Políticas de Certificación

Certificados de Ciudadanos en Formato Software

v1.0

ÍNDICE

CONTROL DE DOCUMENTO

Título:	Políticas de Certificación		
Asunto:	Certificados de Ciudadanos en Formato Software		
Autor:	Benito Galán		
Versión:	v1.0	**Fecha:**	21-06-2017
Código:	OPTIC PC CI SW	**Revisión anterior:**	
Idioma:	Español	**Nº. Páginas:**	64

CONTROL DE CAMBIOS Y VERSIONES		
Fecha	**Versión**	**Motivo del Cambio**
21-06-2017	1.0	Primera versión.

1. INTRODUCCIÓN

1.1. Consideración Inicial

Por no haber una definición taxativa de los conceptos de Declaración de Prácticas de Certificación y Políticas de Certificación y debido a algunas confusiones formadas, entendemos que es necesario establecer sus diferencias en base a las siguientes definiciones:

Políticas de Certificación es el conjunto de reglas que definen la aplicabilidad de un Certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y utilización comunes, es decir, en general una Política de Certificación debe definir la aplicabilidad de tipos de Certificados para determinadas aplicaciones que exigen los mismos requisitos de seguridad y formas de usos.

La **Declaración de Prácticas de Certificación (CPS - Certificate Practice Statement)** es definida como un conjunto de prácticas adoptadas por una Entidad de Certificación (CA) para la emisión de Certificados. En general contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los Certificados, además sobre la relación de confianza entre el Firmante/Suscriptor o Tercero que confía y la Entidad de Certificación. Pueden ser documentos absolutamente comprensibles y robustos, que proporcionan una descripción exacta de los servicios ofertados, procedimientos detallados de la gestión del ciclo vital de los Certificados, etc.

Estos conceptos de Políticas de Certificación y Declaración de Prácticas de Certificación son distintos, pero aún así es muy importante su interrelación.

Una CPS detallada no forma una base aceptable para la interoperabilidad de Entidades de Certificación. Las Políticas de Certificación sirven mejor como medio en el cual basar estándares y criterios de seguridad comunes.

En definitiva una política define **"qué"** requerimientos de seguridad son necesarios para la emisión de los Certificados. La CPS nos dice **"cómo"** se cumplen los requerimientos de seguridad impuestos por la política.

1.2. Generalidades

El presente documento especifica las Políticas de Certificación del **CERTIFICADO DE CIUDADANOS EN FORMATO SOFTWARE, EMITIDO POR LA CA OPTIC**, y está basada en la especificación del estándar RFC 2527 – *Internet X. 509 Public Key Infrastructure Certificate Policy*, de IETF y del ETSI TS 101 456 V1.2.1.

Estas Políticas de Certificación están en conformidad con las disposiciones legales que rigen **las Firmas Digitales en la República Dominicana**, en especial en lo que establece la Ley No.126-02, su Reglamento de Aplicación (Dec. No. 335-03) y sus normas complementarias, cumpliendo todos los requisitos técnicos y de seguridad exigidos para la emisión de Certificados reconocidos.

Estas Políticas definen las reglas y responsabilidades que deben seguir aquellas Entidades de Certificación que deseen emitir el tipo de Certificado definido en el presente documento, imponiendo además ciertas obligaciones que deben ser tenidas en cuenta por los Firmantes/Suscriptores y Terceros que confían en virtud de su especial relación con este tipo de Certificados.

De esta forma, cualquier CA que emita este tipo de Certificados, se ajustará a los niveles de seguridad que se detallan en estas Políticas de Certificación e informarán a sus Firmantes/Suscriptores de su existencia.

Los Certificados emitidos bajo estas Políticas requerirán la autenticación de la identidad de los Firmantes/Suscriptores. Esta identificación y autenticación se realizará según los términos de estas Políticas.

La CA revocará sus Certificados según lo dispuesto en estas Políticas.

La CA conservará los registros e incidencias de acuerdo con lo que se establece en estas Políticas.

Las funciones críticas del servicio se realizarán al menos por dos personas.

Las contraseñas de los Firmantes/Suscriptores tienen un período de validez determinado por estas Políticas y en ningún caso podrán realizarse copias de *respaldo*, ni almacenarse por la CA.

La información personal recabada del Firmante/Suscriptor se recogerá con el debido consentimiento del interesado y únicamente para los fines propios del servicio de Certificación, el cual podrá ejercitar en todo caso sus oportunos derechos de información, rectificación y

cancelación. La CA respetará así mismo la normativa aplicable en materia de protección de datos.

La actividad de la CA podrá ser sometida a la inspección por la OPTIC como la Autoridad de Políticas (PA) o por personal delegado por la misma.

En lo que se refiere al contenido de estas Políticas de Certificación, se considera que el lector conoce los conceptos básicos de PKI (Public Key Infrastructure), Certificación y firma digital, recomendando que, en caso de desconocimiento de dichos conceptos, el lector se informe al respecto. En la página web de la OPTIC (www.optic.gob.do) se publicarán algunas informaciones útiles, así como en los ANEXOS de este documento.

1.3. Identificación de Política

La forma de identificar los distintos tipos de Certificados de Firma Digital es a través de identificadores de objeto (OID's). Un OID concreto permite a las aplicaciones distinguir claramente el Certificado que se presenta.

El identificador de política está compuesto por una serie de números separados entre sí por puntos y con un significado concreto de cada uno de ellos. Dentro de un mismo tipo de Certificado podemos definir diferentes subtipos en función a algunas características especiales.

Las presentes Políticas de Certificación están identificadas con el siguiente OID:

1.3.6.1.4.1.49353.3.1.1

iso (1)
org (3)
dod (6)
internet (1)
private (4)
enterprise (1)
Certificate Authority for Presidential Office of Information and Communication Technologies of the Dominican Republic (49353)
Políticas de Certificación (3)
Certificados para Ciudadanos (1)
Emitidos en formato software (1)

1.4. Comunidad y Ámbito de Aplicación

1.4.1. Entidad de Certificación (CA)

Es la entidad responsable de la emisión y gestión de los Certificados Digitales. Actúa como tercera parte de confianza entre el Firmante/Suscriptor y el Tercero que confía, en las relaciones electrónicas, vinculando una determinada clave pública con una persona (Firmante/Suscriptor) a través de la emisión de un Certificado.

El emisor de este tipo de Certificado es la CA OPTIC a través de su subCA e instrumentado por aquellas Unidades de Registro autorizadas por ésta.

1.4.2. Unidad de Registro

Una Unidad de Registro (UR) o Autoridad de Registro (RA – Registration Authority) es un ente que actúa conforme estas Políticas de Certificación y, en su caso, mediante acuerdo suscrito con la CA, cuyas funciones son la gestión de las solicitudes, identificación y registro de los solicitantes de los Certificados y aquellas que se dispongan en las Prácticas de Certificación concretas.

Para las presentes Políticas de Certificación, **la OPTIC actuará con sus propias Unidades de Registro.**

1.4.3. Firmante o Suscriptor

Bajo estas Políticas el Firmante o Suscriptor es una persona física cuya identidad personal queda vinculada a los datos firmados electrónicamente a través de la clave pública contenida en el Certificado.

1.4.4. Tercero que confía

En estas Políticas se entiende por Tercero que confía la persona que voluntariamente confía en el Certificado emitido a favor del emisor por la CA, lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado y en consecuencia se sujeta a lo dispuesto en estas Políticas, por lo que no se requerirá acuerdo posterior alguno.

1.4.5. Solicitante

Se entenderá por Solicitante la persona física que solicita el Certificado. A efectos de estas Políticas, la figura del Solicitante coincidirá con la figura del Firmante/Suscriptor.

1.4.6. Institución

No aplica en estas políticas.

1.4.7. Ámbito de Aplicación y Usos

El Certificado emitido bajo las presentes Políticas permite identificar a una persona física en el ámbito de sus actividades. El Certificado emitido bajo estas Políticas puede ser utilizado con los siguientes propósitos:

- Identificación del Firmante/Suscriptor: El Firmante/Suscriptor del Certificado puede autenticar frente a otra parte su identidad, demostrando la asociación de su clave privada con la respectiva clave pública contenida en el Certificado.

- El Firmante/Suscriptor podrá identificarse válidamente ante cualquier persona mediante la firma de un correo electrónico o cualquier otro tipo de documento.

- Integridad del documento firmado: La utilización de este Certificado garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Firmante/Suscriptor. Se certifica que el mensaje recibido por el Tercero que confía es el mismo que fue emitido por el Firmante/Suscriptor.

- No repudio de origen: Con el uso de este Certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Firmante/Suscriptor que ha firmado no puede negar la autoría o la integridad del mismo.

- A pesar de ser posible su utilización para la encriptación de datos, la CA ni la UR se responsabilizan por esta actividad, debido a que, por motivos de seguridad, estas Políticas determinan que la CA y la UR no guarden copia de la clave privada del Firmante/Suscriptor. No se garantiza, por tanto, la recuperación de los datos cifrados en caso de pérdida de la clave privada por parte del Firmante/Suscriptor.

1.4.7.1. Usos Prohibidos y no Autorizados

Los Certificados sólo podrán ser utilizados con los límites y para los usos para los que hayan sido emitidos en cada caso.

El uso de los Certificados que implique la realización de operaciones no autorizadas según las Políticas de Certificación aplicables a cada uno de los Certificados, según el conjunto de prácticas adoptadas por la UR, según los Contratos suscritos entre la UR y sus Firmantes/Suscriptores y aquellos prohibidos por las leyes aplicables serán considerados como usos indebidos, exonerándose a la CA y a la UR, de cualquier responsabilidad por este uso indebido de los Certificados que realice el Firmante/Suscriptor o cualquier Tercero en función de la legislación vigente.

En función de los servicios prestados por la CA mediante la emisión de sus Certificados, no es posible por parte de la CA ni de la UR el acceso o conocimiento del contenido del mensaje al que haya sido adjuntado o con el que se relacione el uso de un Certificado emitido por la CA.

Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de la CA ni de la UR emitir valoración alguna sobre dicho contenido, asumiendo por tanto el signatario del Certificado de Firma Digital cualquier responsabilidad derivada del contenido de dicho mensaje atado al uso de un Certificado emitido por la CA. Asimismo, le será imputable al signatario del Certificado de Firma Digital cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en las Políticas de Certificación aplicables a cada uno de los Certificados, el conjunto de prácticas adoptadas por la UR , los contratos suscritos entre la UR y sus Firmantes/Suscriptores y aquellos prohibidos por la leyes aplicables, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

1.5. Contacto de la CA

Las presentes Políticas de Certificación están administradas y gestionadas por la Autoridad de Políticas de la CA OPTIC, pudiendo ser contactada por los siguientes medios:

E-mail:	firmadigital@optic.gob.do
Teléfono:	+1 809-286-1009
Web:	https://ca.optic.gob.do/politicas

2. CLÁUSULAS GENERALES

2.1. Obligaciones

2.1.1. Obligaciones de la CA

La CA OPTIC 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) No almacenar ni copiar la clave privada o los datos de creación de firma del Firmante/Suscriptor para la instalación 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.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1.1. Identificación en la Unidad de Registro

La Unidad de Registro que actúa bajo estas Políticas de Certificación estará obligadas a cumplir con lo dispuesto por la normativa vigente, y además a:

a) Respetar lo dispuesto en estas Políticas.

b) Comprobar la identidad de los solicitantes de Certificados.

c) Verificar la exactitud y autenticidad de la información suministrada por el solicitante.

d) Archivar por período dispuesto en la legislación vigente los documentos suministrados por el Firmante/Suscriptor.

e) Respetar lo dispuesto en los contratos firmados con la CA y con el Firmante/Suscriptor.

f) Informar a la CA las causas de revocación, siempre y cuando tenga conocimiento.

3.1.2. Solicitante

El solicitante de un Certificado estará obligado a cumplir con lo dispuesto por la normativa aplicable y además a:

a) Suministrar a la Unidad de Registro la información necesaria para realizar una correcta identificación.
b) Confirmar la exactitud y veracidad de la información suministrada.
c) Notificar cualquier cambio en los datos aportados para la creación del Certificado durante su período de validez.
d) Confirmar durante el proceso de renovación de su Certificado que sus datos siguen siendo válidos y no han cambiado respecto a los informados durante el proceso de registro y creación del Certificado.

3.1.3. Firmante/Suscriptor

El Firmante/Suscriptor de un Certificado estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

a) Custodiar su clave privada de manera diligente.
b) Usar el Certificado según lo establecido en las presentes Políticas de Certificación.
c) Respetar lo dispuesto en el contrato firmado con la Unidad de Registro.
d) Informar de la existencia de alguna causa de revocación.
e) Notificar cualquier cambio en los datos aportados para la creación del Certificado durante su período de validez.

3.1.4. 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 confía, y aceptar sujetarse a las mismas.

3.1.5. Institución

No aplica.

3.1.6. Repositorio

La información relativa a la revocación de los Certificados se mantendrá accesible al público en los términos establecidos en la normativa vigente.

3.2. Responsabilidad

La CA dispondrá en todo momento de un seguro de responsabilidad civil en los términos que marque la legislación vigente.

La CA actuará en la cobertura de sus responsabilidades por sí o a través de la entidad aseguradora, satisfaciendo los requerimientos de los solicitantes de los Certificados, de los signatarios y de los Terceros que confíen en los Certificados.

Las responsabilidades de la CA incluyen las establecidas por las presente Políticas de Certificación, así como las que resulten de aplicación como consecuencia de la normativa dominicana e internacional.

La CA será responsable del daño causado ante el Firmante/Suscriptor o cualquier persona que de buena fe confíe en el Certificado, siempre que exista dolo o culpa grave respecto de:

a) La exactitud de toda la información contenida en el Certificado en la fecha de su emisión.

b) la verificación de que, en el momento de la entrega del Certificado, se comprobó que la clave privada correspondía a la clave pública dada o identificada en el Certificado.

c) La garantía de que la clave pública y la privada funcionan conjunta y complementariamente.

d) La correspondencia entre el Certificado solicitado y el Certificado entregado.

e) Cualquier responsabilidad que se establezca por la legislación vigente.

3.2.1. Exoneración de responsabilidad

La CA y la Unidad de Registro no serán responsables en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

a) Estado de Guerra, desastres naturales o cualquier otro caso de fuerza mayor.

b) Por el uso de los Certificados siempre y cuando incumpla lo dispuesto en la normativa vigente y las presentes Políticas de Certificación.

c) Por el uso indebido o fraudulento de los Certificados emitidos por la Entidad de Certificación.

d) Por el uso de la información contenida en el Certificado.

e) Por el incumplimiento de las obligaciones establecidas para el Firmante/Suscriptor o Terceros que confían en la normativa vigente, las presentes Políticas de Certificación o en las Prácticas Correspondientes.

f) Por el perjuicio causado durante el período de verificación de la solicitud de revocación.

g) Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.

h) Por la no recuperación de documentos cifrados con la clave pública del Firmante/Suscriptor.

i) Fraude en la documentación presentada por el solicitante.

3.2.2. Límite de responsabilidad en caso de pérdidas por transacciones

Independientemente del importe de las transacciones, este tipo de Certificados tienen un límite de responsabilidad por cuenta de la OPTIC igual a ochenta mil dólares de los Estados Unidos de América (USD$ 80,000.00) o su equivalente en moneda de la República Dominicana. Para los casos no previstos por la ley, deberán establecerse garantías particulares a través de seguros específicos que se negociarán individualmente.

3.2.3. Responsabilidad financiera

Ni la CA ni la UR asumen ningún tipo de responsabilidad financiera por el uso dado por el Firmante/Suscriptor al Certificado Digital.

3.3. Interpretación y ejecución

3.3.1. Legislación

La ejecución, interpretación, modificación o validez de las presentes Políticas se regirá por lo dispuesto en la legislación dominicana vigente.

3.3.2. Independencia

La invalidez de una de las cláusulas contenidas en estas Políticas de Certificación no afectará al resto del documento. En tal caso, la mencionada cláusula no tendrá efecto.

3.3.3. Notificación

Cualquier notificación referente a las presentes Políticas de Certificación se realizará a través de carta, correo electrónico, o por cualquier otro medio fehaciente, con al menos treinta (30) días de anticipación a su implementación.

3.3.4. Procedimiento de resolución de disputas

Toda controversia o conflicto que se derive del presente documento se resolverá definitivamente en base a los procedimientos recogidos en el Reglamento de Solución de Controversias asociado a la Ley 126-02.

4. REQUERIMIENTOS OPERACIONALES

4.1. Solicitud de Certificados

La CA, por sí misma, o por medio de la Unidad de Registro, se asegurará de que el titular del Certificado esté correctamente acreditado.

Las solicitudes podrán hacerse de forma en línea (online), accediendo al formulario web habilitado para cada caso, y aportando la información requerida.

Esta información se ajustará a la validación de datos configurada para cada caso, y será verificada posteriormente por un registrador durante el proceso de acreditación y registro.

La solicitud debe ir acompañada de una **copia de la cédula de identidad y electoral o del pasaporte**. Esta copia se refiere a una copia digital en formato PDF, PNG o JPG, y que podrá adjuntar a la solicitud desde la herramienta habilitada en internet para tal efecto.

Durante el proceso de acreditación física, el Firmante/Suscriptor debe presentar la Cédula de identidad y electoral original o el pasaporte original.

El punto de acceso a las solicitudes en línea (online), asociadas a las presentes Políticas estará identificado debidamente en el menú principal de la herramienta habilitada a la Unidad de Registro, disponible en la siguiente dirección:

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

4.1.1. Registro

a) Antes de comenzar una relación contractual, la CA, por medio de la Unidad de Registro, informará al Firmante/Suscriptor de los términos y condiciones relativos al uso del Certificado.

b) Se comunicará esta información a través de un medio de comunicación perdurable, susceptible de ser transmitido electrónicamente y en un lenguaje comprensible.

c) La CA, por medio de la UR, comprobará, de acuerdo con la legislación vigente, la identidad y los atributos específicos del Firmante/Suscriptor. La comprobación de la identidad se realizará

mediante la presentación física del Firmante/Suscriptor y la exhibición por éste de la cédula de identidad y electoral o del pasaporte.

d) Para las presentes políticas, se registrará la siguiente información:

- Nombre
- Apellidos
- Cédula de identidad y electoral
- Correo Electrónico

Estos campos son obligatorios.

Además se recoge otro tipo de información con fines estadísticos como:

- Número de teléfono
- ¿Es poseedor de algún otro tipo de certificado?

De toda la información registrada, sólo se incluirá como parte del Certificado Digital la siguiente:

- Nombre
- Apellidos
- Cédula de identidad y electoral
- País. Valor constante DO. No se muestra en el formulario
- Correo Electrónico

f) La Unidad de Registro registrará toda la información usada para comprobar la identidad de los Firmantes/Suscriptores, incluyendo cualquier número de referencia en la documentación empleada para la verificación y los límites de su validez.

g) La Unidad de Registro guardará el contrato firmado con el Firmante/Suscriptor, el cual incluirá:

1) Acuerdo de las obligaciones del Firmante/Suscriptor.

2) Consentimiento para que la Unidad de Registro guarde la información usada para el registro, así como para el traspaso de información a la propia CA.

3) Si, y bajo qué condiciones el Firmante/Suscriptor consiente la publicación de su Certificado.

4) Que la información contenida en el Certificado es correcta.

h) Los registros identificados se conservarán durante el período de tiempo que se indicó al Firmante/Suscriptor y que es necesario a efectos probatorios en los procedimientos legales.

i) Si el par de claves no es generado por la CA, ésta realizará los esfuerzos que razonablemente estén a su alcance para confirmar que el Firmante/Suscriptor está en posesión de la clave privada asociada a la clave pública.

j) La CA cumplirá con todos los requisitos impuestos por la legislación aplicable en materia de protección de datos, en concreto, los referidos en la Ley No. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados

4.2. Emisión de Certificados

4.2.1. Emisión de Nuevo Certificado

La CA, y en su nombre la Unidad de Registro, pondrá todos los medios a su alcance para garantizar que la emisión de Certificados se realice de una forma segura, en concreto:

a) Cuando la CA genere las claves del Firmante/Suscriptor, que el procedimiento de emisión del Certificado está ligado de manera segura a la generación del par de claves.

b) Cuando la CA no genere las claves del Firmante/Suscriptor, que la clave fue generada en un navegador compatible y que únicamente desde ese mismo navegador el Certificado finalmente podrá ser instalado.

c) La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar la unicidad de los nombres e identificadores asignados por la CA a los Firmantes/Suscriptores.

d) La confidencialidad y la integridad de los datos registrados serán especialmente protegidos cuando estos datos sean intercambiados con el Firmante/Suscriptor o entre distintos componentes del sistema de Certificación.

e) La CA, y en su nombre la Unidad de Registro, verificará que el registro de los datos es intercambiado con proveedores de servicios reconocidos, cuya identidad es autenticada.

f) La CA, y en su nombre la UR, notificará al solicitante de la emisión de su Certificado.

4.2.2. Renovación del Certificado

La CA, y en su nombre la Unidad de Registro, pondrá todos los medios a su alcance para asegurar que la renovación de Certificados se realice de una forma segura, en concreto:

a) Que el Certificado que va a proceder a su renovación quede vinculado en los registros con el nuevo Certificado que se va a emitir.

b) Que el Certificado que va a renovar, será revocado automáticamente una vez haya sido confirmada la renovación, de forma que no podrá ser usado al mismo tiempo que el nuevo Certificado.

c) Que los datos registrados en el nuevo Certificado se corresponden con los informados para el Certificado que se va a renovar, y si éstos ya no están vigentes, se ofrezca la posibilidad al Firmante/Suscriptor de solicitar los cambios oportunos, y en cuyo caso, la CA, y en su nombre la Unidad de Registro, verificará que el registro de los datos es intercambiado con proveedores de servicios reconocidos, cuya identidad es autenticada.

d) La CA, y en su nombre la UR, notificará al solicitante de la revocación de su anterior Certificado y de la creación del nuevo Certificado.

4.3. Aceptación de Certificados

La entrega del Certificado, por cualquiera de las vías previstas, y la firma del Contrato para la emisión del certificado asociado a la presente, implicarán la aceptación del Certificado por parte del Firmante/Suscriptor.

No obstante, a partir de la entrega del Certificado, el Firmante/Suscriptor dispondrá de un período de siete días calendario para revisar el mismo, determinar si es adecuado y si los datos se corresponden con la realidad. En caso de que existiera alguna diferencia entre los datos suministrados a la UR y el contenido del Certificado, el Firmante/Suscriptor se comunicará de inmediato con la UR para que proceda a su revocación y a la emisión de un nuevo Certificado. La CA, a través de la UR, entregará el nuevo Certificado sin coste para el Firmante/Suscriptor. Transcurrido dicho período sin que haya existido comunicación, se entenderá que el Firmante/Suscriptor ha confirmado la aceptación del Certificado y de todo su contenido. La sustitución del Certificado de Firma Digital por cualquier discrepancia en los datos reportados fuera del indicado plazo de siete (7) días será pagada por el Firmante/Suscriptor como si se tratara de un nuevo Certificado.

Aceptando el Certificado, el Firmante/Suscriptor confirma y asume la exactitud del contenido del mismo, con las consiguientes obligaciones que de ello se deriven frente a la Unidad de Registro, la CA o cualquier Tercero que de buena fe confíe en el contenido del Certificado.

4.4. Revocación de Certificados

4.4.1. Aclaraciones previas

Se entenderá por revocación aquel cambio en el estado de un Certificado motivado por la pérdida de validez de un Certificado en función de alguna circunstancia distinta a la caducidad del mismo. Al hablar de revocación nos referiremos siempre a la pérdida de validez definitiva.

4.4.2. Causas de revocación

Los Certificados se revocarán cuando concurra alguna de las circunstancias siguientes:

a) Solicitud voluntaria del Firmante/Suscriptor.

b) Pérdida o inutilización por daños del soporte del Certificado.

c) Fallecimiento del Firmante/Suscriptor o incapacidad sobrevenida, total o parcial.

d) Cese en la actividad del prestador de servicios de Certificación salvo que los Certificados expedidos por aquel sean transferidos a otro prestador de servicios.

e) Inexactitudes graves en los datos aportados por el signatario para la obtención del Certificado, así como la concurrencia de circunstancias que provoquen que dichos datos, originalmente incluidos en el Certificado, no se adecuen a la realidad.

f) Que se detecte el Certificado del Firmante/Suscriptor o el Certificado Raíz de la CA han sido comprometidos, bien porque concurran las causas de pérdida, robo, hurto, modificación o su divulgación o revelación, bien por cualquier otra circunstancia, incluidas las fortuitas, que indiquen el uso del Certificado por persona distinta al titular.

g) Por incumplimiento por parte de la Unidad de Registro, de la CA o el Firmante/Suscriptor de las obligaciones establecidas en estas Políticas.

h) Por la resolución del contrato suscrito por la UR con el Firmante/Suscriptor.

i) Por cualquier causa que razonablemente induzca a creer que el servicio de Certificación haya sido comprometido hasta el punto que se ponga en duda la fiabilidad del Certificado.

j) Por resolución judicial o administrativa que lo ordene.

k) Por la concurrencia de cualquier otra causa especificada en las presentes Políticas.

4.4.3. Quién puede solicitar la revocación

La revocación de un Certificado podrá solicitarse únicamente por:

- el Firmante/Suscriptor.
- por la propia CA.

Todas las solicitudes serán en todo caso autenticadas.

4.4.4. Procedimiento de solicitud de revocación

La UR realizará los esfuerzos que razonablemente estén a su alcance para confirmar que los Certificados son revocados basándose en solicitudes de revocación autorizadas y validadas.

El Firmante/Suscriptor cuyo Certificado haya sido revocado será informado del cambio de estado de su Certificado. La UR utilizará todos los medios a su alcance para conseguir este objetivo, pudiendo intentar la mencionada comunicación por correo electrónico o teléfono.

Una vez que un Certificado es revocado, este no podrá volver a su estado activo. La revocación de un Certificado es una acción, por tanto, definitiva.

El servicio de gestión de las revocaciones estará disponible las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema, servicio o cualquier otro factor que no esté bajo el control de la CA y la UR, ambas realizarán los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio no se encuentre indisponible durante más tiempo que el período máximo dispuesto en estas Políticas.

La información relativa al estado de los Certificados estará disponible públicamente mediante los dos canales previstos, esto es, mediante la publicación de CRL's (Listas de Certificados Revocados) y OCSP (Servicio Online para la Comprobación del Estado de un Certificado).

4.4.5. Período de revocación

Desde el momento en el que una solicitud de revocación haya sido autenticada debidamente y confirmada por la CA, y en su nombre, por la Unidad de Registro, la revocación se hará efectiva en un plazo nunca superior a 24 horas.

4.4.6. Suspensión

No aplica en las presentes Políticas.

4.4.7. Procedimiento para la solicitud de suspensión

No aplica en las presentes Políticas.

4.4.8. Límites del período de suspensión

No aplica en las presentes Políticas.

4.4.9. Frecuencia de emisión de CRL 's

La frecuencia de emisión de las CRL' s y otras propiedades se describen en el capítulo 7.2 “Perfil de las CRL' s” de las presentes Políticas.

4.4.10. Requisitos de comprobación de CRL' s

Las CRL' s asociadas a las presentes Políticas son publicadas de forma libre y gratuita. El Tercero que confía deberá emplear todos los medios a su alcance para comprobar la autenticidad de las CRL' s consultadas, es decir, que estén firmadas por la CA y que su fecha de caducidad esté vigente.

Se publicarán dos fuentes con la misma información disponible en las siguientes direcciones:

https://ca.optic.gob.do/crl/opticcrl1.crl

https://ca.optic.gob.do/crl/opticcrl2.crl

4.4.11. Servicio OCSP (Online Certificate Status Protocol)

Se proporcionará un servicio en línea (*online)* de comprobación de revocaciones, el cual estará disponible las 24 horas del día, los 7 días de la semana, de forma pública y gratuita. En caso de fallo del sistema, del servicio o de cualquier otro factor que no esté bajo el control de la CA, la CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio de información no se encuentre indisponible durante más tiempo que el período máximo dispuesto en estas Políticas.

La comprobación en línea (*online)* está basada en el protocolo OCSP (RFC6960) y estará accesible en la siguiente dirección:

https://ca.optic.gob.do/ocsp

4.5. Procedimientos de Control de Seguridad

La CA y la UR realizará los esfuerzos que razonablemente estén a su alcance para confirmar que toda la información relevante concerniente a un Certificado es conservada durante el período de tiempo que pueda ser necesario a efectos probatorios en los procedimientos legales. En particular:

General

a) Se realizarán los esfuerzos que razonablemente estén a su alcance para confirmar la confidencialidad y la integridad de los registros relativos a los Certificados, tanto de los actuales como de aquellos que hayan sido previamente almacenados.

b) Los registros relativos a los Certificados serán almacenados, completa y confidencialmente, de acuerdo con las prácticas de negocio.

c) Los registros relativos a los Certificados estarán disponibles si estos son requeridos a efectos probatorios en los procedimientos legales.

d) Será almacenado el momento exacto en que se produzcan los eventos relativos a la gestión de las claves y la gestión de los Certificados.

e) Los registros relativos a los Certificados serán mantenidos durante un período de tiempo necesario para dotar de la evidencia legal necesaria a las firmas digitales.

f) Los eventos se registrarán de manera que no puedan ser fácilmente borrados o destruidos (excepto para su transferencia a medios duraderos) durante el período de tiempo en el que deban ser conservados.

g) Los eventos específicos y la fecha de registro serán documentados por la CA y la UR.

Registro

h) La CA y la UR realizarán los esfuerzos que razonablemente estén a su alcance para confirmar que todos los eventos relativos al registro, incluyendo las solicitudes de renovación y revocación serán registrados.

i) La CA y la UR realizarán los esfuerzos que razonablemente estén a su alcance para confirmar que toda la información relativa al registro es almacenada, incluyendo la siguiente:

1. La documentación presentada por el solicitante para el registro, en concreto, la copia de su cédula de identidad y electoral o del pasaporte en la fase de solicitud, y revisión de la original en el momento de la acreditación.

2. Algunas cláusulas específicas contenidas en el contrato (p.ej. el consentimiento de la publicación del Certificado).

3. Método empleado por los registradores de la Unidad de Registro para comprobar la validez de los documentos de identidad, si existe.

4. Datos relativos a la Unidad de Registro.

Generación del Certificado

k) La CA registrará todos los eventos relativos al ciclo de vida de las claves de la CA.

l) La CA y la UR registrarán todos los eventos relativos al ciclo de vida de los Certificados.

Entrega del dispositivo al Firmante/Suscriptor

m) La CA registrará todos los eventos relativos al ciclo de vida de las claves gestionadas por la misma, incluyendo las claves de los Firmantes/Suscriptores generadas por la CA.

Gestión de la revocación

n) La CA y la UR realizarán los esfuerzos que razonablemente estén a su alcance para confirmar que las solicitudes e informes relativos a una revocación, así como su resultado sean registrados.

4.5.1. Tipos de eventos registrados

Toda la información auditada y especificada en el apartado anterior será archivada.

La CA registrará y guardará los *historiales* de todos los eventos relativos al sistema de seguridad de la CA. Estos incluirán eventos como:

a) encendido y apagado del sistema.

b) encendido y apagado de la aplicación de la CA.

c) intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.

d) cambios en los detalles de la CA y/o sus claves.

e) cambios en la creación de políticas de Certificados.

f) intentos de inicio y fin de sesión.

g) intentos de accesos no autorizados al sistema de la CA a través de la red.

h) intentos de accesos no autorizados al sistema de archivos.

i) generación de claves propias.

j) creación y revocación de Certificados.

k) intentos de dar de alta, eliminar, habilitar y deshabilitar Firmantes/Suscriptores y actualizar.

l) acceso físico a los *historiales*.

m) cambios en la configuración y mantenimiento del sistema.

n) cambios de los usuarios de la CA y/o Unidad de Registro.

o) registros de la destrucción de los medios que contienen las claves y datos de activación.

4.5.2. Frecuencia de procesado de Historiales

La CA revisará sus *historiales* periódicamente y en todo caso cuando se produzca una alerta del sistema motivada por la existencia de algún incidente.

La CA se asegurará así mismo de que los *historiales* no han sido manipulados y documentará las acciones tomadas ante esta revisión.

4.5.3. Períodos de retención para los Historiales de auditoría

La información almacenada se conservará al menos durante 40 años.

4.5.4. Protección de los Historiales de auditoría

El soporte de almacenamiento de los *historiales* debe ser protegido por seguridad física o por una combinación de seguridad física y protección criptográfica. Además será adecuadamente protegido de amenazas físicas como la temperatura, la humedad, el fuego y la magnetización.

4.5.5. Procedimientos de Respaldo de los historiales de auditoría

Debe establecerse un procedimiento adecuado de respaldo, de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un período corto de tiempo las correspondientes copias de respaldo de los historiales.

4.5.6. Sistema de recogida de información de auditoría

No estipulado

4.5.7. Notificación al sujeto causa del evento

No estipulado.

4.6. Archivo de registros

4.6.1. Tipo de archivos registrados

Los siguientes datos y archivos deben ser almacenados por la CA y la UR de ésta.

a) todos los datos de la auditoría.

b) todos los datos relativos a los Certificados, incluyendo los contratos con los Firmantes/Suscriptores y los datos relativos a su identificación.

c) solicitudes de emisión y revocación de Certificados.

d) todos los Certificados emitidos o publicados.

e) CRL' s emitidas o registros del estado de los Certificados generados.

f) la documentación requerida por los auditores.

g) historial de claves generadas.

h) las comunicaciones entre los elementos de la PKI.

La CA y la UR son responsables del correcto archivo de todo este material.

4.6.2. Período de retención para el archivo

La información detallada en el apartado 4.5 i), k) y l), los contratos con los Firmantes/Suscriptores y cualquier información relativa a la identificación y autenticación del Firmante/Suscriptor se conservará durante al menos 40 años.

4.6.3. Protección del archivo

El soporte de almacenamiento debe ser protegido por medio de seguridad física o por una combinación de seguridad física y protección criptográfica. Además el soporte será adecuadamente protegido de amenazas físicas como la temperatura, la humedad, el fuego y la magnetización.

4.6.4. Procedimientos de respaldo del archivo

Debe establecerse un procedimiento adecuado de *respaldo*, de manera que, en caso de pérdida o destrucción de archivos relevantes estén disponibles en un período corto de tiempo las correspondientes copias de *respaldo*.

4.6.5. Requerimientos para el sellado de tiempo de los registros

No estipulado.

4.6.6. Sistema de recogida de información de auditoría

No estipulado.

4.6.7. Procedimientos para obtener y verificar información archivada

La CA dispondrá de un procedimiento adecuado que limite la obtención de información sólo a las personas debidamente autorizadas.

Este procedimiento regulará tanto los accesos internos como externos a la información, debiendo exigir en todo caso un acuerdo de confidencialidad previo a la obtención de la información.

4.7. Cambio de clave de la CA

Antes de que el uso de la clave privada de la CA caduque se realizará un cambio de claves. La vieja CA y su clave privada se desactivarán y se generará una nueva CA con una clave privada nueva y un nuevo identificador único.

Los siguientes Certificados serán puestos a disposición pública en el directorio:

a) Clave pública de la nueva CA firmada por la clave privada de la vieja CA.

b) Clave pública de la vieja CA firmada con la clave privada de la nueva CA.

4.8. Recuperación en caso de desastre o compromiso de la clave de la CA

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar, en caso de desastre o compromiso de la clave privada de la CA, que ésta será restablecida tan pronto como sea posible.

4.8.1. La clave de la CA se compromete

El plan de la continuidad de negocio de la CA (o el plan de contingencia) tratará el compromiso o el compromiso sospechado de la clave privada de la CA como un desastre.

En caso de compromiso, la CA tomará como mínimo las siguientes medidas:

a) Informar a la UR, a todos los Firmantes/Suscriptores, Terceros que confían y otras CA' s con los cuales tenga acuerdos u otro tipo de relación del compromiso.

b) Indicar que los Certificados e información relativa al estado de la revocación firmados usando esta clave a partir de la fecha de compromiso pueden no ser válidos.

4.8.2. Instalación de seguridad después de un desastre natural u otro tipo de desastre

La CA debe tener un plan apropiado de contingencias para la recuperación en caso de desastres.

La CA debe restablecer los servicios de acuerdo con estas Políticas dentro de las 48 horas posteriores a un desastre o emergencia imprevista. Tal plan incluirá una prueba completa y periódica de la preparación para tal restablecimiento.

4.9. Cese de la CA

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que se minimizan los posibles perjuicios que se puedan crear a los Firmantes/Suscriptores o Terceros que confían como consecuencia del cese de su actividad y en particular del mantenimiento de los registros necesarios a efectos probatorios en los procedimientos legales. En particular:

a) Antes del cese de su actividad realizará, como mínimo, las siguientes actuaciones:

1) Informar a la UR, a todos los Firmantes/Suscriptores, Terceros que confían y otras CA' s con los cuales tenga acuerdos u otro tipo de relación del cese.

2) La CA revocará toda autorización a entidades subcontratadas para actuar en nombre de la CA en el procedimiento de emisión de Certificados.

3) La CA realizará las acciones necesarias para transferir sus obligaciones relativas al mantenimiento de la información del registro y de los *historiales* durante el período de tiempo indicado a los Firmantes/Suscriptores y Terceros que confían.

4) Las claves privadas de la CA serán destruidas y deshabilitadas para su uso.

b) La CA tendrá contratado un seguro que cubra hasta el límite contratado los costes necesarios para satisfacer estos requisitos mínimos en caso de quiebra o por cualquier otro motivo por el que no pueda hacer frente a estos costes por sí mismo.

c) Se establecerán en la CPS las previsiones hechas para el caso de cese de actividad. Estas incluirán:

1) informar a la UR y a las entidades afectadas.

2) transferencia de las obligaciones de la CA a otras partes.

3) cómo debe ser tratada la revocación de Certificados emitidos cuyo período de validez aún no ha expirado.

4) En particular, la CA:

   a) informará puntualmente a la UR, a todos los Firmantes/Suscriptores, empleados, y Terceros que confían con una anticipación mínima de 3 meses antes del cese.

   b) transferirá todas las bases de datos importantes, archivos, registros y documentos a la entidad designada durante las 24 horas siguientes a su terminación.

5. CONTROLES DE SEGURIDAD FÍSICA, PROCEDIMENTAL Y DE PERSONAL

Descripción detallada en la CPS de la CA OPTIC, disponibles en el siguiente enlace:

https://ca.optic.gob.do/politicas

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves de la CA

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que las claves de la CA sean generadas de acuerdo a los estándares.

En particular:

a) La generación de la clave de la CA se realizará en un entorno asegurado físicamente por el personal adecuado según los roles de confianza y al menos con un control dual. El personal autorizado para desempeñar estas funciones estará limitado a aquellos requerimientos desarrollados en la CPS.

b) La generación de la clave de la CA se realizará en un dispositivo Gemalto/Safenet Luna PCI-E-1700, que se refiere al estándar de seguridad aplicable a los dispositivos hardware criptográficos.

6.1.2. Generación del par de claves del Firmante/Suscriptor

El par de claves será generado por el emisor o bajo su control.

Si las claves del Firmante/Suscriptor son generadas por la CA, ésta realizará los esfuerzos que razonablemente estén a su alcance para confirmar que las claves son generadas de forma segura y que se mantendrá la privacidad de las mismas. En particular:

a) Las claves serán generadas usando un algoritmo adecuado para los propósitos de la firma digital.

b) Las claves tendrán una longitud adecuada para los propósitos de la firma digital y para el algoritmo de la clave pública empleada.

c) Las claves serán generadas y guardadas de forma segura antes de entregárselas al Firmante/Suscriptor.

d) Las claves serán destruidas de forma segura después de su entrega al Firmante/Suscriptor.

6.1.3. Entrega de la clave privada al Firmante/Suscriptor.

La entrega de la clave privada se hará en consecuencia al proceso elegido durante la solicitud del Certificado. Se contemplan dos tipos de procesos:

- Clave privada generada por la CA.
- Clave privada generada por el Firmante/Suscriptor.

6.1.3.1. Clave Privada generada por la CA

Cuando la clave privada del Firmante/Suscriptor sea generada por la CA, ésta le será entregada de manera que la confidencialidad de la misma no sea comprometida y sólo el Firmante/Suscriptor tenga acceso a la misma.

La clave privada será almacenada en un medio de almacenamiento tipo software basado en el estándar PKCS#12 cuyos datos de activación (contraseña) se enviarán al Firmante/Suscriptor de manera separada al medio de almacenamiento.

La generación de la clave privada por parte de la CA se podrá realizar de dos formas:

- Solicitud en línea.
- Solicitud asistida/presencial.

6.1.3.1.1. Solicitud en Línea

Durante el proceso de solicitud en línea, el Firmante/Suscriptor elije los datos de activación del certificado (contraseña), los cuales no serán ni comunicados por correo electrónico ni almacenados en el sistema.

6.1.3.1.2. Solicitud Asistida/Presencial

En el caso de solicitudes generadas desde el back-office se ofrecen dos opciones, asistidas por un registrador autorizado, los datos de activación (contraseña) podrán generarse de dos formas:

- contraseña autogenerada de forma aleatoria por el sistema y remitida al usuario por correo electrónico.

- contraseña elegida por el Firmante/Suscriptor de manera confidencial (el registrador le entrega un teclado al usuario y le invita a que establezca su contraseña).

6.1.3.2. Clave Privada no generada por la CA

En esta política no se permite la generación externa de claves privadas.

6.1.4. Entrega de la clave pública del Firmante/Suscriptor al emisor del Certificado

6.1.4.1. Clave Pública generada por la CA

Cuando la clave privada del Firmante/Suscriptor sea generada por la CA, ésta le será entregada en el mismo medio de almacenamiento tipo software basado en el estándar PKCS#12 en el que se le entrega su clave privada.

6.1.4.2. Clave Pública no generada por la CA

No aplica para esta política.

6.1.5. Entrega de la clave pública de la CA a los Terceros que confían

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que la integridad y la autenticidad de la clave pública de la CA y los parámetros a ella asociados son mantenidos durante su distribución a los Terceros que confían. En particular:

a) La clave pública de la CA estará disponible a los Terceros que confían de manera que se asegure la integridad de la clave y se autentique su origen.

b) El Certificado de la CA y su huella digital estarán a disposición de los Terceros que confían a través de su página web.

6.1.6. Tamaño y período de validez de las claves de la CA

La CA usará claves basadas en el algoritmo RSA con una longitud mínima de 2048 bits para firmar Certificados.

El período de uso de una clave privada será de 10 años, después del cual se cambiarán estas claves.

El período de validez del Certificado de la CA se establecerá como mínimo en atención a lo siguiente:

a) El período de uso de la clave privada de la CA, y

b) El período máximo de validez de los Certificados de los Firmantes/Suscriptores firmados con esa clave

6.1.7. Tamaño y período de validez de las claves del Firmante/Suscriptor

El Firmante/Suscriptor usará claves basadas en el algoritmo RSA con una longitud mínima de 2048 bits.

El período de uso de la clave pública y privada del Firmante/Suscriptor no será superior a 1 año y no excederá del período durante el cual los algoritmos de criptografía aplicada y sus parámetros correspondientes dejan de ser criptográficamente fiables.

6.1.8. Parámetros de generación de la clave pública

No estipulado.

6.1.9. Comprobación de la calidad de los parámetros

No estipulado.

6.1.10. Hardware/software de generación de claves

Las claves de la CA serán generadas en un módulo criptográfico validado al menos por el nivel 2 de FIPS 140-1 o por un nivel de funcionalidad y seguridad equivalente.

El par de claves y las claves simétricas para los Firmantes/Suscriptores serán generados en un módulo de software y/o hardware criptográfico.

6.1.11. Fines del uso de la clave.

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que las claves de firma de la CA son usadas sólo para los propósitos de generación de Certificados y para la firma de CRL' s.

La clave privada del Firmante/Suscriptor será usada únicamente para la generación de firmas digitales, de acuerdo con el apartado 1.4.7.

6.2. Protección de la clave privada.

De la CA

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que las claves privadas de la CA continúan siendo confidenciales y mantienen su integridad. En particular:

a) La clave privada de firma de la CA será mantenida y usada en un dispositivo criptográfico seguro, el cual cumple con los requerimientos que se detallan en el FIPS 140-1, en su nivel 2 o superior.

b) Cuando la clave privada de la CA esté fuera del módulo criptográfico estará cifrada.

c) Se hará una *copia de respaldo* de la clave privada de firma de la CA, que será almacenada y recuperada sólo por el personal autorizado según los roles de confianza, usando al menos un control dual en un medio físico seguro. El personal autorizado para desempeñar estas funciones estará limitado a aquellos requerimientos desarrollados en la CPS.

d) Las copias de *respaldo* de la clave privada de firma de la CA se regirán por el mismo o más alto nivel de controles de seguridad que las claves que se usen en ese momento.

Del Firmante/Suscriptor

Cuando la clave privada ha sido generada por la CA, su activación estará protegida por una contraseña, que el propio Firmante/Suscriptor generó en unos casos, y que el sistema generó de forma aleatoria en otros, tal y como se explica en el capítulo 6.1.3.

Cuando la clave privada ha sido generada por el Firmante/Suscriptor, la CA no dispone de los medios a su alcance para asegurar el uso de la misma por parte del Firmante/Suscriptor.

6.3. Estándares para los módulos criptográficos

Todas las operaciones criptográficas deben ser desarrolladas en un módulo validado por al menos el nivel 2 de FIPS 140-1 o por un nivel de funcionalidad y seguridad equivalente. En este caso, el módulo HSM utilizado por la CA cumple con certificaciones FIPS 140-2 Level 3.

6.3.1. Control multipersona (n de entre m) de la clave privada

Se requerirá un control multipersona para la activación de la clave privada de la CA. Este control será definido adecuadamente por la CPS en la medida en que no se trate de información confidencial o pueda comprometer de algún modo la seguridad del sistema.

6.3.2. Depósito de la clave privada (*key escrow*)

La clave privada de la CA debe ser almacenada en un medio seguro protegido criptográficamente y al menos bajo un control dual.

En ningún caso la CA podrá almacenar la clave privada de firma del Firmante/Suscriptor.

6.3.3. Copia de seguridad de la clave privada

La CA realizará una copia de *respaldo* de su propia clave privada que haga posible su recuperación en caso de desastre o de pérdida o deterioro de la misma de acuerdo con el apartado anterior.

Las copias de las claves privadas de los Firmantes/Suscriptores se regirán por lo dispuesto en el punto anterior, es decir, en ningún caso la CA almacenará la clave privada del Firmante/Suscriptor ni siquiera para hacer copias de seguridad.

6.3.4. Archivo de la clave privada

La clave privada de la CA no podrá ser archivada una vez finalizado su ciclo de vida.

La clave privada del Firmante/Suscriptor no puede ser archivada por la CA.

6.3.5. Introducción de la clave privada en el módulo criptográfico

Ya visto en el capítulo 6.1.10.

6.3.6. Método de activación de la clave privada

La clave privada de la CA será activada conforme al apartado 6.3.1.

Se protegerá el acceso a la clave privada del Firmante/Suscriptor por medio de una contraseña. Si estos datos de activación deben ser entregados al Firmante/Suscriptor, esta entrega se realizará por medio de un canal seguro.

Estos datos de activación tendrán una longitud de entre 6 y 8 caracteres.

Los datos de activación deben ser memorizados por el Firmante/Suscriptor y no deben ser anotados en un lugar de fácil acceso ni compartidos.

6.3.7. Método de desactivación de la clave privada.

Sólo aplica para claves generadas en dispositivos criptográficos como smartcard, cuyo caso no está contemplado en las presentes Políticas.

6.3.8. Método de destrucción de la clave privada.

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que la clave privada de la CA no será usada una vez finalizada su ciclo de vida.

Todas las copias de la clave privada de firma de la CA serán destruidas o deshabilitadas de forma que la clave privada no pueda ser recuperada.

La destrucción o desactivación de las claves se detallará en un documento creado al efecto.

Las claves privadas de los Firmantes/Suscriptores serán destruidas o se harán inservibles después del fin de su ciclo de vida por el propio Firmante/Suscriptor.

6.4. Otros aspectos de la gestión del par de claves.

6.4.1. Archivo de la clave pública.

La CA conservará todas las claves públicas de verificación.

6.4.2. Período de uso para las claves públicas y privadas

Las claves de la CA tendrán una validez de 10 años, ver capítulo 6.1.6, y el período de uso de las claves del Firmante/Suscriptor se definen en el capítulo 7.1 de las presentes Políticas.

6.5. Ciclo de vida del dispositivo seguro de almacenamiento de los datos de creación de firma (DSADCF) y del dispositivo seguro de creación de firma (DSCF)

Para las presentes políticas no se contempla el uso de Dispositivos Seguros de Creación de Firma (DSCF).

Los Dispositivos Seguros para el Almacenamiento de Datos y Creación de Firma contemplados en las presentes Políticas se refieren a los ofrecidos por los navegadores (browsers) utilizados por el Firmante/Suscriptor durante el proceso de solicitud en línea (online) para la solicitud de creación o renovación de su Certificado Digital.

Para éstos, la CA, por si misma o por delegación de esta función, realizará los mayores esfuerzos para asegurar que:

a) El browser utilizado por el Firmante/Suscriptor permita la generación de claves.

b) El browser utilizado para la instalación y activación del Certificado corresponde con el browser desde el que se realizó la generación de claves.

6.6. Controles de seguridad informática

La CA empleará sistemas fiables y productos que estén protegidos contra modificaciones. En particular, los sistemas cumplirán las siguientes funciones:

a) identificación de todos los Terceros que confían

b) controles de acceso basados en privilegios

c) control dual para ciertas operaciones relativas a la seguridad

d) generación de *historiales*, revisión de auditoría y archivo de todos los eventos relacionados con la seguridad

e) *copia de respaldo* y recuperación

6.6.1. Requerimientos técnicos de seguridad informática específicos

Cada servidor de la CA incluirá las siguientes funcionalidades:

a) control de acceso a los servicios de la CA y gestión de privilegios

b) imposición de separación de tareas para la gestión de privilegios

c) identificación y autenticación de roles asociados a identidades

d) archivo del historial del Firmante/Suscriptor y la CA y los datos de auditoría

e) auditoría de eventos relativos a la seguridad

f) auto-diagnóstico de seguridad relacionado con los servicios de la CA

g) mecanismos de recuperación de claves y del sistema de CA

Las funcionalidades de arriba pueden ser provistas por el sistema operativo o mediante una combinación de sistemas operativos, software de PKI y protección física.

6.6.2. Valoración de la seguridad informática

No estipulado.

6.7. Controles de seguridad del ciclo de vida

6.7.1. Controles de desarrollo del sistema

La CA empleará sistemas fiables y productos que estén protegidos contra modificaciones.

6.7.2. Controles de gestión de la seguridad

6.7.2.1. Gestión de seguridad

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que los procedimientos administrativos y de gestión son aplicados, son adecuados y se corresponden con los estándares reconocidos. En particular:

a) La CA será responsable por todos los aspectos relativos a la prestación de servicios de Certificación, incluso si algunas de sus funciones han sido subcontratadas con terceras partes. Las responsabilidades de las terceras partes serán claramente definidas por la CA en los acuerdos concretos que la CA suscriba con esas terceras partes para asegurar que éstas están obligadas a implementar cualquier control requerido por la CA. La CA será responsable por la revelación de prácticas relevantes.

b) La CA desarrollará las actividades necesarias para la formación y concientización de los empleados en material de seguridad.

c) La información necesaria para gestionar la seguridad de la CA se mantendrá en todo momento. Cualquier cambio que pueda afectar al nivel de seguridad establecido será aprobado por el foro de gestión de la CA.

d) Los controles de seguridad y procedimientos operativos para las instalaciones de la CA, sistemas e información necesarios para los servicios de Certificación serán documentados, implementados y mantenidos.

e) La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que se mantendrá la seguridad de la información cuando la responsabilidad respecto a funciones de la CA haya sido subcontratada a otra organización.

6.7.2.2. Clasificación y gestión de información y bienes

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que sus activos y su información reciben un nivel de protección adecuado. En particular, la CA mantendrá un inventario de toda la información y hará una clasificación de los mismos y sus requisitos de protección en relación al análisis de sus riesgos.

6.7.2.3. Operaciones de gestión

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que los sistemas de la CA son seguros, son tratados correctamente, y con el mínimo riesgo de fallo. En particular:

a) se protegerá la integridad de los sistemas de CA y de su información contra virus y software malintencionado o no autorizado.

b) los daños derivados de incidentes de seguridad y los errores de funcionamiento serán minimizados por medio del uso de reportes de incidencias y procedimientos de respuesta.

c) Los soportes y copias de respaldo serán custodiados de manera segura para protegerlos de daños, robo y accesos no autorizados.

d) Se establecerán e implementarán los procedimientos para todos los roles administrativos y de confianza que afecten a la prestación de servicios de Certificación.

Tratamiento de los soportes y seguridad

e) Todos los soportes serán tratados de forma segura de acuerdo con los requisitos del plan de clasificación de la información. Los soportes que contengan datos sensibles serán destruidos de manera segura si no van a volver a ser requeridos.

Planificación del sistema

f) Se controlará la capacidad de atención a la demanda y la previsión de futuros requisitos de capacidad para asegurar la disponibilidad de recursos y de almacenamiento.

Reportes de incidencias y de respuestas

g) La CA responderá de manera inmediata y coordinada para dar respuesta rápidamente a los incidentes y para reducir el impacto de los fallos de seguridad. Todos los incidentes serán reportados con posterioridad al incidente tan pronto como sea posible.

Procedimientos operacionales y responsabilidades

h) Las operaciones de seguridad de la CA serán separadas de las operaciones normales.

6.7.2.4. Gestión del sistema de acceso

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas. En particular:

CA General

a) Se implementarán controles (p. ej. Cortafuegos o *Firewalls*) para proteger la red interna de redes externas accesibles por terceras partes.

b) Los datos sensibles serán protegidos cuando estos sean transmitidos por redes no protegidas.

c) La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar la efectiva administración de acceso de Terceros que confían (incluyendo operadores, administradores y cualquier usuario que tenga un acceso directo al sistema) para mantener el sistema de seguridad, incluida la gestión de cuentas de Terceros que confían, auditorías y modificación o supresión inmediata de accesos.

d) La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que el acceso a la información y a las funciones del sistema está restringido de acuerdo con la política de control de accesos, y que el sistema de la CA dispone de los controles de seguridad suficientes para la separación de los roles de confianza identificados en la CPS, incluyendo la separación del administrador de seguridad y las funciones operacionales. Concretamente, el uso de utilidades del sistema estará restringido y estrictamente controlado.

e) El personal de la CA identificado y autenticado antes de usar aplicaciones críticas relativas a la gestión de Certificados.

f) El personal de la CA será responsable de sus actos, por ejemplo, por retener *historiales* de eventos.

g) Se protegerán los datos sensibles contra medios de almacenamiento susceptibles de que la información sea recuperada y accesible por personas no autorizadas.

Generación del Certificado

h) La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que los componentes de la red local (p. ej. Enrutadores o *routers*) están guardados en un medio físico seguro y sus configuraciones son periódicamente auditadas.

i) Las instalaciones de la CA estarán provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y/o irregular.

6.7.2.5. Gestión de la revocación

j) Las instalaciones de la CA estarán provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y/o irregular.

6.7.2.6. Gestión del ciclo de vida del hardware criptográfico

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar la seguridad del hardware criptográfico a lo largo de su ciclo de vida. En particular, que:

a) el hardware criptográfico de firma de Certificados no se manipule durante su transporte.

b) el hardware criptográfico de firma de Certificados no se manipule mientras está almacenado.

c) el uso del hardware criptográfico de firma de Certificados requiere el uso de al menos dos empleados de confianza.

d) el hardware criptográfico de firma de Certificados está funcionando correctamente, y

e) La clave privada de firma de la CA almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

6.7.3. Evaluación de la seguridad del ciclo de vida

No estipulado.

6.8. Controles de seguridad de la red

Ya definido.

6.9. Controles de ingeniería de los módulos criptográficos.

Todas las operaciones criptográficas de la CA deben ser desarrolladas en un módulo validado por al menos el nivel 2 de FIPS 140-1 o por un nivel de funcionalidad y seguridad equivalente.

7. PERFILES DE CERTIFICADOS Y CRL

7.1. Perfil de Certificado

Todos los Certificados emitidos bajo esta política serán conformes al estándar X.509 versión 3 y al RFC 3039 "*Internet X.509 Public Key Infrastructure Qualified Certificates Profile*".

VERSIÓN	
Número de serie	<número de serie único para cada certificado>
Versión	3
Algoritmo de firma	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)

DATOS DEL TITULAR/SUSCRIPTOR	
Common Name	Para la presente política el common name estará formado por el nombre + apellidos (given name + surname).
Serial Number	Número de cédula.
Given Name	Nombre del titular.
Surname	Apellido o apellidos del titular.
Country	Iniciales del país al que pertenece la CA de origen. En estas políticas tendrá el siguiente valor fijo: <DO>

EMISOR	
Common Name	OPTICSUBCA
Organization	OFICINA PRESIDENCIAL DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACION
Locality	DISTRITO NACIONAL - REPUBLICA DOMINICANA
Country	DO

PLAZO DE VALIDEZ	
Not valid before	<fecha/hora> <timezone> de emisión
Not valid after	<fecha/hora> <timezone> de vencimiento (para estas Políticas la vigencia del Certificado será de 1 año.

INFORMACIÓN DE LA CLAVE PÚBLICA	
Identificador del Algoritmo de Cifrado RSA	RSA Encryption (1.2.840.113549.1.1.1)
Tamaño	256 bytes
Exponente	65537
Longitud	2048 bits
Uso de la clave pública	La clave pública podrá ser usada para cifrar, verificar, “envolturas seguras” (wrap) y derivación de claves.

EXTENSIONES	
Identificador para el uso de la clave	(2.5.29.15)
Uso de la clave privada	La clave privada podrá ser usada para Firma Digital y Cifrado de datos.
Identificador de las Restricciones Básicas	(2.5.29.19)
Identificador para el uso extendido de la clave privada	(2.5.29.37)
Identificador de uso #1	Autenticación de clientes (1.3.6.1.5.5.7.3.2)
Identificador de uso #2	Protección de Correo Electrónico (1.3.6.1.5.5.7.3.4)
Nombre alternativo del sujeto (2.5.29.17)	RFC 822 Name <coincide con el valor Email Address del titular> Email Address es el Email del titular

POLÍTICAS	
Identificador de Políticas (2.5.29.32)	Policy ID # 1.3.6.1.4.1.49353.3.1.1
User Notice (1.3.6.1.5.5.7.2.2)	Certificados de Ciudadanos emitidos en Software https://ca.optic.gob.do/politicas/optic_pc_ci_sw.pdf
Identificador de Prácticas de Certificación (1.3.6.1.5.5.7.2.1)	CPS URI = https://ca.optic.gob.do/optic_cps.pdf
Identificadores de puntos de distribución de CRLs (2.5.29.31)	https://ca.optic.gob.do/crl/opticcrl1.crl https://ca.optic.gob.do/crl/opticcrl2.crl
Identificador del punto de acceso a información de la CA (1.3.6.1.5.5.7.1.1)	https://ca.optic.gob.do/ocsp

7.1.1. Identificadores de los algoritmos de firma

PKCS #1 SHA-256 With RSA Encryption RSA Encryption

7.1.2. Restricciones de los nombres

No estipulado.

7.2. Perfil de CRL

Versión	2
Emisor	C=DO, L=DISTRITO NACIONAL - REPUBLICA DOMINICANA, O= OFICINA PRESIDENCIAL DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACION, CN=OPTICSUBCA
Algoritmo de firma	SHA256withRSA
Puntos de distribución	https://ca.optic.gob.do/crl/opticcrl1.crl https://ca.optic.gob.do/crl/opticcrl2.crl
Número de CRL (2.5.29.35)	<99>

7.2.1. Número de versión

Ver tabla anterior.

7.2.2. CRL y extensiones

Ver tabla anterior.

8. ESPECIFICACIONES DE LA ADMINISTRACIÓN

8.1. Autoridad de las Políticas

La Gerencia de la OPTIC constituye la Autoridad de las Políticas (PA) y es responsable de la administración de las Políticas.

8.2. Procedimientos de especificación de cambios

Cualquier elemento de estas Políticas es susceptible de ser modificado.

Todos los cambios realizados sobre las Políticas serán inmediatamente publicados en la web de la OPTIC.

En la web de la OPTIC se mantendrá un histórico con las versiones anteriores de las Políticas.

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 PA.

Si un cambio en las Políticas afecta de manera relevante a un número significativo de Terceros que confían de las Políticas, la PA puede discrecionalmente asignar un nuevo OID a la Política modificada.

8.3. Publicación y copia de las Políticas

Una copia de estas políticas estará disponible en formato electrónico en la dirección de Internet:

https://ca.optic.gob.do/politicas

8.4. Procedimientos de aprobación de la CPS

Para la aprobación y autorización de una CA se respetarán los procedimientos especificados por la PA. Las partes de la CPS de una CA que contenga información relevante en relación a su seguridad, toda o parte de esa CPS no estarán disponibles públicamente.

ANEXO I: ACRÓNIMOS

CA - *Certificate Authority* o *Certification Authority*. Entidad de Certificación

CPS - *Certification Practice Statement*. Declaración de Prácticas de Certificación

CRL - *Certificate Revocation List*. Lista de Certificados Revocados

CSR - *Certificate Signing Request*. Solicitud de Firma de Certificado

DES - *Data Encryption Standard*. Estándar de Cifrado de Datos

DN - *Distinguished Name*. Nombre Distintivo dentro del Certificado Digital

DSA - *Digital Signature Algorithm*. Estándar de Algoritmo de Firma

DSCF - Dispositivo Seguro de Creación de Firma

DSADCF - Dispositivo Seguro de Almacén de Datos de Creación de Firma

FIPS – Federal Information Processing Standard Publication - *Publicación Estándar de Procesamiento de Información Federal. En ambientes de Infraestructuras de Clave Pública (PKI), los HSM pueden ser usados por las CA' s y Unidades de Registro para generar, almacenar y manejar el par de claves.*

HSM - Un HSM es un dispositivo de hardware diseñado para propósitos criptográficos, y sus niveles de seguridad se regulan con estándares FIPS.

IETF - *Internet Engineering Task Force*. Grupo de Trabajo de Ingeniería de Internet

ISO - *International Organization for Standardization*. Organismo Internacional de Estandarización

ITU - *International Telecommunications Union*. Unión Internacional De Telecomunicaciones

LDAP - *Lightweight Directory Access Protocol*. Protocolo De Acceso A Directorios

OCSP - *On-Line Certificate Status Protocol*. Protocolo De Acceso Al Estado de Los Certificados

OID - *Object Identifier*. Identificador de Objeto

PA - *Policy Authority*. Autoridad de Políticas

PC - Políticas de Certificación

PKI - *Public Key Infrastructure*. Infraestructura de Clave Pública

PSC - Prestador De Servicios De Certificación

RA - *Registration Authority*. Autoridad de Registro

RU - *Registration Unity*. Unidad de Registro

RSA - Rivest-Shimar-Adleman. Tipo de Algoritmo de Cifrado

SHA-1 - *Secure Hash Algorithm*. Algoritmo Seguro de Resumen

SSL - *Secure Sockets Layer*. Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.

TCP/IP - *Transmission Control Protocol/Internet Protocol*. Protocolo de Control de Transmisión/Protocolo de Internet. Sistema de protocolos, definidos en el marco de la IEFT. El protocolo TCP se usa para dividir en origen la información en paquetes, para luego recomponerla en destino. El protocolo IP se encarga de direccionar adecuadamente la información hacia su destinatario.

ANEXO II: DEFINICIONES

Autoridad de Políticas - Persona o conjunto de personas responsables de todas las decisiones relativas a la creación, administración, mantenimiento y eliminación de las Políticas de Certificación y CPS.

Autoridad de Registro - Entidad responsable de la gestión de las solicitudes e identificación y registro de los solicitantes de un Certificado.

Certificación cruzada - El establecimiento de una relación de confianza entre dos CA' s, mediante el intercambio de Certificados entre las dos en virtud de niveles de seguridad semejantes.

Certificado - Archivo que asocia la clave pública con algunos datos identificativos del Firmante/Suscriptor y es emitido por la CA.

Clave pública - Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos. También llamada datos de verificación de firma.

Clave privada - Valor matemático conocido únicamente por el Firmante/Suscriptor y usado para la creación de una firma digital o el descifrado de datos. También llamada datos de creación de firma.

La clave privada de la CA será usada para firma de Certificados y firma de CRL' s.

CPS – (Certificate Practice Statement) - Conjunto de Prácticas Adoptadas por una Entidad de Certificación para la emisión de Certificados en conformidad con una Política de Certificación concreta.

CRL – (Certificate Revocation List) - Lista de Revocación de Certificados. Archivo que contiene una lista de los Certificados que han sido revocados en un período de tiempo determinado y que es firmada por la CA.

Datos de Activación - Datos privados, contraseñas, empleados para la activación de la clave privada.

DSADCF - *Dispositivo Seguro de Almacén de los Datos de Creación de Firma*. Elemento software o hardware empleado para custodiar la clave privada del Firmante/Suscriptor de forma que solo él tenga el control sobre la misma.

DSCF - *Dispositivo Seguro de Creación de Firma*. Elemento software o hardware empleado por el Firmante/Suscriptor para la generación de firmas digitales, de manera que se realicen las operaciones criptográficas dentro del dispositivo y se garantice su control únicamente por el Firmante/Suscriptor.

Entidad de Certificación – *Autoridad de Certificación o Certification Authority (CA)* es la entidad responsable de la emisión y gestión de los Certificados Digitales. Actúa como tercera parte de confianza, entre el Firmante/Suscriptor y el Tercero que confía, vinculando una determinada clave pública con una persona.

Institución - Aquella empresa u organización de cualquier tipo a la cual pertenece o se encuentra estrechamente vinculado el Firmante/Suscriptor.

Firma Digital - El resultado de la transformación de un mensaje o cualquier tipo de dato por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera:

a) que los datos no han sido modificados (integridad)

b) que la persona que firma los datos es quien dice ser (identificación)

c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen)

OID - Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.

Par de claves - Conjunto formado por la clave pública y privada, ambas relacionadas entre sí matemáticamente.

PKI - Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que componen un sistema basado en la creación y gestión de Certificados de clave pública.

Política de Certificación - Conjunto de reglas que definen la aplicabilidad de un Certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y de utilización comunes.

Prestador de Servicios de Certificación - entidad que presta los servicios concretos relativos al ciclo de vida de los Certificados, propietaria del datacenter donde está ubicada la PKI.

Firmante/Suscriptor - Dentro del contexto de estas Políticas de Certificación, persona cuya clave pública es certificada por la CA y dispone de una clave privada válida para generar firmas digitales.

Solicitante - Persona física que solicita el Certificado y que en el contexto de estas Políticas coincide con la figura del Firmante/Suscriptor.

Tercero que confía - Dentro del contexto de estas Políticas de Certificación, persona que voluntariamente confía en el Certificado Digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado.