Consorci
Administració Oberta
de Catalunya

Declaración de Prácticas de Certificación
Entidad de CertificaciónIdCAT
(EC-IDCAT)

Referencia:	D1111_E0650_N-DPC EC-IDCAT
Versión:	4.0
Fecha:	05/08/2016

Control documental

Estado formal	**Elaborat per:** Servei de Certificació Digital	**Aprovat per:** Direcció del Consorci AOC
Fecha de creación	26/09/2006	
Control de versiones	**Fecha:**	05/08/2016
	Descripción:	Revisión Global – Integración CATCert en Consorci AOC
Nivel de acceso información	pública	
Título	Declaración de Prácticas de Certificación – Entidad de CertificaciónIdCAT	
Fichero	D111 E0650 N-DPC EC-IDCATv4r0 CAS	
Control de copias	Sólo las copias disponibles en https://www.aoc.cat/ garantizan la actualización de los documentos. Toda copia impresa o guardada en ubicaciones diferentes se considerarán copias no controladas.	
Derechos de Autor	 	

Índice

1. Introducción

Este documento es la Declaración de Prácticas de Certificación de la Entidad de Certificación 'IdCAT' (en adelante EC-IDCAT, Entidad de Certificación Raíz de la jerarquía pública de certificación de Catalunya.

En esta DPC se regulan técnicamente y operativamente los servicios de certificación de la EC-IDCAT.

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

1.1 Presentación

En desarrollo del 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 la comunicación en el ámbito de las administraciones públicas catalanas, se decidió establecer sistemas de interrelación entre dichas 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 de dicho pacto institucional y para desarrollar el programa Catalunya en Xarxa (Cataluña en Red), Localret y la Generalitat de Catalunya acordaron la creación del Consorci per a l'Administració Oberta Electrònica de Catalunya (Consorcio para la Administración Abierta Electrónica de Catalunya), con la finalidad 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 de 2002 tuvo lugar la sesión constitutiva del Consorci per a l'Administració Oberta Electrònica de Catalunya, una sesión en que el Consejo General adoptó, entre otros, el acuerdo de constituir un ente de gestión directa bajo la forma de organismo autónomo de carácter comercial, con la denominación de Agència Catalana de Certificació (CATCert), con el objeto 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 Electrónica de Catalunya, de 29 de abril de 2002, como organismo autónomo de carácter comercial, los estatutos de la cual fueron publicados en el Diario Oficial de la Generalitat de Catalunya el 30 de mayo de 2003, por Resolución PRE/1574/2003, de 15 de mayo.

Por tanto, la Agencia Catalana de Certificació se constituyó en la entidad principal del sistema público catalán de certificación que regulaba la emisión y la gestión de los certificados que se emitieranpara las instituciones de autogobierno de Catalunya, 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 solicitaran la correspondiente clasificación.

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

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

L’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 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-Ciutadania

La EC-IDCAT es la Entidad de Certificación Vinculada a la jerarquía pública de certificación de Catalunya encargada de emitir certificados a los ciudadanos catalanes que necesitan relacionarse con las administraciones y otras instituciones.

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 Agència Catalana de Certificació 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 meidante el citado 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 Catalunya y el propietario de la infraestructura de clave pública (PKI) que antes era titularidad de CATCert.

1.1.1 Tipos y clases de certificados

El Consorci AOCha definido una tipología de servicios de certificación que le permitenemitir certificados digitales para diversos usos y usuarios finales diferentes.

La EC-idCAT emite certificados idCAT, que son certificados reconocidos de identificación y firma electrónica avanzada, destinados a ciudadanos y ciudadanas catalanas mayores de edad, así como a otras personas (colectivamente llamados suscriptores) que necesiten relacionarse con las Administraciones públicas y otras instituciones.

El certificado idCAT es un certificado reconocido de acuerdo con lo establecido en el artículo 11.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, con el contenido prescrito por el artículo 11.2, y emitido cumpliendo las obligaciones de los artículos 12, 13, 18 y 20 de la mencionada Ley.

El procedimiento de validación de la identidad requiere la comparecencia personal de la persona física que obtiene el certificado ante una oficina de registro colaboradora del Consorci AOC.

1.1.2 Relación entre la Declaración de prácticas de certificación y otros documentos

Este documento contiene la declaración de prácticas de certificación de la EC-idCAT.

La EC-idCAT emite certificados dentro de la Jerarquía del Consorci AOC. Por tanto tiene que disponer de una declaración de prácticas de certificación, de acuerdo con la Política General de Certificación del Consorci AOC.

Esta Declaración de Prácticas de Certificación (DPC) incluye los procedimientos que el Consorci AOC y las entidades que colaboran aplican en la prestación de sus servicios, en cumplimiento de los requisitos establecidos por las políticas que gestiona y el artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

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 la EC-IDCAT”.

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

1.3.6.1.4.1.15096.1.2.6

1.2.2. Identificación de políticas de certificación cubiertas por esta DPC

El Consorci AOC ha definido y aprobado la siguiente especificación de política para los certificados idCAT:

CIPISR – Certificado de infraestructura de operador, emitido por la EC-IdCAT

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

CIC – Certificado de infraestructura de Entidad de Certificación Vinculada, emitido por la EC-IdCAT

CIC-1. OID: 1.3.6.1.4.1.15096.1.3.1.11

CIC-2. OID: 1.3.6.1.4.1.15096.1.3.1.12

CIC-3. OID: 1.3.6.1.4.1.15096.1.3.1.13

CIDS-1 – Certificado de infraestructura de servidor seguro, emitido por la EC-IdCAT

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.17

CIDA-1 – Certificado de infraestructura de aplicación, emitido por la EC-IdCAT

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.18

CIO-1 – Certificado de infraestructura de servidor de estado de certificados en línea, emitido por la EC-IdCAT

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.19

CIV-1 – Certificado de infraestructura de entidad de validación, emitido por la EC-IdCAT

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.20

CIT-1– Certificado de infraestructura de entidad de sellos de tiempo, emitido por la EC-AL

Clase 1. 1.3.6.1.4.1.15096.1.3.1.111

idCAT basado en certificado CPIXSA – Certificado de persona física de identificación, cifrado y firma electrónica avanzada

Clase 2. OID: 1.3.6.1.4.1.15096.1.3.1.86.1

idCAT-CEX basado en certificado CPIXSA - Certificado de persona física de nacionalidad extranjera de identificación, cifrado y firma electrónica avanzada

Clase 2. OID: 1.3.6.1.4.1.15096.1.3.1.86.2

idCAT-T basado en certificado CPIXSA - Certificado de persona física ciutadano de identificación, cifrado y firma electrónica avanzada, con soporte tarjeta o token

Clase 2. OID: 1.3.6.1.4.1.15096.1.3.1.86.3

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

1.3. Comunidad de usuarios de certificados

Esta declaración de prácticas de certificación regula una comunidad de usuarios, que obtienen certificados para diversas relaciones administrativas y privadas, de acuerdo con la Ley 59/2003 y la normativa administrativa correspondiente.

Los certificados idCAT siempre se emiten al público.

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 Ley 59/2003, de 19 de diciembre, de firma electrónica.

El Consorci AOC será el prestador de servicios de certificación de la EC-IDCAT.

En su función de prestador de servicios de certificación,el Consorci AOC será responsable dela actuación de la EC-IDCAT 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

El Consorci AOC dispone de una autoridad de certificación principal, que es la raíz de la jerarquía pública de certificación de Cataluña: la , cuya finalidad es integrar otras entidades de certificación en el sistema público catalán de certificación mediante la vinculación técnica de las autoridades de certificación correspondientes.
La citada vinculación técnica se consigue mediante la emisión de certificados de infraestructura de entidad de certificación vinculada (CIC).

1.3.3 EC-idCAT

La EC-idCAT es la Entidad de Certificación habilitada para emitir certificados a los ciudadanos de Catalunya, vinculada a la jerarquía de certificación de las entidades públicas de Catalunya, que emite los certificados indicados en el punto 1.1.1.1

La huella digital del certificado de la EC-IdCAT es la siguiente:
`50 49 88 bd b7 df e0 dd a8 eb f6 98 e0 b5 c4 65 02 fb 41 fc`

1.3.4 Entidades de Registro

Son Entidades de Registro para certificados idCAT, todas aquellas entidades que se hayan adherido a las Condiciones Generales del Servicio de Certificación Digital del Consorci AOC.

El proceso de creación de entidades de registro es responsabilidad del administrador de la Entidad de Certificación. Mediante convenio entre la Institución y Consorci AOC se constituye la entidad de registro. El Consorci AOC verifica que la Entidad de Registro cuenta con los recursos materiales y humanos necesarios, y de la designación del personal responsable. Asimismo, es responsable, en todo caso, de la formación del personal que emita los certificados como operadores de la entidad de registro y, a tal efecto, de la emisión de los certificados de operador correspondientes (típicamente, CIPISR). El Consorci AOC validará las peticiones de certificados de las Entidades de Registro examinando la solicitud y haciendo las comprobaciones necesarias para el cumplimiento de la Política General de Certificación y de la Declaración de Prácticas de Certificación.

.

1.3.5 Usuarios finales

Los usuarios finales son las personas (físicas o jurídicas) que obtienen y utilizan los certificados dispositivo emitidos por la EC-IDCAT;concretamente, podemos distinguir los siguientes usuarios finales:

- Los solicitantes de certificados
- Los suscriptores de certificados o los titulares de certificados
- Los verificadores de firmas y de los certificados

1.3.5.1 Solicitantes de certificados

Los certificados idCAT son solicitados por personas mayores de edad, en su propio nombre.

Pueden ser socilitantes:

a) La persona que será el futuro suscriptor

b) Una persona autorizada por el futuro suscriptor (representante)

La autorización se debe realizar de forma expresa mediante documento público.

1.3.5.2 Suscriptores de certificados

Los suscriptores son las instituciones y las personas, físicas o jurídicas, así identificadas en el campo “Subject” del certificado.

El suscriptor tiene licencia de uso del certificado.

1.3.5.3 Usuarios de certificados

Los usuarios de los certificados son los verificadores.

1.3.5.4 Verificadores de certificados

Los verificadores son las personas físicas y jurídicas que reciben firmas electrónicas y certificados digitales y tienen que verificarlos, como paso previo a confiar.

1.4. Uso de los certificados

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

1.4.1 Usos típicos de los certificados

Los certificados idCAT de firma avanzada son certificados reconocidos de acuerdo con lo que se establece en el artículo 11.1, con el contenido prescrito por el artículo 11.2, y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y que dan cumplimiento a aquello dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Los certificados idCAT no funcionan necesariamente con dispositivos seguros de creación de firma electrónica de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Los certificados idCAT garantizan la identidad del suscriptor resultando idóneos para ofrecer soporte a la firma electrónica avanzada.

Aunque la firma electrónica avanzada no se equipara directamente a la firma escrita, esta equiparación se puede producir igualmente en virtud de un contrato de firma electrónica o de una norma jurídica específica (por ejemplo la “ORDEN HAC/1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria”), que establecerá las condiciones adicionales necesarias para que se produzca dicha equiparación.

Además se pueden utilizar para diversos usos, entre los que se pueden indicar los siguientes:

- Identificación distribuida, basada en presentación de la credencial
- Autenticación en sistemas de control de acceso, de sistema operativo o centralizados.

Los certificados idCAT tienen la posibilidad de recibir mensajes de datos confidenciales, en cualquier formato, protegidos mediante el cifrado del texto del mensaje, por parte del remitente del mensaje, utilizando la clave pública del suscriptor indicada en el certificado.

El suscriptor utilizará su clave privada para descifrar el mensaje o documento.

1.4.2 Aplicaciones prohibidas

Los certificados idCAT (excepción hecha del CIPISR) no pueden utilizarse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC), ni para realizar ningún tipo de transacciones económicas.

Los certificados idCAT 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 requieran 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 pudiera directamente comportar la muerte, lesiones personales o daños medioambientales severos.

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 organización

Consorci Administració Oberta de Catalunya – Consorci AOC

Domicili social: Via Laietana, 26 – 08003 Barcelona

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

Web del Consorci AOC: www.aoc.cat

Web del servicio de certificación digitaldel 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 el/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-IDCAT 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 fallo del sistema fuera de control de la EC-IDCAT, ésta realiza sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 5.7.4 de la presente DPC.

2.2. Publicación de información de la EC-IDCAT

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

a) Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.

b) La política general de certificación y, cuando sea conveniente, las políticas específicas.

c) Los perfiles de los certificados y de las listas de revocación de los certificados.

d) La Declaración de Prácticas de Certificación.

e) Los instrumentos jurídicos vinculantes con suscriptores y verificadores.

Todo cambio en las especificaciones o condiciones del servicio se comunica a los usuarios por la EC-IDCAT, 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-IDCAT 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 lo establecido en la sección 9.12.1.

Al cabo de 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 la EC-IDCAT, pudiendo ser consultadas por los interesados.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en la sección 4.10.7.

2.4. Control de acceso

Sin estipulación adicional.

3. Identificación y autenticación

3.1. Gestión de nombres

En esta sección se establecen requisitos relativos a 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. Tipos de nombres

3.1.1.1 Estructura sintáctica

Sin estipulación adicional.

3.1.1.2 Perfils dels certificats

Els perfils dels certificats emesos per l'EC-IDCAT es publiquen al 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

No se pueden usar pseudónimos para identificar a una organización.

3.1.4. Interpretación de formatos de nombres

Sin estipulación adicional.

3.1.5. Unicidad de los nombres

Sin estipulación adicional.

3.1.6. Resolución de conflictos relativos a nombres

Sin estipulación adicional.

Referente al tratamiento de marcas registradas, ver el apartado **Error! No s'ha trobat l'origen de la referència.**.

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

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

Para acreditar la identidad del suscriptor, éste se personará en una Entidad de Registro a su elección que puede ser la más cercana a su domicilio.

Recordemos que en el anterior paso de la solicitud del certificado, la web ofrece al solicitante la posibilidad de buscar la Entidad de Registro por provincia, comarca o población.

La acreditación de la identidad puede realizarse directamente ante las Entidades de Registro, en el que el solicitante consigna los datos directamente a los operadores, que los contrastan con los documentos originales aportados (DNI, NIE, pasaporte). Una vez recogidos los datos se procede a emitir el certificado.

El solicitante también puede consignar los datos de identidad en la web del Consorci AOC. Seguidamente, el solicitante se persona ante la Entidad de Registro que elige. Una vez el solicitante se encuentre en las dependencias de la Entidad de Registro se presenta con el documento que lo identifica y que ha indicado en la solicitud (DNI, NIF, NIE o pasaporte, dependiendo del caso), con una fotocopia de dicho documento, y si así lo desea una copia impresa del formulario de confirmación de datos que le muestra la web justo al final del proceso de solicitud.

El encargado de recibir dicha documentación en la Entidad de Registro, comprueba visualmente que la fotografía del documento que identifica al solicitante sea exactamente la correspondiente al suscriptor y la mayoría de edad.

Seguidamente imprime el documento de comparecencia con los datos de la solicitud del certificado para que el solicitante lo firme.

El encargado comprueba también que la firma que el suscriptor acaba de realizar en la solicitud de certificado corresponda a la firma que se haya en el documento que lo identifica.

Hechas todas estas comprobaciones se valida la solicitud en el sistema informático enviándolo electrónicamente y de forma segura a la EC-idCAT.

Todos los documentos que aporte el suscriptor tienen que estar en vigor. En su caso, deberá aportar el resguardo de renovación. Si éste no contiene fotografía podrá completarse la verificación de la identidad utilizando el documento caducado.

3.2.2.1 Necesidad de presencia personal

La identificación de la persona física que obtiene un certificado idCAT puede realizarse

- Mediante su presencia ante los encargados de verificar su identidad.

- Se puede prescindir de la presencia si la firma contenida en la solicitud de expedición de un certificado ha sido legitimada notarialmente, y en los casos previstos por el artículo 13.4 de la Ley 59/2003, de 19 de diciembre.
- Mediante el procedimiento que establece la normativa administrativa, cuando la presencia se realice ante las Administraciones Públicas.

3.2.2.2 Informaciones adicionales para suscriptores de nacionalidad española

El suscriptor se identifica obligatoriamente con su tarjeta de residencia o documento NIE (ciudadanos comunitarios y de otros estados, exentos de la tarjeta de residènciaDocumento Nacional de Identidad.

3.2.2.3 Informaciones adicionales para suscriptores de nacionalidad no española residentes en Catalunya

El suscriptor se identifica obligatoriamente con su DNI, su tarjeta de residencia o documento NIE (ciudadanos comunitarios y de otros estados, exentos de la tarjeta de residencia).

3.2.3. Información no verificada

Los certificados incluyen información no verificada, como la dirección de correo electrónico.

3.3. Identificación y autenticación de solicitudes de renovación

3.3.1. Validación para la renovación de certificados

El sistema de certificación comunica al suscriptor la fecha de la finalización de la vigencia del certificado con una antelación de 60 días y en caso de no haber tramitado la renovación, también con una antelación de 30 días.

La renovación se inicia cuando el suscriptor del certificado, todavía en vigor, solicita la renovación siguiendo la ruta indicada en el mensaje electrónico.

En el caso en que en el momento de la renovación no hayan pasado 5 años respecto de la última identificación del ciudadano en una Entidad de Registro, el suscriptor no se tiene que personar ante las entidades de registro. El sistema no permitirá modificar ningún dato respecto a los validados en la primera emisión. Si alguno de estos datos ya no es válido, el suscriptor deberá solicitar una nueva emisión identificándose con el nuevo documento en la Entidad de Registro.

En caso que ya hayan pasado más de 5 años respecto a la última identificación (por ejemplo, en casos de segunda renovación), el suscriptor deberá personarse nuevamente ante la Entidad de Registro, o aportar el acta notarial correspondiente, para proceder a la nueva emisión.

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

La renovación de certificados después de la 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 emsión de certificado

4.1.1 Legitimación para solicitar la emisión

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

Todos aquellos que desean convertirse en suscriptores realizan una solicitud de certificado idCAT, a través de la web http://www.idcat.cat/ o directamente presentándose en las oficinas de cualquiera de las entidades de registro idCAT (Ayuntamientos, Diputaciones, etc.) que ofrecen esta posibilidad, siguiendo los pasos que allí se indican.

4.1.2 Procedimiento de alta; Responsabilidades

La EC-idCAT se asegura que las solicitudes de certificados son completas, precisas y están debidamente autorizadas.

Para realizar la solicitud previa es necesario acceder a la página web de presentación de este servicio (www.idcat.cat), que contiene un menú con los pasos a seguir para realizar la solicitud.

El primer paso de necesaria ejecución es cargar en nuestro sistema informático las claves públicas de la jerarquía pública de certificación.

El siguiente paso consiste en el deber de visualización del texto divulgativo de la política de certificación idCAT y la declaración de intenciones de uso de los datos personales y su protección.

A continuación nos encontramos con el formulario donde introducimos nuestros datos personales y de contacto. Es muy importante rellenar el formulario con los datos exactamente como están escritos en los documentos que nos identifican, para que el operador de la Entidad de Registro que nos atienda pueda comprobar y validar posteriormente dichos datos.

Seguidamente aparece una pantalla con los datos que hemos introducido para que los podamos visualizar y si son correctos, enviarlos a la EC-idCAT activando la casilla correspondientes (típicamente, haciendo clic en el botón “Enviar dades”).

Para terminar nos aparece una pantalla con los datos introducidos donde se nos pide que lo imprimamos para tener una copia escrita de nuestra solicitud y se nos informa de las Entidades de Registro más cercanas al domicilio indicado en la solicitud.

4.2 Procesamiento de la solicitud de certificación

Después que la Entidad de Registro compruebe la identidad del solicitante, verifique la documentación presentada, se envía la solicitud de emisión de certificado a la EC-idCAT y el ciudadano firma el documento de comparecencia correspondiente.

Si alguna de las comprobaciones es errónea, se introducen los cambios, se envía la solicitud a la EC-idCAT y se hace firmar por el solicitante el documento de comparecencia con los datos modificados.

La EC-idCAT recibe la autorización de la Entidad de Registro, recupera la correspondiente solicitud de la tabla de solicitudes, la almacena en la estructura de certificados, la firma, completando así la generación del certificado.

A partir de este momento el solicitante ya puede descargar desde la web su certificado y comenzar a utilizarlo.

Además la EC-idCAT tiene en cuenta los siguientes aspectos:

- Genera los certificados vinculándolos de forma segura con la información que el futuro suscriptor indica en el formulario de registro.
- Protege el secreto y la integridad de los datos de registro.
- Incluye en el certificado las informaciones establecidas en el artículo 11 de la Ley 59/2003, de acuerdo con lo establecido en la sección 7 de este documento.
- Garantiza la fecha y la hora en que se expide un certificado
- Utiliza sistemas y productos fiables que están protegidos contra toda alteración y que garantizan la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Se asegura que el certificado es emitido por sistemas que utilicen protección contra falsificación.

En el caso de certificados emitidos en dispositivos (llaveros, tarjetas criptográficas), la emisión y entrega del certificado se realiza en el acto de personación ante la entidad de registro.

4.3 Emisión de certificado

4.3.1 Acciones de la EC-idCAT durante el proceso de emisión

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

Después de la aprobación de la solicitud de certificación se procede a la emisión del certificado, de forma segura y se pone el certificado a disposición del suscriptor, en el soporte correspondiente.

Los procedimientos establecidos en esta sección también se aplicarán en caso de renovación de certificados, ya que ésta implica la emisión de un nuevo certificado.

La EC-idCAT:

- Utilizar un procedimiento de generación de certificados que vincule de forma segura el certificado con la información de registro, incluyendo la clave pública certificada
- En caso de que la Entidad de Certificación genere el par de claves, utilizar un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves y, que la clave privada es entregada de forma segura al suscriptor, en caso de certificados individuales, o al poseedor de claves en caso de certificados de organización.

- Proteger la confidencialidad e integridad de los datos de registro, especialmente en caso de que sean intercambiados con el suscriptor, en caso de certificados individuales, con el poseedor de claves, en caso de certificados de organización o con el tercer solicitante, en su caso.
- Incluir en el certificado las informaciones establecidas en el artículo 11.2 de la Ley 59/2003, de acuerdo con lo establecido en la sección correspondiente de esta política.
- Indicar la fecha y la hora en las que se expidió un certificado.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garantizan la seguridad técnica y en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Tomar medidas contra la falsificación de certificados y, en caso de que la Entidad de Certificación genere claves privadas, que garanticen el secreto de las claves durante el proceso de generación de estas claves.

4.3.2 Notificación de la emisión al suscriptor

La EC-idCAT comunica por correo electrónico al solicitante, una vez la emisión ha finalizado satisfactoriamente y las instrucciones para iniciar el uso del certificado.

Para que el suscriptor obtenga el certificado idCAT (en caso de emisión en software) debe acceder a la página web que se le indica en el correo electrónico y proceda a descargar el certificado.

4.4 Aceptación del certificado

4.4.1 Responsabilidades del Prestador de Servicios de Certificación

La EC-idCAT proporciona acceso al certificado al suscriptor.

4.4.2 Conducta que constituye aceptación del certificado

El suscriptor acepta el certificado y las condiciones de uso del mismo al firmar el documento emitido por la Entidad de Registro.

En el caso de certificado emitido en dispositivo, el certificado se descarga en la propia oficina de la Entidad de Registro.

4.4.3 Publicación del certificado

La publicación de los certificados idCAT requiere siempre el consentimiento de los suscriptores.

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 los suscriptores

El certificado IdCAT sirve para los ciudadanos catalanes y otras personas físicas mayores de edad que necesiten relacionarse con las Administraciones públicas catalanas, realizando los correspondientes trámites telemáticos entre ambas partes con todas las garantías jurídicas y técnicas recogidas en las normas vigentes

Además puede utilizarse por el suscriptor en sus relaciones telemáticas con otras personas físicas o jurídicas que lo acepten, siempre y cuando su uso no implique una transferencia de valor económico directo o indirecto.

También permite enviar correo electrónico seguro (firmado y cifrado) con otros ciudadanos u organizaciones.

4.5.2 Uso por el tercero que confía en certificados

El certificado IdCAT sirve para uso administrativo (cuando el tercero es una Administración pública) o privado (cuando el tercero no es Administración pública). El tercero verificador que quiera permitir el uso profesional del IdCAT en sus sistemas deberá firmar un convenio específico de extensión del uso del certificado, que permitirá al Consorcio AOC asumir el riesgo correspondiente.

4.6 Renovación de certificado sin renovación de claves

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

4.7 Renovación de certificado con renovación de claves

Cuando se solicite la renovación de un certificado con renovación del par de claves, el ciudadano solo podrá renovarlo de forma no presencial en caso que no hayan transcurrido 5 años desde la última identificación de la Entidad de Registro y además, los datos asociados al certificado no podrán ser modificados, de la forma como se especifica en la sección correspondiente de esta política.

Si las condiciones jurídicas de prestación del servicio han variado desde la emisión del certificado, será necesario que la Entidad de Certificación o bien, la Entidad de Registro tengan que informar de este hecho al solicitante.

La renovación de un certificado se inicia 60 días antes de la fecha de expiración del certificado, cuando el suscriptor recibe un correo electrónico donde se le informa de los pasos a seguir para ejecutar la renovación del certificado. Este correo se vuelve a enviar 30 días antes de la expiración, en caso que el suscriptor no haya solicitado aún la nueva emisión.

4.8 Modificación de certificados

El subscriptor solamente puede modificar los datos de contacto asociados al certificado pero no los datos identificativos del mismo. Para poder cambiar los datos de contacto, es

necesario solicitarlo a través de la web www.idcat.cat, seleccionando su certificado e introduciendo los datos nuevos.

4.9 Revocación y suspensión de certificados

4.9.1 Causas de revocación de certificados

La EC-idCAT revoca un certificado por las siguientes causas:

1. Circunstancias que afectan la información contenida en el certificado
    - Modificación de alguno de los datos contenidos en el certificado.
    - Descubrimiento que alguno de los datos aportados en la solicitud de certificado es incorrecto, así como la alteración o modificación de las circunstancias verificadas para la expedición del certificado.
    - Descubrimiento que alguno de los datos contenidos en el certificado es incorrecto.
2. Circunstancias que afectan la seguridad de la clave o del certificado
    - Compromiso de la clave privada o de la infraestructura o sistemas de la EC-idCAT, siempre que afecte la fiabilidad de los certificados emitidos a partir de este incidente.
    - Infracción, por la EC-idCAT, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en este documento.
    - Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del suscriptor,.
    - Acceso o utilización no autorizados, por un tercero, de la clave privada del suscriptor.
    - El uso irregular del certificado por el suscriptor o falta de diligencia en la custodia de la clave privada.
3. Circunstancias que afectan el suscriptor.
    - Finalización de la relación entre la EC-idCAT y suscriptor.
    - Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado al suscriptor.
    - Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de éste.
    - Infracción por el suscriptor, de sus obligaciones, responsabilidad y garantías, establecidas en el instrumento jurídico correspondiente o en este documento.
    - La incapacidad sobrevenida o la muerte del suscriptor.
    - Solicitud del suscriptor de revocación del certificado.
4. Otras circunstancias
    - La suspensión del certificado digital por un período superior a 120 días.

- La finalización del servicio de la EC-idCAT, de acuerdo con lo establecido en la sección 5.8 de este documento.
- La finalización de la prestación de servicios por parte del Consorci AOC, de acuerdo con lo que establece la Política General de Certificación.
- Resolución judicial o administrativa que lo ordene (Art. 8.1 de la Ley 59/2003, de firma electrónica).

Revocación de oficio por error en la generación del certificado, ya sea pos una incidencia técnica o por error del operador en la introducción de datos del suscriptor. Si la entidad a la que se dirige la solicitud de revocación no dispone de toda la información necesaria para determinar la revocación de un certificado, pero tiene indicios de su compromiso puede decidir la suspensión.

En este caso se considera que las actuaciones realizadas durante el periodo de suspensión no son válidas, siempre que el certificado finalmente sea revocado. Son válidas si se levanta la suspensión, a través de la habilitación y el certificado vuelve a pasar al estado de vigencia.

El instrumento jurídico que vincula a la EC-idCAT con el suscriptor establece que el suscriptor solicita la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias indicadas anteriormente.

4.9.2 Legitimación para solicitar la revocación

Pueden solicitar la revocación de un certificado:

- El suscriptor a nombre del que el certificado fue emitido.
- La Entidad de Registro idCAT que intervino en la emisión.
- La EC-idCAT

4.9.3 Procedimientos de solicitud de revocación

Para proceder a la solicitud de revocación, el suscriptor se persona en la Entidad de Registro. La solicitud de revocación debe ser entregada personalmente, enviada por correo electrónico firmado o por correo certificado convencional. Debe incluirse la información suficiente para poder identificar razonablemente, a criterio de la EC-idCAT, por un lado, el certificado que se solicita revocar y, por otra parte, la autenticidad y autoridad del solicitante.

Esta información suficiente debe estar compuesta 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.

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

Se archiva y se comprueba la documentación, se autentica y se autoriza el solicitante. Por último se realiza la revocación en la aplicación informática correspondiente, y a continuación y de forma automática e inmediata se indica dicha revocación en el estado del certificado en la lista de revocaciones.

La EC-idCAT no puede reactivar el certificado, una vez revocado.

Nota: Un certificado revocado no puede volver a utilizarse; eso quiere decir que no puede alzarse la revocación, ni no anularse de ninguna otra forma: es un estado definitivo del certificado.

4.9.4 Plazo temporal de solicitud de revocación

Las solicitudes de revocación se remiten de forma inmediata cuando se tenga conocimiento de la causa de revocación.

4.9.5 Plazo máximo de procesamiento de la solicitud de revocación

La solicitud de revocación será procesada en el mínimo plazo posible, siempre dentro de los horarios de oficina de la Entidad de Certificación.

En caso de encontrarse fuera de horas de oficina, el suscriptor solicita la suspensión cautelar del certificado.

4.9.6 Obligación de consulta de información de revocación de certificados

Los verificadores comprueban el estado de aquellos certificados en los que deseen confiar.

Un método por el que se verifica el estado de los certificados es consultando la lista de revocación de certificados o LRC más reciente emitida por la EC-idCAT. El estado de vigencia también se puede comprobar online mediante el protocolo OCSP

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

4.9.7 Frecuencia de emisión de listas de revocación de certificados (LRCs)

La EC-idCAT emite una LRC al menos cada veinticuatro (24) horas. Además se emite una después de cada revocación.

Se indica en la LRC el momento programado de emisión de una nueva LRC, si bien se puede emitir una LRC antes del plazo indicado en la LRC anterior.

Los certificados revocados que expiren son retirados de la LRC transcurridos sesenta días desde su expiración.

4.9.8 Periodo máximo de publicación de LRCs

Las LRCs son publicadas inmediatamente en la web del Consorci AOC.

4.9.9 Disponibilidad de servicios de comprobación de estado de certificados

Los verificadores de certificados digitales pueden consultar un servicio en linea 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 el que se confía.

El Consori AOC ofrece de manera gratuïta 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 dicho 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 en http://www.aoc.cat/catcert .

4.9.10 Obligación de consulta de servicios de comprobación de estado de certificados

El verificador que no utilice LRC para comprobar la validez de un certificado, tiene que utilizar el Directorio de la EC-idCAT, al cual se habrá de poder acceder directamente a través de la página web del Servicio de Certificaicón Digital del Consorci AOC.

Los verificadores comprueban el estado de aquellos certificados en los que deseen confiar.

Una forma por la que se puede verificar el estado de los certificados es consultando la LRC más reciente emitida por la EC-idCAT.

La EC-idCAT suministra información a los verificadores referente a cómo y dónde encontrar la LRC correspondiente.

4.9.11 Otras formas de información de revocación de certificados

La EC-idCAT también informará sobre la revocación de los certificados, mediante el protocolo OCSP, que permite conocer el estado de vigencia de los certificados on-line.

En la petición de consulta de vigencia de un certificado en línea se ha de consignar un número de serie del certificado sobre el cual se realiza la petición y los datos identificativos de la autoridad de certificación emisora.

Si la petición no está válidamente realizada o si el servicio no puede dar respuesta en el momento de la solicitud, el servicio OCSP devolverá una respuesta que identifique el motivo por el cual no se devuelve esta respuesta (solicitante no autorizado, error en la respuesta o inoperatividad temporal del prestador requerido).

Si la petición está válidamente realizada y los servicios no tienen ninguna disfunción, se responderá a la petición con la consignación de que el certificado es válido o que está revocado (en este caso se consignará también el momento de la finalización de la vigencia del certificad firmada por la autoridad de certificación raíz del Consorci AOC (EC-ACC).

Esta respuesta será firmada con el certificado correspondiente (en este caso, el certificado de infraestructura de servidor de estado de certificados en línea –que recibe el acrónimo CIO). Esta respuesta será almacenada.

4.9.12 Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de la EC-idCAT es notificado, en la medida posible, a todos los participantes en la jerarquía pública de certificación de Catalunya, mediante el Directorio del Servicio de Certificación Digital del Consorci AOC.

4.9.13 Causas de suspensión de certificados

Los certificados se pueden suspender:

- Cuando lo solicite el poseedor de claves o el suscriptor o un tercero autorizado (artículo 9.1 de la Ley 59/2003).
- En los casos legalmente previstos en el artículo 9.1 de la Ley de Firma electrónica, esto es, en el caso de que una resolución judicial o administrativa lo ordene.
- Cuando la documentación requerida en la solicitud de revocación sea suficiente pero no se pueda identificar razonablemente al poseedor de claves.
- Si el suscriptor no utiliza el certificado durante un periodo prolongado de tiempo, conocido previamente.
- Si se sospecha el compromiso de una clave, hasta que éste sea confirmado. En este segundo caso, la EC-idCAT se asegura que el certificado no está suspendido durante más tiempo del necesario para confirmar su compromiso.
- Cuando no se activa el certificado en un plazo de 120 días a partir de la data de emisión.

4.9.14 Legitimación para solicitar la suspensión

Pueden solicitar la suspensión de un certificado:

- El suscriptor a nombre del que el certificado fue emitido.
- La EC-idCAT

4.9.15 Procedimientos de solicitud de suspensión

La suspensión de los certificados digitales se puede realizar de las formas que se detallan a continuación, informando al suscriptor de acuerdo con los términos establecidos en el artículo 10.2 de la Ley de Firma Electrónica

1. La suspensión puede ser solicitada por el poseedor de las claves y se puede llevar a cabo mediante una llamada al 902901080
2. La suspensió pot ser sol·licitada per l'Entitat de Registre. En cas que l'Entitat de Registre disposi d'autorització del Consorci AOC, pot realitzar ella mateixa el procés de suspensió. En cas contrari, realitza la tramitació de la suspensió a través del Consorci AOC.
3. La suspensió pot ser realitzada per l'EC-IDCAT directament, a través del component LRA o des de la web de consulta avançada de certificats.

Para iniciar la suspensión se requiere la siguiente información:

- Fecha y hora de la solicitud de la suspensión
- Identidad del suscriptor que solicita la suspensión
- Información de contacto de la entidad que solicita la suspensión

- Nombre y apellidos del poseedor de claves a quien se le ha de suspender el certificado digital
- DNI del poseedor de claves a quien se le tiene que suspender el certificado digital
- Número de serie (serial number) del certificado digital del que se solicita suspender
- Razón detallada de la petición de suspensión
- Código de suspensión asociado al certificado

Una vez suspendida la vigencia de un certificado se informará al suscriptor y, en su caso, al poseedor de claves, sobre el cambio de estado de suspensión y que el plazo máximo será de 120 días (arts. 10.2 y 10.4 de la Ley 59/2003)

4.9.16 Plazo máximo de suspensión

El plazo máximo de suspensión será de ciento veinte días naturales.

4.9.17. Habilitación de un certificado suspendido

El suscriptor podrá habilitar el certificado que permanece suspendido, personándose e identificándose ante la Entidad de Registro, firmando el correspondiente documento de solicitud de habilitación comunicando que se ha extinguido el motivo que provocó la suspensión.

4.10 Servicios de comprobación de estado de certificados

4.10.1 Características de operación de los servicios

Las LCRs 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 la EC-IdCAT.

4.10.2 Disponibilidad de los servicios

Los verificadores de certificados digitales pueden consultar un servicio en linea 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 el que se confía.

El Consori 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 dicho 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 en http://www.aoc.cat/catcert

4.10.3 Otras funciones de los servicios

Sin estipulación adicional.

4.11 Finalización de la suscripción

La finalización de la suscripción no implica la revocación de los certificados que hayan sido emitidos, sino que estos pueden utilizarse hasta que expiren.

4.12 Depósito y recuperación de claves

No se practica.

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

Sin estipulación adicional.

5.1 Controles de seguridad física

5.1.1 Localización y construcción de las instalaciones

Sin estipulación adicional.

5.1.2 Acceso físico

Sin estipulación adicional.

5.1.3 Electricidad y aire acondicionado

Sin estipulación adicional.

5.1.4 Exposición al agua

Sin estipulación adicional.

5.1.5 Advertencia y protección de incendios

Sin estipulación adicional.

5.1.6 Almacenaje de soportes

Sin estipulación adicional.

5.1.7 Tratamiento de residuos

Sin estipulación adicional.

5.1.8 Copia de seguridad fuera de las instalaciones

Sin estipulación adicional.

5.2 Controles de procedimientos

La EC-IDCAT garantiza que sus sistemas se operan de forma segura, y por esto establece e implanta procedimientos para las funciones que afecten a la provisión de sus servicios.

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

5.2.1 Funciones fiables

Sin estipulación adicional.

5.2.2 Número de personas por tarea

Sin estipulación adicional.

5.2.3 Identificación y autenticación para cada función

Sin estipulación adicional.

5.2.4 Roles que requieren separación de tareas

Sin estipulación adicional.

5.3 Controles de personal

La EC-IDCAT tiene en cuenta los siguientes aspectos:

- Se mantiene confidencialidad de la información, poniendo los medios necesarios y manteniendo una actitud adecuada en el desarrollo de sus funciones dentro y fuera del ámbito laboral en lo referente a la seguridad de las infraestructuras.
- Se es diligente y responsable en el tratamiento, mantenimiento y custodia de los activos de la infraestructura identificados en la política, en los planes de seguridad o en este documento.
- No se revela información no pública fuera del ámbito de la infraestructura, ni se extraen soportes de información a niveles de seguridad inferiores.

- Se reporta al Responsable de Seguridad, lo mejor posible, cualquier incidente que se considere que afecta a la seguridad de la infraestructura, o limitar la calidad del servicio.
- Se utilizan los activos de la infraestructura para las finalidades que les 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 medidas de seguridad a que está sometido.
- El responsable de seguridad vela porque el punto anterior sea ejecutado, proveyendo a los responsables de área toda la información que fuera necesaria.
- No se instalan 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 de Certificación Digital.
- el Responsable de la EC-IDCAT.
- 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.
- los Usuarios de laEC-IDCAT.

Además, se ve afectado el siguiente personal del Consorci AOC:

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

5.3.1 Requisitos de historial, calificaciones, experiencia y autorización

Sin estipulación adicional.

5.3.2 Requisitos de formación

Sin estipulación adicional.

5.3.3 Requisitos y frecuencia de actualización formativa

Sin estipulación adicional.

5.3.4 Secuencia y frecuencia de rotación laboral

Sin estipulación adicional.

5.3.5 Sanciones por acciones no autorizadas

Sin estipulación adicional.

5.3.6 Requisitos de contratación de profesionales

Sin estipulación adicional.

5.3.7 Suministro de documentación al personal

Sin estipulación adicional.

5.4 Procedimientos de auditoría de seguridad

5.4.1 Tipos de acontecimientos registrados

Sin estipulación adicional.

5.4.2 Frecuencia de tratamiento de registros de auditoría

Sin estipulación adicional.

5.4.3 Periodo de conservación de registros de auditoría

Sin estipulación adicional.

5.4.4 Protección de los registros de auditoría

Sin estipulación adicional.

5.4.5 Procedimientos de generación de copias de seguridad

Con el fin de conservar correctamente las copias de seguridad se han implantado los siguientes puntos:

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

5.4.6 Localización del sistema de acumulación de registros de auditoría

Sin estipulación adicional.

5.4.7 Notificación del acontecimiento de auditoría al causante del acontecimiento

Sin estipulación adicional.

5.4.8 Análisis de vulnerabilidades

Sin estipulación adicional.

5.5 Archivo de informaciones

Sin estipulación adicional.

5.5.1 Tipos de acontecimientos registrados

La EC-IDCAT guarda registros de todos los acontecimientos que tengan lugar durante el ciclo de vida de un certificado, incluyendo la renovación de éste.

La EC-IDCAT guarda un registro de lo siguiente:

Documentos originales:

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

Fotocopias de:

- Carta de entrega de certificados
- Carta PIN y PUK, con acuse de recibo.

La EC-IDCAT guarda, en relación con los certificados Extended Validation:

- Logs y pistas de auditoria
- Documentación relativa a peticiones, verificaciones y revocaciones de certificados Extended Validation

5.5.2 Periodo de conservación de registros

5.5.2.1 Requisitos para todos los tipos de certificados

La EC-IDCAT guarda los registros especificados en la sección 5.5.1 durante 15 años, contados desde el momento de la expedición del certificado.

5.5.3 Protección del archivo

- Sin estipulación adicional.

5.5.4 Procedimientos de generación de copias de seguridad

Sin estipulación adicional.

5.5.5 Requisitos de sellado de cautela de fecha y hora

Sin estipulación adicional.

5.5.6 Localización del sistema de archivo

La EC-ACC tiene un sistema de mantenimiento de datos de archivo fuera de sus propias instalaciones, así como se especifica en la sección 5.1.8.

5.5.7 Procedimientos de obtención y verificación de información de archivo

Sin estipulación adicional.

5.6 Renovación de claves

Los certificados de la EC-IDCAT que se hayan renovado, se comunican a los usuarios finales, mediante su publicación en la pàgina web del Servei de Certificació Digital del Consorci AOC.

5.7 Compromiso de claves y recuperación de desastre

5.7.1 Procedimiento de gestión de incidencias y compromisos

La EC-IDCAT establece los procedimientos que aplica en la gestión de las incidencias que afectan sus claves y, muy especialmente, en 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 la EC-IDCAT inicia las gestiones necesarias, según los documentos Plan 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 Entidad

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

En caso de compromiso la EC-IDCAT:

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

5.7.4 Desastre sobre las instalaciones

La EC-IDCAT 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 cómo 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 en el Plan de Seguridad.

La EC-IDCAT es capaz de restaurar la operación normal de la PKI en las 24 horas siguientes al desastre, pudiendo, como mínimo, ejecutarse las siguientes acciones:

- Revocación de certificados (excepto en el mes de agosto).
- Publicación de información de revocación.

La base de datos de recuperación de desastres utilizada por la EC-IDCAT 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 la EC-IDCAT tienen las medidas de seguridad físicas especificadas en el Plan de Seguridad.

5.8 Finalización del servicio

5.8.1 EC-IDCAT

Sin estipulación adicional.

5.8.2 Entidad de Registro

Las Entidades de Registro tendrán que conservar y custodiar diligentemente toda la información generada en su actividad como Entidad de Registro durante 15 años después de finalizar las actividades relacionadas con la Entidad de Registro.

6. Controles de seguridad técnica

La EC-IDCAT 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 soporte.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

El par de claves podrá ser generado por el futuro suscriptor o por la Entidad de Registro.

6.1.2. Envío de la clave pública al emisor del certificado

El método de envío de la clave pública a la EC-IDCAT es PKCS #10

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

La clave de la EC-IDCAT y las claves de las Entidades de Certificación anteriores de la jerarquía pública de certificación de Catalunya son están a disposición de los verificadores, asegurando la integridad de la clave y autenticando el origen.

La clave pública de la EC-ACC (Entidad de Certificación raíz de la jerarquía operada por el Consorci AOC) se publica en el directorio de la EC-IDCAT, en forma de certificado auto firmado, junto a una declaración referente a que la clave permite autenticar a la EC-IDCAT.

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

La clave pública de la EC-IDCAT se publica en el directorio de la EC-IDCAT, en forma de certificado CIC firmado por el Consorci AOC.

Los usuarios acceden al Directorio para obtener las claves públicas de la EC-IDCAT.

Una vez que el suscriptor ha generado el par de claves del certificado ambas claves serán almacenadas al poseedor de claves del sistema operativo instalado en la máquina del Suscriptor o en el llavero pero además, la clave pública junto con los datos de la solicitud se insertarán en un archivo PKCS#10 (firmado por la clave privada). Este archivo es, en definitiva la petición de certificación que se envía a la EC-IdCAT.

6.1.4. Medidas de claves

Las claves de la EC-IDCAT es al menos de 2.048 bits.

Las claves de todos los certificados emitidos por la EC-IDCATson de 2.048 bits.

6.1.5. Generación de parámetros de clave pública

Sin estipulación adicional.

6.1.6. Comprobación de calidad de parámetros de clave pública

Se realiza de acuerdo con el informe especial del ETSI TS 101 276, que indica la calidad de los algoritmos de firma electrónica.

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

Los pares de claves de la EC-IDCAT son generados utilizando hardware criptográfico que cumple los requisitos establecidos por la especificación técnica CEN CWA 14167 o equivalente.

Los pares de claves de los suscriptores de certificados CPISR, CPX, CEISR, CEX, CDS-1 de sede electrónica de nivel alto y CDA-1 de sello electrónico de nivel alto deben generarse en el componente de Autoridad de Registro Local 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 puede realizarse mediante aplicaciones informáticas.

6.1.8. Propósitos de uso de claves

La EC-IDCAT 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

Las claves privadas de las Entidades de Certificación se protegen utilizando hardware criptográfico que cumple los requisitos establecidos por la especificación técnica FIPS 140-2 Nivel 3 o superior.

Los pares de claves de los suscriptores de certificados reconocidos y de certificados de nivel alto están protegidos por tarjetas inteligentes que cumplen los requisitos establecidos por la especificación técnica CEN CWA 14169 o equivalente.

6.2.1.2. Ciclo de vida de las tarjetas con circuito integrado

Las tarjetas con circuito integrado (también tarjetas inteligentes) se entregan en cada emisión de nuevo certificado por la Entidad de Registro, o bien directamente por el Consorci AOC cuando actúa como Entidad de Registro Virtual.

Por cada nueva emisión o renovación de los certificados se entrega una tarjeta nueva, es decir, no se carga certificados en tarjetas usadas.

Cuando el Consorci AOC detecte errores o defectos en las tarjetas, podrá retirar de oficio las tarjetas afectadas. En caso de detectar defectos o errores en casos puntuales, se sustituirá la tarjeta afectada, previa revocación del certificado y se emitirá un nuevo certificado que se librará en una tarjeta nueva sin coste adicional para el suscriptor.

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

De los 5 posibles dispositivos criptográficos que existen la EC-IDCAT 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 de ellas conoce más que una de las claves de acceso.

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

6.2.3. Depósito de la clave privada

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

Las claves privadas de los certificados de cifrado sí se podrán almacenar en la EC-IDCAT.

6.2.4. Copia de seguridad de la clave privada

Existe copia de seguridad de la clave privada de la EC-IDCAT y de los medios necesarios para acceder, en dependencia independiente de aquella donde se almacena habitualmente.

6.2.5. Archivo de la clave privada

La clave privada de la EC-IDCAT cuenta con una copia de seguridad realizada, almacenado, y recuperado 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 en las prácticas de la EC-IDCAT.

Los controles de seguridad a aplicar en copias de seguridads de la EC-IDCAT son de igual o superior nivel a las que se apliquen a las claves habitualmente en uso.

Cuando las claves se almacenen en un módulo hardware de proceso dedicado, se proveen los controles oportunos para que estas nunca puedan abandonar el dispositivo.

No se almacenan copias de las claves privadas de los certificados, excepto en el caso de los certificados de cifrado, para garantizar la recuperación de los datos.

6.2.6. Introducción de la clave privada en el módulo criptográfico

Las claves privadas de la EC-IDCAT 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. Almacenaje 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 la EC-IDCAT.

Para certificados personales y de entidad, la clave privada del suscriptor se activa mediante la introducción del PIN en la tarjeta inteligente.

6.2.9. Método de desactivación de la clave privada

No aplicable.

6.2.10. Método de destrucción de la clave privada

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

6.2.11. Clasificación de los módulos criptográficos

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

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

6.3. Otros aspectos de gestión del par de claves

6.3.1. Archivo de la clave pública

La EC-IDCAT archiva sus claves públicas, de acuerdo con lo establecido en la sección 5.5

6.3.2. Periodos de utilización de las claves pública y 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 puede continuar utilizándose hasta después de la expiración del certificado.

6.4. Datos de activación

6.4.1. Generación e instalación de los datos de activación

La generación e instalación de los datos de activación se basa en el Cryptographic Service Provider.

6.4.2. Protección de los datos de activación

6.4.2.1. Para certificados personales y de entidad

El suscriptor es responsable de proteger su clave privada, con una contraseña lo más completa posible, a través de la aplicación (Cryptographic Service Provider).

Se aconseja que la citada contraseña no sea demasiado corta y formada por números y letras.

El suscriptor ha de recordar la citada contraseña.

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:

- La EC-IDCAT 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.

- La EC-IDCAT garantiza que el acceso a los sistemas de información y aplicaciones se restringe de acuerdo a lo establecido en la política de control de acceso, así como que los sistemas proporcionan los controles de seguridad suficientes para implementar la segregación de funciones identificada en las prácticas de la EC-IDCAT, 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 la EC-IDCAT está identificado y reconocido antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del certificado.

- El personal de la EC-IDCAT es responsable y tiene que poder justificar sus actividades, por ejemplo mediante un archivo de acontecimientos.

- Debe evitarse la posibilidad de revelación de datos sensibles mediante la reutilización de objetos de almacenaje (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 acceso irregulares o no autorizados a sus recursos (por ejemplo, mediante un sistema de detección de intrusiones, monitorización y alarma).

- El acceso a los depósitos públicos de la información de la EC-IDCAT (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, evaluándose el grado de cumplimiento mediante una auditoria de seguridad informática conforme a la especificación técnica CWA 14172-3 y un perfil de protección adecuado, 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 dichos componentes.

6.6.2. Controles de gestión de seguridad

La EC-IDCAT garantiza que sus funciones de gestión de las operaciones de los módulos criptográficos son suficientemente seguras y, en particular, ha de asegurar que 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 código malicioso, para garantizar la integridad y la validez de la información que procesan

La EC-IDCAT mantiene un inventario de todos los activos informáticos y realiza una clasificación de los mismos de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

La configuración de los sistemas se audita de forma periódica, de acuerdo con lo establecido en la sección .

Se realiza un seguimiento de las necesidades de capacidad, y se planificarán procedimientos para garantizar suficiente disponibilidad electrónica y de almacenaje para los activos informativos.

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 a las diferentes redes de la EC-IDCAT es limitado a individuos debidamente autorizados. En particular:

- Se implementan controles (como 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 la EC-IDCAT.

- Los datos sensibles se protegen cuando se intercambian a través de redes no seguras (incluyendo los datos de registro del suscriptor).

- Se garantiza que los componentes locales de red (como enrutadores) se encuentran ubicados en entornos seguros, así como 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 diferentes perfiles de dertificados digitales que emite la EC-IdCAT 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 la web del Consorci AOC http://www.aoc.cat/catcert/..

8. Auditoría de conformidad

La EC-IDCAT 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 Catalunya.

La EC-IDCAT puede delegar la ejecución de las auditorías en una tercera entidad contratada por el Consorci AOC. En este caso la EC-IDCAT coopera completamente con el personal que lleva a término la investigación.

8.1 Frecuencia de la auditoría de conformidad

Sin estipulación adicional

8.2 Identificación y calificación del auditor

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

8.3 Relación del auditor con la entidad auditada

Las auditorías externas de conformidad ejecutadas por terceros están realizadas por una entidad independiente de la EC-IDCAT.

8.4 Relación de elementos objeto de auditoría

Sin estipulación adicional.

8.5 Acciones a emprender como resultado de una falta de conformidad

Sense estipulació addicional.

8.6 Tratamiento de los informes de auditoría

Los informes de resultados de las auditorias serán entregados al Consorci AOC en tanto que 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 Tarifa de emisión o renovación de certificados

El Consorci AOC establece las tarifas que aplica la EC-IDCAT, 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 acceso a los certificados.

9.1.4 Tarifas de otros servicios

Sin estipulación adicional

9.1.5 Política de reintegro

El Consorci AOCno practicará reembolsos. 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 AOCdispone de una garantía de cobertura de su responsabilidad civil suficiente, en los términos previstos en el artículo 20.2 de la Ley 59/2003, de 19 de diciembre, excepto cuando se encuentre eximida 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 Consorcio AOC (o la EC-IDCAT) no actuarà como agente fiduciario ante suscriptores y terceras personas, que

deberán dirigirse contra el infractor de las condiciones de uso de los certificados establecidas por el Consorcio AOC (o la EC-IDCAT).

9.3 Confidencialidad

9.3.1 Informaciones confidenciales

Sin estipulación adicional.

9.3.2 Informaciones no confidenciales

Sin estipulación adicional.

9.3.3 Responsabilidad para la protección de información confidencial

Sin estipulación adicional.

9.4 Protección de datos personales

9.4.1 Política de Protección de Datos Personales

Sin estipulación adicional.

9.4.2 Datos de carácter personal no disponibles a terceros

Sin estipulación adicional.

9.4.3 Datos de carácter personal disponibles a terceros

Sin estipulación adicional.

9.4.4 Responsabilidad correspondiente a la protección de los datos personales

Sin estipulación adicional.

9.4.5 Gestión de incidencias relacionadas con los datos de carácter personal

Sin estipulación adicional.

9.4.6 Prestación del consentimiento en el uso de los datos personales

Sin estipulación adicional.

9.4.7 Comunicación de datos personales

Sin estipulación adicional.

9.5 Derechos de propiedad intelectual

9.5.1 Propiedad de los certificados e información de revocación

Sin estipulación adicional.

9.5.2 Propiedad de la política de certificado y Declaración de Prácticas de Certificación

Sin estipulación adicional

9.5.3 Propiedad de la información relativa a nombres

Sin estipulación adicional.

9.5.4 Propiedad de claves

Sin estipulación adicional..

9.6 Obligaciones y responsabilidad civil

9.6.1 Entidades de Certificación

9.6.1.1 Obligaciones generales de la EC-IDCAT

- Sin estipulación adicional.

9.6.1.2 Garantías ofrecidas a suscriptores y verificadores

Sin estipulación adicional.

9.6.2 Obligaciones y otros compromisos de las Entidades de REgistro

9.6.2.1 Obligaciones y otros compromisos

La Entidad de Certificación puede delegar algunas funciones a Entidades de Registro, que en este caso quedan obligadas a su cumplimiento, en las mismas condiciones que la Entidad de Certificación.

La Entidad de Registro actúa en su propio nombre, sin perjuicio de la responsabilidad de la EC-idCAT.

La Entidad de Registro queda obligada a registrar los datos del certificado y su aprobación en caso de ser correctos, así como al registro de los datos de este certificado, por el que realiza las comprobaciones que considere necesarias al respecto de la identidad y el resto de datos personales y complementarios de los suscriptores, y si fuera necesario, de los poseedores de claves.

Estas comprobaciones incluyen la justificación documental aportada por el solicitante y, si la Entidad de Registro lo considerase necesario, cualquier otro documento e información relevante, facilitados por el suscriptor, por el poseedor de claves o por terceras personas.

Si la Entidad de Registro detectase errores en los datos que son incluidos en los certificados, o en los documentos que justificasen estos datos, está obligada a realizar los cambios que considere necesarios antes de la emisión del certificado, o a la paralización del proceso de emisión y a gestionar con el suscriptor la incidencia correspondiente.

En el caso que la Entidad de Registro corrija los datos sin gestión previa de la incidencia correspondiente con el suscriptor, queda obligada a notificar los datos que finalmente se certifiquen al suscriptor en el momento de la entrega.

La Entidad de Registro se reserva el derecho a no aprobar la solicitud de emisión del certificado, cuando la justificación documental aportada por el solicitante sea insuficiente para la correcta identificación y/o autenticación del suscriptor.

9.6.3 Garantías ofrecidas a suscriptores y verificadores

9.6.3.1 Garantía del Consorci AOC por los servicios de certificación digital

9.6.3.2 Sin estipulación adicional**Exclusión de la garantía**

a. Sin estiopulación adicional

9.6.4 Suscriptores

9.6.4.1 Obligaciones y otros compromisos

Sin estipulación adicional

9.6.4.2 Garantías ofrecidas por el suscriptor

Sin estipulación adicional

9.6.4.3 Protección de la clave privada

Sin estipulación adicional.

9.6.5 Verificadores

9.6.5.1 Obligaciones y compromisos

Sin estipulación adicional.

9.6.5.2 Garantías ofrecidas por el verificador

Sin estipulación adicional

9.6.6 Otros participantes

9.6.6.1 Obligaciones y garantías del directorio

Sin estipulación adicional

9.6.6.2 Garantías ofrecidas por el directorio

La EC-IDCAT tiene la responsabilidad civil del directorio de certificación.

9.7 Renuncias de garantías

9.7.1 Rechazo de garantías de la EC-IDCAT

La EC-IDCAT puede rechazar todas las garantías del servicio, que no se encuentren vinculadas a obligaciones establecidas por la Ley 59/2003, de 19 de diciembre, de firma electrónica, 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 la EC-IDCAT

La EC-IDCAT 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) subministrados por ésta.

La EC-IDCAT puede limitar su responsabilidad mediante la inclusión de límites de uso del certificado, y límites de valor de las transacciones para las que puede utilizarse el certificado.

9.8.2 Caso fortuito y fuerza mayor

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

9.9 Indemnizaciones

9.9.1 Cláusula de indemnidad de suscriptor

No se establecerá cláusula de indemnidad del suscriptor.

9.9.2 Cláusula de indemnidad de verificador

No se establecerá cláusula de indemnidad del verificador.

9.10 Plazo y finalización

9.10.1 Plazo

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

9.10.2 Finalización

La EC-IDCAT establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, una cláusula que determina las consecuencias de la finalización de la relación jurídica en virtud de la que suministra certificados a los suscriptores.

9.10.3 Supervivencia

Sin estipulación adicional

.

9.11 Notificaciones

Sin estipulación adicional.

9.12 Modificaciones

9.12.1 Procedimiento para las modificaciones

Sin estipulación adicional.

9.12.2 Periodo y mecanismos para notificaciones

Las modificaciones deeste documento serán aprobadas por el Consorci AOC, conforme se establece en el apartado 1.5.

9.12.3 Circunstancias en las que un OID tiene que ser cambiado

Sin estipulación adicional.

9.13 Resolución de conflictos

9.13.1 Resolución extrajudicial de conflictos

Sin estipulación adicional.

9.13.2 Jurisdicción competente

Sin estipulación adicional.

9.14 Ley aplicable

Sin estipulación adicional.

9.15 Conformidad con la ley aplicable

La EC-AL manifiesta, en este documento y en los instrumentos jurídicos con suscriptores, el cumplimiento de la Ley 59/2003, de 19 de diciembre, de firma electrónica. La prestación de servicios se ajusta a la legislación vigente, en especial, la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico.

9.16 Cláusulas diversas

9.16.1 Acuerdo íntegro

Sin estipulación adicional.

9.16.2 Subrogación

Sin estipulación adicional.

9.16.3 Divisibilidad

Sin estipulación adicional.

9.16.4 Aplicaciones

Sin estipulación adicional.

9.16.5 Otras cláusulas

Sin estipulación adicional.

ANEXO – Control documental

Control de versiones DPC EC-IDCAT 1er semestre 2016

Proyecto:	**Informe modificación del documento DPC EC-IDCAT**
Entidad de destino:	**Consorci AOC**
Código de referencia:	**Revisión 1r semestre 2016**
Versión:	**Cambios de la v3.8 a la v4.0 en catalán y en castellano**
Fecha de la edición:	**05/08/2016**

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
4.0	Totes	Revisión global. Integración de CATCert en Consorci AOC	Servei de Certificació Digital AOC	18/05/2016