Consorci
Administració Oberta
de Catalunya

Declaración de Prácticas de Certificación
Entidad de Certificación ACC
(EC-ACC)

Referéncia:	D1111_E0650_N-DPC EC-ACC
Versión:	3.0
Fecha:	09/05/2018

Índice

1. Introducción

Este documento es la Declaración de Prácticas de Certificación de la Entidad de Certificación 'Agencia Catalana de Certificación' (en adelante, EC-ACC), Entidad de Certificación Raíz de la jerarquía pública de certificación de Cataluña.

En esta DPC se regulan técnica y operativamente los servicios de certificación de la EC-ACC.

Los apartados con el contenido "Sin estipulación adicional" indican que se tiene que consultar la Política General de Certificación del Consorci AOC.

1.1. Presentación

Cuando se desarrolló el pacto institucional firmado el 23 de julio del 2001 por los grupos parlamentarios del *Parlament de Catalunya*, la *Generalitat de Catalunya* y el *Consorci d'Ens Locals de Catalunya (Localret)*, para el desarrollo de políticas que permitan afrontar el cambio fundamental en las estructuras sociales y económicas derivado de la confluencia de las nuevas tecnologías de la información y de la comunicación en el ámbito de las administraciones públicas catalanas, se decidió establecer sistemas de interrelación entre las mencionadas administraciones, y entre las administraciones y los ciudadanos, por vía telemática y electrónica, en las condiciones de seguridad necesarias y, especialmente, haciendo uso de certificados digitales de identidad y firma electrónica.

En cumplimiento del mencionado pacto institucional y para desarrollar el programa *Catalunya en Xarxa*, Localret y la *Generalitat de Catalunya* acordaron la creación del Consorci per la Administració Oberta Electrònica de Catalunya, con el fin de desarrollar políticas públicas en materia de servicios electrónicos a las administraciones públicas y de ejercer la condición de autoridad (técnica) de certificación de firma electrónica para garantizar el secreto, la integridad, la identidad y la autenticidad en las comunicaciones y documentos electrónicos que se producen en el ámbito de las administraciones públicas catalanas.

El 25 de febrero del 2002 tuvo lugar la sesión constitutiva del *Consorci per la Administració Oberta Electrònica de Catalunya*, una sesión en la cual el Consejo General adoptó, de entre otros, el acuerdo de constituir un ente de gestión directa bajo la forma de organismo autónomo de carácter comercial con la denominación de *Agencia Catalana de Certificació* (CATCert) y con el objetivo de gestionar certificados digitales y prestar otros servicios relacionados con la firma electrónica en el ámbito público catalán.

CATCert se creó por acuerdo de la Comisión Ejecutiva del *Consorci de l'Administració Oberta Electrònica de Catalunya*, de 29 de abril del 2002, como organismo autónomo de carácter comercial, los estatutos de la cual fueron publicados al Diario Oficial de la Generalitat de Cataluña el 30 de mayo del 2003, por Resolución PRE/1574/2003, de 15 de mayo.

Por lo tanto, la *Agencia Catalana de Certificació* se constituye en la entidad principal del sistema público catalán de certificación que regula la emisión y la gestión de los certificados que se emiten para las instituciones de autogobierno de Cataluña, las instituciones que integran el mundo local y el resto de entidades públicas y privadas que integran el sector público catalán; así como la admisión y el uso de los certificados emitidos a ciudadanos y

empresas por otros Prestadores de servicios de certificación y que soliciten la correspondiente clasificación.

Estas instituciones emitirán certificados por medio de una infraestructura técnica proporcionada por CATCert, denominada “jerarquía pública de certificación de Cataluña”, y podrán admitir y utilizar certificados otros Prestadores mediante los servicios de clasificación y validación de CATCert.

En este sentido, CATCert creó el 8 de enero del 2003, una jerarquía de entidades de certificación, la raíz de la cual es la propia Agencia.

La Entidad de certificación de CATCert (denominada EC-ACC) es la raíz de la jerarquía de confianza, y certifica las Entidades de Certificación que se crean dentro del marco de las administraciones públicas catalanas.

Actualmente existen nueve entidades de certificación vinculadas a la jerarquía pública de certificación de las administraciones públicas catalanas: EC-GENCAT, EC-SAFP, EC-AL, EC-idCAT, EC-UR, EC-URV, EC-Parlament, EC-SectorPublic y EC-Ciudadanía.

En fecha 2 de agosto de 2011, el Gobierno de la Generalitat aprobó el acuerdo sobre medidas de racionalización y simplificación de la estructura del sector público de Cataluña, en el marco de las cuales se instaba los departamentos competentes a formular e implantar estrategias de reordenación del sector público que incidieran especialmente en la mejora de la eficiencia organizativa de la cual se tiene que derivar una eficiencia económica.

En esta línea, dentro de una larga lista de actuaciones que afectaban a un número elevado de entidades que integran el sector público de la Generalitat de Cataluña, se acordó promover las actuaciones necesarias para la integración de CATCert en el Consorci AOC y proceder a la extinción de CATCert como organismo autónomo.

El Acuerdo de Gobierno de 16 de octubre de 2013, asigna la prestación de servicios de certificación al Consorci Administració Oberta de Catalunya (AOC), como medida de racionalización del sector público, que se concreta en la integración de la Agencia Catalana de Certificación en el Consorci AOC, en el cual revertirán todas las marcas, derechos, deberes y servicios gestionados hasta la fecha por CATCert.

La integración se hizo efectiva mediante el mencionado acuerdo con efectos contables y jurídicos el 30 de junio de 2013, fecha en la cual el Consorci AOC asume los derechos y obligaciones así como la prestación del servicio, incluyendo el Servicio de Certificación Digital, responsable de la emisión y gestión del ciclo de vida de los certificados digitales. En adelante, el Consorci Administració Oberta de Catalunya es el Prestador de los servicios de certificación (TSP) públicos de Cataluña y el propietario de la infraestructura de clave pública (PKI) que antes era titularidad de CATCert.

1.1.1. Tipo y clases de certificados

EC-ACC ha definido una tipología de servicios de certificación, que le permiten emitir certificados digitales para varios usos y usuarios finales diferentes.

Los certificados de infraestructura son aquellos que se emiten para gestionar y operar la infraestructura de clave pública (PKI), que es el sistema técnico, jurídico, de seguridad y de organización que ofrece apoyo a los servicios de certificación y de firma electrónica.

EC-ACC emite los siguientes tipos de Certificados de infraestructura:

1) Certificado de infraestructura de entidad de certificación vinculada (CIC), que se expide a las Entidades de Certificación que se vinculan a la jerarquía.
   Las Entidades de Certificación vinculadas pueden, a su vez, emitir certificados de infraestructura o certificados de entidad final (personales, de entidad y de dispositivo), según la clase del certificado CIC que posean, desde el momento en el cual hayan obtenido un certificado CIC válido, y mientras el mencionado certificado sea vigente
2) Certificado de infraestructura personal de firma electrónica cualificada de operadores (CIPISQ), que se emplea para autorizar operaciones relacionadas con los servicios de certificación, como la aprobación de solicitudes de certificación.
3) Certificado de infraestructura de dispositivo servidor seguro (CIDS), que utiliza una aplicación informática servidor de SSL o de TLS de infraestructura para identificarse ante las aplicaciones cliente que se conectan y para proteger el secreto de las comunicaciones entre el cliente y el servidor, como por ejemplo los servidores de las entidades de certificación.
4) Certificado de infraestructura de dispositivo de aplicación digitalmente asegurada (CIDA), que se utiliza por aplicaciones informáticas de la infraestructura que se identifican digitalmente, firman electrónicamente webservices u otros protocolos y que reciben documentos y mensajes cifrados, como por ejemplo las aplicaciones de notificación de mensajes de las entidades de certificación.
5) Certificado de infraestructura de servidor de estado de certificados en línea (CIO), que utiliza un servidor OCSP Responder para firmar sus respuestas sobre el estado de validez de los certificados.
6) Certificado de infraestructura de entidad de sellos de tiempos (CIT), que utiliza una entidad para firmar los sellos de tiempos que emite.
7) Certificado de infraestructura de entidad de validación (CIV), que utilizado un servidor de entidad de validación para firmar sus informes.

1.1.1.1. Certificados de infraestructura de entitat de certificación vinculada (CIC)

Los certificados CIC son aquellos certificados de infraestructura emitidos únicamente a otras Entidades de Certificación que, de esta forma, quedan vinculadas a la jerarquía pública de certificación de Cataluña.

Los certificados CIC se expiden para ofrecer servicios a una comunidad de usuarios concreta dentro de la jerarquía pública de certificación de Cataluña y pueden ser de diferentes niveles (nivel 1, 2 o sucesivos).
Con estos certificados, se faculta a las Entidades de Certificación a emitir certificados a usuarios finales o a otras Entidades de Certificación dentro de su propia comunidad de usuarios, en función de sus necesidades concretas y siempre que técnicamente no afecte al funcionamiento, plataformas, sistemas y aplicaciones empleados habitualmente por los usuarios finales.

Cada certificado CIC recibe un nivel, adecuado a su periodo de duración, que se utilizará para la programación de la renovación periódica de la infraestructura de certificación.
Estos certificados permiten que las Entidades de Certificación suscriptoras puedan expedir certificados a otros usuarios, ya sean otras Entidades de Certificación de nivel inferior dentro de la jerarquía, como entidades finales (personales, de dispositivo y de objeto),

desde el momento en que hayan obtenido un certificado CIC válido y mientras este certificado sea vigente.

Estos certificados generalmente son emitidos por el Consorci AOC, como Entidad de Certificación Raíz, a organizaciones que operan una Entidad de Certificación dentro de su jerarquía para diferentes usos, según su clase.

Estos certificados CIC se obtienen después de un proceso de admisión de la EC Vinculada a los servicios de certificación del Consorci AOC.

La futura EC Vinculada no podrá solicitar el Certificado CIC hasta que no haya completado su procedimiento de admisión en la Jerarquía de Entidades de Certificación de Cataluña de acuerdo con la Política General de Certificación.

Atendiendo al nivel de la Entidad de Certificación a la cual se emite el Certificado CIC, se distinguen los siguientes tipos de Certificados:

a. Certificado de Infraestructura de Entidad de Certificación Raíz (CIC Raíz)

El Certificado CIC Raíz es el certificado que el Consorci AOC se expide de forma exclusiva a sí misma como Entidad de Certificación Raíz de la Jerarquía pública de certificación de Cataluña para emitir y gestionar los certificados de las Entidades de Certificación Vinculadas a la mencionada Jerarquía.

La duración de la licencia del CIC del EC-ACC es de hasta treinta (30) años, a contar desde la fecha de su emisión.

b. Certificado de Infraestructura de Entidad de Certificación de nivel 1 (CIC-1)

El Certificado CIC-1 es el certificado que el Consorci AOC expide de forma exclusiva a si mismo como Entidad de Certificación intermedia de la Jerarquía pública de certificación de Cataluña para emitir y gestionar los certificados de las Entidades de Certificación Vinculadas a la mencionada Entidad de Certificación.

La duración de la licencia de los CIC de nivel 1 es de hasta veinticuatro (24) años, a contar desde la fecha de su emisión.

De entre las entidades de certificación vinculadas de nivel 1 se encuentra:

- la Entidad de Certificación de la Generalitat de Cataluña (EC-GENCAT), encargada de ofrecer apoyo a la jerarquía pública de certificación de Cataluña en el ámbito del sector público de Cataluña a través de la EC-SAFP.

c. Certificado de Infraestructura de la Entidad de Certificación de nivel 2 (CIC-2)

La duración de la licencia de los CIC de nivel 2 es de hasta dieciséis (16) años, a contar desde la fecha de su emisión.

De entre las entidades de certificación vinculadas de nivel 2 se encuentran:

- la Entidad de Certificación de la Secretaría de Administración y Función Pública (EC-SAFP), que expide certificados al personal y a los dispositivos de los Organismos, Departamentos y Empresas Públicas de la Secretaría de Administración y Función Pública.la Entidad de Certificación de Ciutadans (EC-idCAT), que expide certificados al público, es decir, los ciudadanos y ciudadanas catalanes, así como a otras personas (denominados colectivamente suscriptores) que necesitan relacionarse con las Administraciones públicas y otras instituciones.

- la Entidad de Certificación de la Administración Local (EC-AL), los certificados de los cuales se expiden al público, al personal y a los dispositivos de los Ayuntamientos, Consejos comarcales, Diputaciones, así como a Organismos Autónomos y a Empresas Públicas de los anteriores.
- la Entidad de Certificación de Universidades e Investigación (EC-UR), los certificados de los cuales se destinan al personal, a los estudiantes y a los dispositivos de las universidades y de los centros de investigación de Cataluña, en su caso, conectados a la "Anella Científica".
- la Entidad de Certificación del Parlamento de Cataluña (EC-Parlament), los certificados de los cuales se expiden a los Parlamentarios y al Personal de Administración y Servicios del Parlamento de Cataluña, a los Síndicos y al Personal de Administración y a los Servicios de la Sindicatura de Cuentas, a los dispositivos del Parlamento de Cataluña; y al personal asesor de los partidos políticos o grupos parlamentarios dentro de la infraestructura del Parlamento de Cataluña.
- la Entidad de Certificación del Sector Público (EC-SECTORPUBLIC), que se encarga de la prestación de servicios de certificación a la comunidad de usuarios de la Generalitat de Cataluña y el conjunto de las instituciones
- la Entidad de Certificación Ciudadanía (EC-Ciudadanía), encargada de la prestación de servicios de certificación al conjunto de la ciudadanía.

d. Certificado de Infraestructura de la Entidad de Certificación de nivel 3

La duración de la licencia de los CIC de nivel 3 es de hasta dieciséis (16) años, a contar desde la fecha de su emisión.
Actualmente, la Entidad de Certificación vinculada de nivel 3 es:

- la Entidad de Certificación de Universitat Rovira i Virgili (EC-URV), que expide certificados al personal, a los estudiantes y a los dispositivos de las facultades y de los centros universitarios de la Universitat Rovira i Virgili.

1.1.1.2. Certificado de infraestructura personal de firma electrónica cualificada de operadores (CIPISQ)

Los CIPISQ son certificados de infraestructura emitidos a operadores de Entidades de Registro para los trabajos de emisión y gestión del ciclo de vida de certificados de una Entidad de Certificación.

En consecuencia, estos certificados se utilizan únicamente para autorizar operaciones relacionadas con los servicios de certificación, como la aprobación de solicitudes de certificación, y no se pueden utilizar para ningún otro uso que no sea el de operador de Entidad de Registro.

Los CIPISQ se emiten en dos modalidades: de trabajador público y de persona vinculada.

Los CIPISQ de trabajador público se expiden a operadores de Entidades de Registro en el ámbito de las instituciones integrantes del sector público catalán, mientras que los CIPISQ de persona vinculada se expiden a operadores de entornos cerrados de usuarios en el ámbito privado.

La duración de la licencia de los CIPISQ, es de cuatro (4) años, a contar desde la fecha de su emisión.

1.1.1.3. Certificado de infraestructura de dispositivo servidor seguro (CIDS)

Los CIDS son certificados de infraestructura emitidos a Entidades de Certificación responsables de la operación de servidores seguros SSL o TLS con el fin de identificarse ante las aplicaciones cliente que se conectan y la protección del secreto de las comunicaciones entre el cliente y el servidor.

Los certificados CIDS se caracterizan por el hecho de que el poseedor de la clave privada es un dispositivo informático que realiza las operaciones de firma y descifrado de forma automática, bajo la responsabilidad del suscriptor del certificado.

Los certificados CIDS son certificados destinados a ser utilizados exclusivamente en un servidor del suscriptor identificado en el propio certificado, que lo identifican electrónicamente y protegen la información entre el cliente y el servidor. Por eso, es condición esencial para la validez del certificado CIDS la especificación de los sistemas del suscriptor en los cuales se utilizarán los certificados.

La duración de la licencia de los CIDS es de cuatro (4) años, a contar desde la fecha de su emisión.

1.1.1.4. Certificado de infraestructura de dispositivo de aplicación digitalmente asegurada (CIDA)

Los certificados CIDA son certificados de infraestructura, emitidos a Entidades de Certificación responsables de la operación de aplicaciones informáticas que se identifican digitalmente, firman electrónicamente webservices u otros protocolos y reciben documentos y mensajes cifrados.

Como certificado de dispositivo, los certificados CIDA se caracterizan por el hecho que el poseedor de la clave privada es un dispositivo informático que realiza las operaciones de firma y descifrado de forma automática, bajo la responsabilidad del suscriptor del certificado.

Los certificados CIDA son certificados destinados a ser utilizados exclusivamente en un dispositivo del suscriptor identificado en el propio certificado y, por lo tanto, en los sistemas del suscriptor del certificado.

La duración de la licencia de los CIDA es de cuatro (4) años, a contar desde la fecha de su emisión.

1.1.1.5. Certificado de infraestructura de servidor de estado de certificados en línea (CIO)

Los certificados CIO son aquellos certificados de infraestructura, emitidos para gestionar los servicios de certificación, que se expiden a Entidades responsables de la operación de servidores OCSP Responder, para firmar sus respuestas sobre el estado de validez de los certificados.

Los certificados CIO son certificados destinados a ser utilizados exclusivamente en un servidor OCSP Responder de la Entidad suscriptora, servidor que se encuentra identificado en el propio certificado. Por eso, es condición esencial para la validez del certificado CIO la especificación de los sistemas del suscriptor en los cuales se utilizarán los certificados.

La duración de la licencia de los CIO es de cuatro (4) años, a contar desde la fecha de su emisión.

1.1.1.6. Certificado de infraestructura de entidad de sellos de tiempo (CIT), que es utilizado por una entidad para firmar los sellos de tiempos que emite

Los certificados CIT son certificados expedidos a las Entidades responsables de la operación de autoridades de sellado de tiempos y hora (de ahora en adelante, TSA) que se utilizan para firmar los sellos de tiempos que emiten estas autoridades.

Los CIT son certificados ordinarios que sirven para gestionar los servicios de certificación y para garantizar la fecha y la hora de un acto determinado.

La duración de la licencia de los CIT es de cuatro (4) años, a contar desde la fecha de su emisión.

Los certificados CIT son emitidos exclusivamente para que las Entidades suscriptoras firmen los sellos de tiempos que emiten.

1.1.1.7. Certificado de infraestructura de entidad de validación (CIV)

Los certificados CIV son certificados de infraestructura, emitidos para gestionar los servicios de certificación, que se expiden a Entidades de Validación para que firmen los informes de validación que emiten.

El certificado CIV ofrece, respeto de los Informes de Validación firmados con este certificado, las garantías siguientes:

- Garantía de verificación de los certificados o firmas respecto a los que se haya realizado la solicitud del Informe de Validación.
- Garantía del contenido de los mencionados certificados o firmas previamente verificados.
- Garantía de la fecha y hora del informe.

La duración de la licencia de los CIV es de cuatro (4) años, a contar desde la fecha de su emisión.

Adicionalmente, en función de los requerimientos técnicos y de las necesidades de los usuarios, es posible que los mencionados tipos de certificados puedan incorporar otras funcionalidades que, en cualquier caso, se identificarán a cada política específica de certificación que tendrá que ser aprobada por el Consorci AOC.

1.1.2. Relación entre la Declaración de Prácticas de Certificación (DPC) y otros documentos

Este documento contiene la declaración de prácticas de certificación de EC-ACC.
EC-ACC emite certificados dentro de la Jerarquía pública de certificación del Consorci AOC. Por lo tanto, dispone de una Declaración de Prácticas de Certificación (DPC) de acuerdo con la Política General de Certificación del Consorci AOC.
Esta DPC incluye los procedimientos que aplica EC-ACC en la prestación de sus servicios, en cumplimiento de los requisitos establecidos por las políticas que gestiona y la legislación aplicable, que se describe en el apartado 9.15. Conformidad con la ley aplicable
Esta DPC se relaciona con documentación auxiliar, entre la cual se encuentran los

instrumentos jurídicos reguladores de la prestación del servicio, de la documentación y de las políticas de seguridad, así como de la documentación de operaciones.

1.2. Nombre del documento e identificación

1.2.1. Identificación de este documento

Este documento se denomina “Declaración de Prácticas de Certificación (DPC) de EC-ACC”.

Esta Declaración de Prácticas de Certificación se identifica con el siguiente OID:
1.3.6.1.4.1.15096.1.2.2

1.2.2. Identificación de políticas de certificación cubiertas por esta DPC

EC-ACC emite y gestiona certificados de acuerdo con las políticas siguientes:

- **CIC.- Certificado de infraestructura de entidad de certificación vinculada:**

  - Los CIC de nivel 0 se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.10.

    - **Certificado de Infraestructura de Entidad de Certificación Raíz (CIC Raíz)**

      El certificado CIC Raíz se identifica con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.10.

  - Los CIC de nivel 1 se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.11.

    - **Certificado de Infraestructura de la Entidad de Certificación de la Generalitat de Cataluña (EC-GENCAT)**

      El certificado CIC del EC-GENCAT es de nivel 1 y se identifica con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.11.

  - Los CIC de nivel 2 se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.12.

    - **Certificado de Infraestructura de la Entidad de Certificación de la Secretaría de Administración y Función Pública (EC-SAFP)**

      El certificado CIC del EC-SAFP es de nivel 2 y se identifica con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.12.

    - **Certificado de Infraestructura de la Entidad de Certificación de Ciutadans (EC-idCAT)**

      El certificado CIC del EC-idCAT es de nivel 2 y se identifica con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.12.

- **Certificado de Infraestructura de la Entidad de Certificación de la Administración Local (EC-AI)/AL)**

  El certificado CIC de EC-AL es de nivel 2 y se identifica con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.12.

- **Certificado de Infraestructura de la Entidad de Certificación de Universidades e Investigación (EC-UR)**

  El certificado CIC de EC-UR es de nivel 2 y se identifica con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.12.

- **Certificado de Infraestructura de la Entidad de Certificación del Parlamento de Cataluña (EC-Parlament)**

  El certificado CIC del EC-Parlament es de nivel 2 y se identifica con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.12.

- **Certificado de Infraestructura de la Entidad de Certificación del Sector Público de Cataluña (EC-SECTORPUBLIC)**

  El certificado CIC del EC-SECTORPUBLIC es de nivel 2 y se identifica con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.12.

- **Certificado de Infraestructura de la Entidad de Certificación Ciudadanía (EC-Ciudadanía)**

  El certificado CIC del EC-Ciudadanía es de nivel 2 y se identifica con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.12.

- Los CIC de nivel 3 se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.13.

  - **Certificado de Infraestructura de la Entidad de Certificación de Universitat Rovira i Virgili (EC-URV)**

    El certificado CIC del EC-URV es de nivel 3 y se identifica con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.13.

- **CIPISQ – Certificado de infraestructura personal de firma electrónica qualificadad'operadores**

Los certificados CIPISQ emitidos por el EC-ACC se identifican con el identificador de objeto (OID):

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.15

Clase 2. OID: 1.3.6.1.4.1.15096.1.3.1.16

- **Certificado de infraestructura de dispositivo servidor seguro (CIDS)**

  Los certificados CIDS emitidos por EC-ACC se identifiquen con el identificador de objeto (OID):
  Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.17

- **Certificado de infraestructura de dispositivo de aplicación digitalmente asegurada (CIDA)**

Los certificados CIDA emitidos por EC-ACC se identifican con el identificador de objeto(OID):

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.18

Certificado de infraestructura de servidor de estado de certificados en linea (CIO)

Los certificados CIO emitidos por el EC-ACC se identifican con el identificador de objeto (OID):

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.19

- **Certificado de infraestructura de entidad de sellos de tiempo (CIT)**
- **CIT-1**–

  Certificado de infraestructura de entidad de sellos de tiempos, emitido por la EC-ACC

  Clase1.3.6.1.4.1.15096.1.3.1.111

- **Certificat d'infraestructura d'entitat de validació (CIV)**

Los certificados CIV emitidos por el EC-ACC -Certificado de infraestructura de entidad de validación (CIV)- se identifican con el identificador de objeto (OID):

Clase 1. OID:: 1.3.6.1.4.1.15096.1.3.1.20

Los documentos descriptivos de estos perfiles de certificados se publican en el web del Consorci AOC.

1.3. Comunidad de usuarios de certificados

Esta DPC regula una comunidad de usuarios, que obtienen certificados para varias relaciones administrativas y privadas, de acuerdo con la legislación aplicable, que se describe en el apartado 9.15. Conformidad con la ley aplicable y la normativa administrativa correspondiente.

Los certificados de infraestructura de la EC-ACC no se expiden al público, sino a:

- La propia Entidad de Certificación Raíz de la jerarquía (EC-ACC).
- La Entidad de Certificación de la Generalitat de Catalunya (EC-GENCAT).
- La Entidad de Certificación SectorPúblic (EC-SECTORPUBLIC)
- La Entidad de Certificación Ciudadanía (EC-CIUDADANÍA)
- La Entidad de Certificación de la Secretaría de Administración Pública (EC-SAFP).
- La Entidad de Certificación de Ciutadans (EC-idCAT).
- La Entidad de Certificación de la Administración Local (EC-AI)/AL).
- La Entidad de Certificación de la Universidad e Investigación (EC-UR).
- La Entidad de Certificación de la Universitat Rovira i Virgili (EC-URV).

La Entidad de Certificación del Parlamento de Cataluña (EC-Parlament).

1.3.1. Prestadores de servicios de certificación

Un Prestador de servicios de certificación es una persona física o jurídica que produce certificados y presta otros servicios en relación con la firma electrónica, de acuerdo con la legislación aplicable, que se describe en el apartado 9.15. Conformidad con la ley aplicable. El Consorci AOC será el Prestador de servicios de certificación de EC-ACC.

Conforme a esta función, el Consorci AOC será responsable por la actuación de EC-ACC, ante los usuarios finales y los terceros verificadores de certificados y firmas electrónicas, por la actuación de las autoridades de certificación que operan en nombre de las diferentes entidades de certificación.

1.3.2. Entidad de Certificación Raíz

La Entidad de Certificación Raíz, que es el Consorci AOC, dispone de una autoridad de certificación principal, denominada “Raíz de la jerarquía pública de certificación de Cataluña” y tiene la finalidad de integrar otras entidades de certificación en el sistema público catalán de certificación mediante la vinculación técnica de las autoridades de certificación correspondientes.
La mencionada vinculación técnica se consigue mediante la emisión de certificados de infraestructura de entidad de certificación vinculada (CIC).

La huella digital del certificado de la Entidad de Certificación EC-ACC es:
28 90 3a 63 5b 52 80 hace @e6 77 4c 0b 6d a7 d6 ba a6 4a f2 @e8

1.3.3. Entidades de certificación vinculadas

Las Entidades de Certificación Vinculadas son las instituciones, a las cuales el prestador del servicio de certificación presta los servicios de expedición y de gestión de los certificados mediante las autoridades de certificación, y que se encuentran inscritas a la jerarquía pública de certificación de Cataluña.

Con una Entidad de Certificación Vinculada, la institución emite certificados a otras entidades de certificación vinculadas o a usuarios finales, mediante la emisión de los certificados de infraestructura, personales, de entidad, de dispositivos y de objetos.

Cuando la institución delega al Consorci AOC la operación de la entidad de certificación vinculada, en su calidad legal de prestador de servicios de certificación, la institución queda como responsable de la organización y las decisiones de gestión referidas a la entidad de certificación. Esta función, que no puede ser objeto de delegación, se denomina Entidad de Certificación Virtual.

El Consorci AOC puede crear, a su vez, Entidades de Certificación Vinculadas de su propia titularidad cuando no exista una institución única responsable de una comunidad de usuarios que precisan certificados.

1.3.4. Entidades de Registro

Las Entidades de Registro son las personas físicas o jurídicas que asisten a las Entidades de Certificación Vinculadas a determinados procedimientos y relaciones con los solicitantes y suscriptores de certificados, especialmente a los trámites de identificación, registro y autenticación de los suscriptores de los certificados y de los poseedores de claves.

1.3.5. Usuarios finales

Los usuarios finales son las personas que obtienen y utilizan los certificados emitidos por EC-ACC. En concreto, se pueden distinguir los usuarios finales siguientes:

- Los solicitantes de certificados.
- Los suscriptores o titulares de certificados.
- Los poseedores de claves.
- Los verificadores de firmas y certificados.

1.3.5.1. Solicitantes de certificados

Los solicitantes de los certificados indicados en esta DPC son las personas autorizadas por las Entidades de Certificación suscriptoras.

Pueden ser solicitantes:

- La persona que será el futuro poseedor de claves.
- Una persona autorizada por:
    - La Entidad de Certificación Raíz de la jerarquía (EC-ACC).
    - La Entidad de Certificación de la Generalitat de Cataluña (EC-GENCAT).
    - La Entidad de Certificación SectorPúblic (EC-SECTORPUBLIC)
    - La Entidad de Certificación Ciudadanía (EC-CIUDADANÍA)
    - La Entidad de Certificación de la Secretaría de Administración Pública (EC-SAFP).
    - La Entidad de Certificación de Ciutadans (EC-idCAT).
    - La Entidad de Certificación de la Administración Local (EC-AI)/AL).
    - La Entidad de Certificación de la Universidad e Investigación (EC-UR).
    - La Entidad de Certificación de la Universitat Rovira i Virgili (EC-URV).
    - La Entidad de Certificación del Parlamento de Cataluña (EC-Parlament).

La autorización se podrá realizar de forma expresa o tácita y, en aquellos casos en los cuales el EC-ACC lo considere conveniente, se tendrá que formalizar documentalmente.

1.3.5.2. Suscriptores de certificados

Los suscriptores de los certificados son las instituciones y las personas, físicas o jurídicas, que se identifican en el campo “Subject” del certificado.

El subcriptor de los certificados de infraestructura es:

- La Entidad de Certificación Raíz de la jerarquía (EC-ACC).
- La Entidad de Certificación de la Generalitat de Cataluña (EC-GENCAT).
- La Entidad de Certificación SectorPúblic (EC-SECTORPUBLIC).
- La Entidad de Certificación Ciudadanía (EC-Ciudadanía)
- La Entidad de Certificación de la Secretaría de Administración Pública (EC-SAFP).
- La Entidad de Certificación de Ciutadans (EC-idCAT).
- La Entidad de Certificación de la Administración Local (EC-AI)/AL).
- La Entidad de Certificación de la Universidad e Investigación (EC-UR).
- La Entidad de Certificación de la Universitat Rovira i Virgili (EC-URV).
- La Entidad de Certificación del Parlamento de Cataluña (EC-Parlament).

1.3.5.3. Poseedores de claves

Los poseedores de claves son las personas físicas que poseen de forma exclusiva las claves de firma digital de certificados personales, que están debidamente autorizadas para eso por el suscriptor y debidamente identificadas al certificado mediante su nombre y apellidos o mediante un pseudónimo.

1.3.5.4. Usuarios de certificados

Los usuarios de los certificados son los verificadores.

1.3.5.5. Verificadores de certificados

Los verificadores son las personas (se incluyen las personas físicas, instituciones, personas jurídicas y otras organizaciones y entidades) que reciben firmas digitales y certificados digitales y tienen que verificarlos como paso previo para confiar.

1.4. Uso de los certificados

Esta sección lista las aplicaciones para las que se puede utilizar cada tipo de certificado, estableciendo limitaciones, y prohíbe algunas aplicaciones de los certificados.

1.4.1. Uso típico de los certificados

1.4.1.1. Certificado de infraestructura de entidad de certificación vinculada (CIC) que se expide a las Entidades de Certificación que se vinculan a la jerarquía

Estos certificados permiten que las Entidades de Certificación suscriptoras puedan expedir certificados a otros usuarios, ya sean otras Entidades de Certificación de nivel inferior dentro de la jerarquía, como entidades finales (personales, de entidad, de dispositivo y de objeto), desde el momento en que hayan obtenido un certificado CIC válido y mientras este sea vigente.

Estos certificados generalmente son emitidos por la Agencia Catalana de Certificació, como EC Raíz, a organizaciones que operan una EC dentro de su jerarquía, para diferentes usos, según su clase:

- Firma de peticiones de renovación, suspensión y revocación de certificados CIC.
- Emisión y firma de certificados CIC, CIPISQ, CIDS, CIDA, CIO, CIT, CIV, CPSR, CPSA, CPISR, CPISA, CPI, CDS, CDA, y CUERPO.
- Emisión y firma de listas de revocación de certificados (LRC).

a. Certificado de Infraestructura de Entidad de Certificación Raíz (CIC Raíz)

Los usos permitidos del certificado CIC de EC-ACC son:

- Firma de peticiones de renovación, suspensión y revocación de certificados CIC.
- Emisión y firma de certificados CIC, CIPISQ, CIDS, CIDA, CIO, CIT y CIV.
- Emisión y firma de listas de revocación de certificados (LRC).

b. Certificado de Infraestructura de la Entidad de Certificación de la Generalitat de Cataluña (EC-GENCAT)

Los usos permitidos del certificado CIC del EC-GENCAT son:

- Emisión y firma de certificados CIC, CIPISQ, CIDS, CIDA, CIT, CIO y CIV.
- Emisión y firma de listas de revocación de certificados (LRC).

c. Certificado de Emisión y firma de listas de revocación de certificados (LRC).do de Infraestructura de la Entidad de Certificación de la Secretaría de Administración y Función Pública (EC-SAFP)

Esta EC se encuentra en modo semiactivo, no emitiendo nuevos certificados y sólo revocando los vigentes cuando procede hasta la la extinción de la validez del último certificado emitido.

Los usos permitidos del certificado CIC del EC-SAFP son:

d. Certificado de Infraestructura de la Entidad de Certificación SectorPúblic (EC-SECTORPUBLIC)

Los usos permitidos del certificado CIC del EC-SectorPúblic son:

- CPI-1, CPSQ-1, CPSQ-2, CPISA-1, CPISA-2, CPPI-1, CPPSQ-1, CPRISQ-1, CDS-1, CDS-1_SENM, CDSQ-1, CDA-1, CDA-1_SGNM, CPISA-1_idCAT CIPISQ-1 y CIPISQ-2.
- Emisión y firma de listas de revocación de certificados (LRC).

e. Certificado de Infraestructura de la Entidad de Certificación Ciudadanía (EC-CIUDADANÍA)

Los usos permitidos del certificado CIC del EC-CIUDADANÍA son:

- Emisión y firma de certificados: CIPISQ-1, CIPISQ-2, CPISA-2_idCAT
- Emisión y firma de listas de revocación de certificados (LRC).

f. Certificado de Infraestructura de la Entidad de Certificación de Ciutadans (EC-idCAT)

Esta EC se encuentra en modo semiactivo, no emitiendo nuevos certificados y sólo revocando los vigentes cuando procede hasta la la extinción de la validez del último certificado emitido.

g. Certificado de Infraestructura de la Entidad de Certificación de la Administración Local (EC-/AL)

Esta EC se encuentra en modo semiactivo, no emitiendo nuevos certificados y sólo revocando los vigentes cuando procede hasta la la extinción de la validez del último certificado emitido.

h. Certificado de Infraestructura de la Entidad de Certificación de Universidades e Investigación (EC-UR)

Esta EC se encuentra en modo semiactiu, no emitiendo nuevos certificados y sólo revocando los vigentes cuando procede hasta la la extinción de la validez del último certificado emitido.

i. Certificado de Infraestructura de la Entidad de Certificación de Universitat Rovira i Virgili (EC-URV)

Esta EC se encuentra en modo semiactivo, no emitiendo nuevos certificados y sólo revocando los vigentes cuando procede hasta la la extinción de la validez del último certificado emitido.

j. Certificado de Infraestructura de la Entidad de Certificación del Parlamento de Cataluña (EC-Parlament)

Esta EC se encuentra en modo semiactivo, no emitiendo nuevos certificados y sólo revocando los vigentes cuando procede hasta la la extinción de la validez del último certificado emitido.

1.4.1.2. Certificado de infraestructura personal de firma electrónica cualificada de operadores (CIPISQ)

Estos Certificados permiten que los operadores de Entidades de Registro realicen los trabajos de emisión y de gestión del ciclo de vida de certificados de una Entidad de Certificación.

Por consiguiente, estos certificados se utilizan únicamente para autorizar operaciones relacionadas con los servicios de certificación, como la aprobación de solicitudes de certificación, y no se pueden utilizar para ninguno otro uso que no sea lo de operador de Entidad de Registro.

1.4.1.3. Certificado de infraestructura de dispositivo servidor seguro (CIDS)

Estos Certificados permiten que las Entidades de Certificación responsables de la operación de servidores seguros SSL o TLS:

- Se identifiquen ante las aplicaciones cliente que se conecten,
- protejan el secreto de las comunicaciones entre el cliente y el servidor.

Los Certificados CIDS están destinados a ser utilizados exclusivamente en un servidor del suscriptor identificado en el propio certificado, que lo identifican electrónicamente y protegen la información entre el cliente y el servidor. Por eso, es condición esencial para la validez del certificado CIDS la especificación de los sistemas del suscriptor en los cuales se utilizarán los certificados.

1.4.1.4. Certificado de infraestructura de dispositivo de aplicación digitalmente asegurada (CIDA)

Estos Certificados permiten que las Entidades de Certificación responsables de la operación de aplicaciones informáticas que se identifican digitalmente firmen electrónicamente webservices u otros protocolos y reciban documentos y mensajes cifrados.

Los Certificados CIDA están destinados a ser utilizados exclusivamente en un dispositivo del suscriptor identificado en el propio certificado y, por lo tanto, en los sistemas del suscriptor del certificado.

1.4.1.5. Certificado de infraestructura de servidor de estado de certificados en línea (CIO)

Estos Certificados permiten que las Entidades responsables de la operación de servidores OCSP Responder firmen sus respuestas sobre el estado de validez de los certificados.

Los certificados CIO son certificados destinados a ser utilizados exclusivamente en un servidor OCSP Responder de la Entidad suscriptora, servidor que se encuentra identificado en el propio certificado. Por eso, es condición esencial para la validez del certificado CIO la especificación de los sistemas del suscriptor en los cuales se utilizarán los certificados.

1.4.1.6. Certificado de infraestructura de entidad de sellos de tiempo (CIT)

Estos Certificados permiten que las Entidades responsables de la operación de autoridades de sellado de tiempos y hora (de ahora en adelante, TSA) firmen los sellos de tiempos que estas Entidades emiten.

Los CIT son certificados ordinarios que sirven para gestionar los servicios de certificación y para garantizar la fecha y la hora de un acto determinado.

1.4.1.7. Certificado de infraestructura de entitat de validación (CIV)

Estos Certificados permiten que las Entidades de Certificación, actuando como Entidades de Validación, firmen los informes de validación que emiten.

1.4.2. Aplicaciones prohibidas

1.4.2.1. Informaciones para todo tipo de certificados

Los certificados sólo se podrán utilizar dentro de los límites de uso recogidos de una manera expresa en su licencia de uso y sus correspondientes Condiciones de Uso. Cualquiera otro uso fuera de los descritos en los mencionados documentos, quedan excluidos expresamente del ámbito contractual y prohibidos formalmente.

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

1.4.2.2. Requisitos específicos para los CIC

Los certificados CIC se atenderán a aquello que se dispone en esta DPC y, en todo caso, las limitaciones estarán delimitadas por la clase de certificado CIC y por la política del certificado en cuestión.

1.4.2.3. Requisitos específicos para los CIPISQ

Los CIPISQ no se pueden utilizar para ningún otro uso que no sea lo de operador de Entidad de Registro.

1.4.2.4. Requisitos específicos para los CIDS, CIDA, CIO, CIT i CIV

Los CIDS, CIDA, CIO, CIT y CIV no se pueden utilizar en sistemas diferentes de los de Entidad de Certificación.

1.5. Administración de la Declaración de Prácticas

1.5.1. Organización que administra la especificación

Consorci Administració Oberta de Catalunya – Consorci AOC

1.5.2. Datos de contacto de la organització

Consorci Administració Oberta de Catalunya – Consorci AOC

Domicilio social: Via Laietana, 26 – 08003 Barcelona

Dirección postal comercial: Tànger, 98, planta baixa (22@ Edifici Interface) - 08018 Barcelona

Web del Consorci AOC: www.aoc.cat

Web del servicio de certificación digital del Consorci AOC:

www.aoc.cat/catcert

Servicio de Atención al'Usuario: 902 901 080, en horario 24x7 para la gestión de suspensiones de certificados.

1.5.3. Persona que determina la conformidad de una Declaración de Prácticas de Certificación (DPC) con la política

La persona que determina la conformidad de una DPC con la Política General de Certificación es lo/la Responsable del Servicio de Certificación Digital del Consorci AOC, basándose en los resultados de una auditoría al efecto, realizada por un tercero, bianualmente.

1.5.4. Procedimiento de aprobación

El sistema documental y de organización de la EC-ACC garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de la Declaración de prácticas de certificación y de las especificaciones de servicio relacionadas con ella.

Esto incluye el procedimiento de modificación de especificación del servicio y el procedimiento de publicación de especificaciones de servicio.

La versión inicial de esta Declaración de prácticas es aprobada por la Comisión Ejecutiva del Consorci AOC, que es el órgano colegiado de dirección ejecutiva del Consorci AOC.
El Director Gerente del Consorci AOC es competente para aprobar las sucesivas modificaciones de esta Declaración de prácticas.

2. Publicación de información y directorio de certificados

2.1. Directorio de certificados

El servicio de directorio de certificados está disponible durante las 24 horas de los 7 días de la semana y, en caso de error del sistema fuera de control del EC-ACC, esta última realiza sus mejores esfuerzos porque el servicio se encuentre disponible de nuevo en el plazo establecido a la sección 5.7.4 de esta DPC.

2.2. Publicación de información de EC-ACC

EC-ACC publica las informaciones siguientes en su web (http://www.aoc.cat/catcert/):

- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- La política general de certificación y, cuando sea conveniente, las políticas específicas.
- Los perfiles de los certificados y de las listas de revocación de los certificados.
- La Declaración de Prácticas de Certificación.
- Los instrumentos jurídicos vinculantes con suscriptores y verificadores.

Cualquier cambio en las especificaciones o en las condiciones del servicio se comunica a los usuarios por el EC-ACC a través del directorio.

En todos los casos se hace una referencia explícita a los cambios en la página principal del web del servicio.

No se retira la versión anterior del documento objeto del cambio, pero se indica que ha sido sustituido por la versión nueva.

2.3. Frecuencia de publicación

La información de la EC-ACC se publica cuando se encuentra disponible y en especial, de forma inmediata cuando se emiten las menciones relativas a la vigencia de los certificados.

Los cambios en este documento se rigen por el establecido a la sección 9.12.1.

A los 15(quince) días desde la publicación de la nueva versión, se retira la referencia al cambio de la página principal y se inserta en el directorio.

Las versiones antiguas de la documentación son conservadas, por un periodo de 15 (quince) años por el EC-ACC, pueden ser consultadas por los interesados.

La información de estado de revocación de certificados se publica de acuerdo con el establecido a la sección 4.10.7.

2.4. Control de acceso

Sin estipulación adicional.

3. Identificación y autenticación

3.1. Gestión de nombre

En esta sección se establecen requisitos relativos en los procedimientos de identificación y autenticación que se utilizan durante las operaciones de registro que realizan, con anterioridad a la emisión y entrega de certificados, las Entidades de Registro.

3.1.1. Tipo de nombres

3.1.1.1. Estructura sintáctica

Todos los certificados contienen un nombre diferenciado X.501 en el campo Subject, incluyendo un componente CommonName (CN=).

La estructura sintáctica y el contenido de los campos de cada certificado, así como su significado semántico, se encuentran descritos en el documento “perfil de certificado” correspondiente que el Consorci AOC publica en su web (http://www.aoc.cat/catcert/).

3.1.1.2. Perfiles de los certificados

Los perfiles de los certificados emitidos por EC-ACC se publican en el web del Consorci AOC (http://www.aoc.cat/catcert/).

3.1.2. Significado de los nombres

Sin estipulación adicional.

3.1.3. Utilización de anónimos y pseudónimos

El uso de pseudónimos está previsto en los perfiles CPPI-1 i CPPSQ-1.

3.1.4. Interpretación de formatos de nombres

Sin estipulación adicional.

3.1.5. Unicidad de los nombres

EC-ACC emite diferentes tipos de certificados. Los nombres de los suscriptores de certificados son únicos para cada servicio de generación de certificados operado por EC-ACC y para cada tipo de certificado, es decir, una misma persona sólo puede tener a su nombre certificados de tipos diferentes emitidos por EC-ACC.

No se puede volver a asignar un nombre de suscriptor que ya haya sido ocupado a un suscriptor diferente.

3.1.6. Resolución de conflictos relativos a nombres

Sin estipulación adicional.
En lo referente al tratamiento de marcas registradas, ver el apartado 9.5.3.

3.2. Validación inicial de la identidad

3.2.1. Prueba de posesión de clave privada

Sin estipulación adicional.

3.2.2. Autenticación de la identidad de una organización

Esta sección contiene los requisitos para la comprobación de la identidad de una organización identificada en el certificado.

En general, EC-ACC no tendrá que determinar que un solicitante de certificados tiene derecho sobre el nombre que aparece en una solicitud de certificado. Tampoco actuará como árbitro o mediador, ni tendrá que resolver ninguna disputa concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales (por ejemplo, relativos a direcciones electrónicas).

3.2.2.1. Entidades de Certificación Vinculadas

No se requiere realizar procedimiento de autenticación de las Entidades de Certificación Vinculadas a la jerarquía pública de certificación del Consorci AOC, puesto que estas se crean en el seno de la jerarquía mediante un procedimiento aprobado por la propia EC-ACC denominado “Ceremonia de Claus”, descrito en la sección correspondiente de esta DPC.

3.2.2.2. Entidades de Registro

EC-ACC autentica, previamente a la emisión y a la entrega de un certificado CIPISQ, para cualquiera de los componentes de una Entidad de Registro, la identidad de la Entidad de Registro y del operador conforme a la sección correspondiente de esta DPC.

3.2.2.3. Suscriptores de Certificados

No se requiere realizar procedimiento de autenticación de la organización titular del certificado, puesto que se trata de certificados corporativos, en los cuales la organización suscriptora del certificado y la Entidad de Registro coinciden.

3.2.3. Autenticación de la identidad de una persona física

Esta sección contiene informaciones para la comprobación de la identidad de una persona física identificada en un certificado.

3.2.3.1. Elementos de identificación

El número y tipo de documentos necesarios para acreditar la identidad del poseedor de claves son los que admite el EC-ACC,, tal como se recoge en su normativa reguladora.

En todo caso, estos documentos identificativos contendrán como mínimo:

- Nombre y apellidos de la persona
- Número de identidad cualificado legalmente (DNI, NIF o ANIDO de los países firmantes del Acuerdo de Schengen; pasaporte en el caso de los certificados de extranjero)
- Fecha y lugar de nacimiento.
- Cualquier otra información que pueda ser utilizada para diferenciar a una persona de otra, dentro del ámbito de la Institución (por ejemplo: fotografía, corréis-@e, categoría, cargo, etc.).

3.2.3.2. Validación de los elementos de identificación

Sin estipulación adicional.

3.2.3.3. Necesidad de presencia personal

Sin estipulación adicional.

3.2.3.4. Vinculación de la persona física con la organización

3.2.3.4.1. Requisitos para certificados de Trabajador Público

Se expiden, pues, certificados a las instituciones de autogobierno de Cataluña, las instituciones que integran el mundo local y el resto de entidades que integran el Sector Público de Cataluña (en adelante “LAS INSTITUCIONES”); los reciben y los utilizan su personal, sus entidades y sus dispositivos.

3.2.3.4.2. Requisitos para certificados de Persona Vinculada

Pueden expedirse, en libre concurrencia con otros Prestadores de servicios de certificación, a personas físicas y jurídicas, incluidas aquellas sujetas en una relación administrativa de sujeción especial – como la de los estudiantes universitarios con la universidad pública en la cual cursan sus estudios superiores, o la de las empresas privadas cuando contratan con la Administración pública.

EC-ACC puede utilizar Entidades de Registro para esta tarea.

3.2.4. Información no verificada

EC-ACC se responsabiliza de que toda la información incluida en la solicitud del certificado sea exacta y completa para la finalidad del certificado; y que tiene derecho a su uso (por ejemplo, derecho a utilizar cierto nombre en la dirección de correo electrónico o la legitimidad en el uso de un servidor web).

Sin embargo, los certificados pueden incluir información no verificada, como por ejemplo la dirección de correo electrónico, siempre que se indique a los usuarios finales en el propio certificado o en los instrumentos jurídicos correspondientes.

3.3. Identificación y autenticación de solicitudes de renovación

3.3.1. Validación para la renovación de certificados

Tanto si se trata de una renovación ordinaria, como si es posterior a la revocación del certificado a renovar, el proceso a seguir para la renovación de un certificado será el mismo que para la emisión de certificados nuevos: EC-ACC tendrá que comprobar – mediante la intervención de una Entidad de Registro - que la información utilizada para verificar la identidad y el resto de datos del suscriptor y del poseedor de la clave continúan siendo válidas.

Si cualquier información del suscriptor o del poseedor de la clave ha cambiado, se registrará adecuadamente la nueva información, de acuerdo con aquello establecido en la sección 3.2Validación inicial de la identidad.

3.3.2. Validación para la renovación de certificados después de la revocación

La renovación de certificados después de su revocación no es posible.

4. Características de operación del ciclo de vida de los certificados

Nota: el término “notificación” se utiliza en este documento como equivalente de “comunicación”, a excepción de las tramitaciones documentales con otros organismos públicos exigibles por la legislación aplicable.

4.1. Solicitud de emisión de certificado

4.1.1. Legitimación para solicitar la emisión

4.1.1.1. Requisitos generales

Únicamente pueden solicitar certificados de infraestructura las Entidades de Certificación Vinculadas a la jerarquía pública de certificación de Cataluña, operada por el Consorci AOC.

4.1.1.2. Requisitos específicos para el Certificado CIC

La futura Entidad de Certificación no podrá solicitar el Certificado CIC hasta que no haya completado su procedimiento de admisión, a la Jerarquía de Entidades de Certificación del Consorci AOC.

4.1.2. Procedimento de alta; Responsabilidades

EC-ACC, con carácter previo a la emisión de un certificado, se asegura de que las solicitudes de certificados estén completas, precisas y debidamente autorizadas.
Antes de la emisión y entrega de un certificado, EC-ACC informará al suscriptor o, en su caso, el poseedor de claves de los términos y condiciones aplicables al certificado. Este requisito se cumple mediante la entrega del instrumento jurídico que vincula EC-ACC con el suscriptor o la hoja de entrega al poseedor de claves, en el cual se incluirá la mencionada información. Esta información se comunicará en apoyo perdurable, en papel o electrónicamente, y en lenguaje fácilmente comprensible.

4.2. Procesamiento de la solicitud de certificación

4.2.1. Requisitos para todo tipo de certificados

Una vez ha tenido lugar una petición de certificado, el EC-ACC, a través de una persona autorizada, verifica la información proporcionada conforme a los requisitos previstos en esta DPC.

- Si la verificación no es correcta, la EC-ACC deniega la petición. En el supuesto que las irregularidades no se puedan corregir, la EC-ACC deniega la solicitud definitivamente.

- Si la verificación és correcta, EC-ACC:
    - Aprueba la solicitud.
    - Genera, en su caso, el par de claves y el certificado.

4.2.2. Requisitos adicionales para el Certificado CIC

Cuando la Entidad de Certificación que solicita ser vinculada a la jerarquía pública de certificación de Cataluña no esté operada por el Consorci AOC, se comprobará, antes de emitir el certificado, que el Prestador de servicios de certificación correspondiente pueda demostrar la fiabilidad necesaria de sus servicios.

El EC-ACC comprobará, en el proceso de admisión de la Entidad de Certificación, los aspectos siguientes:

- Que las políticas y procedimientos operados por la Entidad de Certificación no son discriminatorios.
- Que la Entidad de Certificación ofrecerá sus servicios a todos sus solicitantes, las actividades de las cuales entran en el ámbito de operación declarado a su DPC, de acuerdo con el establecido a la sección 1.3 de la Política General de Certificación del Consorci AOC.
- Que la Entidad de Certificación es una entidad legal, de acuerdo con el establecido a la sección 1.3.1 de la Política General de Certificación del Consorci AOC, dato que se autenticará de acuerdo con el establecido a la sección correspondiente la Política General de Certificación del Consorci AOC.
- Que la Entidad de Certificación dispone de sistemas de gestión de la calidad y la seguridad adecuados para la prestación del servicio, dato que se comprobará en la auditoría de conformidad prevista a la sección 8 de la Política General de Certificación del Consorci AOC.
- Que la Entidad de Certificación utiliza personal cualificado y con la experiencia necesaria para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos adecuados de seguridad y de gestión.
- Que la Entidad de Certificación cumple los requisitos de capacidad financiera establecidos a la sección 9.2 de la Política General de Certificación del Consorci AOC.
- Que la Entidad de Certificación cumpla con los requisitos relativos a los procedimientos de resolución de disputas, establecidos a la sección 9.13 de la Política General de Certificación del Consorci AOC.
- Que la Entidad de Certificación ha documentado de manera adecuada las relaciones jurídicas en virtud de las que externaliza parte o la totalidad de sus servicios.

4.3. Emisión de certificado

4.3.1. Acciones de la EC-ACC durante el proceso de emisión

Para cada sol·licitud de certificat tramitada, EC-ACC:

- Utiliza un procedimiento de generación de certificados X.509 v3 que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada, mediante la firma digital de EC-ACC.
- Protege la confidencialidad y la integridad de los datos de registro.
- Incluye a los certificados personales las informaciones establecidas a la legislación aplicable que se describe a 9.15 Conformidad con la ley aplicable.
- Cumple las obligaciones establecidas a la legislación correspondiente, en la generación de certificados cualificados.
- Cumple los controles establecidos por esta Declaración de Prácticas de Certificación.

Nota: Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, puesto que la renovación implica la emisión de un certificado nuevo.

4.3.2. Notificación de la emisión al suscriptor

EC-ACC notifica al Consorci AOC la emisión del certificado, o la incidencia correspondiente. Así mismo, se indicará la disponibilidad del certificado y la forma de obtenerlo.

4.4. Aceptación del certificado

4.4.1. Responsabilidades del Prestador de Servicios de Certificación

EC-ACC:

- Si no lo ha hecho antes, y cuando resulte necesario, acreditará la identidad del suscriptor.

- Proporcionará al suscriptor acceso al certificado.

- Entregará, en su caso, el dispositivo criptográfico de firma, verificación de firma, cifrado o descifrado.
- Proporcionará la información siguiente:
    - Información básica sobre la política y el uso del certificado, incluyendo especialmente información sobre la Entidad de Certificación Vinculada y la Declaración de Prácticas de Certificación aplicable, así como sus obligaciones, facultades y responsabilidades.
    - Información sobre el certificado y el dispositivo criptográfico.
    - Reconocimiento del poseedor de recibir el certificado y, en su caso, el dispositivo criptográfico, y aceptación de los mencionados elementos.
    - Obligaciones del poseedor de claves.
    - Responsabilidad de poseedor de claves.
    - Método de imputación exclusiva al poseedor de su clave privada y de sus datos de activación del certificado y, en su caso, del dispositivo criptográfico,

de acuerdo con el establecido a las secciones correspondientes de esta política.

- La fecha del acto de entrega y aceptación.

4.4.2. Conducta que constituye aceptación del certificado

El certificado se puede aceptar mediante la firma de la hoja de poseedor o responsable de la custodia de claves.

También se puede aceptar el certificado mediante un mecanismo telemático de activación del certificado.

4.4.3. Publicación del certificado

Los certificados se pueden publicar sin el consentimiento previo de los poseedores de claves.

4.4.4. Notificación de la emisión a terceros

No aplicable.

4.5. Uso del par de claves y del certificado

4.5.1. Uso por parte de los posseedores de claves

Sin estipulación adicional.

4.5.2. Uso por el tercero que confía en certificados

Sin estipulación adicional.

4.6. Renovación de certificados sin renovación de claves

No se permite la renovación de certificados sin renovación de claves.

4.7. Renovación de certificados con renovación de claves

Sin estipulación adicional.

4.8. Renovación telemática

Sin estipulación adicional.

4.9. Modificación de certificados

Sin estipulación adicional.

4.10. Revocación y suspensión de certificados

4.10.1. Causas de revocación de certificados

Sin estipulación adicional.

4.10.2. Legitimación para solicitar la revocación

Sin estipulación adicional.

4.10.3. Procedimientos de solicitud de revocación

La solicitud de revocación tiene que ser enviada telemáticamente. Excepcionalmente se podrá enviar por correo electrónico firmado o por correo certificado convencional. Se tiene que incluir la información suficiente para poder identificar razonablemente, en criterio del EC-ACC, por un lado, el certificado que se solicita revocar y, por otra, la autenticidad y autoridad del solicitante.

Esta información suficiente tiene que estar formada por los datos de contacto del poseedor de claves, incluido su DNI o equivalente y de la entidad que pide la revocación, la fecha y la razón de la petición, así como el número de serie del certificado.
Quién haga la solicitud de revocación puede pedir a la Entidad de Registro más información sobre este procedimiento.

La petición de revocación con la documentación necesaria es recogida y registrada por la Entidad de Registro.

Las Entidades de Registro tienen las solicitudes de revocación dentro de su horario de oficina. Fuera de este horario, cuando sea urgente dejar sin efecto un certificado, se puede solicitar la suspensión cautelar del certificado mediante llamada telefónica al Centro de Atención al Usuario del Consorci AOC, el horario de atención del cual es 24x365.

La acción de revocación la lleva a cabo uno de los operadores de la Entidad de Registro, quien accede a la aplicación web al efecto, autenticándose intermediando un certificado digital de operador (CIPISQ, de clase 1 si es operador de la Entidad de Registro o de clase 2 cuando sea un operador del Centro de Atención a el Usuario) emitido por EC-ACC.

Una vez registrado el cambio de estado del certificado en el sistema de EC-ACC, de forma automática y a la mayor brevedad posible, se genera y publica una nueva Lista de Certificados Revocados (LCR o CRL) en la cual constará la referencia de este certificado.
Se informa al suscriptor y, en su caso, al poseedor de claves, sobre el cambio de estado del certificado, de acuerdo con la legislación aplicable.

4.10.4. Plazo temporal de solicitud de revocación

Sin estipulación adicional.

4.10.5. Plazo máximo de procesamiento de la solicitud de revocación

Sin estipulación adicional.

4.10.6. Obligación de consulta de información de revocación de certificados

Los verificadores comprueban el estado de aquellos certificados en que desean confiar.
Un método por el cual se verifica el estado de los certificados es consultando la lista de revocación de certificados o LRC más reciente emitida por el EC-ACC.

EC-ACC suministra información a los verificadores sobre cómo y dónde encontrar la LRC correspondiente.

4.10.7. Frecuencia de emisión de listas de revocación de certificados (LRCs)

Sin estipulación adicional.

4.10.8. Período máximo de publicación de LRCs

Sin estipulación adicional.

4.10.9. Disponibilidad de servicios de comprobación de estado de certificados

Sin estipulación adicional.

4.10.10. Obligación de consulta de servicios de comprobación de estado de certificados

Sin estipulación adicional.

4.10.11. Otras formas de información de revocación de certificados

Sin estipulación adicional.

4.10.12. Requerimientos especiales en caso de compromiso de la clave privada

Sin estipulación adicional.

4.10.13. Causas de suspensión de certificados

Sin estipulación adicional.

4.10.14. Quién puede solicitar la suspensión

Conforme a aquello establecido a la Política General de Certificación en relación a la suspensión de certificados corporativos.

4.10.15. Procedimentos de solicitud de suspensión

Sin estipulación adicional.

4.10.16. Período máximo de suspensión

Sin estipulación adicional.

4.10.17. Habilitación de un certificado suspendido

Sin estipulación adicional.

4.11. Servicios de comprobación de estado de certificados

4.11.1. Características de operación de los servicios

Las LRCs se publican en la web del Consorci AOC y en las URLs indicadas en los certificados emitidos.

De forma alternativa, los verificadores podrán consultar los certificados publicados en el directorio de EC-ACC.

4.11.2. Disponibilidad de los servicios

Los verificadores de certificados digitales pueden consultar un servicio en línea que responda sobre el estado de certificados (servicio OCSP responder u otros servicios de validación de certificados) operado por un Prestador de servicios de validación en quien se confía.

El Consorci AOC ofrece de manera gratuita un servicio OCSP responder para la comprobación en línea del estado de los certificados emitidos por las Entidades de Certificación que integran la jerarquía pública de certificación de Cataluña.

La URL en la que se encuentra disponible el mencionado servicio se indica en el contenido de los certificados emitidos. La información relativa al perfil OCSP y, en general, al funcionamiento del servicio se puede encontrar a http://www.aoc.cat/catcert/.

4.11.3. Otras funciones de los servicios

Sin estipulación adicional.

4.12. Finalización de la suscripción

Sin estipulación adicional.

4.13. Dipósito y recuperación de claves

4.13.1. Política y prácticas de dipósito y recuperación de claves

No se practica recuperación de claves para los certificados de firma electrónica emitidos por EC-ACC.

4.13.2. Política y prácticas de encapsulado y recuperación de claves de sesión

Sin estipulación adicional.

5. Controles de seguridad física, de gestión y de operaciones

EC-ACC se asegura de la aplicación de los procedimientos administrativos y de gestión adecuados conformes con los estándares reconocidos y, en particular:

a. Se realiza un análisis de gestión de riesgo para evaluar las medidas necesarias de seguridad.

b. Se es responsable por la provisión de los servicios de forma segura, incluso cuando una parte de los mismos sea subcontratada. Las responsabilidades de terceros se definen y se tienen que implantar los controles jurídicos necesarios para garantizar que los terceros cumplen sus obligaciones con un nivel de seguridad equivalente.

c. Se establecen las normas principales en materia de seguridad mediante un órgano de alto nivel que define la política de seguridad de la información de la Entidad y da la publicidad necesaria mediante acciones de comunicación interna.

d. Se mantiene en todo momento la infraestructura necesaria para gestionar la seguridad de las operaciones. Cualquier cambio que tenga impacto en el nivel de seguridad tiene que ser aprobado por el órgano referido al número anterior.

e. Se documentan, implantan y mantienen los controles de seguridad y procedimientos de operación de las instalaciones, los sistemas y los activos de información en que se sustenta la prestación de los servicios.

f. En caso de subcontratación total de los servicios, se garantiza el mantenimiento del nivel necesario de seguridad de la información.

5.1. Controles de seguridad física

5.1.1. Áreas seguras

EC-ACC dispone de instalaciones que protegen físicamente la prestación, al menos, de los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos.

La protección física se consigue mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación. La parte de las instalaciones compartida con otras organizaciones se encuentra fuera de estos perímetros.

5.1.2. Controles de seguridad física

EC-ACC establece controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los mismos sistemas y los equipamientos utilizados para las operaciones. La política de seguridad física y ambiental aplicable a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación establece prescripciones para las contingencias siguientes:

- Controles de acceso físico.
- Protección ante desastres naturales.
- Medidas de protección ante incendios.
- Error de los sistemas de apoyo (energía eléctrica, telecomunicaciones, etc.).
- Demolición de la estructura.
- Inundaciones.
- Protección antirobos.
- Conformidad y entrada no autorizada.
- Recuperación del desastre.
- Salida no autorizada de equipamientos, informaciones, apoyos y aplicaciones relativos a componentes utilizados para los servicios del EC-ACC.

5.1.3. Localización y construcción de las instalaciones

La localización de las instalaciones permite la presencia de fuerzas de seguridad en un plazo de tiempo razonablemente inmediato desde el momento en que se los notifica una incidencia.

La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos niveles de protección adecuados ante intrusiones a la fuerza sucia.

5.1.4. Acceso físico

EC-ACC establece niveles de seguridad con restricción de acceso a los diferentes perímetros y barreras físicas definidas.

Para el acceso a las dependencias de EC-ACC donde se lleven a cabo procesos relacionados con el ciclo de vida del certificado, es necesaria la autorización previa, la identificación en el momento del acceso y el registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Esta identificación, ante el sistema de control de accesos, se realiza mediante reconocimiento de algún parámetro biométrico del individuo, excepto en caso de visitas escoltadas.

La generación de claves criptográficas de EC-ACC, así como su almacenamiento, se realiza en dependencias específicas para estas finalidades y requieren de acceso y de permanencia dobles.

5.1.5. Electricidad y aire acondicionado

Los equipos informáticos de EC-ACC están protegidos convenientemente ante fluctuaciones o cortes de suministro eléctrico que puedan dañarlos o interrumpir el servicio. Las instalaciones cuentan con un sistema de estabilización de la corriente, así como de un sistema de generación propio con autonomía suficiente para mantener el suministro durante el tiempo que requiera el cierre ordenado y completo de todos los sistemas informáticos.

Los equipos informáticos están ubicados en un entorno donde se garantiza una climatización (temperatura y humedad) adecuada a sus condiciones óptimas de trabajo.

5.1.6. Exposición al agua

EC-ACC dispone de sistemas de detección de inundaciones adecuados para proteger los equipos y los activos ante esta eventualidad, dado el caso que las condiciones de ubicación de las instalaciones lo hicieran necesario.

5.1.7. Advertencia y protección de incendios

Todas las instalaciones y activos de EC-ACC cuentan con sistemas automáticos de detección y extinción de incendios.

En concreto, los dispositivos criptográficos y apoyos que almacenan claves de las Entidades de Certificación tendrán que contar con un sistema específico y adicional al resto de la instalación para la protección ante el fuego.

5.1.8. Almacenamiento de soportes

El almacenamiento en apoyos de información se realiza de forma que se garantiza tanto su integridad como su confidencialidad, de acuerdo con la clasificación de la información que se haya establecido.

Las copias se guardan en formato CD, y estos en una caja fuerte en la misma sala.
El acceso a estos apoyos, incluso para su eliminación, está restringido a personas específicamente autorizadas.

5.1.9. Tratamiento de resíduos

La eliminación de apoyos, tanto papel como de magnéticos, se realiza mediante mecanismos que garantizan la imposibilidad de recuperación de la información.
En el caso de apoyos magnéticos, se procede al formateo, borrado permanente o destrucción física del apoyo.

En el caso de documentación en papel, este se somete a un tratamiento físico de destrucción.

5.1.10. Copia de seguridad fuera de las instalaciones

Periódicamente, el EC-ACC almacena unacòpia de seguridad de los sistemas de información en dependencias físicamente separadas de aquellas en las cuales se encuentran los equipos.

Se realizará una copia de seguridad incremental diaria y una copia de seguridad semanal.
En el momento de realizar una salida de información de las dependencias, se tienen que adoptar medidas adecuadas para impedir cualquier recuperación indebida de la mencionada información (cómo por ejemplo la utilización de carteras con dispositivos seguros de claves o combinaciones o la utilización de ficheros cifrados).

5.2. Controles de procedimientos

EC-ACC garantiza que sus sistemas se operan de forma segura y, por eso, establece e implanta procedimientos para las funciones que afectan la provisión de sus servicios.

El personal al servicio de EC-ACC realiza los procedimientos administrativos y de gestión de acuerdo con la política de seguridad de EC-ACC.

5.2.1. Funciones fiables

Las personas que ocupan estos lugares son nombradas formalmente por el alta dirección de la EC-ACC.

Las funciones fiables incluyen:

- Personal responsable de la seguridad.
- Administradores del sistema.
- Operadores del sistema.
- Operadores de registro.
- Auditores del sistema.
- Cualquier otra persona con acceso a datos de carácter personal.

Las funciones y obligaciones fiables se definen a la sección 5.3 de esta DPC.

5.2.2. Nombre de personas por tarea

Las funciones fiables identificadas a la política de seguridad de la EC-ACC y sus responsabilidades asociadas están documentadas en descripciones de puestos de trabajo.

5.2.3. Identificación y autenticación para cada función

EC-ACC identifica y autentica el personal antes de acceder a la correspondiente función fiable.

5.2.4. Roles que requieren separación de tareas

EC-ACC identifica, a su política de seguridad, funciones o roles fiables.

Las funcionas fiables incluyen:

a) Oficial de Seguridad
b) Operador de registro
c) Administradoers del sistema
d) Operadores del sistema
e) Auditores del sistema
f) Cualquier otra persona con acceso a datos de carácter personal

Las mencionadas restricciones se aplican en todo caso:

1. La persona que actúa como oficial de seguridad o como operador de registro no puede ser auditor del sistema.

2. La persona que actúa como administrador del sistema no puede ser oficial de seguridad ni auditor del sistema.

Las funciones y obligaciones fiables se definen a la sección 5.3 de este documento.

5.3. Controles de personal

EC-ACC tiene en cuenta los aspectos siguientes:

- Se mantiene confidencialidad de la información, poniendo los medios necesarios y manteniendo una actitud adecuada en el desarrollo de sus funciones y, fuera del ámbito laboral, en aquello en lo referente a la seguridad de las infraestructuras.
- Se es diligente y responsable en el tratamiento, el mantenimiento y la custodia de los activos de la infraestructura identificados en la política, en los planes de seguridad o en esta DPC.
- No se revela información no pública fuera del ámbito de la infraestructura, ni se extraen apoyos de información a niveles de seguridad inferiores.
- Se reporta al Responsable de Seguridad, el más bien posible, cualquier incidente que se considere que afecta la seguridad de la infraestructura o limita la calidad del servicio.
- Se utilizan los activos de la infraestructura para las finalidades que los han sido encomendadas.
- Se exigen manuales o guías de usuario de los sistemas que utiliza, que permiten desarrollar su función correctamente.
- Se exige documentación escrita que marque sus funciones y las medidas de seguridad a que está sometido.
- El responsable de seguridad vela porque el punto anterior sea ejecutado y provee los responsables de área de toda la información que fuera necesaria.
- No se instala, en ninguno de los sistemas de la infraestructura, software o hardware que no sea expresamente autorizado por escrito por el responsable de sistemas de información.
- No se accede voluntariamente ni se elimina o altera información no destinada a su persona o perfil profesional.

El personal afectado por esta normativa es:

- el Responsable del Servicio.
- el Responsable de EC-ACC.
- el Responsable de Seguridad.
- el Responsable de Operaciones.
- el Operador de Ceremonias de Claves.
- El Equipo técnico de administración, operación y explotación.
- los Administradores de la Red y
- los Usuarios de EC-ACC.

El Consorci AOC, además, se ve afectado por el siguiente personal:

- quién hace las peticiones de los certificados.
- quién hace la aprobación y la validación de las peticiones de certificados.
- quién hace la generación / personalización de certificados.
- quién custodia las claves o los tokens criptográficos.
- quién custodia las claves o las combinaciones de seguridad de acceso a la sala de operaciones.
- quién accede a información clasificada.
- el personal de comunicaciones y de operaciones.
- el personal de seguridad (física y lógica) involucrado en la operación.
- el responsable del servicio.

5.3.1. Requisitos de historial, cualificaciones, experiencia y autorización

EC-ACC lo ocupa personal cualificado y con la experiencia necesaria para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuada.

Este requisito se aplicará al personal de gestión de EC-ACC, especialmente en relación con procedimientos de personal de seguridad.

La calificación y la experiencia se pueden suplir mediante una formación y un entrenamiento apropiados.

El personal en lugares fiables se encuentra libre de intereses personales que entra en conflicto con el desarrollo de la función que tenga encomendada.

5.3.2. Requisitos de formación

EC-ACC forma el personal en lugares fiables y de gestión hasta que consiguen la calificación necesaria.

La formación incluye los contenidos siguientes:

- Principios y mecanismos de seguridad de la jerarquía pública de certificación de Cataluña, así como la en torno a usuario de la persona que se tiene que formar.
- Versiones de hardware y de aplicaciones en uso.
- Tareas que tiene que realizar la persona.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

EC-ACC, además, proporciona a todo el personal involucrado en sus operaciones como Entidad de Registro una información adecuada, que incluye los procedimientos de trabajo y los de seguridad. También se realiza una instrucción periódica en normas de seguridad, planes de contingencia y gestión de incidencias.

5.3.3. Requisitos y frecuencia de actualización formativa

Todo el personal vinculado a la Entidad de Registro tiene como requisito imprescindible la asistencia al curso de formación de Entidades de Registro impartido por el Consorci AOC.

5.3.4. Secuencia y frecuencia de rotación laboral

Sin estipulación adicional.

5.3.5. Sanciones por acciones no autorizadas

EC-ACC dispone de un sistema sancionador para depurar las responsabilidades derivadas de acciones no autorizadas.

Las acciones disciplinarias incluyen la suspensión y el despido de la persona responsable de la acción dañosa.

5.3.6. Requisitos de contratación de profesionales

El EC-ACC contrata profesionales para cualquier función, incluso para un lugar fiable. En este caso, se somete a los mismos controles que los empleados restantes.

Dado el caso que el profesional no tenga que someterse a estos controles, está constantemente acompañado por un empleado fiable.

Dado el caso que todos o una parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizados en esta sección 5, o en otras partes de la política de certificado o de esta DPC, son aplicados y completados por el tercero que realiza las funciones de operación de los servicios de certificación. El EC-ACC es responsable, en todo caso, de la efectiva ejecución.

Estos aspectos quedan concretados al instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por el tercero diferente del EC-ACC.

5.3.7. Suministro de documentación al personal

El EC-ACC suministra la documentación que necesite estrictamente su personal en cada momento, con el fin de que sea basta competente.

5.4. Procedimientos de auditoría de seguridad

5.4.1. Tipo de eventos registrados

EC-ACC guarda registro, como mínimo, de los acontecimientos siguientes relacionados con la seguridad de la entidad:

- El encendido y el apagado de los sistemas.

- El inicio y la finalización de la aplicación de Autoridad (técnica) de certificación.
- Los intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema.
- Los cambios en las claves de la Autoridad (técnica) de certificado.
- Los cambios en las políticas de emisión de certificados.
- Los intentos de entrada y de salida del sistema.
- Los intentos no autorizados de entrada a la red de la EC-ACC.
- Los intentos no autorizados de acceso a los ficheros del sistema.
- La generación de las claves de la EC-ACC.
- Los intentos nulos de lectura y escritura en un certificado y en el directorio.
- Acontecimientos relacionado con el ciclo de vida del certificado, como una solicitud, una emisión, una revocación y una renovación de un certificado.
- Acontecimientos relacionado con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de este.

EC-ACC también guarda, ya sea manualmente o electrónicamente, la información siguiente:

- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor.
- Posesión de datos de activación para operaciones con la clave privada de la EC-ACC.
- Informes completos de los intentos de intrusión física a las infraestructuras que apoyan a la emisión y gestión de certificados.

5.4.2. Frecuencia de tratamiento de registros de auditoría

Los registros de auditoría se examinan al menos una vez a la semana para buscar actividad sospechosa o no habitual.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que estos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría también están documentadas.

5.4.3. Período de conservación de registros de auditoría

Los registros de auditoría se retienen durando al menos dos meses después de procesarlos y a partir de aquel momento se archivan de acuerdo con la sección 5.5 de esta DPC.

5.4.4. Protección de los registros de auditoría

Los ficheros de registros, tanto manuales como electrónicos, se protegen de lecturas, modificaciones, borrados o cualquiera otro tipo de manipulación no autorizada usando controles de acceso lógico y físico.

5.4.5. Procedimientos de copia de seguridad

Se generan copias de apoyo incrementales de registro de auditoría diariamente y copias completas semanalmente.

Para conservar correctamente las copias de seguridad realizadas, EC-ACC tiene adoptadas, como mínimo, las medidas de seguridad siguientes:

- Se almacenan en armarios ignífugos.
- Sólo personas autorizadas disponen de acceso a las copias de seguridad.
- Las copias están identificadas.
- Si un material ha contenido copias de seguridad (disquetes, DVD's...) y se quieren reutilizar se asegura que los datos que ha contenido estén completamente borrados haciendo imposible su recuperación.
- Se autoriza expresamente la extracción de las copias de seguridad fuera de la Entidad de Registro, llenando una ficha al respeto y anotando el correspondiente detalle en un libro de registro.
- Se procura ir depositando copias de seguridad periódicamente fuera de la Entidad de Registro.

5.4.6. Localización del sistema de acumulación de registros de auditoría

El sistema de acumulación de registros de auditoría es, al menos, un sistema interno de EC-ACC, compuesto por los registros de la aplicación, por los registros de red, por los registros del sistema operativo y por los datos manualmente generados, que almacenará el personal debidamente autorizado.

5.4.7. Notificación del evento de auditoría al causante

Cuando el sistema de acumulación de registros de auditoría registra un acontecimiento, no es necesario enviar una notificación al individuo, organización, dispositivo o aplicación que causó el acontecimiento.

Se comunica si el resultado de su acción ha tenido éxito o no, pero no que se ha auditado la acción.

5.4.8. Análisis de vulnerabilidades

Los acontecimientos en el proceso de auditoría se guardan, en parte, por monitoritzar las vulnerabilidades del sistema.

Los análisis de vulnerabilidad son ejecutadas, repasadas y revisadas por medio de un examen de estos acontecimientos monitorizados.

Estos análisis se ejecutan diariamente, mensualmente y anualmente de acuerdo con su definición en el Plan de Auditoría de EC-ACC.

5.5. Archivo de informaciones

EC-ACC garantiza que toda la información relativa a los certificados se guarda durante un periodo de tiempo apropiado, según el establecido a la sección 5.5.2 de esta DPC.

5.5.1. Tipo de eventos registrados

EC-ACC guarda todos los acontecimientos que tengan lugar durante el ciclo de vida de un certificado, incluyendo la renovación de este.

EC-ACC guarda un registro del siguiente:

Documentos originales:

- Formulario de solicitud de certificados.
- Certificado de datos.
- Hoja de entrega de suscriptor de certificados.

5.5.2. Periodo de conservación de registros

5.5.2.1. Requisitos para todos los tipos de certificados

EC-ACC guarda los registros especificados a la sección 5.5.1 de esta DPC durante 15 años, contados desde el momento de la expedición del certificado. Toda la información relativa a los Certificados de Infraestructura de Certificación se guarda de forma permanente.

5.5.2.2. Requisitos específicos para los certificados CIPISQ

No obstante aquello que se dispone a la sección 5.2.2.1 anterior, EC-ACC guarda los registros de los certificados CIPISQ durante 15 años, a contar desde el momento de la expedición de estos.

5.5.3. Protección del archivo

EC-ACC:

- Mantiene la integridad y la confidencialidad del archivo que contiene los datos referentes a los certificados emitidos.
- Archiva los datos indicados anteriormente de forma completa y confidencial.

- Mantiene la privacidad de los datos de registro del suscriptor.

5.5.4. Procedimientos de copia de seguridad

Un técnico de comunicaciones de la EC-ACC se encarga de hacer y de verificar la realización de las copias de seguridad de los logs de acceso lógico al sistema operativo de la LRA.

Estas copias de seguridad se realizan con una periodicidad mensual y se guardan en formato CD, y estos discos en una caja fuerte presente en la misma sala.

También se realizan copias de seguridad de la aplicación KeyOne personalizada para EC-ACC. Estas copias las guarda el Consorci AOC a sus instalaciones.

5.5.5. Requisitos de sello de cautela de fecha y hora

EC-ACC emite los certificados y las LRC con información de tiempo y hora.

5.5.6. Localización del sistema de archivo

EC-ACC tiene un sistema de mantenimiento de datos de archivo fuera de sus propias instalaciones, así como se especifica a la sección 5.1.10 de esta DPC.

5.5.7. Procedimientos de obtención y verificación de información de archivo

Sólo las personas autorizadas por EC-ACC tienen acceso a los datos de archivo, ya sea a las mismas instalaciones de EC-ACC como su ubicación externa.

5.6. Renovación de claves

Los certificados de EC-ACC que se hayan renovado, se comunican a los usuarios finales, mediante su publicación al directorio del Consorci AOC.

5.7. Compromiso de claves y recuperación de desastre

5.7.1. Procedimiento de gestión de incidencias y compromisos

EC-ACC establece los procedimientos que aplica á la gestión de las incidencias que afectan sus claves y, muy especialmente, a los compromisos de la seguridad de las claves.

5.7.2. Corrupción de recursos, aplicaciones o datos

Cuando tenga lugar un acontecimiento de corrupción de recursos, aplicaciones o datos, EC-ACC inicia las gestiones necesarias, según los documentos Plano de Seguridad, Plan de Emergencia y Plan de Auditoría, para hacer que el sistema vuelva a su estado normal de funcionamiento.

5.7.3. Compromiso de la clave privada de la Entitat

El plan de continuidad de negocio de EC-ACC (o plan de recuperación de desastres) considera el compromiso o la sospecha de compromiso de la clave privada de la EC-ACC como un desastre.

En caso de compromiso, EC-ACC:

- Informa todos los suscriptores y verificadores del compromiso.
- Indica que los certificados y la información del estado de revocación entregados usando la clave de EC-ACC ya no son válidos.

5.7.4. Desastre sobre las instalaciones

EC-ACC desarrolla, mantiene, prueba y, si es necesario, ejecuta un plan de emergencia en el caso de desastre, ya sea por causas naturales o causado por el hombre, sobre las instalaciones, que indica como se restauran los servicios de los Sistemas de Información. La ubicación de los sistemas de recuperación de desastre dispone de las protecciones físicas de seguridad detalladas al Plan de Seguridad.

EC-ACC es capaz de restaurar la operación normal de la PKI durante las 24 horas siguientes al desastre y se pueden ejecutar, como mínimo, las acciones siguientes:

- Revocación de certificados (excepto al mes de agosto)
- Publicación de información de revocación

La base de datos de recuperación de desastres utilizada por EC-ACC está sincronizada con la base de datos de producción, dentro de los límites temporales especificados en el Plan de Seguridad. Los equipos de recuperación de desastres de EC-ACC tienen las medidas de seguridad físicas especificadas en el Plan de Seguridad.

5.8. Finalización del servicio

5.8.1. EC-ACC

EC-ACC asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios del EC-ACC y, en particular, asegura un mantenimiento continuo de los registros requeridos para proporcionar evidencia de certificación en procedimientos legales.

Antes de acabar sus servicios EC-ACC ejecuta, como mínimo, los procedimientos siguientes:

- Informa todos los suscriptores y verificadores (no se requiere que EC-ACC tenga alguna relación anterior con terceras partes).
- Acaba las autorizaciones de subcontrataciones que actúen en nombre de EC-ACC en el proceso de emisión de certificados.
- Ejecuta las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de acontecimientos durante los periodos de tiempos respectivos indicados al suscriptor y a los verificadores.

- Destruye las claves privadas de EC-ACC o las retira del uso.

EC-ACC declara a sus prácticas las previsiones que tiene que adoptar en caso de fin del servicio. Estas incluyen:

- Notificación a las entidades afectadas con una antel·lació mínima de 2 meses a la finalización efectiva del servicio.
- Notificación a las entidades afectadas con una antel·lació mínima de 2 meses a la finalización efectiva del servicio.
- Cómo se trata el estado de revocación de los certificados emitidos que todavía no han expirado.

EC-ACC transfiere los certificados, en los términos previstos en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

5.8.2. Entidad de Registro

Sin estipulación adicional.

6. Controles de seguridad técnica

EC-ACC utiliza sistemas y productos fiables que están protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de apoyo.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

6.1.1.1. Requisitos para todos los certificados

Las claves pública y privada podrán ser generadas por el futuro poseedor de claves o por la EC-ACC.

6.1.2. Envío de la clave privada al suscriptor

Conforme a aquello establecida la Política General de Certificación.

6.1.3. Envío de la clave pública al emisor del certificado

El método de envío de la clave pública a la EC-ACC es PKCS #10, otra prueba equivalente o cualquiera otro método aprobado por el Consorci AOC.

6.1.4. Distribución de la clave pública del Prestador de Servicios de Certificación

La clavo de EC-ACC y las claves de las Entidades de Certificación anteriores en la jerarquía pública de certificación de Cataluña se comunican a los verificadoras, y así se asegura la integridad de la clave y se autentica el origen.

La clave pública de EC-ACC, que se la raíz de la jerarquía, se publica al directorio de EC-ACC en forma de certificado auto-firmado junto con una declaración que hace referencia al hecho que la clave permite autenticar a EC-ACC.

Se establecen medidas adicionales para confiar en el certificado auto-firmado, como por ejemplo la comprobación de la huella digital del certificado.

La clave pública de EC-ACC se publica al directorio de EC-ACC en forma de certificado CIC firmado por el Consorci AOC.

Los usuarios acceden al directorio para obtener las claves públicas de EC-ACC.

6.1.5. Medidas de claves

Las claves de EC-ACC son de 2.048 bits.
Las claves de todos los certificados emitidos por EC-ACC son de 2.048 bits.

6.1.6. Generación de parámetros de clave pública

Sin estipulación adicional.

6.1.7. Comprobación de calitat de parámetros de clave pública

Se realiza de acuerdo con la especificación técnica ETSI TS 102 176, que indica la calidad de los algoritmos de firma electrónica.

6.1.8. Generación de claves en aplicaciones informáticas o en bienes de equipo

Los padres de claves de EC-ACC son generados utilizando hardware criptográfico que cumple los requisitos establecidos por la especificación técnica CEN CWA 141617 o equivalente.

Los padres de claves de los suscriptoras de certificados CIPISQ se tienen que generar en tarjetas inteligentes o en dispositivos criptográficos que cumplen los requisitos establecidos por las especificaciones técnicas CEN CWA 14169 y CWA 14170 o equivalente.

La generación de claves para el resto de certificados se puede realizar mediante aplicaciones informáticas.

6.1.9. Propósitos de uso de claves

El EC-ACC incluye la extensión KeyUsage en todos los certificados, indicando los usos permitidos de las correspondientes claves privadas.

6.2. Protección de la clave privada

6.2.1. Módulos de protección de la clave privada

6.2.1.1. Estándares de los módulos criptográficos

Conforme a aquello establecido a la Política General de Certificación.

6.2.1.2. Ciclo de vida de las tarjetas con circuito integrado

Conforme a aquello establecido a la Política General de Certificación.

6.2.2. Control para más de una persona (n de m) sobre la clave privada

De los 5 posibles dispositivos criptográficos que existen, EC-ACC requiere la concurrencia de al menos 2 de forma simultánea.

Cada uno de estos dispositivos es responsabilidad de una persona concreta, única conocedora de la clave de acceso al mismo. La clave de acceso es conocida únicamente

por una persona responsable de este dispositivo. Ninguna persona no conoce más de una de las claves de acceso.

Los dispositivos criptográficos quedan almacenados en las dependencias de EC-ACC y para su acceso es necesaria una persona adicional.

6.2.3. Depósito de la clave privada

Las claves privadas de EC-ACC se almacenan en espacios ignífugos y protegidos por controles de acceso físico doble.

6.2.4. Cópia de seguridad de la clave privada

Las claves privadas de EC-ACC se almacenan en espacios ignífugos y protegidos por controles de acceso físico doble.

6.2.5. Archivo de la clave privada

La clave privada de EC-ACC cuenta con una copia de seguridad realizada, almacenada y recuperada en su caso por personal sujeto a la política de confianza del personal. Este personal está expresamente autorizado para estas finalidades y se limita a aquel que necesite hacerlo a las prácticas de EC-ACC.

Los controles de seguridad que se apliquen en copias de seguridad de EC-ACC son de nivel igual o superior a las que se apliquen a las claves habitualmente en uso.
Cuando las claves se almacenan en un módulo hardware de proceso dedicado, se proveen los controles oportunos porque estas nunca puedan abandonar el dispositivo.

6.2.6. Introducción de la clave privada en el módulo criptográfico

Las claves privadas de EC-ACC quedan almacenadas en ficheros cifrados con claves fragmentadas y en tarjetas inteligentes (de las que no pueden ser extraídas).

Estas tarjetas son utilizadas para introducir la clave privada en el módulo criptográfico.

6.2.7. Almacenamietno de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos.

6.2.8. Método de activación de la clave privada

Se requieren al menos dos personas para activar la clave privada de EC-ACC.
Para certificados CIPISQ, la clave privada del suscriptor se activa mediante la introducción del PIN a la tarjeta inteligente o dispositivo criptográfico.
Por acertificats CIPISQ, cuando la tarjeta inteligente o dispositivo criptográfico se retire del dispositivo lector, será necesaria nuevamente la introducción del PIN.

6.2.9. Método de desactivación de la clave privada

Para certificados CIPISQ, cuando la tarjeta inteligente o dispositivo criptográfico se retire del dispositivo lector, será necesaria nuevamente la introducción del PIN.

6.2.10. Métode de destrucción de la clave privada

Las claves privadas son destruidas de forma que impida su robo, modificación, divulgación o uso no autorizado.

6.2.11. Clasificación de los módulos criptográficos

Los módulos de EC-ACC obtienen o superan el nivel EAL 4 de Common Criteria (ISO 15408) con los aumentos que se determinan a la especificación técnica CEN CWA 14167.

Los módulos de los suscriptores de certificados CIPISQ obtienen o superan el nivel EAL 4 de Common Criteria (ISO 15408) con los aumentos que se determinan a la especificación técnica CEN CWA 14169.

6.3. Otros aspectos de gestión del par de claves

6.3.1. Archivo de la clave pública

EC-ACC archiva sus claves públicas, de acuerdo con lo establecido a la sección 5.5.

6.3.2. Períodos de utilización de les claus pública i privada

Los periodos de utilización de las claves son los determinados por la duración del certificado y, una vez transcurrido, no se pueden continuar utilizando.

Como excepción, la clave privada de descifrado se puede continuar utilizando hasta después de la expiración del certificado.

6.4. Dades d'activació

6.4.1. Generació i instal·lació de les dades d'activació

EC-ACC facilita al suscriptor, por un lado, los datos de activación de la tarjeta y, a la cabeza de 3 días, la tarjeta.

6.4.2. Protección de los datos de activación

Para proteger al máximo los datos de activación el Consorci AOC se encarga de distribuir los elementos de los certificados por dos canales diferentes.

- En primer lugar, el responsable de la Entidad de Registro entrega al poseedor de claves el siguiente material:
    - Hoja de entrega de poseedor
    - Tarjeta con los certificados

    - Software necesario para utilizar la tarjeta
    - Carta de entrega de certificados.
- Al mismo tiempo, y por correo electrónico, se envían al poseedor de claves los datos de activación del certificado.

De esta forma se consigue que los datos de activación estén distribuidos separadamente de la tarjeta y también en el tiempo.

6.4.3. Otros aspectos de los datos de activación

Sin estipulación adicional.

6.5. Controles de seguridad informática

6.5.1. Requisitos técnicos específicos de seguridad informática

Se garantiza que el acceso a los sistemas está limitado a individuos debidamente autorizados. En particular:

- EC-ACC garantiza una administración efectiva del nivel de acceso de los usuarios (operadores, administradores, así como de cualquier usuario con acceso directo al sistema) para mantener la seguridad del sistema, incluyendo la gestión de cuentas de usuario, auditoría y modificaciones o denegaciones de acceso oportunas.
- EC-ACC garantiza que el acceso a los sistemas de información y aplicaciones se restringe según el establecido a la política de control de acceso, así como que los sistemas proporcionan los controles de seguridad suficientes para implementar la segregación de funciones identificada a las prácticas de EC-ACC, incluyendo la separación de funciones de administración de los sistemas de seguridad y de los operadores. En concreto, el uso de programas de utilidades del sistema está restringido y estrechamente controlado.
- El personal de EC-ACC se identifica y reconoce antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del certificado.
- El personal de EC-ACC es responsable y tiene que poder justificar sus actividades, por ejemplo, mediante un archivo de acontecimientos.
- Se tiene que evitar la posibilidad de revelación de datos sensibles mediante la reutilización de objetos de almacenamiento (por ejemplo, ficheros borrados) que queden accesibles a usuarios no autorizados.
- Los sistemas de seguridad y monitorización permiten una rápida detección, registro y actuación ante intentos de accesos irregulares o no autorizados a sus recursos (por ejemplo, mediante un sistema de detección de intrusiones, monitorización y alarma).
- El acceso a los directorios públicos de la información de EC-ACC (por ejemplo, certificados o información de estado de revocación) cuenta con un control de accesos para modificaciones o borrado de datos.

6.5.2. Evaluación del nivel de seguridad informática

Las aplicaciones de EC y ER son fiables, de acuerdo con la especificación técnica CEN CWA 14167-1, y se evalúa el grado de cumplimiento mediante una auditoría de seguridad informática conforme a la especificación técnica CWA 14172-2 y un perfil de protección adecuada, de acuerdo con la norma ISO 15408 o equivalente.

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

Se realiza un análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente utilizada en las aplicaciones de Autoridad (técnica) de certificación y de Autoridad (técnica) de Registro, para garantizar que los sistemas son seguros.

Se utilizan procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia de los mencionados componentes.

6.6.2.Controles de gestión de seguridad

EC-ACC garantiza que sus funciones de gestión de las operaciones de los módulos criptográficos son suficientemente seguras; en particular, existen instrucciones para:

a. Operar los módulos de forma correcta y segura
b. Instalar los módulos minimizando el riesgo de fallo de los sistemas
c. Proteger los módulos contra virus y software malicioso para garantizar la integridad y validez de la información que procesan

6.6.3. Evaluación del nivel de seguridad del ciclo de vida

Sin estipulación adicional.

6.7. Controles de seguridad de red

Se garantiza que el acceso en las diferentes redes de la EC-ACC es limitado a individuos debidamente autorizados. En particular:

- Se implementan controles (cómo por ejemplo cortafuegos) para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos se configuran de forma que se impidan accesos y protocolos que no sean necesarios para la operación de EC-ACC.
- Los datos sensibles (incluyendo los datos de registro del suscriptor) se protegen cuando se intercambian a través de redes no seguras
- Se garantiza que los componentes locales de red (como enrutadores/routers) se encuentran ubicados en entornos seguros; también se garantiza la auditoría periódica de sus configuraciones.

6.8. Sello de tiempo

Sin estipulación adicional.

7. Perfiles de certificados y listas de certificados revocados

7.1. Perfil de certificado

Los documentos descriptivos de los varios perfiles de certificados digitales que expide el EC-ACC se publican en la web del Consorci AOC.

7.2. Perfil de la lista de revocación de certificados

El acceso a la información relativa a la lista de revocación de certificados se publica en el web del Consorci AOC http://www.aoc.cat/catcert/.

8. Auditoría de conformidad

EC-ACC realiza periódicamente una auditoría de conformidad para probar que cumple los requisitos de seguridad y de operación necesarios para formar parte de la jerarquía pública de certificación de Cataluña.

EC-ACC puede delegar la ejecución de las auditorías en una tercera entidad contratada por el Consorci AOC. En estos casos EC-ACC coopera completamente con el personal que lleva a cabo la investigación.

8.1. Frecuencia de la auditoría de conformidad

Sin estipulación adicional.

8.2. Identificación y calificación del auditor

EC-ACC acude a auditores independientes externos para la realización de las auditorías anuales de conformidad.Estos tienen que demostrar experiencia en seguridad informática, en seguridad de Sistemas de Información y en auditorías de conformidad de Autoridades de Certificación y de los elementos relacionados.

8.3. Relación del auditor con la entidad auditada

Las auditorías externas de conformidad ejecutadas por terceros son realizadas por entidades independientes de la EC-ACC.

8.4. Relación de elementos objeto de auditoría

Sin estipulación adicional.

8.5. Acciones a emprender como resultado de una falta de conformidad

Una vez recibido el informe de la auditoría de cumplimiento llevado a cabo, EC-ACC discute, con la entidad que ha ejecutado la auditoría y con el Consorci AOC, las deficiencias encontradas y desarrolla y ejecuta un plano correctivo que las soluciona.

Si EC-ACC, una vez auditada, es incapaz de desarrollar y/o ejecutar el mencionado plano o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o la integridad del sistema, se tiene que realizar una de las acciones siguientes:

- Revocar la clave de EC-ACC, tal como se describe a la sección 4.9 de esta DPC.
- Acabar el servicio de EC-ACC, tal como se describe a la sección 5.8 de esta DPC.

8.6. Tratamiento de los informes de auditoría

Los informes de resultados de las auditorías serán entregados al Consorci AOC, en cuanto que es el Prestador de Servicios de Certificación, en un plazo máximo de 15 días después de la ejecución de la auditoría, para su evaluación y gestión diligente.

9. Requisitos comerciales y legales

9.1. Tarifas

9.1.1. Requisitos comerciales y legales

El Consorci AOC establece las tarifas que aplica la EC-ACC en la prestación de sus servicios. Las tarifas se pueden consultar en la web del servicio de certificación digital del Consorci AOC.

9.1.2. Tarifa de acceso a certificados

No se puede establecer una tarifa por el acceso a los certificados.

9.1.3. Tarifa de acceso a información de estado de certificado

No se puede establecer una tarifa por el acceso a la información de estado de los certificados.

9.1.4. Tarifas otros servicios

Sin estipulación adicional.

9.1.5. Política de reintegro

El Consorci AOC no practicará reembolso. En caso de productos defectuosos, se procederá a sustituir el producto defectuoso por otro en buen estado.

9.2. Capacidad financiera

9.2.1. Seguro de responsabilidad civil

El Consorci AOC dispone de una garantía de cobertura de su responsabilidad civil suficiente, en los términos previstos al artículo 20.2 de la Ley 59/2003, de 19 de diciembre, excepto cuando se encuentre eximido por Ley de esta obligación. Este seguro cubre las actuaciones del Consorci AOC como Prestador de servicios de certificación.

9.2.2. Otros activos

Sin estipulación adicional.

9.2.3. Cobertura de aseguramiento para suscriptores y terceros que confíen en certificados

En caso de uso incorrecto o no autorizado de los certificados, el Consorci AOC (o EC-ACC) no actuará como agente fiduciario ante suscriptores y terceras personas, que tendrán que

dirigirse contra el infractor de las condiciones de uso de los certificados establecidas por el Consorci AOC (o EC-ACC).

9.3. Confidencialidad

9.3.1. Informaciones confidenciales

Las informaciones siguientes se mantienen de forma confidencial por EC-ACC:

a. Información de negocio suministrada por sus proveedores y otras personas con quienes el Consorci AOC o EC-ACC tienen una obligación de guardar secreto, establecida legalmente o convencionalmente.

b. Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.

c. Registros de auditoría interna y externa, creados y/o mantenidos por la EC-ACC y sus auditores.

d. Planes de continuidad de negocio y de emergencia.

e. Política y planes de seguridad.

f. Documentación de operaciones y restantes de planes de operación, como por ejemplo el archivo, la monitorización y otras de análogos.

g. Cualquier otra información identificada como “Confidencial”.

9.3.2. Informaciones no confidenciales

Las informaciones siguientes no tienen carácter confidencial:

- Esta Declaración de Prácticas de Certificación de la EC-ACC.
- Cualquier otra información identificada como “Pública”.

9.3.3. Responsabilidad para la protección de información confidencial

EC-ACC es responsable del establecimiento de las medidas apropiadas de protección de la información confidencial.

Estas medidas incluyen las cláusulas apropiadas de información confidenciales a los instrumentos jurídicos con todas las personas.

9.4. Protección de datos personales

9.4.1. Política de Protección de Datos Personales

El Consorci AOC desarrolla una política de protección de los datos personales, de acuerdo con la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y la normativa reglamentaria de aplicación en materia de protección de datos de carácter personal

Con motivo de la prestación de servicios propios de certificación digital, acontece responsable de los ficheros “Suscriptores de certificados” y “Personas físicas certificadas”, creados en conformidad con la LOPD y notificados al Registro de la Agencia Catalana de Protección de Datos.

La estructura de los ficheros de datos de carácter personal es la siguiente:

SUSCRIPTORES DE CERTIFICADOS:

- Datos identificativos del colectivo suscriptor: nombre de la entidad o del organismo que solicita los certificados, CIF, dirige postal completa, dirección electrónica, página web.
- Datos identificativos de la persona que asume el rol de responsable del servicio: nombre, apellidos, DNI o equivalente, teléfono, fax, dirección postal, dirección electrónica.

PERSONAS FÍSICAS CERTIFICADAS:

- Datos identificativos: nombre, apellidos y DNI o equivalente de la persona física certificada. Opcionalmente, otros datos personales la inclusión de las cuales sea solicitada por la persona autorizada, como el código CIP de la Tarjeta Individual Sanitaria.
- Datos de contacto: dirección postal completa a efectos de notificaciones, así como la dirección electrónica.
- Datos de la entidad a la que prestan sus servicios.
- Denominación de la entidad, CIF, área de adscripción política, orgánica, laboral o profesional.

Los datos recogidos y tratados por el prestador de servicios de certificación tienen la consideración legal de datos de nivel básico.

El Consorci AOC desarrolla los procedimientos indicados en este documento, que aplica en la prestación de sus servicios, en los cuales, en cumplimiento de los requisitos establecidos por las políticas de certificados que gestiona, y de acuerdo con el artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, se detallan los requisitos y obligaciones en relación con la obtención y gestión de los datos personales que obtenga, cumpliendo a tal efecto, las disposiciones de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, y del Real decreto 1720/2007, de 21 de diciembre, que aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (RLOPD).

El Consorci AOC establece las medidas de seguridad de cariz técnico y organizativo necesarias para dar cumplimiento a las medidas de seguridad aplicables a ficheros y tratamientos automatizados de la LOPD y que se describen al Documento de Seguridad LOPD. Con cariz meramente informativo se detallan a continuación las medidas aplicadas, el precepto de la LOPD y la sección de este documento y de la Política General de Certificación del Consorci AOC donde se desarrollan:

a. Ámbito de aplicación del documento de seguridad con especificación detallada de los recursos protegidos (artículo 88 del RD 1720/2007) - sección 6.1.
b. Medidas, normas, procedimientos, reglas y estándares que garanticen el nivel de seguridad exigido por el RD 1720/2007 - sección 6.1, y, en general, todos los

controles técnicos de las secciones 5 y 6 de la Política General de Certificación del Consorci AOC.

c. Funciones y obligaciones del personal (artículo 89 del RD 1720/2007) - sección 5.3.
d. Registro de incidencias (artículo 90 del RD 1720/2007), procedimiento de notificación, gestión y respuesta ante las incidencias – sección 9.4.5
e. Control de acceso (artículo 91 del RD 1720/2007) – secciones 5 y 6.
f. Gestión de apoyos (artículo 92 del RD 1720/2007) – sección 5.
g. Identificación y autenticación (artículo 93 del RD 1720/2007) – sección 5.2.
h. Procedimientos de copia de seguridad y recuperación de datos (artículo 94 del RD 1720/2007) - sección 5.5.

9.4.2. Datos de carácter personal no disponibles a terceros

En conformidad con lo establecido al artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, se consideran datos de carácter personal cualquier información relativa a personas físicas identificadas o identificables.

Los datos de carácter personal que tengan que ser incluidas a los certificados y al mecanismo indicado de comprobación del estado de los certificados son consideradas datos de carácter público a los efectos de la Ley de Firma Electrónica. En este sentido, no serán consideradas datos públicos disponibles a terceros:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados.
- Claves privadas generadas y/o almacenadas por la Entidad de Certificación.
- Cualquier otro dato de carácter personal que no sea susceptible de consulta, almacenamiento o acceso por terceros.

En cualquier caso, los datos captados por el Prestador de servicios de certificación tienen la consideración legal de datos de nivel básico.

Los datos personal se tratan de acuerdo con el artículo 9 de la LOPD y garantizando en todo caso la seguridad de las mismas para evitar alteraciones, pérdidas y accesos no autorizados y de acuerdo con las prescripciones establecidas a Real decreto 1720/2007, de 21 de diciembre, que aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

9.4.3. Datos de carácter personal disponibles a terceros

Esta información se trata de información personal que se incluye a los certificados y al referido mecanismo de comprobación del estado de los certificados, de acuerdo con la sección 3.1 de este documento.

La mencionada información, proporcionada a la solicitud de certificados en los términos que se prevén a la legislación aplicable, es incluida a sus certificados y al mecanismo de comprobación del estado de los certificados.

Estos datos de carácter personal tienen que estar disponibles por terceros por imperativo legal ("datos públicos").

En todo caso, es considerada no confidencial la siguiente información:

a. Los certificados emitidos o en trámite de emisión.
b. La sujeción del suscriptor a un certificado emitido por la Entidad de Certificación.
c. El nombre y los apellidos del suscriptor del certificado, así como cualesquier otras circunstancias o datos personales del titular, en el supuesto que sean significativas en función de la finalidad del certificado, de acuerdo con este documento.
d. La dirección electrónica del suscriptor del certificado.
e. Los usos y límites económicos reseñados al certificado.
f. El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
g. El número de serie del certificado.
h. Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
i. Las listas de revocación de certificados (LRCs), así como el resto de informaciones de estado de revocación.

La información contenida en la parte pública del Registro de la Entidad de Certificación..

9.4.4. Responsabilidad correspondiente a la protección de datos personales

El Consorci AOC, como mínimo, garantiza el cumplimiento de sus obligaciones legales como Prestador de servicios de certificación, en conformidad con la legislación aplicable, como se describe en 9.15Conformidad con la ley aplicable, en relación con la protección de datos personales.

9.4.5. Gestión de incidencias relacionadas con los datos de carácter personal

El Consorci AOC incluye en este documento su procedimiento de notificación, gestión y respuesta ante las incidencias relacionadas con los datos personales.

Este procedimiento de notificación se inicia cuando el administrador de los sistemas de la Entidad de Certificación, a sus instalaciones, comunica inmediatamente por teléfono con el Responsable de la Entidad de Certificación, describiendo el tipo de incidencia y los efectos que se observan.

Si durante la gestión de la incidencia hace falta hacer modificaciones del software o en la configuración de los sistemas, o hay que restaurar copias de seguridad u otras intervenciones parecidas, el administrador se espera a recibir la petición correspondiente por correo electrónico firmado digitalmente, que lo envía el Responsable la Entidad de Certificación o el responsable técnico del proyecto afectado (en este caso, con copia del mensaje al Responsable de la Entidad de Certificación).

Una vez hechas las actuaciones necesarias y restablecido el normal funcionamiento de los sistemas, el administrador de los sistemas envía por correo electrónico dirigido al

Responsable de la Entidad de Certificación un informe descriptivo, que en el caso de las incidencias producidas sobre ficheros que contienen datos de carácter personal, no es más que el formulario tipo debidamente rellenado.

El Responsable de la Entidad de Certificación mantiene copia de los formularios correspondientes a las incidencias registradas durante los 12 últimos meses sobre los ficheros que contienen datos de carácter personal. Estos se guardan en un directorio dedicado dentro del servidor que comparten los usuarios de la Entidad de Certificación, protegido convenientemente porque sólo pueda acceder el personal autorizado; así queda garantizado que se hacen copias de seguridad de su contenido.

Al formulario de Registro de Incidencias se hacen constar los siguientes datos:

- Qué recurso tiene la incidencia
- Su código y descripción
- El día y la hora
- El tipo de incidencia
- Los efectos
- El comunicante y el destinatario
- La respuesta
- Los procedimientos previstos a realizar
- La persona que los realizará
- El procedimiento para la recuperación
- La persona (y autorización) para la recuperación

Los datos restaurados.

9.4.6. Prestación del consentimiento para el tratamiento de los datos personales

Para la prestación del servicio, el Consorci AOC necesita recoger y almacenar ciertas informaciones que comporta tratamiento de datos personales.

En la expedición de certificados de clase 1, estos datos son comunicados por los suscriptores, sin necesidad de consentimiento de los afectados poseedores de claves, de acuerdo con el establecido por la normativa reguladora de la relación del personal al servicio del suscriptor del certificado u otra normativa que resulte aplicable, como prevé el artículo 6 de la LOPD.

El Consorci AOC informa los poseedores de claves de la obtención de sus datos personales en conformidad con el artículo 5 de la LOPD.

9.4.7. Comunicación de datos personales

El Consorci AOC sólo comunica los datos de carácter personal a terceros en los casos legalmente previstos.

En concreto, el Consorci AOC está obligada a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tengan atribuidas y en el resto de supuestos previstos al artículo 11.2 de la LOPD.

El Consorci AOC da cumplimiento a todas las prescripciones legales en conformidad con la política de protección de datos prevista a la sección 9.4.1.

Excepcionalmente y por la situación prevista en la Política General de Certificación, que contempla el caso de acabamiento de la Entidad de Certificación, el Consorci AOC cederá los datos personales para el supuesto de transferencia de prestación del servicio.

9.5. Derechos de propiedad intelectual

9.5.1. Propiedad de los certificados e información de revocación

EC-ACC es la única entidad que disfruta de los derechos de propiedad intelectual sobre los certificados que emite.

EC-ACC concede licencia no exclusiva para reproducir, distribuir, verificar y utilizar los certificados, sin ningún coste, en relación a firmas digitales y/o sistemas de cifrado dentro del ámbito de aplicación de esta DPC, de acuerdo con el correspondiente instrumento vinculante entre EC-ACC y la parte que reproduzca y/o distribuya el certificado.

Las normas anteriores figuran a los instrumentos jurídicos que existen entre EC-ACC y los suscriptores y los verificadores.

Adicionalmente, los certificados emitidos por EC-ACC contienen un aviso legal relativo a la propiedad de estos certificados. Esta normativa resulta igualmente de aplicación en el uso de información de revocación de certificados.

9.5.2. Propiedad de la Política de Certificación y Declaración de Prácticas de Certificación

El Consorci AOC es la única entidad que disfruta de los derechos de propiedad intelectual sobre la política de certificación de la jerarquía pública de certificación de Cataluña.

EC-ACC es propietaria de esta DPC.

9.5.3. Propiedad de la información relativa a nombres

El suscriptor (o el poseedor de claves, si procede) conserva cualquier derecho, de existir este, relativo en la marca, producto o nombre comercial contenido al certificado.

El suscriptor (o el poseedor de claves, si procede) es el propietario del nombre distinguido del certificado, formado por las informaciones especificadas a la sección 3.1 de esta DPC.

9.5.4. Propiedad de claves

Los pares de claves son propiedad de los suscriptores de los certificados.

Cuando una clave se encuentre fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

9.6. Obligaciones y responsabilidad civil

9.6.1. EC-ACC

9.6.1.1. Obligaciones y otros compromisos ACC

EC-ACC se obliga a cumplir lo siguiente:

- Determina la comunidad de suscriptores y verificadores de EC-ACC.
- Aprueba las políticas de certificación y, si procede, las políticas específicas de certificación.
- Aprueba, si procede, este documento la documentación contractual y reguladora de los servicios de certificación en la comunidad de usuarios de EC-ACC, de acuerdo con el procedimiento previsto en esta Declaración de Prácticas de Certificación.
- Informa puntualmente al Consorci AOC de todas las informaciones relativas a los cambios a realizar, incidencias en el servicio, reclamaciones, denuncias e inspecciones del servicio.
- Garantiza, bajo su plena responsabilidad, que cumple con todos los requisitos establecidos en esta DPC.
- Es la única entidad responsable del cumplimiento de los procedimientos descritos en esta DPC, incluso cuando una parte o la totalidad de las operaciones sean subcontratadas externamente.
- Presta sus servicios de certificación de acuerdo con esta DPC, donde se detallan, al menos, los contenidos previstos en la legislación aplicable, descrita a 9.15
- De conformidad con la ley aplicable, antes de la emisión y entrega del certificado, EC-ACC informa de los aspectos previstos a la legislación aplicable, así como de los siguientes aspectos:
    - Indicación de la política aplicable, con indicación que los certificados no se expiden al público y la necesidad de utilización de dispositivo cualificado de creación de firma.
    - Forma en que se garantiza la responsabilidad patrimonial de EC-ACC.
    - EC-ACC se declara de acuerdo con la política de certificación, la certificación del Prestador de servicios de certificación y la certificación de los productos de firma electrónica utilizados.

  Este requisito se cumple mediante un “Texto divulgativo de la política de certificado” aplicable que se transmite electrónicamente utilizando un medio de comunicación duradero en el tiempo y en lenguaje comprensible.
- EC-ACC obliga a los suscriptores, poseedores de claves y a los verificadores mediante instrumentos jurídicos apropiados en cada situación, los cuales se transmiten electrónicamente, en lenguaje escrito y comprensible, a tener en cuenta los contenidos mínimos siguientes:
    - Prescripciones para dar cumplimiento a lo establecido en esta DPC.

- Indicación de la política aplicable, con indicación de si los certificados se expiden al público y de la necesidad de uso del dispositivo cualificado de creación de firma.
- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para la publicación del certificado al directorio y acceso por terceros al mismo.
- Consentimiento para el almacenamiento de la información utilizada para el registro del suscriptor y del poseedor de claves, para la provisión del dispositivo cualificado de creación de firma y para la cesión de la mencionada información en terceros, en caso de final de operaciones de la EC-ACC sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo los establecidos en la sección 4.5 de esta DPC.
- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como verificador.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales EC-ACC acepta o excluye su responsabilidad.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.

EC-ACC identifica al poseedor de claves, de acuerdo con la legislación aplicable y esta DPC. Especialmente, EC-ACC, comprueba por sí misma la identidad y otras circunstancias personales de los solicitantes de los certificados.

9.6.1.2. Garantías ofrecidas

9.6.1.2.1. Garantías ofrecidas a los suscriptores

EC-ACC garantiza al suscriptor, como mínimo:

El cumplimiento de sus obligaciones legales como Prestador de servicios de certificación, de acuerdo con la legislación aplicable.

Que no hay errores en las informaciones contenidas a los certificados, conocidos o realizados por esta, ni debidos a la carencia de diligencia en la gestión de la solicitud de certificado o en la creación de este.

Que los certificados cumplen todos los requisitos materiales establecidos en la DPC.

Que los servicios de revocación y el uso del directorio cumplen todos los requisitos materiales establecidos en la DPC.

a) Que, en caso de que haya generado las claves privadas, se mantiene la confidencialidad durante el proceso.
b) La responsabilidad de EC-ACC, con los límites que se establezcan.

9.6.1.2.2. Garantías ofrecidas a los verificadores

EC-ACC garantiza al verificador, como mínimo:

a. El cumplimiento de sus obligaciones legales como Prestador de servicios de certificación, de acuerdo con la legislación aplicable.

b. Que la información contenida o incorporada por referencia al certificado es correcta, excepto cuando indique expresamente el contrario.

c. En caso de certificados publicados al directorio, que el certificado ha sido emitido al suscriptor identificado en este y que el certificado ha sido aceptado, de acuerdo con la sección 4.4 de esta DPC.

d. Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en esta DPC.

e. La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y de directorio.

f. Que los certificados cumplan todos los requisitos materiales establecidos en esta DPC.

g. Que, en caso de que haya generado las claves privadas, se mantiene la confidencialidad durante el proceso.

h. Que los servicios de revocación y el uso del directorio cumplen todos los requisitos materiales establecidos en esta DPC.

La responsabilidad de EC-ACC, con los límites que se establezcan.

9.6.2.Entidades de Registro

9.6.2.1. Obligaciones y otros compromisos

La Entidad de Registro se obliga a cumplir lo siguiente:

a. Actúa exclusivamente en relación con personas vinculadas a la Entidad de Registro.

b. Nombra como operador de la autoridad de registro, a uno o más de sus trabajadores, y comunica al Consorci AOC los datos correspondientes a estas personas para la emisión de los certificados de operador correspondiente. Cuando un operador deja de tener capacidad para actuar como el que es, bajo el control y la autoridad de la Entidad de Registro, esta Entidad solicita de forma inmediata a la EC-ACC la revocación del certificado de operador correspondiente.

c. Valida y aprueba las solicitudes de certificados y, a continuación, genera las tarjetas para los poseedores de claves, de acuerdo con los procedimientos e instrumentos técnicos establecidos por EC-ACC, de acuerdo con esta DPC y su documentación de operaciones.

d. Si la Entidad de Registro Interna no dispone de información actualizada del poseedor de claves, comprueba la identidad personalmente o de acuerdo con el establecido a la legislación aplicable, registra un justificante acreditativo del nombre completo, lugar y fecha de nacimiento, DNI y/o cualquier otra información que pueda ser utilizada para diferenciar una persona respecto de otra en el ámbito de la Entidad de Registro Interna.

e. Verifica, cuando sea necesario, cualquier atributo específico del poseedor de claves, y registra un justificante acreditativo de la información.
Realiza o tramita las solicitudes de suspensión, reactivación, revocación y renovación de certificados, de acuerdo con los procedimientos y los instrumentos técnicos establecidos por el EC-ACC, de acuerdo con esta DPC, y su documentación de operaciones.

f. Almacena los registros, ya sea en papel o de forma electrónica, con las medidas adecuadas de seguridad, autenticidad, integridad y conservación, relativas a la información contenida al certificado, durante un periodo de 15 años. Estos registros están a disposición delEC-ACC.

9.6.3. Suscriptores

9.6.3.1. Obligaciones y otros compromisos

9.6.3.1.1. Requisitos para todos los tipos de certificados

EC-ACC obliga al suscriptor de los certificados a:

a. Facilitar a EC-ACC la información completa y adecuada conforme a los requisitos de esta DPC, en especial, en aquello en lo referente al procedimiento de registro.

b. Manifestar su consentimiento previo a la emisión y entrega de un certificado.

c. Cumplir las obligaciones que se establecen para el suscriptor en esta DPC y a la legislación vigente descrita a la sección 9.15 de esta DPC.

d. Utilizar el certificado de acuerdo con el establecido a la sección 1.4 de esta DPC.

e. Notificar a EC-ACC, sin retrasos injustificables, la pérdida, la alteración, el uso no autorizado, el robo o el compromiso de su dispositivo cualificado de creación de firma.

f. Notificar a EC-ACC y a cualquier persona que el suscriptor crea que pueda confiar en el certificado sin retrasos injustificables:

    a La pérdida, el robo o el compromiso potencial de su clave privada.

    b La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN del dispositivo cualificado de creación de firma) o por cualquier otra causa.

    c Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.

g. Dejar de utilizar la clave privada una vez transcurrido el periodo indicado a la sección correspondiente.

h. Transferir a los poseedores de claves las obligaciones específicas de estos.

i. No monitoritzar, manipular o realizar actas de ingeniería reversa sobre la implantación técnica de la Jerarquía de la Agencia Catalana de Certificación sin permiso previo por escrito.

j. No comprometer intencionadamente la seguridad de la Jerarquía de la Agencia Catalana de Certificación.

9.6.3.2. Garantías ofrecidas por el suscriptor

EC-ACC obliga, mediante el correspondiente instrumento jurídico, al suscriptor a garantizar que:

a. Todas las manifestaciones realizadas a la solicitud son correctas.
b. Todas las informaciones suministradas por el suscriptor que se encuentren contenidas al certificado son correctos.
c. El certificado se utiliza exclusivamente para usos legales y autorizados, de acuerdo con esta DPC.
d. Cada firma digital creada con la clave privada correspondiente a la clave pública listada al certificado es la firma digital del suscriptor y que el certificado ha sido aceptado y se encuentra operativo (no ha expirado ni ha sido revocado) en el momento de creación de la firma.
e. El suscriptor es una entidad final y no una Entidad de Certificación y no utiliza la clave privada correspondiente a la clave pública listada al certificado para firmar ningún certificado (o cualquiera otro formato de clave pública certificada) ni LRC.
f. Ninguna persona no autorizada no ha tenido nunca acceso a la clave privada del suscriptor.

9.6.3.3. Protección de la clave privada

EC-ACC se obliga, mediante el correspondiente instrumento jurídico, a garantizar que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.

9.6.4. Verificadores

9.6.4.1. Obligaciones y otros compromisos

EC-ACC obliga al usuario de certificados a:

a. Asesorarse sobre el hecho que el certificado es apropiado para el uso que se pretende.
b. Verificar la validez, suspensión o revocación de los certificados emitidos, para lo cual utilizará información sobre el estado de los certificados.
c. Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía.
d. Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el mismo certificado o en el contrato de verificador.
e. Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
f. No monitoritzar, manipular o realizar actas de ingeniería inversa sobre la implantación técnica de la jerarquía pública de certificación de Cataluña, sin permiso previo por escrito.
g. No comprometer intencionadamente la seguridad de la jerarquía pública de certificación de Cataluña.

h. Reconocer que las firmas electrónicas producidas por certificados cualificados de firma cualificada son firmas electrónicas equivalentes a firmas escritas, de acuerdo con el artículo 3.4 de la Ley 59/2003, de 19 de diciembre.

9.6.4.2. Garantías ofrecidas para el verificador

EC-ACC obliga al verificador, mediante el correspondiente instrumento jurídico, a manifestar que:

a. Dispone de suficiente información para tomar una decisión informada para confiar o no en el certificado.

b. Es el único responsable de confiar o no en la información contenida al certificado.

c. Será el único responsable si incumple sus obligaciones como verificador.

9.6.5. Consorci AOC

9.6.5.1. Obligaciones y compromisos

El Consorci AOC tiene las obligaciones siguientes:

a. Operar EC-ACC, Entidad de certificación raíz de la jerarquía pública de certificación de Cataluña, de manera diligente, en conformidad con las políticas, prácticas y normativa de la mencionada jerarquía.

b. Operar sus Entidades de Certificación Vinculadas, propias o que presten servicios a las Entidades de Certificación Virtuales, de acuerdo con aquello que se dispone a la Política General de Certificación.

c. Garantizar la equivalencia de la seguridad de la operación de las Entidades de Certificación Vinculadas de terceros Prestadores de servicios de certificación y, especialmente, velar porque estos cumplan con las obligaciones previstas a la Política General de Certificación.

9.6.5.2. Garantías ofrecidas a los suscriptores

El Consorci AOC garantiza que la clave privada de EC-ACC no ha sido comprometida, salvo que así lo indique expresamente mediante el directorio del Consorci AOC.

El Consorci AOC únicamente garantiza:

a. Que los certificados contienen toda la información exigida por la legislación aplicable, descrita en la sección 9.15 de esta DPC. Que no ha originado ni introducido declaraciones falsas o erróneas en la información de los certificados, ni tampoco ha dejado de incluir información necesaria aportada por EC-ACC y validada por el Consorci AOC o la Entidad de Registro, en el momento de emisión de los certificados.

b. Que todos los certificados emitidos cumplen los requisitos formales y de contenido.

El Consorci AOC está vinculada a los procedimientos operativos y de seguridad descritos en esta DPC.

9.6.5.3. Garantías ofrecidas a los verificadores

La responsabilidad del Consorci AOC, que deriva de una relación indirecta, es la prevista en la legislación aplicable, descrita a la sección 9.15 de esta DPC.

9.6.5.4. Exclusión de garantías

El Consorci AOC no garantiza ningún software utilizado por el suscriptor o por cualquier otra persona, para generar, verificar o no utilizar de forma diferente ninguna firma digital o certificado digital emitido por el Consorco AOC, a excepción de los casos en que haya una declaración escrita del Consorci AOC en sentido contrario.

9.6.6. Directorio

9.6.6.1. Obligaciones y compromisos

EC-ACC puede delegar algunas funciones al directorio, que en este caso está obligado a su cumplimiento, en iguales condiciones que esta.

Las funciones, obligaciones y deberes del directorio se establecen en detalle en esta DPC, así como en la documentación jurídica auxiliar, especialmente la entregada a suscriptores, poseedores de claves y verificadores.

9.6.6.2. Garantías

EC-ACC establece en esta DPC la responsabilidad civil del directorio cuando sea operado por una tercera entidad.

9.7. Renuncias de garantías

9.7.1. Rechazo de garantías de EC-ACC

EC-ACC puede rechazar todas las garantías del servicio que no se encuentren vinculadas a obligaciones establecidas por la legislación aplicable, descrita a la sección 9.15 de esta DPC , incluyendo especialmente la garantía de adaptación para un propósito particular o garantía de uso mercantil del certificado.

9.8. Limitaciones de responsabilidad

9.8.1. Limitaciones de responsabilidad de EC-ACC

EC-ACC limita su responsabilidad restringiendo el servicio a la emisión y gestión de certificados y, en su caso, de pares de claves de suscriptores y depósitos criptográficos (de firma y verificación de firma, así como de cifrado o descifrado) suministrados por esta.

EC-ACC puede limitar su responsabilidad mediante la inclusión de límites de uso del certificado límites de valor de las transacciones para las cuales se puede utilizar el certificado.

9.8.2. Caso fortuito y fuerza mayor

EC-ACC incluye cláusulas para limitar su responsabilidad en caso fortuito y en caso de fuerza mayor, a los instrumentos jurídicos con que vincule suscriptores y verificadores.

9.9. Indemnizaciones

9.9.1. Cláusula de indemnización de suscriptor

No se establecerá cláusula de indemnización del suscriptor.

9.9.2. Cláusula de indemnidad de verificador

No se establecerá cláusula de indemnización del verificador.

9.10. Plazo y finalización

9.10.1. Plazo

EC-ACC establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, una cláusula que determina el periodo de vigencia de la relación jurídica en virtud de la cual suministra certificados a los suscriptores.

9.10.2. Finalización

EC-ACC establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, una cláusula que determina el periodo de vigencia de la relación jurídica en virtud de la cual suministra certificados a los suscriptores.

9.10.3. Supervivencia

EC-ACC establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, cláusulas de supervivencia, en virtud de las cual ciertas reglas continúan vigentes después de la finalización de la relación jurídica reguladora del servicio entre las partes.

A tal efecto, EC-ACC vela porque, al menos los requisitos contenidos a las secciones Obligaciones, Responsabilidad civil, Auditoría de conformidad y Confidencialidad, continúen vigentes después de la finalización de la política de certificación y de los instrumentos jurídicos que vinculen EC-ACC con suscriptores y verificadores.

El Consorci AOC determinará un Plan de Continuidad de Negocio. Este Plan de Continuidad de Negocio establecerá las obligaciones que asume el Consorci AOC en caso de cese de actividades, dirigidas a mantener en vigencia los certificados emitidos hasta su expiración y el uso y custodia de toda la información generada por el Consorci AOC en su actividad de Prestador de servicios de certificación, como por ejemplo, las copias de seguridad, logs y documentos de todo tipos, independientemente del apoyo en que hayan sido generados o almacenados. A tal efecto, el Consorci AOC se asegura que se genera

una copia de seguridad con periodicidad, como previsión complementaria de la actividad corriente e igualmente del aseguramiento de la continuidad de negocio.

9.11. Notificaciones

EC-ACC establece, en sus instrumentos jurídicos vinculantes con suscriptores y verificadores, cláusulas de notificación, en las cuales se establece el procedimiento por el cual las partes se notifican hechos mutuamente.

9.12. Modificaciones

9.12.1. Procedimiento para las modificaciones

EC-ACC puede modificar, de forma unilateral, esta DPC, siempre que proceda según el procedimiento siguiente:

- La modificación tiene que estar justificada desde el punto de vista técnico, legal o comercial.
- La modificación propuesta por EC-ACC no puede ir en contra de la política de certificación establecida por el Consorci AOC.
- Se establece un control de modificaciones para garantizar, en todo caso, que las especificaciones resultantes cumplen los requisitos que se intentan cumplir y que dieron pie al cambio.
- Se establecen las implicaciones que el cambio de especificaciones tiene sobre el usuario, y se prevé la necesidad de notificarle las mencionadas modificaciones.
- La nueva política tiene que ser aprobada por el Consorci AOC.

9.12.2. Periodo y mecanismos para notificaciones

Las modificaciones de esta DPC se notifican al Consorci AOC, para su posterior aprobación.

9.12.3. Circunstancias en les cuales un OID se ha de cambiar

Sin estipulación adicional.

9.13. Resolución de conflictos

9.13.1. Resolución extrajudicial de conflictos

EC-ACC establece, en sus instrumentos jurídicos con suscriptores y verificadores, los procedimientos de mediación y resolución de conflictos aplicables.

Con cuyo objeto, se tiene en cuenta la consideración como Administración Pública de EC-ACC.

Las situaciones de discrepancia que se deriven del uso de los certificados emitidos por EC-ACC se resuelven aplicando los mismos criterios de competencia que en los casos de los documentos firmados por escrito.

9.13.2. Jurisdicción competente

EC-ACC establece, en sus instrumentos jurídicos vinculantes con suscriptores y verificadores, una cláusula de jurisdicción competente, que indica que la competencia judicial internacional corresponde a los jueces españoles.

La competencia territorial y funcional se determina en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

Así mismo, se tiene en cuenta la legislación administrativa que resulte aplicable.

9.14. Ley aplicable

EC-ACC establece, en sus instrumentos jurídicos con suscriptores y verificadores, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación es la siguiente:

- En general, la ley española, siempre y cuando EC-ACC continúe establecida en el Estado Español, y/o sus servicios de certificación se presten por medio de un establecimiento permanente situado al Sido Espanyol.
- Y la normativa administrativa correspondiente, estatal y autonómica.

9.15. Conformidad con la ley aplicable

Conforme a aquello establecido a la Política General de Certificación.

9.16. Cláusulas diversas

9.16.1. Acuerdo íntegro

EC-ACC establece, en sus instrumentos jurídicos vinculantes con suscriptores y verificadores, cláusulas de acuerdo íntegro, en virtud de las cuales se entiende que el instrumento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.

9.16.2. Subrogación

Los derechos y los deberes asociados a la condición de Entidad de Certificación no pueden ser objeto de cesión a terceros de ningún tipo, ni ninguna tercera entidad se puede subrogar en la posición jurídica de una Entidad de Certificación.

En caso de que se produzca una cesión o subrogación, se procede a la finalización de la mencionada Entidad de Certificación.

9.16.3. Divisibilidad

EC-ACC establece cláusulas de divisibilidad, en sus instrumentos jurídicos vinculantes con suscriptores y verificadores, en virtud de las cuales la invalidez de una cláusula no afecta el resto del contrato.

Dado el caso que, como causa a los artículos 7 y 8 de la Ley 7/1998 sobre condiciones generales de la contratación, se considerarán no incorporadas al contrato, o nulas algunas o cualquiera de las cláusulas indicadas, la referida no incorporación o nulidad no determina la ineficacia total del contrato, si este pudiera subsistir sin las cláusulas indicadas.

9.16.4. Aplicaciones

Sin estipulación adicional.

9.16.5. Otras cláusulas

Sin estipulación adicional.

10. ANEXO – Control documental

Proyecto:	**Informe modificación del documento DPC EC-ACC**
Entidad de destino:	**Consorci AOC**
Código de referencia:	**Revisión 1er semestre 2018**
Versión:	**3.0**
Fecha de la edición:	**09/05/2018**

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
2.0	Todas	Revisión global - Integración de CATCert al Consorci AOC	Servicio de Certificación Digital -Consorci AOC	05/08/2016
3.0	Todas	Revisión global, cumplimiento eIDAS.	Servicio de Certificación Digital -Consorci AOC	09/05/2018