Declaración de Prácticas de Certificación y Seguridad

OGTIC CA - Prestador Cualificado de Servicios de Confianza

ÍNDICE

CONTROL DE DOCUMENTO

Título:	Declaración de Prácticas de Certificación y Seguridad		
Autor:	OGTIC CA - Prestador Cualificado de Servicios de Confianza		
Estado:	Aprobado		
Versión:	2		
Código:	PCSC-CPS-OGTIC-CA	**Fecha:**	16-05-2022
Idioma:	Castellano	**Última revisión:**	16-05-2022
		Núm. Páginas:	60

CONTROL DE CAMBIOS Y VERSIONES		
Fecha	**Versión**	**Motivo del Cambio**
20-06-2017	1	Primera versión.
16-05-2022	2	Adecuación a CA Cualificada como OGTIC CA.

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 este documento 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, 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 Declaración de Prácticas de Certificación y Seguridad (CPS), codificado con el código PCSC-CPS-OGTIC-CA, y disponible en su última versión en la siguiente URL de acceso público: https://ca.ogtic.gob.do.

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 jurídica 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 jerarquía de autoridades de certificación de OGTIC PCSC queda definida de la siguiente forma:

La Autoridad de Certificación de la OGTIC es OGTIC QUALIFIED CERTIFICATES, queda definida y regulada por su Autoridad de Certificación raíz OGTIC PCSC ROOT CA.

1.3.2. Autoridades de Registro

Las Autoridades de Registro, en adelante RA (Register Authority), serán definidas en las correspondientes políticas de certificación conforme al alcance del servicio.

1.3.3. Suscriptores

Serán definidos en cada una de las Políticas de Certificados.

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 Política de Certificación correspondiente.

1.4. Uso del Certificado

1.4.1. Usos apropiados del certificado

Serán definidos en cada una de las Políticas de Certificados gestionadas por OGTIC PCSC.

1.4.2. Usos prohibidos del certificado

Serán definidos en cada una de las Políticas de Certificados gestionadas por OGTIC PCSC.

1.5. Administración de Políticas

1.5.1. Autoridad de políticas

La autoridad de políticas de OGTIC PCSC está compuesta por los roles de confianza incluidos en el comité de seguridad del PCSC.

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 CPS y Políticas de Certificados serán revisadas y aprobadas por la Autoridad de Políticas.

1.5.4. Procedimiento de aprobación de las CPS

Cualquier elemento de esta CPS es susceptible de ser modificada. Todos los cambios autorizados sobre las CPS 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 probación de políticas o cualquier cambios que afecten a éstas serán debidamente notificadas tal y como se recoge en el capítulo 2.3 de las presentes prácticas.

1.6. Definiciones y Acrónimos

- **TSA**: TimeStamp Authority, Autoridad de Sellado de Tiempo.
- **TSU**: TimeStamping Unit, Unidad de Sellado de Tiempo.
- **PSC**: Prestador de Servicios de Confianza.

- **PCSC**: Prestador Cualificado de Servicios de Confianza.
- **TSP**: Trust Services Provider, correspondencia en inglés a PSC.
- **QTSP**: Qualified Trust Services Provider (PSC cualificado).
- **HSM**: Hardware Security Module, módulo de seguridad hardware.
- **NTP**: Network Time Protocol.
- **ROA**: Real Instituto y Observatorio de la Armada.
- **OID**: Object identifier, identificador de objeto único.
- **PKI**: Public Key Infrastructure, iInfraestructura de clave pública.
- **UTC**: Coordinated Universal Time.
- **TSP**: TimeStamping Protocol, protocolo de sellado de tiempo.
- **TST**: TimeStamping Token, token de sellado de tiempo.
- **eIDAS** : electronic IDentification, Authentication and trust Services (Reglamento UE 910/2014).
- **iNDOTE**L: instituto dominicano de las telecomunicaciones
- **SGSI**: Sistema de Gestión de la Seguridad de la Información.

2. PUBLICACIÓN Y REPOSITORIO DE CERTIFICADOS

2.1. Repositorios

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

Root-CA: https://ca.ogtic.gob.do/cer/ogticroot.crt

SubCA OGTIC QUALIFIED CERTIFICATES: https://ca.ogtic.gob.do/cer/ogticqualifiedcertificates.crt

No se publicará información de otros certificados finales, a excepción de aquellos que fueron revocados, los cuales sí serán informados mediante los mecanismos previstos para ello, como los servicios de CRL y OCSP.

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

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

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

En cada una de las políticas de certificados se indicarán las fuentes de verificación específicas para cada tipo de certificado emitido por OGTIC PCSC.

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/PCSC-CPS-OGTIC-CA.pdf

2.3. Frecuencia de publicación

Cualquier versión que actualice la presente CPS 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, cuando sea necesario por implicar cambios en los servicios prestados, los cambios en las presentes prácticas de certificación serán notificados acorde al procedimiento establecido por el correspondiente órgano regulador.

En cuanto a la frecuencia de publicación de las listas de revocación de certificados finales será definida en sus correspondientes Políticas de Certificados. Reservándose la opción, de manera extraordinaria, para la publicación con carácter extraordinario ante cualquier eventualidad que así lo recomiende y apruebe la Autoridad de Políticas. Y la frecuencia de publicación de la CRL firmada por OGTIC PCSC ROOT CA será de 6 meses.

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

El Firmante/Suscriptor se describe en los certificados mediante un nombre distintivo (DN o distinguished name) conforme al estándar X509. El formato y sintaxis del DN del Firmante/Suscriptor del certificado serán definidos en cada una de las Políticas de Certificados gestionadas por OGTIC PCSC.

3.1.1. Tipo de Nombres

El Firmantes/Suscriptor se describe en los certificados mediante un nombre distintivo (DN o distinguished name) conforme al estándar X509. Los tipos de nombres serán definidos en cada una de las Políticas de Certificados gestionadas por OGTIC PCSC.

3.1.2. Significado de los nombres

Los nombres utilizados en la emisión de certificados emitidos por OGTIC PCSC serán definidos en sus Políticas de Certificados.

3.1.3. Seudónimos

OGTIC PCSC no permite el uso de seudónimos en los certificados que emite.

3.1.4. Reglas para interpretar varios formatos de nombre

En las correspondientes Políticas de Certificados quedarán recogidas las reglas aplicadas para la interpretación de los formatos de nombres admitidos.

3.1.5. Unicidad de nombres

OGTIC PCSC realizará los esfuerzos que razonablemente estén a su alcance para confirmar unicidad de los DN asignados a los Firmantes/Suscriptores. Entre estas medidas se incluye la configuración en los perfiles de los certificados que no permite la generación de nuevos certificados cuyo DN sea similar a uno anteriormente emitido.

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 PCSC, 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 OGTIC, 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

Se contempla como mecanismo de validación la comprobación de las solicitudes en formato PKCS#10 solo para aquellos suscriptores que generaron su propia clave privada acorde a lo previsto en cada una de las distintas Políticas de Certificados de OGTIC PCSC que así lo contemple.

3.2.2. Autenticación de la identidad de una organización

OGTIC PCSC determinará en cada una de sus Políticas de Certificación los mecanismos previstos y autorizados para autenticar la identidad de la entidad u organización que solicita un certificado. Contando cuando proceda, con mecanismos remotos que se ajusten a la normativa vigente.

3.2.3. Autenticación de la identidad de un individuo

OGTIC PCSC determinará en cada una de sus Políticas de Certificación los mecanismos previstos y autorizados para autenticar la identidad de un individuo que solicita un certificado. Contando cuando proceda, con mecanismos remotos que se ajusten a la normativa vigente.

3.2.4. Información no verificada del suscriptor

OGTIC PCSC, y sus Autoridades de Registro autorizadas, no procederán a la validación de documentación aportada cuya validación o verificación no pueda realizarse por mecanismos razonablemente a su alcance. En cada una de las Políticas de Certificación se definirá qué tipo de

documentación será necesaria aportar en cada caso así como sus posibles validaciones y verificaciones.

3.2.5. Validación de la autoridad

OGTIC PCSC, y sus Autoridades de Registro autorizadas emplearán los mecanismos a su alcance para la validación de identidades, tanto de personas jurídicas como físicas, y serán definidas en sus correspondientes Políticas de Certificación.

3.2.6. Criterios de interoperabilidad

OGTIC PCSC, y sus Autoridades de Registro autorizadas no tienen previstos entre sus procedimientos el uso de esquemas de interoperabilidad para la validación de identidades.

3.3. Identificación y autenticación para la renovación de certificados

3.3.1. Identificación y autenticación para la renovación de certificado vigente

OGTIC PCSC, y sus Autoridades de Registro autorizadas permitirán de forma general en sus procedimientos de renovación de certificados la identificación mediante certificado y firma digital siempre y cuando el certificado que se desee renovar no se encuentre caducado o revocado. Y de forma específica los procedimientos indicados en cada una de sus Políticas de Certificados.

3.3.2. Identificación y autenticación para la renovación un certificado caducado

La identificación y autenticación de individuos o personas jurídicas que deseen renovar un certificado caducado será similar al procedimiento de nueva emisión ya que OGTIC PCSC no permite la renovación de certificados ya caducados.

3.4. Identificación y autenticación para solicitudes de revocación

OGTIC PCSC define en sus correspondientes Políticas de Certificación los mecanismos previstos para la identificación, autenticación y en general, la gestión de solicitudes de revocación de certificados.

4. CICLO DE VIDA DEL CERTIFICADO Y REQUISITOS OPERACIONALES

4.1. Solicitud de Certificados

4.1.1. Quién puede solicitar un certificado

OGTIC PCSC regula en sus respectivas Políticas de Certificados quién podrá solicitarlos.

4.1.2. Proceso de registro

OGTIC PCSC regula en sus respectivas Políticas de Certificados el proceso de registro de solicitudes.

4.2. Proceso de solicitud de un certificado

4.2.1. Funciones de identificación y autenticación

OGTIC PCSC regula en sus respectivas Políticas de Certificados las funciones de identificación y autenticación durante el proceso de solicitud.

4.2.2. Aprobación o rechazo de solicitudes

OGTIC PCSC regula en sus respectivas Políticas de Certificados los mecanismos y casos previstos para la aprobación o rechazo de solicitudes.

4.2.3. Plazos del proceso de solicitud

OGTIC PCSC regula en sus respectivas Políticas de Certificados los plazos contemplados para cada fase de la solicitud de certificados.

4.3. Emisión de certificados

4.3.1. Acciones de la CA durante la emisión de certificados

OGTIC PCSC y sus Autoridades de Registro se reservan las acciones necesarias derivadas de los eventos generados durante cualquier fase del ciclo de vida de una emisión de certificado.

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

A partir de los datos facilitados y autorizados a OGTIC PCSC o alguna de sus Autoridades de Registro autorizadas, el suscriptor podrá ser notificado a lo largo del ciclo de vida del proceso de emisión del certificado.

4.4. Aceptación del certificado

4.4.1. Hechos que constituyen la aceptación del certificado

La entrega del certificado, por cualquiera de las vías previstas, y la firma del contrato del certificado 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 periodo de siete días naturales 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 OGTIC PCSC y el contenido del certificado, se comunicará de inmediato a OGTIC PCSC para que proceda a su revocación y a la emisión de un nuevo certificado. OGTIC PCSC entregará el nuevo certificado sin coste para el Firmante/Suscriptor en el caso de que la diferencia entre los datos sea causada por un error no imputable al Firmante/Suscriptor. Transcurrido dicho periodo sin que haya existido comunicación, se entenderá que el Firmante/Suscriptor ha confirmado la aceptación del certificado y de todo su contenido.

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 OGTIC PCSC o a cualquier tercero que de buena fe confíe en el contenido del Certificado.

4.4.2. Publicación del certificado por parte de la CA

OGTIC PCSC se reserva el derecho de publicar en su sitio web la lista de claves públicas correspondientes a los certificados emitidos. Con independencia a esta publicación, OGTIC PCSC sí publicará de forma periódica la lista de claves públicas que han sido revocadas, tal y como se recoge en el capítulo 2 del presente documento.

4.4.3. Notificación de la emisión a otras entidades

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

4.5. Uso del certificado

El uso de los certificados emitidos por OGTIC PCSC quedará recogido explícitamente en su correspondiente Política de Certificado.

4.5.1. Uso de clave privada del suscriptor

La clave privada de los certificados emitidos por OGTIC PCSC podrá ser usada acorde al alcance y limitaciones para el que fueron emitidos, tal y como se recoge en su correspondiente Política de Certificado y Contrato de Certificado.

El suscriptor deberá proteger el uso de la clave privada ante usos no autorizados, y deberá dejar de hacer uso de clave privada cuando ésta haya expirado o haya sido revocada.

4.5.2. Confianza y uso de la clave pública

Será obligación de los terceros que confían en las claves públicas de OGTIC PCSC 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

OGTIC PCSC determinará en cada una de sus Políticas de Certificados la situaciones previstas por las que un suscriptor puede solicitar la renovación de su certificado.

4.6.2. Quién puede solicitar la renovación

OGTIC PCSC determinará en cada una de sus Políticas de Certificados quién puede solicitar la renovación de un certificado.

4.6.3. Proceso de solicitudes de renovación

OGTIC PCSC determinará en cada una de sus Políticas de Certificados el procedimiento disponible para la renovación de un certificado.

4.6.4. Notificación de la renovación del certificado al suscriptor

OGTIC PCSC, a través de sus Autoridades de Registro autorizadas, procederá a la notificación periódica al suscriptor durante los períodos próximos a la renovación del certificado.

4.6.5. Hechos que constituyen la aceptación del certificado renovado

OGTIC PCSC establece los mismos hechos constitutivos de aceptación del certificado renovado que los estipulados en el capítulo 4.4.1 las presentes prácticas.

4.6.6. Publicación del certificado renovado

OGTIC PCSC se reserva el derecho de publicar en su sitio web la lista de claves públicas correspondientes a los certificados renovados. Con independencia a esta publicación, OGTIC PCSC sí publicará de forma periódica la lista de claves públicas que han sido revocadas, tal y como se recoge en el capítulo 2 del presente documento.

4.6.7. Notificación de la renovación a otras entidades

OGTIC PCSC no establece entre sus procedimientos la notificación a otras entidades de la renovación de un certificado.

4.7. Reemisión del Certificado

4.7.1. Circunstancias para la reemisión del certificado

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

OGTIC PCSC determinará en cada una de sus Políticas de Certificados la situaciones previstas por las que un suscriptor puede solicitar la revocación de su certificado.

4.9.2. Quién puede solicitar la revocación

OGTIC PCSC determinará en cada una de sus Políticas de Certificados quién puede solicitar la revocación de un certificado.

4.9.3. Proceso para la revocación del certificado

OGTIC PCSC determinará en cada una de sus Políticas de Certificados el procedimiento disponible para la revocación de un certificado.

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

OGTIC PCSC determina los plazos para el procesamiento efectivo de una solicitud de revocación en las respectivas políticas de certificados.

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

La frecuencia de generación de CRLs queda definida en las correspondientes Políticas de Certificados.

4.9.8. Latencia máxima de la CRL

La latencia máxima de las CRLs queda definida en las correspondientes Políticas de Certificados.

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 el 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.

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.

4.11. Fin de la suscripción

OGTIC PCSC considera como fin de la suscripción el acto voluntario por parte del suscriptor de dejar caducar su certificado o bien solicitar su revocación previa a su fecha de caducidad. Si el suscriptor no inicia, en los términos previstos, ningún proceso de renovación o nueva emisión tras alguno de estos dos eventos, OGTIC PCSC considera como finalizada la suscripción.

4.12. Depósito de claves y recuperación

4.12.1. Prácticas para el depósito y recuperación de claves

OGTIC PCSC contempla entre sus procedimientos el respaldo de las claves asociadas a los certificados raíz y TSU, realizados éstos mediante un proceso de derivación de claves (wrapping-key) e importación en un dispositivo seguro de backup (HSM Backup) FIPS 140-2 Level 3 EAL4+ diseñado exclusivamente para su recuperación ante cualquier contingencia que lo requiera.

Para el respaldo y recuperación se requiere la intervención de al menos dos de los tres roles de confianza estipulados en el procedimiento.

4.12.2. Prácticas de encapsulado y recuperación de recuperación de claves

OGTIC PCSC contempla entre sus procedimientos el respaldo de las claves asociadas a los certificados raíz y TSU, realizados éstos mediante un proceso de derivación de claves (wrapping-key) e importación en un dispositivo seguro de backup (HSM Backup) FIPS 140-2 Level 3 EAL4+ diseñado exclusivamente para su recuperación ante cualquier contingencia que lo requiera.

Para el respaldo y recuperación se requiere la intervención de al menos dos de los tres roles de confianza estipulados en el procedimiento.

5. INSTALACIÓN, GESTIÓN Y CONTROLES OPERACIONALES

5.1. Controles físicos

Cuenta con monitorización y vigilancia permanente 24 horas al día, 7 días a la semana y 365 días al año. El sistema de gestión del edificio centraliza todos los datos sobre la situación y el estado de la infraestructura del edifico y recibe y procesa posibles alarmas. Los sistemas principales conectados y gestionados son: el centro de seccionamiento, el centro de transformación, los grupos electrógenos, los sistemas de alimentación ininterrumpida, los cuadros eléctricos principales de media y baja tensión, la distribución eléctrica, los sistemas de climatización, la detección y extinción de incendios, la detección de humedad y la apertura de puertas.

La infraestructura está conectada de manera directa a Internet mediante circuitos de alta capacidad redundantes, asegurando así alta disponibilidad y calidad de acceso. La red troncal es una red multiservicio, basada en las más novedosas tecnologías, que incorpora los protocolos IP Multicast, BGP4 y MPLS. El acceso de la plataforma a Internet se realiza mediante múltiples conexiones con otras redes IP en puntos de intercambio y carriers de tránsito. Gracias al protocolo BGP4 se asegura un encaminamiento eficiente del tráfico IP y reacciones dinámicas a cualquier cambio que se produzca en la red Internet.

5.1.1. Localización y construcción

La infraestructura de PKI de OGTIC PCSC está desplegada en un Data Center ubicado en España. El diseño de la construcción cuenta con los métodos convencionales de detectores de presencia, proximidad y circuito cerrado de televisión, además de controles de acceso y control.

5.1.2. Acceso físico

Únicamente el personal autorizado dispone de acceso a los equipos alojados en el Data Center, debiendo superar un mínimo de tres anillos físicos de seguridad hasta llegar a la infraestructura de PKI de OGTIC PCSC .

5.1.3. Alimentación eléctrica y aire acondicionado

El datacenter donde está ubicada la PKI de OGTIC PCSC cuenta con alimentación eléctrica redundante soportada con SAIs y grupos electrógenos. En el diseño de las instalaciones eléctricas existe redundancia de equipos, añadiéndole una serie de elementos alternativos tales como sistemas de by-pass, transferencias de cargas críticas sin cortes de tensión, aislamiento galvánico, red equipotencial de tierra, etc., que permiten asegurar el máximo nivel de disponibilidad eléctrica para los equipos alojados.

El sistema de climatización se realiza mediante equipos autónomos que aseguran unos niveles de temperatura y humedad óptimos para el funcionamiento de los servidores y la electrónica de red.

5.1.4. Exposición al agua

El datacenter dispone de sistemas de detección de fugas de agua o combustible. Todo ello telegestionado por un sistema central de control y gestión del edificio.

5.1.5. Protección y prevención de incendios

En cuanto a los medios físicos de seguridad, el datacenter dispone de los sistemas más modernos de protección contra incendios y extinción por agentes de nulo impacto ambiental, y todo ello telegestionado por un sistema central de control y gestión del edificio.

5.1.6. Sistema de almacenamiento

Se cuenta con cajas de fuerte ignífugas separadas del datacenter principal, donde se almacenan copias de respaldo y otros elementos de seguridad para la gestión de la PKI, como los Token criptográficos utilizados por los Roles de Confianza para activación de claves en los módulos HSM.

5.1.7. Eliminación de residuos

La eliminación de soportes magnéticos, ópticos e información en papel se realiza de forma segura siguiendo procedimientos establecidos para este fin, adoptando procesos de reseteo de fábrica, de destrucción o triturado en función del tipo soporte a tratar.

5.1.8. Backup remoto

Acorde a los procedimientos y políticas internas de backup, se realizan copias diarias incrementales y una Full semanal que se realizará el domingo. Las copias se custodiaran durante 7 días, depositando una copia del respaldo en el mismo datacenter y otra copia del respaldo fuera del mismo.

5.2. Controles procedimentales

5.2.1. Roles de confianza

Los roles de confianza con los que cuenta OGTIC PCSC garantizan una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación. Concretamente:

a) Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.

b) Las tareas de Certificación se realizarán por al menos tres personas necesitándose al menos de dos para activar la clave privada de la CA o TSA. Estas personas no deben formar parte de las tareas de Sistemas ni de Auditoría.

c) Las personas implicadas en Administración de Sistemas no podrán ejercer ninguna actividad en las tareas de Auditoría o Certificación.

Las responsabilidades específicas para los roles de Prestador de Servicios de Confianza son:

- **Security Officers**: encargados de la implementación de las prácticas de seguridad, encargándose además de las tareas asociadas a la generación, revocación suspensión de claves.

- **System Administrators**: serán los responsables de la instalación, configuración y mantenimiento de todos los sistemas asociados a la CA y/o TSU, con especial dedicación a la gestión del sistema principal denominado EJBCA así como al aprovisionamiento y gestión de dispositivos vinculados, como HSM y PED Remote Control.

- **System Operators**: serán los responsables de la operación diaria de los sistemas asociados a la TSA, con especial dedicación a la monitorización de sistemas y gestión de los sistemas de respaldo y recuperación.

- **System Auditors**: estarán facultados para la revisión de logs y ficheros de auditoría para asegurar el cumplimiento de las políticas y prácticas definidas.

- Y de forma específica, los roles encargados de la gestión de cada servicio de confianza quedarán descritos en sus correspondientes políticas, como por ejemplo los roles de confianza asociados a la prestación del Servicio Cualificado de Sello de tiempo y Certificados

digitales, definidos en su correspondiente Política de Certificados así como en sus Términos y Condiciones de uso.

5.2.2. Número de personas requeridas por tarea

Se garantiza al menos dos personas para realizar las tareas que se detallen en las Políticas de Certificación correspondientes.

5.2.3. Identificación y autenticación para cada rol

Se cuenta con procedimientos de identificación y autenticación de las personas implicadas en roles de confianza.

5.2.4. Roles que requieren separación de funciones

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurara que cada persona realiza las operaciones para las que está asignado.

Cada persona sólo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados. El acceso a recursos se realiza dependiendo del activo mediante información de acceso y contraseña, Certificados Digitales, tarjetas de acceso físico y llaves.

5.3. Controles personales

5.3.1. Requisitos de calificación, experiencia y autorización

OGTIC PCSC asegura que todo el personal que desarrolla tareas asociadas a la actividad como prestador de confianza, o tiene acceso a las instalaciones restringidas de seguridad tiene la suficiente cualificación y experiencia en este tipo de servicios.

Se requiere para ellos:

- Experiencia en el sector.
- Conocimientos sobre entornos de certificación digital.
- Formación básica sobre seguridad en sistemas de información.
- Formación especifica para su puesto.

5.3.2. Procedimientos de verificación de antecedentes

OGTIC PCSC analiza la documentación presentada por el personal antes de aplicar al puesto, como CV o referencias previas.

5.3.3. Requisitos de formación

El programa de formación del personal directa o indirectamente vinculado a los servicios de confianza ofrecidos por OGTIC PCSC incluye cursos con temática y contenidos específicos asociados, en especial, criptografía.

5.3.4. Requisitos y frecuencia de formación

Acorde a los procedimientos internos de OGTIC PCSC , se establece un mínimo de una formación anual.

5.3.5. Frecuencia y secuencia de rotación de tareas

No se han definido procedimientos para la rotación de tareas en los perfiles asociados a los servicios de confianza prestados por OGTIC PCSC .

5.3.6. Sanciones por acciones no autorizadas

El incumplimiento de algunas de las prácticas de certificación o de cualquier otra norma interna que regule el servicio de confianza prestado por OGTIC PCSC podrá derivar en sanciones disciplinarias. En función de la gravedad de las acciones detectadas, se podrá retirar con carácter inmediato el acceso a los servicios y/o instalaciones.

En función de la naturaleza de las acciones reportadas la compañía podrá concurrir a los cauces legalmente establecidos, tanto del ámbito laboral como del ámbito civil o penal.

5.3.7. Requisitos para personal independiente

No se cuenta con un procedimiento específico para la contratación de profesionales independientes para la prestación de los servicios de confianza ofrecidos por OGTIC PCSC . Cualquier actividad o tarea que requiera de la participación de un profesional o empresa externa se rige por los procedimientos de confidencialidad y seguridad estipulados en la organización.

5.3.8. Documentación entregada al personal

El personal directamente relacionado con las actividades y los servicios de confianza ofrecidos por OGTIC PCSC cuentan con acceso al repositorio de la intranet corporativa donde se publican todos los procedimientos necesarios para su puesto, incluyendo además las propias prácticas de certificación presentes así como todas y cada una de las políticas de certificados.

5.4. Procedimientos para el registro de auditoría

5.4.1. Tipo de eventos registrados

Se cuentan con distintos sistemas de información involucrados en la gestión de los servicios de confianza ofrecidos por OGTIC PCSC. Para todos ellos se permite la configuración, análisis y gestión de eventos, registrándose en cada caso para todas las operaciones, entre ellas:

- Acceso y login a los sistemas,
- Actualización y mantenimiento del sistema operativo,
- Eventos generados por operadores en el software de PKI, como login, emisión, renovación, revocación, etc.
- Eventos generados por los dispositivos seguros de creación y almacenamiento de claves (HSM),
- Eventos asociados a la actividad de la TSA, como el registro de operaciones, autenticaciones exitosas y fallidas, etc.
- Eventos asociados a las operaciones de respaldo (backup y restauración).

5.4.2. Frecuencia del procesamiento de registros

Los registros de logs están almacenados en sistemas que no permiten la modificación, sólo incrementan la información añadiendo nuevos registros. Los logs de actividad de la PKI y la TSA son procesados al menos con carácter semanal y mensual.

5.4.3. Período de retención del registro de auditoría

Todos los registros almacenados son retenidos durante 15 años.

5.4.4. Protección del registro de auditoría

Los registros de auditoría no cuentan con un cifrado o protección distinta al del resto de logs y eventos del servicio.

5.4.5. Procedimiento del backup del registro de auditoría

Los registros de auditoría quedan incluidos en los procedimientos de backup aprobados por la compañía.

5.4.6. Sistema de recolección de auditoría

La auditoría gestionada por el servicio de la PKI de OGTIC PCSC queda registrada en la base de datos, donde se cuenta con tablas específicas de auditoría.

5.4.7. Notificación de eventos

El procesamiento automático de logs cuenta con automatismos encargados de la notificación de aquellos eventos considerados de especial tratamiento como para que requiera de la ejecución de algún procedimiento específico o intervención del equipo de administradores del servicio.

5.4.8. Evaluación de vulnerabilidades

Se cuenta un sistema de sondas y otros tipos de indicadores encargados del análisis automático de logs, identificando patrones previamente configurados que desencadenan notificaciones de seguridad o acciones preconfiguradas. Por ejemplo, intentos fallidos de login para un mismo usuario en una fracción de tiempo determinada.

Al mismo tiempo los sistemas están sujetos a un calendario de análisis de vulnerabilidades, llevado a cabo por empresas externas en unos casos, y por personal interno en otros.

5.5. Archivo de registros

5.5.1. Tipos de archivo de registros

Se gestionarán distintos niveles de registro atendiendo al servicio asociado que lo generó. Todos ellos estarán categorizados acorde a los procedimientos específicos que afecten al servicio.

Se cuenta con registros de operaciones de sello de tiempo, emisión de certificados, registro de acceso a sistemas, registro de operaciones asociadas al ciclo de vida de un certificado: creación, activación, renovación, revocación, etc.

También se registra toda la documentación contractual asociada a la gestión del servicio, como contratos y documentación anexa requerida a suscriptores.

5.5.2. Período de retención del archivo

Se establece un período de retención de los archivos registrados por OGTIC PCSC de 15 años.

5.5.3. Protección del archivo

El acceso y revisión de los archivos registrados estará restringido al personal autorizado para cada uno de los tipos de archivos registrados. Además se habilitan distintos mecanismos de firma electrónica a cierta información asociada a documentación contractual o de servicio para demostrar su integridad y autenticidad.

5.5.4. Procedimientos para el backup del archivo

Los archivos de registro seguirán el procedimiento de backup establecido en las políticas de respaldo de OGTIC PCSC.

5.5.5. Requisitos para el sellado de tiempo del registro

No se ha definido una política de sellado de tiempo para el fichero de registro.

5.5.6. Sistema de recolección del archivo

La recuperación y tratamiento del archivo se ajusta a los procedimientos de backup y recuperación del archivado de logs.

5.5.7. Procedimientos para obtener y verificar la información del archivo

La verificación del archivo se ajusta a los procedimientos de backup y recuperación del archivado de logs.

5.6. Cambio clave

El cambio de la clave pública de un certificado será definido en las correspondientes Políticas del Certificado afectado.

5.7. Recuperación en caso de compromiso de la clave o desastre

5.7.1. Procedimientos para la gestión de incidentes

OGTIC PCSC cuenta con un procedimiento para la gestión de incidentes relacionados con los servicios ofrecidos como prestador de confianza.

5.7.2. Obsolescencia y deterioro

OGTIC PCSC cuenta con procedimientos para la gestión de la obsolescencia o deterioro de aquellos elementos que intervienen en los servicios de confianza, en especial el uso de tarjetas criptográficas para el acceso a los sistemas de gestión de la PKI, Tokens criptográficos para la activación de claves y los módulos criptográficos (HSM) utilizados para la generación y activación de claves.

5.7.3. Procedimientos ante compromiso de clave de una entidad

En el caso de que se detecte el compromiso de la clave privada de una de las Autoridades, se procederá a la revocación de dicha clave y a la actualización y publicación de la CRLs correspondientes, cesando por tanto la actividad de dicha Autoridad y sus posibles subordinadas.

Posteriormente, se procedería a la emisión de una nueva Autoridad con los mismos datos (subject, CN, etc.), pero modificando el identificador de versión asociada.

Debe así mismo darse traslado a las autoridades siguiendo el procedimiento de notificación de brechas de seguridad incorporado en este documento, así como a los potenciales terceros / clientes que puedan estar afectados por el mismo problema, así como los posibles procedimientos que deban realizar de su parte, tales como modificar las fuentes de verificación.

Los certificados de TSU que potencialmente pudieran estar afectados también deberán ser revocados, procediendo a la emisión de nuevos certificados.

5.7.4. Plan de continuidad de negocio ante desastres

OGTIC PCSC cuenta con un plan de continuidad de negocio donde se establece, entre otros, los casos de recuperación ante desastre.

5.8. Cese de la CA o RA

OGTIC PCSC cuenta entre sus procedimientos con un Plan de Cese de la actividad general o de algunos de los servicios de confianza prestados.

En dichos procedimientos se incluyen las comunicaciones oficiales a supervisores, así como a suscriptores y terceras partes afectadas. El procedimiento de plan de cese está ajustado a las pautas recogidas en el ETSI EN 319 401 7.12 y se incluyen disposiciones como las enumeradas a continuación:

- OGTIC PCSC comunicará al supervisor, acerca del cese de actividades con una antelación mínima de dos meses. Se especificará si se extingue o se transfiere la gestión del servicio a un tercero.

- OGTIC PCSC comunicará a todos los suscriptores el cese del servicio con una antelación de al menos tres meses, así como a las terceras partes que puedan ser identificadas o empresas con las que tenga acuerdos.

- OGTIC PCSC publicará la información relacionada con el cese en su página web con una antelación mínima de tres meses.

- En el caso de que existiesen, OGTIC PCSC retirará las autorizaciones a terceras empresas subcontratadas para actuar en nombre de OGTIC en materia de emisión de tokens de servicios de confianza.

- OGTIC PCSC tratará de alcanzar acuerdos para transferir la provisión de los servicios de confianza a otro Prestador Cualificado de Servicios de Confianza.

- En el momento del cese, OGTIC PCSC procederá a la revocación de la cadena completa de certificados: root CA, sub CA o sub CAs que existan en ese momento, certificados de TSU o de firma emitidos, etc.

- Posteriormente, OGTIC PCSC destruirá las claves privadas asociadas al servicio de Prestador de Servicios de Confianza, incluyendo copias de seguridad, asegurando que las claves no podrán ser recuperadas. El borrado se realizará mediante un RESET de los servidores criptográficos HSM, así

como un borrado seguro de los dispositivos de HSM Backup, garantizando la eliminación efectiva de las claves.

- OGTIC PCSC transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios, al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio.

- En el caso de no ser posible dicha transferencia, OGTIC PCSC mantendrá activos los sistemas de verificación asociados a los certificados de sello de tiempo y de firma emitidos, hasta la extinción de los mismos.

- OGTIC PCSC dispone de un Seguro de Responsabilidad Civil para cubrir los costes de los requisitos del plan de cese en caso de bancarrota o en el caso de que no disponga de la capacidad de los costes asociados a la finalización de las actividades.

6. CONTROLES TÉCNICOS DE SEGURIDAD

6.1. Generación del par de claves y su instalación

6.1.1. Generación del par de claves

El procedimiento para la generación del par de claves se definirá en las correspondientes políticas del certificado.

6.1.2. Entrega de la clave privada al suscriptor

El procedimiento para la entrega de clave privada del suscriptor se definirá en las correspondientes políticas del certificado.

6.1.3. Entrega de la clave pública al suscriptor

El procedimiento para la entrega de clave pública del suscriptor se definirá en las correspondientes políticas del certificado.

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

La clave pública de todas las CA´s que formen parten de la jerarquía de OGTIC PCSC estarán disponibles en el sitio web https://ca.ogtic.gob.do/. Esta información también estará disponible en los atributos del certificado destinados para este propósito (OID 1.3.6.1.5.5.7.48.2 "Certificate authority issuers" con los siguientes valores para cada caso:

Root-CA: https://ca.ogtic.gob.do/cer/ogticroot.crt

SubCA OGTIC QUALIFIED CERTIFICATES: https://ca.ogtic.gob.do/cer/ogticqualifiedcertificates.crt

No se publicará información de otros certificados finales, a excepción de aquellos que fueron revocados, los cuales sí serán informados mediante los mecanismos previstos para ello, como los servicios de CRL y OCSP.

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

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

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

6.1.5. Tamaño de las claves

Con carácter general, el tamaño de las claves generadas por OGTIC PCSC serán de 2048 para los certificados finales, y de 4096 para los certificados de entidades intermedias y raíz de su jerarquía.

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

Los parámetros necesarios para la generación de la clave pública serán definidos en las correspondientes políticas de certificados.

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 el propósito de uso de las claves será definido en sus respectivas políticas de certificados.

6.2. Protección de clave privada y controles del módulo criptográfico

6.2.1. Controles y estándares del módulo criptográfico

OGTIC PCSC hace uso de dos módulos criptográficos (HSM) para la generación y gestión de las claves de los certificados de las entidades Root e intermedias de la jerarquía.

Los controles y estándares empleados en su gestión están ajustados a lo establecido en la especificación ETSI EN 319 422.

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

OGTIC PCSC cuenta entre sus procedimientos con el uso de Tokens criptográficos, usados a modo de llaves, para aquellas operaciones de activación de calves y gestión de los módulos criptográficos (HSM). Estos tokens criptográficos están a cargo de distintos roles de confianza, estableciendo para su uso un control 2 de 3, es decir, que como mínimo serán necesarias dos tokens, de diferentes roles de confianza autorizados.

6.2.3. Depósito de la clave privada

No se contempla el depósito (escrow) de las claves privadas de la raíz o entidades subordinadas de OGTIC PCSC .

6.2.4. Backup de la clave privada

OGTIC PCSC emplea un procedimiento específico para realizar el Backup de las Claves privadas de la entidad ROOT y sus subordinadas. El procedimiento es ejecutado por distintos roles de confianza, haciendo uso de los módulos criptográficos (HSM) en los que se encuentran las respectivas claves, con un control de acceso 2 de 3.

El procedimiento contempla el uso de otro módulo criptográfico (HSM BACKUP) especialmente diseñado para la copia y respaldo de las claves generadas y almacenadas en otro HSM. El uso de esto otro módulo criptográfico también requiere de un control de acceso 2 de 3 por parte de los distintos roles de confianza establecidos en el procedimiento de backup de claves.

Este procedimiento de backup también incluye las claves privadas de los certificados emitidos por OGTIC PCSC .

El backup de las claves privadas de certificados de certificados finales que hayan sido generadas y almacenadas por OGTIC PCSC se definirá en sus correspondientes políticas de certificados.

6.2.5. Archivo de la clave privada

Lo establecido en el procedimiento interno de OGTIC PCSC para Backup de claves descrito en el punto anterior.

6.2.6. Importación de la clave privada al módulo criptográfico

Las importación de claves privadas al módulo criptográfico (HSM) solo está prevista para los procedimientos de restauración de copias de respaldo, según lo definido en los procedimientos de backup de claves de OGTIC PCSC .

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

Las claves privadas de los certificados de las entidades raíz e intermedias de la jerarquía de OGTIC PCSC están almacenadas en sendos módulos criptográficos (HSM).

De igual forma, la clave privada de los certificados TSU y de firma emitidos por OGTIC PCSC estará almacenada en un módulo criptográfico (HSM).

El almacenamiento de las claves privadas de certificados finales estará definido en las correspondientes políticas de certificado.

6.2.8. Método de activación de la clave privada

La activación de las claves privadas de las entidades raíz e intermedias de la jerarquía de OGTIC PCSC se lleva a acabo acorde a los procedimientos definidos en sus respectivas ceremonias de clave y conforme con las normas ETSI EN 319 421.

Para toda activación se requiere la participación de distintos roles de confianza, con control de uso 2 de 3 a los distintos módulos criptográficos afectados. Este procedimiento afecta a la activación de claves de OGTIC PCSC ROOT CA y OGTIC QUALIFIED CERTIFICATES.

La activación de claves de otros certificados será definida en sus correspondientes políticas de certificación.

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

OGTIC PCSC cuenta con un procedimiento para el Borrado Seguro de las claves privadas OGTIC PCSC ROOT CA y OGTIC QUALIFIED CERTIFICATES.

En todos los casos el procedimiento necesita de la participación de distintos roles de confianza, con control de uso 2 de 3 a los distintos módulos criptográficos (HSM) en los que se encuentren las claves afectadas.

6.2.11. Clasificación del módulo criptográfico

Los módulos criptográficos (HSM) utilizados por OGTIC PCSC se ajustan a las normas ETSI EN 319 421. En concreto, se hace uso de dispositivos Gemalto con certificación FIPS 140-2 Level 3 EAL4+.

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 de TSU 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 del certificado de OGTIC PCSC ROOT CA será de 25 años, mientras que la validez de la subordinada OGTIC QUALIFIED CERTIFICATES será de 20 años.

La validez del resto de certificados finales, incluyendo el certificado de TSU será definida en sus correspondientes políticas de certificados.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Los procedimientos de generación de datos para la activación de las claves privadas de las entidades raíz e intermedias de la jerarquía de OGTIC PCSC 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. Estos procedimientos se refieren a los datos generados para la activación de claves de OGTIC PCSC ROOT CA y OGTIC QUALIFIED CERTIFICATES.

El proceso de generación de datos de activación de claves de otros certificados será definido en sus correspondientes políticas de certificación.

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 necesaria 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

OGTIC PCSC, en su política de implantación del sistema de gestión de la seguridad en la información y acorde a la certificación ISO27001, tiene prevista la protección de información sensible y confidencial, habilitando mecanismos para su consulta ante órganos reguladores, auditores o terceros que justifiquen la necesidad de conocer cierta información, como es el caso del contenido de este punto en particular.

6.6. Ciclo de vida de los controles técnicos

OGTIC PCSC, en su política de implantación del sistema de gestión de la seguridad en la información y acorde a la certificación ISO27001, tiene prevista la protección de información sensible y confidencial, habilitando mecanismos para su consulta ante órganos reguladores, auditores o terceros que justifiquen la necesidad de conocer cierta información, como es el caso del contenido de este punto en particular.

El intervalo máximo de revisiones de los sistemas para la detección de incumplimientos de la política de seguridad es de **seis meses**.

6.7. Controles de seguridad de red

OGTIC PCSC, en su política de implantación del sistema de gestión de la seguridad en la información, tiene prevista la protección de información sensible y confidencial, habilitando mecanismos para su consulta ante órganos reguladores, auditores o terceros que justifiquen la necesidad de conocer cierta información, como es el caso del contenido de este punto en particular.

6.8. Sello de tiempo

No se contempla.

7. CERTIFICADOS, CRL, OCSP Y PERFILES

7.1. Perfil de certificado

7.1.1. Número de versión

Lo establecido en la correspondiente Política de Certificado.

7.1.2. Extensiones del certificado

Lo establecido en la correspondiente Política de Certificado.

7.1.3. Identificador (OID) del algoritmo de firma

Lo establecido en la correspondiente Política de Certificado.

7.1.4. Uso de nombres

Lo establecido en la correspondiente Política de Certificado.

7.1.5. Restricciones de nombres

Lo establecido en la correspondiente Política de Certificado.

7.1.6. Identificador de política de certificado

Lo establecido en la correspondiente Política de Certificado.

7.1.7. Uso de la extensión de política de restricciones

Lo establecido en la correspondiente Política de Certificado.

7.1.8. Sintaxis y semántica de la política de calificadores

Lo establecido en la correspondiente Política de Certificado.

7.1.9. Semántica del procedimiento para las extensiones críticas del certificado

Lo establecido en la correspondiente Política de Certificado.

7.2. Perfil de la CRL

7.2.1. Número de versión

Lo establecido en la correspondiente Política de Certificado.

7.2.2. CRL y extensiones

Lo establecido en la correspondiente Política de Certificado.

7.3. Certificado OCSP

7.3.1. Número de versión

Lo establecido en la correspondiente Política de Certificado.

7.3.2. Extensiones del OCSP

Lo establecido en la correspondiente Política de Certificado.

8. AUDITORÍAS

8.1. Frecuencia o circunstancias de la auditoría

OGTIC PCSC realizará auditorías anuales con carácter ordinario, y con carácter extraordinario se podrán realizar auditorías adicionales sí así lo determina el comité de seguridad establecido en el SGSI de la compañía.

8.2. Identidad y cualificación del auditor

OGTIC PCSC realizará una selección entre distintos candidatos que cuenten con el perfil adecuado y con demostrada experiencia en tecnologías PKI.

8.3. Relación del auditor con el prestador

Se asegurará que el auditor externo seleccionado no tenga vínculos o relación directa con OGTIC PCSC .

8.4. Temas tratados en la auditoría

El programa de cada auditoría contará entre su contenido, al menos, con los siguientes asuntos:

- Cumplimientos de las normas ETSI EN 319 401 y 421.
- Revisión de CPS y Políticas.
- Revisión de Políticas de Seguridad.
- Revisión de Seguridad Física.
- Revisión de Infraestructuras.
- Revisión de los servicios de confianza actualmente prestados.

8.5. Acciones a realizar como resultado de una deficiencia

Se evaluarán los resultados obtenidos tras la auditoría, determinando en cada caso las medidas a adoptar para aquellas observaciones o no conformidades detectadas en la misma, elaborando para todos los casos un informe técnico aprobado por la dirección y comité de seguridad donde se detallará el plan de actuación necesario.

8.6. Comunicación de resultados

En el informe técnico elaborado tras la valoración de resultados de cada auditoría se identificarán aquellos departamentos o áreas afectadas por las observaciones o no conformidades, la cuales serán debidamente notificadas e informadas de las medidas planificadas para su resolución.

Si la medida lo requiere, los órganos reguladores serán debidamente informados antes cualquier cambio que afecte a lo establecido en las CPS o algunas de las políticas de certificados de OGTIC PCSC.

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://ca.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://ca.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 es uso 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://ca.ogtic.gob.do.

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://ca.ogtic.gob.do.

9.2. Responsabilidad financiera

OGTIC PCSC cuenta con un seguro de responsabilidad civil profesional, a favor de la institiución, para las actividades profesionales como Prestador Cualificado de Servicios de Confianza.

9.3. Confidencialidad de la información comercial

9.3.1. Alcance de la información confidencial

Toda información relativa a los procedimientos de seguridad informática, de infraestructura y física tendrá un tratamiento confidencial, excluyéndose por tanto en la información publicada en estas CPS y Políticas de Certificados.

También será considerada información confidencial la utilizada durante los procedimientos de gestión de claves, en especial, procesos de activación.

De igual condición de confidencial será tratada aquella información entregada a OGTIC PCSC como parte de suscriptores de los servicios de confianza prestados, como datos personales utilizados en las altas y gestión del servicio.

Y en general, toda información que de forma explícita haya sido etiquetada como confidencial.

9.3.2. Alcance excluido de la información confidencial

En general toda documentación no clasificada como privada o confidencial será de dominio público, y por tanto estará disponible en el sitio https://ca.ogtic.gob.do, como CPS, Políticas de Certificados, Términos y condiciones de los servicios, políticas de seguridad, tratamiento y protección de datos personales.

También se considera información no confidencial y de dominio público la información de las claves públicas de los certificados raíz y sus subordinadas, así como las claves públicas de los certificados TSU y de firma digital emitidos por OGTIC PCSC, todas ellas disponibles en mismo sitio web mencionado anteriormente.

9.3.3. Responsabilidad para la protección de la información confidencial

OGTIC PCSC cuenta con un procedimiento para la Gestión Documental y de Registros como parte de la implantación en su organización, en el que se definen los distintos mecanismos previstos para el tratamiento y protección de la información confidencial.

9.4. Privacidad de la información personal

9.4.1. Plan de privacidad

OGTIC PCSC cumple con el RGPD y toda la legislación pertinente. Los servicios de confianza prestados quedan por tanto recogidos en los procedimientos de control de acceso a terceros, en los términos previstos.

Se cuenta de igual forma con mecanismos para la entrega y borrado de datos, y para la gestión de notificaciones obligatorias a propietarios de los datos.

9.4.2. Información con tratamiento privado

Acorde a los procedimientos de gestión documental implantados por OGTIC PCSC, será considerada como información privada aquella documentación interna que no requiera de un tratamiento especial de protección, pero no es de dominio público, por lo que su uso estará restringido en los términos establecidos en cada documento.

9.4.3. Información no considerada con tratamiento privado

Acorde a los procedimientos de gestión documental implantados por OGTIC PCSC, aquella información no considerada como confidencial, ni privada, se le dará un tratamiento público, quedando etiquetada debidamente y publicada en los distintos canales previstos para cada caso.

9.4.4. Responsabilidad para la protección de la información privada

OGTIC PCSC cuenta con un procedimiento para la Gestión Documental y de Registros como parte de la implantación en su SGSI de la ISO27001, y en el que se definen los distintos mecanismos previstos para el tratamiento y protección de la información privada.

9.4.5. Consentimiento de uso de la información privada

En todos los casos el suscriptor del servicio prestado por OGTIC PCSC es informado de los tratamientos de la información facilitada, sin perjuicio de lo establecido en los distintos avisos legales de la web donde se le requiere un consentimiento específico.

9.4.6. Divulgación de conformidad con procesos judiciales o administrativos

La información personal que pudiera esta en posesión de OGTIC PCSC solo podría ser divulgada ante requerimientos legales o administrativos por las administraciones competentes.

9.4.7. Otras casos para la divulgación de información

No previstos.

9.5. Derechos de propiedad intelectual

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

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

9.6. Obligaciones y Responsabilidad

9.6.1. Obligaciones de la CA

OGTIC PCSC, como CA está obligada a cumplir con lo dispuesto por la normativa vigente y detallada en el capítulo 9.14, y además a:

- Respetar lo dispuesto en estas CPS.
- Se obliga a custodiar sus claves privadas de forma segura en un dispositivos HSM´s conforme a la especificación ETSI EN 319 422.
- Emitir certificados conforme a estas CPS y sus Políticas de Certificados, y conforme a los estándares vigentes.
- Emitir certificados según la información que obra en su poder en ese momento y libres de errores de entrada de datos.

- Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente para los certificados cualificados.
- Revocar los certificados según lo dispuesto en estas prácticas y sus respectivas políticas, y publicar a través de los distintos servicios previstos la información del certificado revocado.
- Informar a los Firmantes/Suscriptores de la revocación de sus certificados, en tiempo y forma de acuerdo con la legislación vigente.
- Publicar estas CPS y sus correspondientes políticas en su sitio web.
- Informar sobre las modificaciones de estas CPS o sus correspondientes políticas de certificados a los suscriptores.
- Hacer el debido uso de los datos de creación de certificados acorde a las presentes CPS y políticas de certificados, haciendo uso de dispositivos seguros conforme a la especificación ETSI EN 319 422 y que impidan la alteración o manipulación indebida.
- Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida o destrucción o falsificación.
- Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente.
- Se obliga a cumplir lo establecido en la presente política y en la normativa y estándares técnicos de aplicación.
- Se obliga a asegurar la precisión horaria de los sellos de tiempo con un desfase inferior a un segundo respecto a UTC.
- Se obliga a mantener el servicio de sellado de tiempo disponible de forma ininterrumpida conforme a lo declarado en las prácticas.
- Se obliga a detener el servicio de sellos de tiempo cuando exista falta de sincronía con la fuente de hora, con un desfase superior al máximo aceptable de 0.8 segundo.
- Se responsabiliza de la emisión de sellos de tiempo (TSTs) y de certificados de firma digital de acuerdo a las políticas y estándares técnicos.

9.6.2. Obligaciones de la RA

En los servicios prestados inicialmente por OGTIC PCSC, no se hace uso de autoridades de registro y por tanto éstas no quedan reguladas en esta versión de prácticas de certificación.

9.6.3. Obligaciones del suscriptor

Las obligaciones del suscriptor quedan definidas en las correspondientes políticas de certificados.

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:

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

9.6.5. Obligaciones de otras entidades

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 PCSC, en caso de extralimitación del uso o de omisiones del suscriptor.

- Los algoritmos criptográficos ni de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si se ha procedido con la diligencia debida de acuerdo al estado actual de la técnica, y conforme a los documentos publicados y la normativa vigente.
- Problemáticas asociadas al incumplimiento por parte de los suscriptores de las condiciones de contratación (por ejemplo, impagos).

9.9. Indemnizaciones

Las cuantías que en concepto de daños y perjuicios debiera satisfacer por imperativo judicial OGTIC PCSC a los suscriptores en defecto de regulación específica en los contratos o convenios, se limitan a un máximo de CIENTO OCHENTAMIL PESOS DOMINICANOS (RD$180,000.00).

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://ca.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.

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 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, así como la legislación específica civil, mercantil y de protección de datos que sea aplicable.

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

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

9.14. Normativa aplicable

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

- Reglamento (UE) 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (eIDAS).

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

- 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 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 CPS
c) Límites de uso y condiciones del servicio explícitamente contratado