Consorci
Administració Oberta
de Catalunya

Texto divulgativo para certificados electrónicos

Referència:	D1111 E0650 N-Text Divulgatiu
Versió:	1.5
Data:	27/01/2021

Historial de Versiones

Versión	Fecha	Cambios
1.0	21/02/2017	● Versión inicial
1.1	09/05/2018	● Correcciones de formato ● Añadida sección “Notificación de incidencias de autenticación de sitio web y certificados SSL” ● Modificada URL de la CPS
1.2	24/07/2019	● Revisió anual de la documentació, post auditoría eIDAS. ● Aclaradas referencias entre la Declaración de Prácticas de Certificación, la Política General de Certificación (antigua) y las Políticas de Certificación. ● “*2.1. Definiciones sobre destinatarios*”: cambios en las definiciones. ● “*2.3. Tipos de certificados*”: cambios en la validez de los certificados SSL, EV y Sede, a 2 años.
1.3	31/03/2020	● Revisión anual de la documentación ● Incluído teléfono de contacto
1.4	03/08/2020	● Inclusión de certificados de autenticación y firma de trabajador público de nivel medio y de nivel alto
1.5	27/01/2021	● Adaptación a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Índice

1. INTRODUCCIÓN E INFORMACIÓN DE CONTACTO

1.1. Introducción

El presente documento es un texto divulgativo, que tiene por finalidad difundir los aspectos fundamentales contenidos en la Declaración de Prácticas de Certificación (en adelante, DPC) y Políticas de Certificación (en adelante PC) del Consorci Administració Oberta de Catalunya (en adelante Consorci AOC) en relación con los certificados electrónicos, no entendiéndose en ningún caso, que desarrolla, amplía o modifica la citada DPC y PC del Consorci AOC.

El presente Texto de Divulgación se encuentra sujeto a la jerarquía documental que se deduce de la cláusula siete del presente documento; jerarquía que deberá ser respetada y que, en cualquier caso, resultará de aplicación.

1.2. Organización responsable

Consorci Administració Oberta de Catalunya (Consorci AOC)

1.3. Datos de contacto de la organización

Para cualquier consulta, dirigirse a:

Consorci Administració Oberta de Catalunya (Consorci AOC)

Subdirecció de Tecnologia i Serveis

Carrer Tànger, 98

08008 – Barcelona

1.4. Contacto y procedimiento de revocación

Para cualquier consulta, dirigirse a:

Consorci Administració Oberta de Catalunya (Consorci AOC)

Servei de Certificació Digital

Carrer Tanger, 98

08008 - Barcelona

Servicio de Atención al Usuario: 900 90 50 90, o +34 93 272 25 01 para llamadas desde el exterior del estado, en horario 24x7 para la gestión de la revocación de certificados.

1.5. Notificación de incidencias de autenticación de sitio web

Para notificar cualquier cuestión relacionada con el uso, corrección, seguridad o cualquier otro aspecto relacionado con cualquier tipo de autenticación de sitio web emitido por el Consorci AOC, por favor contacte con la siguiente dirección electrónica:

incident_pki@aoc.cat

Indicando, si es posible:

1. Hora y fecha
2. Número de serie del certificado
3. URL a la que está intentando acceder
4. Dirección IP desde donde está intentando acceder a la URL anterior

2. TIPO Y FINALIDAD DE LOS CERTIFICADOS

2.1. Definiciones sobre destinatarios

- **Empleado público** - Personal que desarrolla funciones retribuidas en las Administraciones públicas al servicio de los intereses generales, de acuerdo con las previsiones del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público (TREBEP) o de otra normativa de aplicación.
- **Trabajador público** - Personal al servicio de las entidades que integran el sector público de Cataluña, que mantiene una relación laboral o de alta dirección (como los directivos públicos profesionales)
- **Persona vinculada** - Personal no propio de las administraciones públicas catalanas pero que necesita este certificado para relacionarse con la administración por su condición de contratista (por ejemplo).
- **Empleado público con pseudónimo** - Personal que desarrolla funciones retribuidas en las Administraciones públicas al servicio de los intereses generales, de acuerdo con las previsiones del Real Decreto Legislativo 5/2015, de 30 de octubre, por el quese aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público o de otra normativa de aplicación pero que la identificación de la persona se realiza intermediando a un pseudónimo para casos especiales en que el certificado no tiene que mostrar los datos relativos a la identidad del empleado público.
- **Representante** - Persona que actúa con facultades generales de representación de su organización ante otras administraciones públicas.
- **Persona jurídica** - Cuando hablamos de persona jurídica, entendemos que quien se identifica es la propia administración pública catalana.

2.2. Definiciones sobre finalidades de los certificados

- **Autenticación** - Identificación de la persona para permitir acceso a la aplicación informática
- **Cifrado** - Uso para cifrado y descifrado de archivos, para permitir un tratamiento confidencial
- **Firma electrónica avanzada** - Firma electrónica realizada con un certificado cualificado, de acuerdo con la legislación aplicable
- **Firma electrónica cualificada** - Firma electrónica cualificada, realizada con un certificado cualificado que esta emitido en un dispositivo cualificado de creación de firma
- **Securización web** - para identificarse ante las aplicaciones cliente que se conectan y para proteger el secreto de las comunicaciones entre cliente y servidor, pueden obtenerse alguna de las siguientes variantes:
    - **Securización de webs oficiales**: destinados a garantizar las comunicaciones seguras con las páginas web oficiales de las entidades públicas catalanas
    - **Extended Validation**: garantizan la validación automática en el navegador
- **Identificación y firma automatizada**: cuándo la identificación o firma electrónica es requerida por una aplicación informática, en lugar de una persona. Puede obtenerse la siguiente variante:
    - **Actuación administrativa automatizada**: se utiliza para la identificación y autenticación del ejercicio de la competencia en la actuación administrativa

automatizada (el archivo electrónico automatizado, las compulsas y las copias electrónicas, entre otros)

2.3. Tipos de certificados

Tipos de Certificados	Destinatarios	Finalidades	OID	Vigencia
T-CAT Autenticación	Empleado público	Autenticación	1.3.6.1.4.1.1509 6.1.3.2.7.1.2	Hasta 5 años
T-CAT Firma	Empleado público	Firma cualificada	1.3.6.1.4.1.1509 6.1.3.2.7.1.1	Hasta 5 años
T-CAT persona vinculada	Persona vinculada	Autenticación Firma cualificada	1.3.6.1.4.1.1509 6.1.3.2.82.1	Hasta 5 años
T-CAT P	Empleado público	Autenticación Firma avanzada	1.3.6.1.4.1.1509 6.1.3.2.7.3.1	Hasta 5 años
T-CAT P Persona Vinculada	Persona vinculada	Autenticación Firma avanzada	1.3.6.1.4.1.1509 6.1.3.2.86.1	Hasta 5 años
T-CAT Pseudónimo autenticación	Empleado público con pseudónimo	Autenticación	1.3.6.1.4.1.1509 6.1.3.2.4.1.2	Hasta 5 años
T-CAT Pseudónimo Firma	Persona vinculada anónima	Firma cualificada	1.3.6.1.4.1.1509 6.1.3.2.4.1.1	Hasta 5 años
T-CAT R	Representante ante las AAPP	Autenticación Firma cualificada	1.3.6.1.4.1.1509 6.1.3.2.8.1.1	Hasta 5 años
T-CAT treballador públic	Trabajador público	Autenticación Firma cualificada	1.3.6.1.4.1.1509 6.1.3.2.82.2	Hasta 5 años
T-CATP treballador públic	Trabajador público	Autenticación Firma avanzada	1.3.6.1.4.1.1509 6.1.3.2.86.3	Hasta 5 años
Dispositivo SSL	Empleado público	Securización web	1.3.6.1.4.1.1509 6.1.3.2.51.1	Hasta 2 años
Seu-e nivel medio	Persona jurídica	Securización webs oficiales de la administración pública catalana	1.3.6.1.4.1.1509 6.1.3.2.5.2	Hasta 2 años
Dispositivo SSL EV	Persona jurídica	Extended validation	1.3.6.1.4.1.1509 6.1.3.2.51.2	Hasta 2 años

Dispositivo aplicación	Persona jurídica	Identificación y firma automatizadas	1.3.6.1.4.1.1509 6.1.3.2.91.1	Hasta 5 años
Sede nivel medio	Persona jurídica	Actuaciones administrativas automatizadas	1.3.6.1.4.1.1509 6.1.3.2.6.2	Hasta 5 años
idCAT Certificado	Ciudadanos	Autenticación Firma avanzada	1.3.6.1.4.1.1509 6.1.3.2.86.2	Hasta 5 años

2.4. Validación de los certificados

Las Listas de Revocación de Certificados (en adelante las “LRCs” o las CRLs”) se publican en la web del Consorci AOC y en las URLs indicadas en los certificados emitidos.

2.5. Entidad de Certificación emisora

Los certificados son emitidos por una Entidad de Certificación perteneciente a la jerarquía pública de Certificación de Cataluña.

3. LÍMITES DE USO

Los certificados se utilizarán de conformidad con su función propia y finalidad establecida, sin que pueda utilizarse en otras funciones y con otras finalidades. De la misma forma, los certificados han de utilizarse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

La extensión Key Usage se utilizará para establecer límites técnicos a los usos que se puedan dar a una clave privada correspondiente a una clave pública listada en un certificado X.509v3. Ha de tenerse en cuenta que la efectividad de las limitaciones basadas en extensiones de certificados depende en ocasiones de la operación de aplicaciones informáticas que no han sido fabricadas ni pueden ser controladas por el Consorci AOC.

Los certificados no se han diseñado, y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieran actuaciones o prueba de errores, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas o sistemas de armamento, o un error pueda directamente comportar la muerte, lesiones personales o daños medioambientales severos.

3.1. Límites de uso dirigidos a los suscriptores

El suscriptor ha de utilizar el servicio de certificación digital prestado por el Consorci AOC exclusivamente para los usos autorizados en las “Condiciones específicas del servicio” que se reproducen de modo sucinto en la cláusula cuarta del presente Texto Divulgativo.

Así mismo, el suscriptor se obliga a utilizar el servicio de certificación digital de acuerdo con las instrucciones, manuales de uso y procedimientos y suministros por el Consorci AOC.

El suscriptor ha de cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas que utilice.

El suscriptor no puede adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de certificación digital del Consorci AOC, sin permiso expreso y por escrito del propio Consorci AOC.

3.2. Advertencias de uso dirigidas a los verificadores

El Verificador de los certificados ha de utilizar el servicio de información prestado por el Consorci AOC exclusivamente para los usos autorizados, que se reproducen concisamente en la cláusula quinta del presente documento.

De la misma forma, el Verificador se obliga a utilizar el servicio de información de acuerdo con las instrucciones, manuales de uso y procedimiento suministrados por el Consorci AOC.

El Verificador ha de cumplir cualquier ley y regulación que pueda afectar a su derecho a utilizar las herramientas criptográficas que utilice.

El Verificador no puede adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de certificación digital del Consorci AOC, sin permiso expreso y por escrito de este.

3.3. Archivo de evidencias

Se conservarán todos los registros derivados del ciclo de vida de los certificados, ya sea en papel, o de forma electrónica, con las adecuadas medidas de seguridad, autenticidad, integridad, preservación y conservación, relativos a la información contenida en el certificado, durante un periodo de 15 (quince) años desde la extinción del certificado o finalización del servicio prestado y, en todo caso, durante el periodo que establezca la legislación vigente. Estos registros han de estar a disposición de la Entidad de Certificación Vinculada.

Así mismo, se conservarán las hojas de entrega de certificado durante un periodo de 15 (quince) años. Estos registros han de estar a disposición de la Entidad de Certificación Vinculada.

4. OBLIGACIONES DE LOS SUSCRIPTORES

4.1. Solicitud del certificado y generación de claves

Antes de la emisión y entrega de un certificado, ha de existir una solicitud de certificado.

La solicitud de emisión de un certificado implica la autorización del suscriptor al Consorci AOC para que genere sus claves, y para que emita el correspondiente certificado. El soporte de claves y el uso previsto variarán según el perfil.

El suscriptor se obliga a realizar la solicitud del certificado atendiendo:

- a las especificaciones previstas para cada certificado
- al procedimiento previsto en la DPC y a la documentación de operaciones del Consorci AOC, y
- a los componentes técnicos suministrados por éste, de ser necesarios.

4.2. Veracidad de la información

El suscriptor se responsabiliza de que toda la información incluida, por cualquier medio, en la solicitud del certificado y en el certificado sea exacta, completa para la finalidad del certificado y esté actualizada en todo momento.

El suscriptor tiene que informar inmediatamente al Consorci AOC de cualquier inexactitud detectada en el certificado una vez emitido, así como los cambios que se producen en la información aportada y/o registrada por la emisión del certificado.

En caso de que el poseedor de claves cese en su vinculación con el suscriptor, este ha de solicitar inmediatamente la revocación del certificado.

4.3. Entrega y aceptación del servicio

Con la firma de la hoja de entrega, el suscriptor y en su caso, el poseedor de claves reconoce que se le ha entregado el certificado, la clave privada, y cualquier otro soporte técnico entregado por el Consorci AOC, así como, cuando proceda, el código de identificación personal. Así mismo, reconocerá que estos elementos funcionan correctamente.

El suscriptor y, en su caso el poseedor de claves acepta, con la firma de la hoja de entrega, o mediante el procedimiento telemático de aceptación de certificados, el certificado según se especifica en la Declaración de Prácticas de Certificación del Consorci AOC.

El suscriptor ha de gestionar la firma de la hoja de entrega de poseedor de claves y ha de custodiarla durante un periodo de 15 (quince) años, a contar desde el momento de la extinción del certificado, quedando toda la información a disposición del Consorci AOC, excepto cuando la activación del certificado se realice por medios telemáticos.

4.4. Poseedor de claves

El suscriptor se obliga a informar a los responsables de la custodia de claves de los términos y condiciones relativos al uso de los certificados.

Así mismo, el suscriptor se obliga a que los poseedores de claves cumplan sus obligaciones, especificadas en la hoja de entrega correspondiente.

4.5. Obligaciones de custodia

El suscriptor se obliga a custodiar, cuando sea necesario, el código de identificación personal, la tarjeta o cualquier otro soporte técnico entregado por el Consorci AOC, las claves privadas y, si fuese necesario, las especificaciones propiedad del Consorci AOC que le sean suministradas.

En caso de pérdida o robo de la clave privada del certificado, o en caso de que el suscriptor sospeche que la clave privada ha perdido fiabilidad para cualquier motivo, ha de notificarlo inmediatamente al Consorci AOC.

4.6. Obligaciones de uso correcto

El suscriptor ha de utilizar el Servicio de Certificación Digital, las claves pública y privada, la tarjeta o cualquier otro soporte técnico entregado por el Consorci AOC, exclusivamente para los usos autorizados en la Declaración de Prácticas de Certificación y la Política de Certificación, de conformidad con las “Condiciones específicas del servicio”, así como cualquier otra instrucción, manual de uso y procedimiento suministrado al suscriptor por parte del Consorci AOC. El suscriptor reconocerá que cuando utilice el certificado, y mientras este no haya expirado ni haya sido suspendido o revocado, se tendrá que aceptar el certificado y estará operativo.

4.7. Transacciones prohibidas

El suscriptor se obliga a no utilizar sus claves privadas, los certificados, las tarjetas o cualquier otro soporte técnico entregado por el Consorci AOC en la realización de transacciones prohibidas por la ley aplicable.

Los servicios de certificación digital del Consorci AOC no han sido diseñados, ni permiten su utilización o reventa como equipos de control de situaciones peligrosas, o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo o sistemas de control de armamento, o un error pueda directamente causar la muerte, daños físicos o daños medioambientales graves.

Los certificados son emitidos a los suscriptores para los usos expresamente recogidos en el primer apartado de la cláusula segunda del presente Texto Divulgativo.

Cualquier otro uso fuera de los descritos en la presente cláusula queda expresamente excluido y fundamentalmente prohibido.

5. OBLIGACIONES DEL VERIFICADOR

5.1. Decisión informada

El Consorci AOC informa al Verificador de que tiene acceso a la información suficiente para tomar una decisión informada en el momento de verificar un Certificado y confiar en la información contenida en este.

El verificador reconoce que el uso del Registro y de las LRCs del Consorci AOC, se rige por la Declaración de Prácticas de Certificación del Consorci AOC y se compromete a cumplir los requisitos técnicos, operativos y de seguridad descritos en la mencionada Declaración.

5.2. Requisitos de verificación de la firma electrónica

Para confiar en una firma electrónica, es imprescindible que el Verificador compruebe la existencia y la validez tanto del certificado como de la firma electrónica, mediante la ejecución del procedimiento de verificación.

La verificación implica comprobar la autenticidad y la integridad del documento electrónico firmado, con el fin de determinar que fue generada por la entidad de certificación legítima, que es el Consorci AOC, utilizando la clave privada correspondiente a la clave pública contenida en el certificado del suscriptor, y que el documento no fue modificado desde la generación de la firma electrónica.

La comprobación del Certificado será ejecutado normalmente de forma automática por el software del Verificador en base a los servicios y, en todo caso, de conformidad con la Declaración de Prácticas de Certificación y con los requisitos siguientes:

- Utilizar el programa apropiado para la verificación de la firma digital del Certificado, los algoritmos y las longitudes de claves autorizados en el certificado y/o ejecutar cualquier otra operación criptográfica, y establecer la cadena de certificados en que se basa la firma electrónica a verificar, ya que la firma electrónica se verifica utilizando esta cadena de certificados.
- Asegurar que la cadena de certificados identificada es la más adecuada para la firma electrónica que se verifica, ya que una firma electrónica puede basarse en más de una cadena de certificados, y es decisión del Verificador asegurarse de utilizar la cadena más adecuada para verificarla.
- Comprobar el estado de revocación de los certificados de la cadena con la información suministrada en el Registro del Consorci AOC (con LRCs o CRLs, por ejemplo) para determinar la validez de todos los certificados de la cadena de certificados, pues únicamente puede considerarse correctamente verificada una firma electrónica si todos y cada uno de los certificados de la cadena son correctos y se encuentran vigentes.
- Asegurar que todos los certificados de la cadena autorizan el uso de la clave privada por el suscriptor del certificado y el poseedor de la clave, debido a la posibilidad de que alguno de los certificados incluya límites de uso que impidan confiar en la firma electrónica que se verifica. Cada certificado de la cadena dispone de un indicador que hace referencia a las condiciones de uso aplicables, para su revisión por los verificadores.

- Verificar técnicamente la firma de todos los certificados de la cadena antes de confiar en el certificado utilizado por el firmante.
- Determinar la fecha y hora de generación de la firma electrónica, ya que la firma electrónica sólo puede considerarse correctamente verificada si fue creada dentro del periodo de vigencia de la cadena de certificados en que se basa.
- Delimitar los datos que han sido firmados digitalmente, ya que estas se utilizarán en la verificación de la firma.
- Verificar técnicamente la propia firma con el certificado del firmante avalado por la cadena de certificados.

5.3. Diligencia exigible

El verificador tiene que actuar con la máxima diligencia antes de confiar en los certificados. En concreto, el Verificador se obliga a utilizar el programa de verificación de firma electrónica con la capacidad técnica, operativa y de seguridad suficiente para ejecutar el proceso de verificación de firma correctamente, y permanecerá responsable exclusivo del daño que pueda sufrir por la incorrecta elección del mencionado programa.

La prescripción anterior no será aplicable cuando el Consorci AOC haya suministrado el programa de verificación al Verificador.

El Verificador puede confiar en un Certificado si concurren las condiciones siguientes:

- La firma electrónica se ha de poder verificar de acuerdo con los requisitos establecidos en el apartado segundo de la cláusula quinta.
- El Verificador tiene que haber utilizado información de revocación actualizada en el momento de verificación de la firma.
- El tipo y clase de Certificado tiene que ser apropiado para el uso que se pretende.
- El Verificador ha de tener en cuenta otras limitaciones adicionales de uso del Certificado indicadas de cualquier forma en el certificado, incluyendo aquellas no procesadas automáticamente por el programa de verificación, incorporadas por referencia en el certificado, y contenidas en estas condiciones de uso. En especial, un certificado no constituye una concesión de derechos y facultades por parte del Consorci AOC, al suscriptor o al poseedor de claves, más allá de la descripción del certificado según la cláusula segunda del presente Texto Divulgativo o otra indicación expresa del Consorci AOC o del propio suscriptor.
- Finalmente, la confianza tiene que ser razonable, de acuerdo con las circunstancias. Si las circunstancias requieren garantías adicionales, el verificador deberá obtener estas garantías para que la confianza sea razonable.

En cualquier caso, la decisión final con respecto a confiar o no en un Certificado verificado es exclusivamente del Verificador, que ha de adoptar una actitud activa y al que se le exige acceso a toda la información dispuesta por el Consorci AOC para tomar sus decisiones de forma totalmente informada. En caso de duda, el Verificador no deberá confiar en el Certificado.

5.4. Confianza en una firma no verificada

Queda prohibido confiar o, de cualquier otra forma, hacer uso de una firma o Certificado no verificados.

Si el Verificador confía en un certificado, asumirá todos los riesgos derivados de esta actuación.

5.5. Efecto de la verificación

En virtud de la correcta verificación de una firma y/o Certificado, de conformidad con las Condiciones de uso, el Verificador puede confiar en los datos del certificado y/o en la firma basada en este, dentro de las limitaciones de uso correspondientes.

5.6. Uso correcto y actividades prohibidas

El Verificador se obliga a no utilizar ningún tipo de información de estado de los certificados o de ningún otro tipo que haya sido suministrado por el Consorci AOC, en la realización de cualquier acto prohibido por la ley aplicable a este.

El Verificador se obliga a no inspeccionar, interferir o realizar ingeniería inversa en la implantación técnica de los servicios públicos de certificación del Consorci AOC, sin previo consentimiento escrito del Consorci AOC.

Adicionalmente, el Verificador se obliga a no comprometer intencionadamente la seguridad de los servicios públicos de certificación del Consorci AOC.

Los servicios de certificación digital prestados por el Consorci AOC no han estado diseñados ni permiten la utilización y reventa, como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo, o sistemas de control de armamento, donde un error podría causar la muerte, daños físicos o daños medioambientales graves.

6. GARANTÍAS LIMITADAS Y RECHAZO DE GARANTÍAS

6.1. Garantía del Consorci AOC para los servicios de certificación digital

El Consorci AOC se obliga a la prestación de los servicios de certificación digital en determinadas condiciones técnicas y operativas, tal como se establece en su Declaración de Prácticas de Certificación, incluyendo un registro de certificados, donde se publica información relativa al estado de los certificados.

El Consorci AOC se obliga a emitir información de estado, incluyendo la suspensión y la revocación de los certificados emitidos, de acuerdo con la DPC.

El Consorci AOC garantiza las condiciones del servicio de información siguientes:

- El certificado contiene información correcta y actual en el momento de su emisión, debidamente comprobada, de conformidad con lo que establece la legislación vigente.
- El certificado cumple todos los requisitos relativos al contenido y al formato establecido en la DPC.
- La clave privada del Consorci AOC no ha estado comprometida, excepto notificación en contra mediante el Registro.

6.2. Exclusión de la garantía

El Consorci AOC no garantiza programa alguno utilizado por cualquier persona para generar, verificar o utilizar de manera distinta, ninguna firma digital o certificado digital emitido por el propio Consorci, excepto cuando haya una declaración escrita en sentido contrario.

6.3. Seguro

El Consorci AOC, como prestador de servicios de confianza, dispone de una garantía suficiente de cobertura de su responsabilidad civil, en los términos previstos en la legislación, excepto cuando se encuentre eximida por Ley de esta obligación.

En caso de uso incorrecto no autorizado de los certificados, el Consorci AOC (o la Entidad de Certificación Vinculada correspondiente) no actuará como agente fiduciario ante suscriptores y terceras personas, que deberán dirigirse contra el infractor de las condiciones de uso de los certificados establecidos por el Consorci AOC (o la Entidad de Certificación Vinculada correspondiente).

7. ACUERDOS APLICABLES, DPC Y PC

7.1. Acuerdos aplicables

Los acuerdos aplicables al certificado, se contienen en las “Condiciones específicas del servicio”.

7.2. Declaración de Prácticas de Certificación (DPC)

Los servicios de certificación del Consorci AOC se regulan técnica y operativamente en la Declaración de Prácticas de Certificación, por sus actualizaciones posteriores, así como por documentación complementaria.

La DPC se puede consultar en:

- https://www.aoc.cat/catcert/regulacio

En todo aquello no previsto en el presente Texto Divulgativo, regirá lo que dispone la Declaración de Prácticas de Certificación. Así mismo, en caso de contradicción entre los términos del presente Texto Divulgativo, y la Declaración de Prácticas de Certificación del Consorci AOC, prevalecerá, en todo caso, esta última.

7.3. Políticas de Certificación (PC)

El Consorci AOC dispone de diversas Políticas de Certificación que detallan los requisitos de carácter técnico, jurídico y operativo, así como de regulación de los Certificados, a disposición de la comunidad de usuarios que la solicitan.

Cualquier divergencia que se derive de entre el presente Texto de Divulgación y las Políticas de Certificación del Consorci AOC, se resolverá a favor de estas últimas.

En todo aquello no previsto en el presente Texto de Divulgación, regirá lo que disponen las Políticas de Certificación del Consorci AOC.

8. POLÍTICA DE PRIVACIDAD

El Consorci AOC no puede divulgar ni puede ser obligada a divulgar ninguna información confidencial referente a certificados sin una solicitud específica previa que provenga de:

a) la persona con respecto a la cual el Consorci AOC tiene el deber de mantener la información confidencial, o

b) una orden judicial, administrativa o cualquier otra prevista en la legislación vigente.

Igualmente, el suscriptor acepta que determinada información, personal y de otro tipo, proporcionada en la solicitud de certificados, será incluida en sus certificados y en el mecanismo de comprobación del estado de los certificados, y que la información mencionada no tiene carácter confidencial, por imperativo legal.

El Consorci AOC no se hace responsable del uso que, de estos datos personales, pueda hacer un tercero.

9. POLÍTICA DE REINTEGRO

No aplicable

10. LEY APLICABLE Y JURISDICCIÓN COMPETENTE

Las partes se regirán por las leyes españolas, especialmente por la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y del Reglamento (UE) Nº 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.

La jurisdicción competente es la que se indica en la Ley 29/1998, de 13 de julio, reguladora de la jurisdicción Contencioso-Administrativa.

11. ACREDITACIONES Y SELLOS DE CALIDAD

El Consorci AOC ha superado las auditorías siguientes:

- Conformidad con Reglamento (UE) nº 910/2014.