría 39
5.4.6. Sistema de recolección de auditoría 39
5.4.7. Notificación de eventos 39
5.4.8. Evaluación de vulnerabilidades 39
5.5. Archivo de registros 40
5.5.1. Tipos de archivo de registros 40
5.5.2. Período de retención del archivo 40
5.5.3. Protección del archivo 40
5.5.4. Procedimientos para el backup del archivo 40
5.5.5. Requisitos para el sellado de tiempo del registro 40
5.5.6. Sistema de recolección del archivo 40
5.5.7. Procedimientos para obtener y verificar la información del archivo 40

5.6. Cambio clave 40
5.7. Recuperación en caso de compromiso de la clave o desastre 41
5.7.1. Procedimientos para la gestión de incidentes 41
5.7.2. Obsolescencia y deterioro 41
5.7.3. Procedimientos ante compromiso de clave de una entidad 41
5.7.4. Plan de continuidad de negocio ante desastres 41
5.8. Cese de la CA o RA 41

6. CONTROLES TÉCNICOS DE SEGURIDAD 42

6.1. Generación del par de claves y su instalación 42
6.1.1. Generación del par de claves 42
6.1.2. Entrega de la clave privada al suscriptor 42
6.1.3. Entrega de la clave pública al suscriptor 42
6.1.4. Entrega de la clave pública de la CA a los terceros que confían 42
6.1.5. Tamaño de las claves 42
6.1.6. Control de calidad de los parámetros de generación de la clave pública 42
6.1.7. Propósito de uso de la clave 43
6.2. Protección de clave privada y controles del módulo criptográfico 43
6.2.1. Controles y estándares del módulo criptográfico 43
6.2.2. Control dual n de m para el uso de la clave privada 43
6.2.3. Depósito de la clave privada 43
6.2.4. Backup de la clave privada 43
6.2.5. Archivo de la clave privada 43
6.2.6. Importación de la clave privada al módulo criptográfico 43
6.2.7. Almacenamiento de la clave privada en el módulo criptográfico 43
6.2.8. Método de activación de la clave privada 44
6.2.9. Método de desactivación de la clave privada 44
6.2.10. Método de destrucción de la clave privada 44
6.2.11. Clasificación del módulo criptográfico 44
6.3. Otros aspectos sobre la gestión de par de claves 44
6.3.1. Archivo de la clave pública 44
6.3.2. Periodos operativos de certificado y periodos de uso del par de claves 44
6.4. Datos de activación 44
6.4.1. Generación e instalación de datos de activación 44
6.4.2. Protección de los datos de activación 45
6.4.3. Otros aspectos de los datos de activación 45
6.5. Controles de seguridad informática 45
6.5.1. Requisitos técnicos de los controles de seguridad 45
6.5.2. Clasificación de la seguridad 45

6.6. Ciclo de vida de los controles técnicos 45
6.7. Controles de seguridad de red 45
6.8. Sello de tiempo 46

7. CERTIFICADOS, CRL, OCSP Y PERFILES 47
7.1. Perfil de certificado 47
7.1.1. Número de versión 47
7.1.2. Extensiones del certificado 47
7.1.3. Identificador (OID) del algoritmo de firma 49
7.1.4. Uso de nombres 50
7.1.5. Restricciones de nombres 50
7.1.6. Identificador de política de certificado 50
7.1.7. Uso de la extensión de política de restricciones 50
7.1.8. Sintaxis y semántica de la política de calificadores 50
7.1.9. Semántica del procedimiento para las extensiones críticas del certificado 50
7.2. Perfil de la CRL 51
7.2.1. Número de versión 51
7.2.2. CRL y extensiones 51
7.3. Certificado OCSP 51
7.3.1. Certificado utilizado para firmar el OCSP que valida el certificado de la SUBCA 51
7.3.2. Certificado utilizado para firmar el OCSP que valida el certificado regulado esta política 51

8. AUDITORÍAS 52
8.1. Frecuencia o circunstancias de la auditoría 52
8.2. Identidad y cualificación del auditor 52
8.3. Relación del auditor con el prestador 52
8.4. Temas tratados en la auditoría 52
8.5. Acciones a realizar como resultado de una deficiencia 52
8.6. Comunicación de resultados 52

9. OTROS ASUNTOS LEGALES 53
9.1. Tarifas 53
9.1.1. Tarifa para la emisión y renovación de certificados 53
9.1.2. Tarifa de acceso al certificado 53
9.1.3. Tarifa de acceso a OCSP o CRL 53
9.1.4. Tarifa para otros servicios 53
9.1.5. Política de reembolsos 53
9.2. Responsabilidad financiera 53

9.3. Confidencialidad de la información comercial 54
9.3.1. Alcance de la información confidencial 54
9.3.2. Alcance excluido de la información confidencial 54
9.3.3. Responsabilidad para la protección de la información confidencial 54
9.4. Privacidad de la información personal 54
9.4.1. Plan de privacidad 54
9.4.2. Información con tratamiento privado 54
9.4.3. Información no considerada con tratamiento privado 54
9.4.4. Responsabilidad para la protección de la información privada 54
9.4.5. Consentimiento de uso de la información privada 54
9.4.6. Divulgación de conformidad con procesos judiciales o administrativos 55
9.4.7. Otras casos para la divulgación de información 55
9.5. Derechos de propiedad intelectual 55
9.6. Obligaciones y Responsabilidad 55
9.6.1. Obligaciones de la CA 55
9.6.2. Obligaciones de la RA 56
9.6.3. Obligaciones del suscriptor 56
9.6.4. Obligaciones de los terceros que confían 57
9.6.5. Obligaciones de otras entidades 57
9.7. Renuncias de la garantía 57
9.8. Límites de responsabilidad 57
9.9. Indemnizaciones 58
9.10. Términos de uso y duración 58
9.10.1. Términos de uso 58
9.10.2. Duración 58
9.10.3. Supervivencia tras fin de la duración 58
9.11. Avisos y comunicaciones individuales a los participantes 58
9.12. Resolución de Conflictos 59
9.12.1. Procedimiento de conflictos 59
9.12.2. Mecanismo y período de notificación 59
9.12.3. Circunstancias por las que un OID puede ser modificado 59
9.13. Disposiciones para la resolución de disputas 59
9.14. Normativa aplicable 59
9.15. Cumplimiento de la normativa aplicable 61
9.16. Otras disposiciones 61
9.17. Otras provisiones 61

CONTROL DE DOCUMENTO

Título:	Política de Certificados de OGTIC CA Policy OID 1.3.6.1.4.1.49353.6.3.0		
Asunto:	SOFTWARE QUALIFIED CERTIFICATE FOR PUBLIC EMPLOYEE		
Estado:	Aprobado		
Versión:	v.1		
Código:	CP-OGTIC-EPL-SW	**Fecha de última revisión:**	18-11-2021
Idioma:	Castellano	**Revisión anterior:**	
		Núm. Páginas:	61

CONTROL DE CAMBIOS Y VERSIONES		
Fecha	**Versión**	**Motivo del Cambio**
18-11-2021	1.0	Primera versión.

ACERCA DEL DOCUMENTO

Este documento, con nivel de seguridad público, es propiedad de la Oficina Gubernamental de Tecnologías de la Información y Comunicación (**OGTIC)**. Para más información contacte con:

Av. 27 de Febrero #419 casi esquina Núñez de Cáceres.

Santo Domingo, República Dominicana

Tel.: (809)-286-1009

firmadigital@ogtic.gob.do

https://ca.ogtic.gob.do/ra/ogtic/

1. INTRODUCCIÓN

1.1. Resumen

La Oficina Gubernamental de Tecnologías de la Información y Comunicación (**OGTIC**), es una institución de naturaleza pública de República Dominicana, creada con la responsabilidad de planificar, dirigir y ejecutar las acciones necesarias para implementar el Gobierno Electrónico en el país mediante la difusión y uso de las Tecnologías de la Información y Comunicación (TIC).

Desde la perspectiva estratégica de ese rol, en el marco de la evolución de las TICs en el país, la OGTIC se fijó como objetivo constituirse como Entidad de Certificación, autorizada por Indotel para poder emitir certificados digitales, tanto a los ciudadanos como a todo el aparato de funcionarios y administraciones públicas del Poder Ejecutivo del país. Dicho objetivo fue conseguido mediante la Resolución de Indotel No. 024-18 de fecha 6 de junio de 2018, cuando la actual OGTIC, aún se llamaba OPTIC (Oficina Presidencial de Tecnologías de la Información y Comunicación).

A lo largo de los capítulos de las siguientes Políticas de Certificación, nos referiremos a la Oficina Gubernamental de Tecnologías de la Información y Comunicación, como OGTIC, a todos los efectos, Entidad de Certificación autorizada por Indotel, o según la terminología más actual, Prestador Cualificado de Servicios de Confianza (PCSC).

1.2. Identificación del Documento

Este documento está estructurado acorde al RFC3647, con el nombre **SOFTWARE QUALIFIED CERTIFICATE FOR PUBLIC EMPLOYEE**, codificado con el código **CP-OGTIC-EPL-SW**, y disponible en la url https://ca.ogtic.gob.do.

Las presentes políticas de certificado están identificadas con el OID número **1.3.6.1.4.1.49353.6.3.0**

1.3. Participantes

Se consideran las siguientes partes intervinientes:

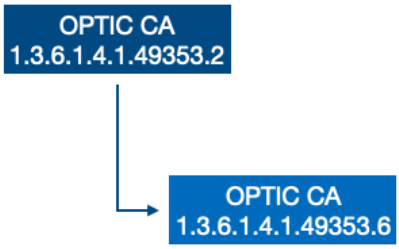
- **OGTIC:** Autoridad de Certificación (CA), que emite el certificado y actúa como Autoridad de Certificación autorizada por el INDOTEL, en adelante Prestador Cualificado de Servicios de Confianza u OGTIC PCSC.

- **Suscriptor**: persona física que adquiere el certificado digital proporcionado por OGTIC, mediante un acuerdo comercial.

- **Terceras partes** que confían en los certificados digitales emitidos por OGTIC.

1.3.1. Autoridad de Certificación

La Autoridad de Certificación de la OGTIC que emite el certificado digital regulado en esta política es OGTIC QUALIFIED CERTIFICATES, queda definida y regulada por su Autoridad de Certificación raíz OGTIC CA.



1.3.2. Autoridades de Registro

Entidad que actúa conforme esta Política de Certificados y, en su caso, mediante acuerdo suscrito con la CA OGTIC 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 OGTIC.

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 OGTIC CA, 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 vinculada a la institución pública en el ámbito de su actividad, permitiéndole asumir las mismas responsabilidades, compromisos o derechos en nombre de la institución que su cargo y posición le otorgue durante el período de validez y vigencia de su Certificado Digital.

Además, y de forma implícita, 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 OGTIC.

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

Av. 27 de Febrero #419 casi esquina Núñez de Cáceres.

Santo Domingo, República Dominicana

Tel.: (809)-286-1009

firmadigital@ogtic.gob.do

https://ca.ogtic.gob.do/ra/ogtic/

1.5.3. Persona que determina la idoneidad de las políticas

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

1.5.4. Procedimiento de aprobación de las políticas

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

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

La aprobación de políticas o cualquier cambio que afecte a éstas será debidamente notificada tal y como se recoge en el capítulo 2.3 de las presentes políticas.

1.6. Definiciones y Acrónimos

- CA: Certificate Authority.

- CP: Certificate Policy.
- CPS: Certificate Practice Statement.
- eIDAS: electronic IDentification, Authentication and trust Services (Reglamento UE 910/2014).
- HSM: Hardware Security Module, módulo de seguridad hardware.
- INDOTEL: Instituto Dominicano de la Telecomunicaciones.
- ONAPI: Oficina Nacional de la Propiedad Industrial.
- NTP: Network Time Protocol.
- OID: Object identifier, identificador de objeto único.
- PKI: Public Key Infrastructure, iInfraestructura de clave pública.
- PSCC: Prestador de Servicios de Certificación Cualificada.
- PCSC: Prestador Cualificado de Servicios de Confianza.
- QSCD: Qualified Signature Creation Device.
- QTSP: Qualified Trust Services Provider (PSC cualificado).
- ROA: Real Instituto y Observatorio de la Armada.
- SGSI: Sistema de Gestión de la Seguridad de la Información.
- TSA: TimeStamp Authority, Autoridad de Sellado de Tiempo.
- TSP: TimeStamping Protocol, protocolo de sellado de tiempo.
- TSP: Trust Services Provider, correspondencia en inglés a PSC.
- TST: TimeStamping Token, token de sellado de tiempo.

- TSU: TimeStamping Unit, Unidad de Sellado de Tiempo.
- UTC: Coordinated Universal Time.

2. PUBLICACIÓN Y REPOSITORIO DE CERTIFICADOS

2.1. Repositorios

Viafirma publicará las claves públicas de toda su cadena de confianza en el sitio web https://ca.ogtic.gob.do/ra/ogtic/. Y de forma explícita en las siguientes direcciones:

Root-CA:

https://ca.ogtic.gob.do/cer/ogticroot.crt

SubCA VIAFIRMA QUALIFIED CERTIFICATES:

https://ca.ogtic.gob.do/cer/ogticqualifiedcertificates.crt

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

http://crl.ogtic.gob.do/ogticqualifiedcertificates.crl

http://crl2.ogtic.gob.do/ogticqualifiedcertificates.crl

http://ca.ogtic.gob.do/ocsp

2.2. Publicación de la información de certificación

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

https://ca.ogtic.gob.do/politicas/CP-OGTIC-EPL-SW.pdf

2.3. Frecuencia de publicación

Cualquier versión que actualice la presente política de certificados será publicada en el sitio web https://ca.ogtic.gob.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} + {title} + {Organization Unit} + {Organization} + {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 se refiere al código de país expresado en dos caracteres según normativa ISO 3166

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 documento de identidad (cédula o pasaporte) acreditado por el suscriptor durante la emisión, precedido de un prefijo basado en el tipo de documento (identidad = IDC , o pasaporte = PAS) y el código país.

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 al departamento del que forma parte el suscriptor, dentro de la institución.

O = { Organization-name} para la pesente política estára asociado al nombre (razón social) de la empresa o institución.

T (title) = { Cargo} para la presente política estará asociado al cargo, posición o rol funcional que ocupa el suscriptor dentro de la institución.

DN Qualifier = para la presennte política se refiere al pefil de certificado digital.

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

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

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 basado en una clave privada custodiada y conocida por el propio suscriptor o titular del certificado. Dicha contraseña es necesaria para instalar el certificado en cualquier dispositivo y sin ella, la instalación y por tanto el uso del certificado, no serían posible. En resumen, el mero uso del certificado digital, evidencia posesión de la clave privada para poder instalar y usar el certificado digital.

3.2.2. Autenticación de la identidad de una organización

Para acreditar que la organización vinculada al certificado solicitado existe, será necesario adjuntar un documento vigente que deje constancia de esa existencia de dicha institución así como de su RNC y razón social. Para ello, se exigirá un documento oficial que acredite la creación o existencia de dicha institución (ley de creación, decreto, etc.).

3.2.3. Autenticación de la identidad de un individuo

La presente política autoriza la video-acreditación en las dos modalidades actualmente soportadas por la OGTIC, 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:

- Copia del documento oficial acreditativo de la creación o existencia de la institución pública.
- Carta de autorización en papel timbrado y con sello de la institución, en la que un superior jerárquico al suscriptor o un órgano colectivo con poder decisión en la institución, autorice la emisión de este perfil de certificado nombrándolo expresamente. En dicha carta, se deben informar los datos generales (nombre, apellidos y cédula) de:
    - Superior jerárquico o miembros del órgano colectivo con poder de decisión, así como sus respectivos roles dentro de la institución, y sus firmas.
    - Persona autorizada a obtener el certificado, así como su rol/cargo en la institución.
    - Datos de la institución (razón social y RNC).
    - Fecha de la carta.

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 la emisión del certificado.

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.
- 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 el pago en línea (si fuera el caso):
    - Integración con la pasarela de pago.

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 o revocado.

La soicitud de renovación podrá hacerse en cualquier momento desde la fecha de su emisión hasta la fecha de su vencimiento, siempre que no haya sido revocado antes de su fecha de 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 de un certificado digital en software (fichero con extensión .p12), el suscriptor podrá solicitar online la renovación de su certificado desde la plataforma publica habilitada al efecto disponible en la URL https://ca.ogtic.gob.do/ra/ogtic/.

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 de un certificado digital en software (fichero con extensión .p12), el suscriptor podrá solicitar online la revocación de su certificado desde la plataforma pública habilitada al efecto disponible en la URL https://ca.ogtic.gob.do/ra/ogtic/, introduciendo un código de revocación, previamente facilitado durante el proceso de solicitud/emisión.

4. CICLO DE VIDA DEL CERTIFICADO Y REQUISITOS OPERACIONALES

4.1. Solicitud de Certificados

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

4.1.1. Quién puede solicitar un certificado

En la presente política la solicitud del certificado puede hacerla cualquier persona natural que pueda ser identificado mediante un documento de identidad, que puede ser cédula o pasaporte, y que pueda jusitificar su vinculación a alguna institución pública.

4.1.2. Proceso de registro

Para la presente política la emisión del certificado implica obligatoriamente el registro de una solicitud de certificado, a instancia del propio suscriptor, consistente en el llenado de una serie de datos expuestos en un formulario web publicado en la URL https://ca.ogtic.gob.do/ra/ogtic/. Dichos datos incluiyen, al menos, nombre, apellidos, número de documento de identidad, dirección de correo electrónico, teléfono, razón social de la institución de la que forma parte, departamento, cargo y la contraseña privada que luego será imprescindible para la instalación local y uso del certificado digital por parte del suscriptor (dicha contraseña privada es encriptada por nuestro propio sistema, de manera que no está disponible ni visible para nadie, incluidos los registradores que tramiten dicha solicitud).

4.2. Proceso de solicitud de un certificado

La solicitud de certificados emitidos bajo la presente política debe originarse desde un único punto autorizado:

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

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 verificación de identidad iniciada mediante procedimiento automático haya sido rechazada, el solicitante podrá intentarlo mediante una solicitud asistida, y donde un registrador contactará con el solicitante para proceder a una vídeo-acreditación asistida. Si durante el proceso de vídeo-acreditación el registrador encargado del proceso considera que no tiene suficientes garantías para verificar la documentación y/o identificación del 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, permite ser tramitado 100% oline, incluyendo pago, validación de documentación, verificación de la identidad del invididuo y firma del contrato, de forma que si no hay inconvenientes en el proceso de solicitud, el proceso puede completarse en el mismo día de la solicitud, sin perjuicio de que el propio suscriptor no haya aportado la documetación requerida para 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 días 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 si tras la emisión del certificado, el suscriptor no contacta con la RA o la CA para informar de algún error en los datos del mismo.

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://ca.ogtic.gob.do/ra/ogtic/.

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.

La clave privada está protegida a través de una contraseña que solo debe conocer y/o estar en posesión del suscriptor, para evitar usurpación de identidad mediante el uso del certificado. Ni la RA ni la CA disponen de medios para conocer o proveer al suscriptor la contraseña privada que protege la clave privada del certificado, la cual fue elegida libremente por el suscriptor durante el llenado de datos del formulario de solicitud.

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, siempre que no haya sido revocado antes de la fecha de caducidad. Una vez superada la fecha de caducidad, el certificado no podrá ser renovado. Para que sea renovado, no basta con que la solicitud de renovación se haga antes de la fecha de caducidad, sino que la emisión del nuevo certificado (es decir, la culminación del proceso de renovación) debe producirse antes de la fecha de caducidad del certificado que se quiere renovar.

4.6.2. Quién puede solicitar la renovación

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

4.6.3. Proceso de solicitudes de renovación

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

4.6.4. Notificación de la renovación del certificado al suscriptor

El 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 si tras la emisión del certificado, el suscriptor no contacta con la RA o la CA para informar de algún error en los datos del mismo.

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://ca.ogtic.gob.do/ra/ogtic/.

4.6.7. Notificación de la renovación a otras entidades

OGTIC 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

OGTIC 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

OGTIC 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

OGTIC 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

OGTIC 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

OGTIC 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

OGTIC 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

OGTIC 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

OGTIC 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

OGTIC 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

OGTIC 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

OGTIC 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

OGTIC 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

OGTIC 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

OGTIC 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: se considera compromiso de claves al hecho de sospechar o tener evidencias de que una persona no autorizada puede conocer la contraseña privada del cetificado.

- Pérdida o extravío del certificado: cuando el titular del certifiado no pueda garantizar que tiene el control de uso del certificado, porque el dispositivo en el que estaba instalado ha sido extravíado.

- Cambios significativos en los datos contenidos en el certificado, como puede ser: nombre, apellido, email o número de cédula o pasaporte, depatamento de trabajo o cargo asignado.

- Desvinculación del suscriptor con la institución ya sea por despido, baja, o cualquier otra circunstancia que rompa la relación profesional que motivaba el uso del certificado.

- 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 por el suscriptor, por institución con la que éste estaba vinculado (justificando documentalmente desvinculación que motiva la revocación), 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 https://ca.ogtic.gob.do/ra/ogtic/, 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.

- 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 firmadigital@ogtic.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

OGTIC 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 página de la Autoridad de Registro (https://ca.ogtic.gob.do/ra/ogtic/), la revocación tendrá efecto inmediato.

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

OGTIC PCSC publica un servicio de validación online de sus certificados a través del protocolo OCSP y disponible en http://ca.ogtic.gob.do/ocsp.

4.9.10. Requisitos para la comprobación online del estado de revocación

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

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

OGTIC 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

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

4.9.14. Quién puede solicitar la suspensión

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

4.9.15. Procedimiento para la solicitud de suspensión

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

4.9.16. Límites del período de suspensión

OGTIC 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

OGTIC 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.

4.10.2. Servicios disponibles

OGTIC 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 página de la Autoridad de Registro (https://ca.ogtic.gob.do/ra/ogtic/).

4.10.3. Características opcionales

OGTIC 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 página de la Autoridad de Registro (https://ca.ogtic.gob.do/ra/ogtic/).

4.11. Fin de la suscripción

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

4.12.2. Prácticas de encapsulado y recuperación de recuperación de claves

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

5. INSTALACIÓN, GESTIÓN Y CONTROLES OPERACIONALES

5.1. Controles físicos

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

5.1.1. Localización y construcción

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

5.1.2. Acceso físico

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

5.1.3. Alimentación eléctrica y aire acondicionado

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

5.1.4. Exposición al agua

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

5.1.5. Protección y prevención de incendios

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

5.1.6. Sistema de almacenamiento

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

5.1.7. Eliminación de residuos

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

5.1.8. Backup remoto

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

5.2. Controles procedimentales

5.2.1. Roles de confianza

Lo establecido en la Declaración de Prácticas de Certificación de OGTIC 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 personas 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 institución 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 OGTIC PCSC.

5.2.3. Identificación y autenticación para cada rol

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

5.2.4. Roles que requieren separación de funciones

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

5.3. Controles personales

5.3.1. Requisitos de calificación, experiencia y autorización

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

5.3.2. Procedimientos de verificación de antecedentes

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

5.3.3. Requisitos de formación

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

5.3.4. Requisitos y frecuencia de formación

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

5.3.5. Frecuencia y secuencia de rotación de tareas

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

5.3.6. Sanciones por acciones no autorizadas

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

5.3.7. Requisitos para personal independiente

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

5.3.8. Documentación entregada al personal

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

5.4.2. Frecuencia del procesamiento de registros

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

5.4.3. Período de retención del registro de auditoría

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

5.4.4. Protección del registro de auditoría

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

5.4.5. Procedimiento del backup del registro de auditoría

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

5.4.6. Sistema de recolección de auditoría

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

5.4.7. Notificación de eventos

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

5.4.8. Evaluación de vulnerabilidades

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

5.5. Archivo de registros

5.5.1. Tipos de archivo de registros

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

5.5.2. Período de retención del archivo

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

5.5.3. Protección del archivo

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

5.5.4. Procedimientos para el backup del archivo

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

5.5.5. Requisitos para el sellado de tiempo del registro

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

5.5.6. Sistema de recolección del archivo

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

5.5.7. Procedimientos para obtener y verificar la información del archivo

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

5.7.2. Obsolescencia y deterioro

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

5.7.3. Procedimientos ante compromiso de clave de una entidad

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

5.7.4. Plan de continuidad de negocio ante desastres

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

5.8. Cese de la CA o RA

Lo establecido en la Declaración de Prácticas de Certificación de OGTIC 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 las claves del certificado son generadas por la CA.

6.1.2. Entrega de la clave privada al suscriptor

La clave privada del certificado es generada por la CA y entregada al susciptor mediante la descarga segurra del par de claves en formato .p12. La CA no retiene copia de la clave privada asociada al certificado generado.

6.1.3. Entrega de la clave pública al suscriptor

La clave pública del certificado emitido será publicada en el sitio web de OGTIC 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 OGTIC PCSC.

6.1.5. Tamaño de las claves

Con carácter general, el tamaño de las claves generadas por OGTIC 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 OGTIC 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 OGTIC 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 OGTIC PCSC.

6.2.3. Depósito de la clave privada

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

6.2.4. Backup de la clave privada

Para esta política no hay backup de la clave privada del certificado.

6.2.5. Archivo de la clave privada

Para esta política no hay archivo de la clave privada del certificado.

6.2.6. Importación de la clave privada al módulo criptográfico

Para esta política no hay importación de la clave privada del certificado.

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

Para esta política no hay almacenamiento de la clave privada del certificado en el módulo criptográfico.

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 OGTIC 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

Para esta política no se contemplan.

6.2.11. Clasificación del módulo criptográfico

Para esta política no aplica.

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 2 años (730 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 OGTIC 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 OGTIC PCSC.

6.5.2. Clasificación de la seguridad

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

6.6. Ciclo de vida de los controles técnicos

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

6.7. Controles de seguridad de red

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

6.8. Sello de tiempo

Lo establecido en la Declaración de Prácticas de Certificación de OGTIC 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	
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>*
Title, title	*<CARGO>*
Organization Unit	*<DEPARTAMENTO>*
Organization Name	*<RAZÓN SOCIAL DE LA ENTIDAD>*
DN Qualifier	*<SOFTWARE QUALIFIED CERTIFICATE FOR PUBLIC EMPLOYEE>*
Issuer Name	
Country or Region	*DO*
Organization	*OFICINA GUBERNAMENTAL DE LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACION - OGTIC*
Common Name	*OGTIC 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 + 2 AÑOS >

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 45 86 27 4C 9C 06 97 DE 8D 44 DA 9B 32 3D 3F 0D FC 97 A2 45

Extension Authority Key Identifier (2.5.29.35)

Critical NO

Key ID D7 9B 06 73 B3 4E 99 F1 C3 6D B7 15 01 A4 FA 8E 5F 39 1A D4

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	(1.3.6.1.4.1.49353.6.3.0)
Policy ID #2	(1.3.6.1.4.1.27395.6.2.3.0)
Qualifier ID #1	User Notice (1.3.6.1.5.5.7.2.2)
User Notice	QUALIFIED CERTIFICATE FOR PUBLIC EMPLOYEE
Qualifier ID #2	Certification Policies Statements (1.3.6.1.5.5.7.2.1)
CPS URI	http://ca.ogtic.gob.do
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://crl.ogtic.gob.do/ogticqualifiedcertificates.crl
URI	http://crl2.ogtic.gob.do/ogticqualifiedcertificates.crl
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO
Method #1	CA Issuers (1.3.6.1.5.5.7.48.2)
URI	http://ca.ogtic.gob.do/cer/ogticqualifiedcertificates.crt
Method #2	Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
URI	http://ca.ogtic.gob.do/ocsp
Other Field	Qualified Certificate Statements (1.3.6.1.5.5.7.1.3)
Data	30 0A 30 08 06 06 04 00 8E 46 01 01
Fingerprints	
SHA-256	6F FA C4 19 68 5A AF 1D 7D 00 C3 B4 16 35 20 20 9E D3 BD 8C 93 84 A6 5D 83 85 CA D3 F5 AA D6 14
SHA-1	41 30 8A 82 2B 28 36 38 6B FF 0C B5 E1 C8 84 AD 47 55 2E 14

7.1.3. Identificador (OID) del algoritmo de firma

SHA-256 with RSA Encryption (1.2.840.113549.1.1.1).

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	(1.3.6.1.4.1.49353.6.3.0)
Policy ID #2	(1.3.6.1.4.1.27395.6.2.3.0)
Qualifier ID #1	User Notice (1.3.6.1.5.5.7.2.2)
User Notice	QUALIFIED CERTIFICATE FOR PUBLIC EMPLOYEE
Qualifier ID #2	Certification Policies Statements (1.3.6.1.5.5.7.2.1)
CPS URI	http://ca.ogtic.gob.do

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 OGTIC PCSC, y debidamente informada en el OID 2.5.29.31 “CRL Number” de la estructura de la CRL.

7.2.2. CRL y extensiones

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

7.3. Certificado OCSP

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

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

C=DO,

O=OFICINA GUBERNAMENTAL DE LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACION - OGTIC,

CN=OGTIC OCSP ROOT

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

C=DO,

O=OFICINA GUBERNAMENTAL DE LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACION - OGTIC,

CN=OGTIC OCSP SUBCA

8. AUDITORÍAS

8.1. Frecuencia o circunstancias de la auditoría

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

8.2. Identidad y cualificación del auditor

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

8.3. Relación del auditor con el prestador

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

8.4. Temas tratados en la auditoría

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

8.5. Acciones a realizar como resultado de una deficiencia

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

8.6. Comunicación de resultados

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

9. OTROS ASUNTOS LEGALES

9.1. Tarifas

9.1.1. Tarifa para la emisión y renovación de certificados

OGTIC 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://ogtic.gob.do.

9.1.2. Tarifa de acceso al certificado

OGTIC 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://ogtic.gob.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 OGTIC PCSC . Su uso es gratuito.

9.1.4. Tarifa para otros servicios

OGTIC 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://ogtic.gob.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

OGTIC 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://ogtic.gob.do.

9.2. Responsabilidad financiera

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

9.3.2. Alcance excluido de la información confidencial

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

9.3.3. Responsabilidad para la protección de la información confidencial

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

9.4. Privacidad de la información personal

9.4.1. Plan de privacidad

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

9.4.2. Información con tratamiento privado

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

9.4.3. Información no considerada con tratamiento privado

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

9.4.4. Responsabilidad para la protección de la información privada

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

9.4.5. Consentimiento de uso de la información privada

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

9.4.6. Divulgación de conformidad con procesos judiciales o administrativos

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

9.4.7. Otras casos para la divulgación de información

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

9.5. Derechos de propiedad intelectual

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

9.6. Obligaciones y Responsabilidad

9.6.1. Obligaciones de la CA

La Entidad de Certificación OGTIC 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) Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida, destrucción o falsificación.

k) 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 OGTIC 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 OGTIC 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 OGTIC 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

OGTIC PCSC no establece obligaciones a otras entidades participantes.

9.7. Renuncias de la garantía

OGTIC 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 OGTIC 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 OGTIC 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

OGTIC 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

OGTIC 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://ogtic.gob.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. De forma general para el perfil de certificado regulado en esta política, la duración estipulada será de un máximo de dos (2) años.

9.10.3. Supervivencia tras fin de la duración

OGTIC 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

OGTIC 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

OGTIC 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 OGTIC 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://ogtic.gob.do.

9.14. Normativa aplicable

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

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

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

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

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

    - Norma Complementaria sobre los Procedimientos de Autorización y Acreditación.

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

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

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

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

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

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

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

- ETSI EN 319 412: Certificate Profiles.

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

- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles.

- RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

- RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs).

9.15. Cumplimiento de la normativa aplicable

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

9.16. Otras disposiciones

No se definen otras disposiciones adicionales.

9.17. Otras provisiones

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

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