Consorci
Administració Oberta
de Catalunya

Declaración de Prácticas de Certificación
Autoridad de Certificación del Consorci AOC

Referencia:	D1111_E0650_N-DPC Consorci AOC
Versión:	6.0
Fecha:	26/07/2018

La versión original en vigor de este documento se encuentra en formato electrónico publicada en el sitio web del Consorci AOC y puede ser accesible a través de la siguiente URL: https://www.aoc.cat/catcert/regulacio

Historial de versiones

Versión	Resumen de los cambios	Fecha
5.0	Adaptación a EIDAS	9/5/2018
6.0	Creación de nueva declaración de prácticas de certificación unificada. Se numera como versión 6.0 a efectos de gestión documental.	26/07/2018

Índice

1. Introducción

1.1. Presentación

Este documento es la Declaración de Prácticas de Certificación (DPC) del Consorci Administració Oberta de Catalunya (AOC), Prestador de los servicios de confianza (PSC) o Trust Service Provider (TSP) que opera al amparo de lo previsto en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

En esta DPC se detallan el conjunto de prácticas adoptadas por el Consorci AOC como Prestador de Servicios de Certificación para la emisión de certificados digitales y servicios de confianza basados en los siguientes estándares:

- ETSI EN 319 401 (General Policy Requirements for Trust Service Providers).
- ETSI EN 319 411-1 (Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements)
- ETSI EN 319 411-2 (Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates)
- ETSI EN 319 412-1 (Certificate Profiles; Part 1: Overview and common data structures)
- ETSI EN 319 412-2 (Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons)
- ETSI EN 319 412-3 (Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons)
- ETSI EN 319 412-4 (Certificate Profiles; Part 4: Certificate profile for web site certificates)
- ETSI EN 319 422 (Certificate profiles for time-stamping protocol and time-stamp token profiles)
- ETSI EN 319 412-5 (Certificate Profiles; Part 5: QCStatements)

La estructura de este documento está basada en la especificación del estándar “RFC3647 - Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework “, creado por el grupo de trabajo PKIX del IETF.

La presente DPC se correlaciona con las diferentes Políticas de Certificación (PC) desarrolladas para cada tipología de certificados digitales emitidos bajo el control del Consorci AOC, los cuales son descritos en el apartado 1.1.1 del presente documento. En caso de contradicción entre la presente DPC y alguna de las PC prevalecerá lo dispuesto en este documento.

El servicio de certificación digital del Consorci AOC cumple con la versión actual de las pautas del CA/Browser Forum para la emisión y gestión de certificados de validación extendida *(extended validation)*, y con las pautas de Baseline Requirements de este mismo organismo para la emisión de certificados de dispositivo de servidor CDS, publicadas en: http://www.cabforum.org.

1.1.1. Tipo y clases de certificados

El Consorci AOC presta sus servicios de certificación con la finalidad de emitir certificados digitales para diversos usos y diferentes usuarios finales. Todos los certificados que emite el Consorci AOC se adecúan a los requerimientos del Reglamento 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

1.1.1.1. Certificados de ciudadanía

- **Certificado cualificado de ciudadano (idCAT):** El certificado idCAT es un certificado cualificado de identificación y firma electrónica avanzada destinado a ciudadanos y ciudadanas con vecindad administrativa catalana, y para otras personas (colectivamente denominados "subscriptores") que necesitan relacionarse con las Administraciones públicas y otras instituciones de Cataluña.

1.1.1.2. Certificados Personales del Sector Público

- **Certificado de autenticación de trabajador público de nivel alto (T-CAT autenticació).** Permite la identificación de un trabajador público en el ejercicio de sus funciones, como instrumento para la actuación en el ámbito electrónico de una Administración Pública, órgano, organismo público o entidad de derecho público catalán conforme a lo previsto en la regulación aplicable.

- **Certificado cualificado de firma de trabajador público de nivel alto (T-CAT signatura).** Permite la firma electrónica por parte de un trabajador público en el ejercicio de sus funciones, como instrumento para la actuación en el ámbito electrónico de una Administración Pública, órgano, organismo público o entidad de derecho público catalán conforme a lo previsto en la regulación aplicable. Los

certificados T-CAT de Autenticación y T-CAT de Firma se emiten y almacenan conjuntamente en un único dispositivo criptográfico.

- **Certificado cualificado de autenticación y firma de trabajador público de nivel medio/sustancial (T-CATP).** Este tipo de certificados de autenticación y firma se emiten para su uso en software por parte de trabajadores públicos catalanes en el ejercicio de sus funciones en actuaciones que no requieran un nivel alto de seguridad, conforme a lo previsto en la regulación aplicable.

- **Certificado de autenticación de trabajador público con pseudónimo de nivel alto (T-CAT pseudònim autenticació).** La emisión de estos certificados se hará bajo la valoración previa de la acreditación legal del pseudónimo que deberá acompañar la solicitud. Se aceptarán muy específicamente para usos justificados en que no se puedan mostrar los datos del titular y por personas que, dentro de su organización ya dispongan de pseudónimo regulado, caso de los funcionarios de prisiones, Mossos d'esquadra, etc. Salvo en lo que respecta al uso de pseudónimo, sus características son iguales a las del certificado T-CAT de Autenticación.

- **Certificado cualificado de firma de trabajador público con pseudónimo de nivel alto (T-CAT pseudònim signatura).** Para la emisión de estos certificados se tendrán en cuenta las mismas circunstancias que en el caso de los certificados T-CAT con Pseudónimo y de Autenticación. Salvo en lo que respecta al uso de pseudónimo, sus características son iguales a las del certificado T-CAT de Firma. Los certificados T-CAT con Pseudónimo y de Autenticación y T-CAT con Pseudónimo y de Firma se emiten y almacenan conjuntamente en un único dispositivo criptográfico.

- **Certificado cualificado de autenticación y firma de persona vinculada de nivel alto (T-CAT persona vinculada):** Certificado personal de identificación y firma electrónica cualificada, con cargo opcional. Estos certificados se emiten y almacenan en dispositivo criptográfico. Estos certificados están destinados a aquellas personas que tienen una relación funcional o de servicio con una institución pública, pero carecen de un contrato laboral con dicha institución.

- **Certificado cualificado de autenticación y firma de persona vinculada de nivel medio/sustancial (T-CATP Persona vinculada):** Certificado personal de identificación y firma electrónica cualificada, con cargo opcional. Estos certificados se emiten y almacenan en software.

- **Certificado cualificado de autenticación y firma de representante ante las Administraciones Públicas (T-CAT Representant)**: Certificado personal de identificación y firma electrónica cualificada, con cargo opcional. Este certificado se emite en dispositivo criptográfico. Va dirigido a personas físicas y dispone de información referente al titular que permite identificarlo y a su organización. Se

suministra al personal de las administraciones públicas catalanas como elemento identificativo en las comunicaciones electrónicas, permitiendo firmar documentos en formato electrónico para hacer posible los trámites y las consultas en línea. Este certificado permite identificarse como persona poseedora de un determinado cargo en su organización.

1.1.1.3. Certificados de Dispositivos e Infraestructuras

- **Certificado de Aplicación (Dispositiu aplicació):** Este certificado se almacena en un servidor (preferiblemente en un dispositivo criptográfico) y es requerido por una aplicación para sellar documentos, ficheros o mensajes con el objetivo de asegurar su autenticidad e integridad. Jurídicamente opera como un sello electrónico avanzado del ente o departamento de la Administración Pública a nombre del cual se emite, conforme a lo previsto en el Reglamento UE 910/2014, aunque su uso queda limitado al intercambio de datos entre aplicaciones.

- **Certificado de Sello Electrónico Avanzado (Segell nivell mig/substancial)**: Sirve para la identificación y la autenticación de documentos, ficheros o mensajes derivados de la actuación administrativa automatizada, para la prestación de servicios públicos conforme a lo previsto en el artículo 37 del Reglamento UE 910/2014. Este certificado puede utilizarse para el intercambio de datos (entre administraciones, administraciones y ciudadanos y entre administraciones y empresas), la identificación y autenticación de un sistema, servicio web o aplicación, el archivo electrónico automatizado, las compulsas y copias electrónicas, entre otros. Estos certificados se emiten y almacenan en software.

- **Certificado de Sede Electrónica (Seu-e nivell mig/substancial)**: Sirve para identificar y garantizar la integridad y autenticidad de la sede electrónica de un ente, entendiendo sede electrónica en los términos descritos en el artículo 38 de la Ley 40/2015, y el establecimiento de comunicaciones seguras

  Este certificado puede utilizarse para la conexión segura de los ciudadanos a páginas web oficiales, la autenticación de un sitio web, el alojamiento de registros electrónicos, la consulta y autorización de registros de representación, etc.

  Desde 2011, el Consorcio AOC emite el certificado de Sede siguiendo el Standard Extended Validation SSL Certificate , lo que garantiza el máximo nivel de seguridad en las transacciones que se realicen en el sitio web que utilice.

- **Certificado de Servidor Seguro (Dispositiu SSL):** Este tipo de certificados garantizan la identidad de un dominio ante los usuarios que se conectan, acreditando que el sitio web es el original, el dominio está oficialmente registrado, es válido y no ha sido suplantado, y que nadie ha podido alterar la información publicada ni manipular los datos registrados en el servidor de manera no autorizada.

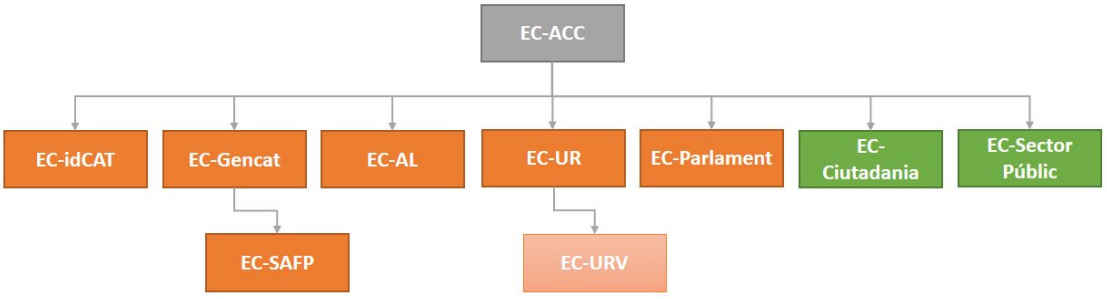
- **Certificado de Servidor Seguro *Extended Validation* (Dispositiu SSL EV):** Los certificados de dispositivo servidor EV (CDS EV) no son estructuralmente o funcionalmente diferentes de los de certificado de dispositivo servidor (CDS), pero se diferencian de éstos en que han sido emitidos por Autoridades de Certificación que, como el Consorcio AOC, han superado los estrictos requisitos de seguridad establecidos en el Standard Extended Validation SSL Certificate.

  La principal ventaja es que los nuevos navegadores web los aceptarán inmediatamente y mostrarán una confirmación de seguridad que permitirá a los usuarios identificar rápidamente un lugar seguro y de confianza, ya que están diseñados para mostrar señales visuales únicas que indican la presencia de un certificado EV.

- **Certificado de Sello Cualificado de Tiempo (Segell de temps):** Permite garantizar la integridad de un archivo o una comunicación electrónicos en una fecha y hora determinadas, tomando una fuente de tiempo confiable. Los Certificados de Sello Cualificado de tiempo emitidos por el Consorcio AOC cumplen con los requisitos establecidos en el artículo 42 del Reglamento UE 910/2014.

1.1.2. Jerarquías

Según se detalla en el gráfico siguiente, a partir de 2015, la jerarquía actual de certificación del Consorcio AOC se ha visto reducida a dos Autoridades de Certificación subordinadas (marcadas en verde) y una Autoridad de Certificación raíz:



La EC-SectorPublic: que concentra la emisión de certificados para el Sector Público de Cataluña, en sustitución de las antiguas EC-SAFP, EC-AL, EC-UR y EC-Parlamento. Estas Autoridades de Certificación han dejado de emitir certificados aunque algunos de ellos aún se encuentran en vigor.

Los certificados emitidos bajo las antiguas Autoridades de Certificación EC-SAFP, EC-AL, EC-UR y EC-Parlamento no se rigen por esta versión de la DPC. A los mismos les resultará

de aplicación lo previsto en las DPC AL, GENCAT, SAFP, PARLAMENT, UR y URV en su versión 5.0, 2.0, 5.0, 2.0, 7.0, 4.0, correspondiente a la última actualización del citado documento antes del cese en la emisión de certificados al amparo de las citadas Autoridades de Certificación.

La EC-Ciudadanía: que emite certificados digitales a ciudadanos en sustitución de la antigua EC-idCAT, la cual también ha dejado de emitir certificados aunque algunos de ellos aún se encuentran en vigor. Los certificados emitidos bajo la antigua Autoridad de Certificación EC-idCAT no se rigen tampoco por esta versión de la DPC. A los mismos les resultará de aplicación lo previsto en la DPC [idCAT] en su versión [4.0], correspondiente a la última actualización del citado documento antes del cese en la emisión de certificados al amparo de la citada Autoridad de Certificación.

1.1.3. Emisión de certificados de pruebas

El Consorci AOC puede emitir certificados de pruebas firmados por una CA real pero con contenido ficticio para que los organismos supervisores y las entidades de validación y los desarrolladores de aplicaciones puedan llevar a cabo sus procesos de integración y/o evaluación para su aceptación. El Consorci AOC incorpora en dichos certificados la siguiente información de forma que cualquier usuario pueda conocer claramente que se trata de un certificado de pruebas sin responsabilidad:

Nombre de la organización	Organització de prova
NIF de la organización	VATES-Q0000000J
Domicilio	Barcelona
Código Postal	08008
Correo electrónico	scd@aoc.cat
Primer Apellido	de la Peça
Segundo Apellido	de Proves
DNI/NIE	00000000T

1.2. Nombre del documento e identificación

1.2.1. Identificación de este documento

Nombre:	Declaración de Prácticas de Certificación (DPC)
Versión:	6.0
Descripción	Declaración de Prácticas de Certificación del Consorci AOC
Fecha de emisión:	26/07/2018
OID:	1.3.6.1.4.1.15096.1.2.2
Localización:	https://www.aoc.cat/catcert/regulacio

1.2.2. Identificación de políticas de certificación cubiertas por esta DPC

Tipo de Certificado	OID	Política
Certificados de ciudadanía		
Certificado de ciudadano (idCAT)	1.3.6.1.4.1.15096.1.3.2.86.2	PC Ciudadano
Certificados personales del sector público		
Certificado de autenticación de trabajador público de nivel alto (T-CAT autenticació)	1.3.6.1.4.1.15096.1.3.2.7.1.2	PC Certificados Personales Sector Público
Certificado cualificado de firma de trabajador público de nivel alto (T-CAT signatura)	1. 3.6.1.4.1.15096.1.3.2.7.1.1	PC Certificados Personales Sector Público
Certificado cualificado de autenticación y firma de trabajador público de nivel medio/sustancial (T-CATP)	1.3.6.1.4.1.15096.1.3.2.7.3.1	PC Certificados Personales Sector Público
Certificado de autenticación de trabajador público con pseudónimo de nivel alto (T-CAT pseudònim autenticació)	1.3.6.1.4.1.15096.1.3.2.4.1.2	PC Certificados Personales Sector Público
Certificado cualificado de firma de trabajador público con pseudónimo de nivel alto (T-CAT pseudònim signatura)	1.3.6.1.4.1.15096.1.3.2.4.1.1	PC Certificados Personales Sector Público
Certificado cualificado de autenticación y firma de persona vinculada de nivel alto (T-CAT persona vinculada)	1.3.6.1.4.1.15096.1.3.2.82.1	PC Certificados Personales Sector Público
Certificado cualificado de autenticación y firma de persona vinculada de nivel medio/sustancial (T-CATP persona vinculada)	1.3.6.1.4.1.15096.1.3.2.86.1	PC Certificados Personales Sector Público
Certificado cualificado de autenticación y firma de representante ante las Administraciones Públicas (T-CAT representant)	1.3.6.1.4.1.15096.1.3.2.8.1.1	PC Certificados Personales Sector Público
Certificados de Dispositivos e Infraestructuras		
Certificado de Aplicación (Dispositiu aplicació)	1.3.6.1.4.1.15096.1.3.2.91.1	PC Dispositivos e Infraestructuras

Certificado de Sello Electrónico Avanzado (Segell nivell mig/substancial)	1.3.6.1.4.1.15096.1.3.2.6.2	PC Dispositivos e Infraestructuras
Certificado de Sede Electrónica (Seu-e nivell mig/substancial)	1.3.6.1.4.1.15096.1.3.2.5.2	PC Dispositivos e Infraestructuras
Certificado de Servidor Seguro (Dispositiu SSL)	1.3.6.1.4.1.15096.1.3.2.51.1	PC Dispositivos e Infraestructuras
Certificado de Servidor Seguro Extended Validation (Dispositiu SSL EV)	1.3.6.1.4.1.15096.1.3.2.51.2	PC Dispositivos e Infraestructuras
Certificado de Sello Cualificado de Tiempo (segell de temps)	1.3.6.1.4.1.15096.1.3.2.111	PC Dispositivos e Infraestructuras

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

1.3. Entidades participantes

1.3.1. Prestador de servicios de confianza

Conforme a la terminología del Reglamento 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, el Consorci AOC actúa en el marco de esta DPC como prestador de servicios de confianza o Trusted Services Provider (TSP), siendo responsable de la emisión y gestión de los certificados digitales generados dentro de la jerarquía de certificación (PKI) mencionada anteriormente en este documento.

1.3.2. Autoridad de Certificación Raíz

La Autoridad de Certificación Raíz es la entidad dentro de la citada jerarquía de certificación que emite certificados a otras autoridades de certificación y cuya clave pública ha sido autofirmada. Su función es firmar el certificado de otras Autoridades de Certificación pertenecientes a dicha jerarquía de certificación.

Los datos de identificación del Certificado Raíz de la jerarquía de certificación del Consorci AOC son los siguientes:

Root CA EC-ACC

CN:	EC-ACC
Hash:	88:49:7F:01:60:2F:31:54:24:6A:E2:8C:4D:5A:EF:10:F1:D8:7E:BB:76:62:6F:4A:E0:B7:F9:5B:A7:96:87:99

Vigencia:	07/01/2031
Tipo de clave:	RSA 2048

1.3.3. Autoridades de Certificación subordinadas

Se denomina Autoridades de Certificación Delegadas o Subordinadas a las entidades dentro de la jerarquía de certificación que emiten certificados de entidad final y cuyo certificado de clave pública ha sido firmado digitalmente por la Autoridad de Certificación Raíz.

Los datos de identificación de las Autoridades de Certificación subordinadas operadas por el Consorci AOC al amparo de esta DPC son los siguientes:

CA EC-CIUTADANIA

CN:	EC-Ciutadania
Hash:	0F:D9:9A:AE:1F:FC:D5:D9:F0:AD:76:ED:DD:CB:EF:6B:88:4C:C8:5C:16:BF:CF:A4:B5:24:61:55:D6:59:7E:D6
Vigencia:	18/9/2030
Tipo de clave:	RSA 2048

CA EC-SECTORPUBLIC

CN:	EC-SectorPublic
Hash:	35:6A:5F:4D:99:4E:9E:FA:7C:AE:FC:49:17:68:91:1D:65:EC:25:97:74:65:B6:10:E2:F2:9A:A4:47:26:31:C3
Vigencia:	18/9/2030
Tipo de clave:	RSA 2048

1.3.4. Autoridades de Registro

Las Autoridades de Registro son las personas físicas o jurídicas que asisten a las Autoridades de Certificación en determinados procedimientos y relaciones con los solicitantes y suscriptores de certificados, especialmente en 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 electrónicos. En concreto, se pueden distinguir los usuarios finales siguientes:

- Los solicitantes de certificados.

- Los suscriptores de certificados.
- Los firmantes o poseedores de claves.
- Tercero que confía en los certificados.

1.3.5.1. Solicitantes de certificados

Solicitante es la persona física que, en nombre propio o en representación de un tercero, solicita la emisión de un certificado digital.

Los requisitos que debe reunir un solicitante dependerán del tipo de certificado solicitado y están recogidos en la "Política de Certificación" aplicable a cada tipo de certificado concreto.

1.3.5.2. Suscriptores de certificados

El Suscriptor es la persona física o jurídica que contrata con el Consorci AOC la prestación de sus servicios.

En algunos casos el Suscriptor podrá actuar como Punto de Verificación Presencial, asumiendo parte de las funciones de registro y responsabilizándose en tal caso frente al Consorci AOC, a sus Autoridades de Registro y a los Usuarios finales de:

- La correcta identificación de los Solicitantes de certificados y Firmantes con respecto a los cuales actúe como Punto de Verificación Presencial.
- La veracidad y exactitud de toda la documentación requerida formalmente para cada clase de certificado.
- La compulsa de copias con respecto a la presentación de documentos originales.
- La custodia de dicha documentación y la entrega de la misma al Consorci AOC en caso de ser requerido para ello.
- La entrega de certificados a los firmantes o poseedores de claves

1.3.5.3. Poseedores de claves o firmantes

Los poseedores de claves o firmantes son las personas físicas que poseen de forma exclusiva las claves de firma o autenticación electrónicas de los certificados, ya sea actuando en su propio nombre y derecho, o bien, en representación de una organización o mediante algún otro tipo de vinculación.

Dichas personas físicas deberán estar debidamente identificadas en el certificado mediante su nombre y apellidos o mediante un pseudónimo, debiendo también identificarse, en su caso, la organización correspondiente de forma unívoca.

Corresponde al firmante o poseedor de claves la custodia de los datos de creación de firma asociados al certificado digital.

1.3.5.4. Tercero que confía en los certificados

Se entiende por tercero que confía en los certificados (en inglés, *relying party*) a toda persona u organización que voluntariamente confía en un certificado emitido bajo alguna de las jerarquías de certificación del Consorci AOC.

Las obligaciones y responsabilidades del Consorci AOC con terceros que voluntariamente confíen en los certificados se limitarán a las recogidas en esta DPC, en el Reglamento UE 910/2014 y en el resto de normativa que resulte de aplicación.

Los terceros que confíen en estos certificados deben tener presente las limitaciones en su uso.

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

Los certificados del Consorci AOC podrán usarse en los términos establecidos por las Políticas de Certificación correspondientes.

1.4.2. Usos prohibidos

Los certificados sólo se podrán utilizar dentro de los límites de uso recogidos de una manera expresa en esta DPC y en la correspondiente Política de Certificación. Cualquier otro uso fuera de los descritos en los mencionados documentos, queda excluido expresamente del ámbito contractual y prohibido formalmente. Queda expresamente prohibido cualquier uso que sea contrario a la Ley.

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.

Los certificados de usuario final no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados.

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

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: 900 90 50 90, o +34 93 272 25 01 para llamadas desde el exterior del estado, 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 PC con la DPC es el 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 del Consorcio AOC 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 del procedimiento de publicación de especificaciones de servicio.

La versión inicial de esta DPC 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, sobre el cual la Autoridad de Certificación no tenga control alguno, 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 la Autoridad de Certificación

La Autoridad de Certificación publica las informaciones siguientes en su web (http://www.aoc.cat/catcert/regulacio):

- Las listas de revocación de certificados y otras informaciones de estado de revocación de los certificados.
- Los perfiles de los certificados y de las listas de revocación de los certificados.
- La Declaración de Prácticas de Certificación.
- Las Políticas de Certificación aplicables a cada tipo de certificado.
- El texto divulgativo para certificados electrónicos.

Cualquier cambio en las especificaciones o en las condiciones del servicio se comunica a los usuarios por la Autoridad de Certificación a través del directorio.

En todos los casos se hace una referencia explícita a los cambios en la página web principal 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 Autoridad de Certificación 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 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 la Autoridad de Certificación, durante un periodo de 15 (quince) años, y las mismas pueden ser consultadas por los interesados.

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

2.4. Control de acceso

La DPC, las Políticas de Certificación, los Textos divulgativos (en inglés PDS: PKI Disclosure Statements), los certificados de CA y las listas de revocación de certificados (LRC) se publican en repositorios de acceso público sin control de acceso.

3. Identificación y autenticación

3.1. Gestión de nombre

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

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/regulacio).

3.1.1.2. Perfiles de los certificados

Los perfiles de los certificados emitidos se publican en la web del Consorci AOC (http://www.aoc.cat/catcert/regulacio).

3.1.2. Significado de los nombres

Sin estipulación adicional.

3.1.3. Utilización de pseudónimos

El posible uso de pseudónimos se regulará en la correspondiente Política de Certificación.

3.1.4. Interpretación de formatos de nombres

Sin estipulación adicional.

3.1.5. Unicidad de los nombres

La Autoridad de Certificación emite diferentes tipos de certificados. Los nombres de los suscriptores de certificados son únicos para cada servicio de generación de certificados operado por la Autoridad de Certificación y para cada tipo de certificado; es decir, una misma persona sólo puede tener a su nombre certificados de tipos diferentes emitidos por la Autoridad de Certificación. El atributo de CIF o NIF se usa para distinguir entre dos identidades cuando exista algún problema de duplicidad de nombres.

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

Todo el personal vinculado a la Autoridad de Registro tiene como requisito imprescindible la asistencia al curso de formación de Autoridades de Registro impartido por la Autoridad de Certificación.

3.1.6. Secuencia y frecuencia de rotación laboral

Sin estipulación adicional.

3.1.7. Resolución de conflictos relativos a nombres

El Consorci AOC no arbitrará ante posibles disputas de nombres ni tendrá responsabilidad al respecto. La asignación de nombres se realizará basándose en el orden de entrada.
En lo referente al tratamiento de marcas registradas, ver la sección 9.5.3.

3.2. Validación inicial de la identidad

3.2.1. Prueba de posesión de clave privada

Cuando se expide un certificado en un dispositivo hardware, la clave privada se crea en el instante previo a la generación del certificado, mediante un procedimiento que garantiza su confidencialidad y su vinculación con la identidad del solicitante.

Cada RA es responsable de garantizar la entrega o el acceso al dispositivo al solicitante de forma segura. En los otros casos, el método de prueba de la posesión de la clave privada por el suscriptor será la entrega de PKCS#10 o una prueba criptográfica equivalente u otro método aprobado por el Consorci AOC.

3.2.2. Autenticación de la identidad de una organización

La Autoridad de Registro deberá verificar los siguientes datos para poder autenticar la identidad de la organización:

- Los datos relativos a la denominación o razón social de la organización.
- Los datos relativos a la constitución, y personalidad jurídica del suscriptor.
- Los datos relativos a la extensión y vigencia de las facultades de representación del solicitante.
- Los datos relativos al código de identificación fiscal de la organización o código equivalente.

El Consorci AOC se reserva el derecho de no emitir el certificado si considera que la documentación aportada no es suficiente o adecuada para la comprobación de los datos anteriormente citados.

3.2.2.1. Autoridades de Registro

La Autoridad de Certificación autentica, previamente a la emisión y a la entrega de un certificado, para cualquiera de los componentes de una Autoridad de Registro, la identidad de la Autoridad de Registro y del operador conforme a la sección correspondiente de esta DPC.

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 Consorci AOC, 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 NIE 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, correo-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

La identificación de la persona física que haya de obtener un certificado cualificado (esto es, del poseedor de las claves) podrá realizarse:

- Mediante su presencia ante los encargados de verificar su identidad.
- Mediante el procedimiento que establece la normativa administrativa, cuando la personación se realice ante las Administraciones Públicas.

Antes de la emisión y entrega de un certificado cualificado, la Autoridad de Certificación - mediante la intervención de una Autoridad de Registro - tendrá que comprobar la identidad del poseedor de claves mediante la personación de éste.

El acto de personación puede diferirse al momento de entrega y aceptación del certificado, aprovechando para validar entonces la identidad de la persona que será poseedora de la clave privada correspondiente al certificado que se entrega.

Se podrá prescindir de la personación si la solicitud de expedición de un certificado, ha estado autenticada mediante el uso de un certificado electrónico de firma cualificada clasificado por el Consorci AOC, siempre que se encuentre vigente y no hayan transcurrido más de cinco años desde la identificación presencial.

Se podría prescindir de la personación si la firma contenida en la solicitud de expedición de un certificado ha estado legitimada notarialmente y en los casos previstos en el artículo 24 del Reglamento UE 910/2014. Pero esta DPC no da soporte a este mecanismo para la inexistencia de un procedimiento al efecto por parte de los notarios.

3.2.3.4. Vinculación de la persona física con la organización

Se regula de manera diferenciada en cada una de las Políticas de Certificación vigentes para cada tipo de Certificado.

3.2.4. Validación del dominio

Para garantizar que una entidad solicitante tiene control sobre el dominio (URL) que solicita incluir en un certificado se realizan dos tipos de comprobaciones:

- **Organizacionales**: se solicita la titularidad del nombre de dominio, certificada por un representante legal de la organización, además del nombre de la persona jurídica a la que se expide el certificado y, cuando proceda, el número de registro, tal como se recojan en los registros oficiales.

- **Técnicas**: se consultan los siguientes servicios whois autenticados:

    - Para dominios “*.es”: https://www.nic.es/sgnd/dominio/publicInformacionDominios.action

    - Para el resto de dominios:

      Consultar en http://www.iana.org/domains/root/db/ cuál es el servidor WHOIS autorizado para buscar información sobre el dominio, dependiendo del dominio de alto nivel (TLD), es decir, dependiendo de si el dominio acaba en .com, .org, .net, ...

- **Validación del registro del dominio**: se envía un correo electrònico a la dirección del registrante del dominio y/o a una dirección construida por “admin”, “administrador”, “webmaster”, “hostmaster” o “postmaster” seguido de @ y el nombre de dominio de autorización, con un número aleatorio único al que deben contestar en un plazo máximo de 30 días.

3.2.5. Información no verificada

La Autoridad de Certificación 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: La Autoridad de Certificación tendrá que comprobar – mediante la intervención de una Autoridad 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 3.2 sobre Validación 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

4.1. Solicitud de emisión de certificado

4.1.1. Legitimación para solicitar la emisión

Los requisitos que debe reunir un solicitante, dependerán del tipo de certificado solicitado y estarán recogidos en la Política de Certificación de cada tipo de certificado concreto.

4.1.2. Procedimiento de alta; Responsabilidades

La Autoridad de Certificación, 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, la Autoridad de Certificación 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 a la Autoridad de Certificación 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

Los requisitos que debe reunir una solicitud de certificación dependerán del tipo de certificado solicitado y estarán recogidos en la Política de Certificación de cada tipo de certificado concreto.

4.3. Emisión de certificado

4.3.1. Acciones de la Autoridad de Certificación durante el proceso de emisión

Para cada solicitud de certificado tramitada, la Autoridad de Certificación:

- 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 la Autoridad de Certificación.
- 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 en la sección 9.15, de conformidad con la ley aplicable.
- Cumple las obligaciones establecidas en 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. Comunicación de la emisión al suscriptor

La Autoridad de Certificación comunica al suscriptor, la emisión del certificado, o la incidencia correspondiente. Asimismo, 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 Confianza

La Autoridad de Certificación (o Prestador de Servicios de Confianza):

- 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 Autoridad de Certificación 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 del 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 DPC.
    - 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 del 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 poseedores 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

La renovación de un certificado se inicia dos meses antes de la fecha de expiración del mismo, 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.

El proceso para la renovación de un certificado es el mismo que se sigue para la emisión de nuevos certificados. Cuando se solicite la renovación de un certificado, la Autoridad de Registro Interna tendrá que verificar que los datos de registro continúen siendo válidas y, si ha cambiado algún dato, este deberá ser verificado. Se ha de guardar evidencia de esta comprobación, y el suscriptor ha de estar de acuerdo con la modificación, tal como se especifica en la sección correspondiente de esta DPC.

En cualquier caso, si han pasado más de cinco años desde la última vez que el suscriptor se identificó presencialmente en una oficina de Autoridad de Registro, tendrá que personarse de nuevo para llevar a cabo la renovación.

La Autoridad de Certificación informará al poseedor de claves de las condiciones jurídicas de prestación del servicio, tal como se hace en el proceso de emisión de nuevos certificados.

Para certificados individuales en soporte llavero, el suscriptor tendrá que personarse en las oficinas de la Autoridad de Registro, ya que las nuevas claves se generarán en este dispositivo.

4.8. Renovación telemática

La Autoridad de Certificación permite la renovación telemática de certificados digitales - a partir de una autenticación segura y la correspondiente firma electrónica de la hoja de entrega o de la solicitud de emisión del nuevo certificado (mediante la cual se acepta este), realizada con el certificado a renovar dentro de los dos últimos meses de vigencia - siempre que no hayan transcurrido más de cinco años desde la última vez que el poseedor de claves se identificó presencialmente en una oficina de Autoridad de Registro.

4.9. Modificación de certificados

La modificación de los datos de los certificados comporta la revocación y la emisión de un nuevo certificado. A todos los efectos, la modificación se considerará renovación.

Cuando el suscriptor de un certificado tenga conocimiento de cambios en la información obligatoria o la relativa a cargos, límites de uso o dispositivos usuarios de los certificados (p.ej direcciones IP o datos de servidores o aplicaciones); o cuando precise la modificación del resto de los datos incluidos en el certificado (dirección de correo electrónico, etc.), podrá gestionar la renovación del certificado vigente. En ciertos casos, en función de la información a modificar, esta revocación podrá hacerse en fecha posterior a la emisión del certificado con los datos actualizados.

La Autoridad de Registro requerirá la acreditación de las condiciones justificativas de la modificación.

4.10. Revocación y suspensión de certificados

4.10.1. Causas de revocación de certificados

La Autoridad de Certificación podrá revocar un certificado por la concurrencia de las siguientes causas:

1. Circunstancias que afectan la información contenida en el certificado
    - Modificación de alguno de los datos contenidos en el certificado.
    - Descubrimiento de que alguno de los datos aportados en la solicitud del certificado es incorrecta, así como la alteración o modificación de las circunstancias verificadas para la expedición del certificado.
    - Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.

2. Circunstancias que afectan a la seguridad de la clave o del certificado
    - Compromiso de la clave privada o de la infraestructura o sistema de la Autoridad de Certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de este incidente.
    - Infracción, por la Autoridad de Certificación, de los requisitos previstos en los procedimientos de gestión de certificados establecidos en la PC de la Autoridad de Certificación.
    - Compromiso o sospecha del compromiso de la seguridad de la clave o del certificado del poseedor de claves.
    - Acceso o utilización no autorizada por un tercero de la clave privada del poseedor de claves.
    - El uso irregular del certificado por el poseedor de claves, o falta de diligencia en la custodia de la clave privada.
3. Circunstancias que afecten a la seguridad del dispositivo criptográfico
    - Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
    - Pérdida o inutilización por daños del dispositivo criptográfico.
    - Acceso no autorizado por un tercero a los datos de activación del poseedor de claves.
4. Circunstancias que afectan al poseedor de claves.
    - Finalización de la relación entre la Autoridad de Certificación con el poseedor de claves.
    - Modificación o extinción de la relación jurídica subyacente o de la causa que motivó la emisión del certificado con el poseedor de claves.
    - Infracción por parte del solicitante del certificado, de los requisitos preestablecidos para su solicitud.
    - Infracción, por parte del poseedor de claves, de sus obligaciones, responsabilidad y garantías, establecidas en el instrumento jurídico correspondiente o en la Declaración de Prácticas de Certificación de la Autoridad de Certificación que le emitió el certificado o en las Políticas de Certificación asociadas.
    - La incapacidad sobrevenida o la muerte del poseedor de claves.
    - En caso de certificados corporativos, la extinción de la persona jurídica suscriptora del certificado, así como la finalización de la autorización del suscriptor al poseedor de claves, o la finalización de la relación entre el suscriptor y el poseedor de claves.
    - Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 3.4 de esta DPC.
5. Circunstancias relativas a los certificados Extended Validation:
    - Solicitud del suscriptor de revocación del certificado.

- La Autoridad de Certificación obtiene pruebas razonables de que la clave privada del suscriptor se ha visto comprometida o que el certificado ha sido usurpado por un tercero.
- La Autoridad de Certificación recibe notificación o comunicación por parte de un tribunal o árbitro sobre la revocación del derecho a utilizar el nombre de dominio que figura en el certificado o conoce la imposibilidad de renovar el dominio.
- La Autoridad de Certificación tiene conocimiento del incumplimiento del Texto Divulgativo para certificados electrónicos o de otras especificaciones establecidas en la documentación jurídica operativa.
- La Autoridad de Certificación cesa actividades que dan soporte a la revocación de certificados Extended Validation o pierde el derecho a emitir certificados Extended Validation. Si la Autoridad de Certificación puede garantizar el mantenimiento de los servicios de validación LRC y OCSP (protocolo de comprobación del estado de un certificado en línea, en inglés Online Certificate Status Protocol), la revocación no es necesaria.
- Compromiso o sospecha de compromiso de las claves de cualquier Autoridad de Certificación de nivel superior en la jerarquía.
- Revocación de las publicaciones de las políticas relativas a certificados Extended Validation.
- Notificación de la inclusión de un suscriptor en el listado de suscriptores prohibidos (también listas negras, confeccionadas para víctimas de phishing o actividades de ingeniería inversa)

6. Otras circunstancias
    - La suspensión del certificado digital para un periodo superior a 120 días.
    - La finalización del servicio de la Autoridad de Certificación.
    - La finalización de la prestación de servicio por parte de la Autoridad de Certificación.
    - Resolución judicial o administrativa que lo ordene.
    - La Autoridad de Certificación tiene conocimiento de que los certificados, en su caso, han realizado firmas sobre código hostil.

El instrumento jurídico que vincula a la Autoridad de Certificación con el suscriptor establecerá que el suscriptor tendrá que solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias indicadas anteriormente.

Si la Autoridad de Certificación no dispone de toda la información necesaria para determinar la revocación de un certificado, pero tiene indicios de su compromiso, puede decidir la suspensión.

4.10.2. Legitimación para solicitar la revocación

Podrán solicitar la revocación de un certificado:

- En caso de certificados individuales, el suscriptor a nombre del cual se emitió el certificado.
- En caso de certificados corporativos, la persona autorizada al efecto para la entidad suscriptora; en ocasiones, a instancia del poseedor de claves.
- La Autoridad de Registro que solicitó la emisión del certificado.

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 (bajo el criterio de la Autoridad de Certificación), por un lado, el certificado que se solicita revocar y, por otro, la autenticidad y autoridad del solicitante. El procedimiento detallado se encuentra disponible en la web del Consorci AOC.

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 realice la solicitud de revocación puede pedir a la Autoridad de Registro más información sobre este procedimiento.

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

Las Autoridades 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 Servicio de Atención al Usuario de la Autoridad de Certificación, el horario de atención del cual es 24x365. Los datos de contacto del Servicio de Atención al Usuario se describen en el punto "1.5.2. Datos de contacto de la organización".

La acción de revocación la lleva a cabo uno de los operadores de la Autoridad de Registro, quien accede a la aplicación web al efecto, autenticándose a través de un certificado digital emitido por la Autoridad de Certificación.

Una vez registrado el cambio de estado del certificado en el sistema de la Autoridad de Certificación, de forma automática y a la mayor brevedad posible, se genera y publica una nueva Lista de Revocación de Certificados (LRC) 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

Las solicitudes de revocación se han de remitir en la mayor brevedad posible, cuando se tenga conocimiento de la causa de revocación.

Fuera del horario de atención de las Autoridades de Registro, el suscriptor puede solicitar la suspensión cautelar del certificado a través del Servicio de Atención al usuario de la Autoridad de Certificación, según el procedimiento definido en la web del Consorci AOC.

4.10.5. Plazo máximo de procesamiento de la solicitud de revocación

Cuando una Autoridad de Registro o una Autoridad de Certificación reciban una solicitud de revocación, esta será procesada en el mínimo plazo posible, y siempre antes de 24 h desde la solicitud de la misma.

Antes de proceder a la revocación efectiva de un certificado, el destinatario de la solicitud ha de autenticarla de acuerdo con los requisitos establecidos en la sección correspondiente de esta DPC.

Cuando la solicitud de revocación haya sido remitida a una Autoridad de Registro, ésta podrá, una vez autenticada la solicitud, revocar directamente el certificado o remitir una solicitud en este sentido a la Autoridad de Certificación.

Se tendrá que informar sobre el cambio de estado del certificado que se ha revocado al poseedor de claves también. Cuando se trate de certificados corporativos, al suscriptor.

4.10.6. Obligación de consulta de información de revocación de certificados

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

Para verificar el estado de los certificados ha de consultarse la lista de revocación de certificados (LRC) vigente emitida por la Autoridad de Certificación que emitió este certificado, o bien consultar un servicio en línea que responda sobre el estado de certificados (Servicio OCSP u otros servicios de validación de certificados) operado por un prestador de servicios de validación en el que se confía.

Las Autoridades de Certificación que integran la jerarquía de certificación operada por el Consorci AOC, publican de manera gratuita la información sobre el estado de los certificados emitidos por ellas. Las URLs en las cuales se publica esta información (listas CRL y servicios OCSP) se indican entre el contenido de los certificados que emiten.

La Autoridad de Certificación 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)

El periodo de frecuencia de emisión de listas de revocación de certificados se determinará en la correspondiente de Política de Certificación aplicable a cada tipo de certificado.

4.10.8. Período máximo de publicación de LRCs

Una vez generadas, las nuevas versiones de las LRCs serán publicadas inmediatamente en la web del Consorci AOC y a las URLs indicadas entre el contenido de los certificados emitidos.

4.10.9. Disponibilidad de servicios de comprobación de estado de certificados

Los verificadores de certificados digitales pueden consultar el servicio en línea que responda sobre el estado de certificados (servicio *OCSP Responder*, de consulta de estado de certificados en línea, u otros servicios de validación de certificados), operado por un prestador de servicios de validación en el cual 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 Autoridades de Certificación que integran la jerarquía pública de certificación de Cataluña.

La URL en la cual se encuentra disponible este servicio se indica entre 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/regulacio

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

Los verificadores han de comprobar el estado de aquellos certificados en los que deseen confiar, si bien no se estipula obligación alguna referente al mecanismo utilizado para la comprobación de este estado.

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

El compromiso de la clave privada de una Autoridad de Certificación será comunicado, en la medida de lo posible, a todos los participantes en la jerarquía pública de certificación de Cataluña, como mínimo mediante la inclusión en la LRC correspondiente de la referencia al certificado digital de esta Autoridad de Certificación.

4.10.13. Causas de suspensión de certificados

La Autoridad de Certificación podrá suspender un certificado en los siguientes casos:

- En los casos legalmente previstos en la normativa sobre firma electrónica y servicios de confianza digital que resulte de aplicación y, en todo caso, cuando 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.
- Cuando la documentación requerida en la solicitud de revocación no sea suficiente, aún cuando se pueda identificar razonablemente al poseedor de claves.
- Cuando la documentación requerida en la solicitud de revocación no sea suficiente y tampoco permita identificar razonablemente al poseedor de claves.
- Cuando no se activa el certificado en un plazo de 120 días a partir de la fecha de emisión del certificado.
- Si se sospecha el compromiso de una clave, hasta que sea confirmado. En este caso, la Autoridad de Certificación ha de asegurarse de que el certificado no está suspendido durante más tiempo del necesario para confirmar su compromiso.

La suspensión está prohibida por los certificados de dispositivo siguientes, pudiendo ser sólo revocados:

- Certificado de Servidor Seguro (Dispositiu SSL)
- Certificado de Servidor Seguro Extended Validation (Dispositiu SSL EV)
- Certificado de Sede Electrónica (Seu-e nivell mig/substancial)

4.10.14. Efecto de la suspensión de certificados

Se considerará que las actuaciones realizadas durante el periodo de suspensión de un certificado no son válidas, siempre que el certificado finalmente sea revocado. Pero si se levanta la suspensión (habilitación) y el certificado vuelve a pasar a estado válido, las actuaciones realizadas durante el periodo de suspensión del certificado se considerarán válidas.

La suspensión es reversible en un plazo máximo de 120 días a contar desde la fecha de suspensión, transcurrido el cual, si no ha solicitado la posterior habilitación, pasará automáticamente a estado revocado.

Para llevar a cabo la habilitación de un certificado suspendido, el poseedor de la clave tendrá que personarse ante la Autoridad de Registro que aprobó la solicitud de emisión de este certificado y presentar el documento acreditativo de su identidad, para que esta pueda comprobarla.

Todo cambio de estado de un certificado (suspensión, habilitación, etc) se tendrá que informar al poseedor de claves y también, cuando se trate de certificados personales del sector público, al suscriptor.

4.10.15. Quién puede solicitar la suspensión

Podrán solicitar la suspensión de un certificado:

- En caso de certificados individuales: el poseedor de claves o la autoridad de registro que solicitó la emisión del certificado, actuando en su nombre.
- En caso de certificados corporativos: un representante autorizado por la entidad suscriptora, la autoridad de registro que solicitó la emisión del certificado, o el poseedor de claves.

4.10.16. Procedimientos de solicitud de suspensión

El procedimiento de suspensión se puede tramitar de las maneras que se detallan a continuación:

1. La suspensión puede ser solicitada por el poseedor de las claves, mediante llamada telefónica al Centro de Atención al Usuario de la Autoridad de Certificación.
2. Cuando se trate de certificados corporativos, la suspensión puede ser solicitada por la entidad suscriptora del certificado, mediante llamada telefónica al Centro de Atención al Usuario de la Autoridad de Certificación.
3. La suspensión puede ser solicitada por la Autoridad de Registro. En caso de que la Autoridad de Registro disponga de la autorización de la Autoridad de Certificación, puede realizar ella misma el proceso de suspensión. En caso contrario, realiza la tramitación de la suspensión a través de la Autoridad de Certificación.

Para iniciar la suspensión se requiere la siguiente información:

- Fecha y hora de la solicitud de la suspensión
- Nombre y apellidos del poseedor de claves a quien se le a de suspender el certificado digital.
- DNI del poseedor de claves a quien se le ha de suspender el certificado digital.
- Número de serie (serialNumber) del certificado digital que se solicita suspender.
- Razón detallada para la petición de suspensión.
- Código de suspensión asociado al certificado o, por defecto, pregunta y respuesta secreta escogida en el momento de activar el certificado.
- Cuando se trata de certificados corporativos:
    - Identidad del suscriptor que solicita la suspensión (en caso de que no sea el mismo poseedor).
    - Información de contacto de la Institución que solicita la suspensión.
    - Organismo y departamento al que está vinculado el poseedor de claves.

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 también que el plazo máximo será de 120 días.

4.10.17. Período máximo de suspensión

El plazo máximo de suspensión será de 120 días naturales.

4.10.18. Habilitación de un certificado suspendido

Para habilitar el certificado que se mantiene suspendido, el suscriptor podrá personarse e identificarse ante la Autoridad de Certificación, a través de la Autoridad de Registro que aprobó la solicitud del certificado y firmar el correspondiente documento de solicitud de habilitación para dejar constancia que se ha extinguido el motivo que provocó la suspensión.

4.10.19. Periodo de validez de los certificados

El periodo de validez será el que se indique en el propio certificado, con un máximo de 5 años.

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 la Autoridad de Certificación.

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*, de consulta de estado de certificados en línea, 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 Autoridades 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/regulacio.

Los sistemas de distribución de LRCs y de consulta en línea del estado de los certificados tendrán que estar disponibles las 24 horas de los 7 días de la semana.

En caso de fallo de los sistemas de comprobación de estado de certificados por causas ajenas a la Autoridad de Certificación, ésta tendrá que realizar sus mejores esfuerzos para asegurar que este servicio se mantiene inactivo el mínimo tiempo posible.

4.11.3. Otras funciones de los servicios

Sin estipulación adicional.

4.12. Finalización de la suscripción

La finalización de la suscripción no implicará la revocación de los certificados que hayan sido emitidos, sino que éstos podrán utilizarse hasta que expiren.

4.13. Depósito y recuperación de claves

4.13.1. Política y prácticas de depósito y recuperación de claves

La Posibilidad de que la Autoridad de Certificación o PSC ofrezca el servicio de depósito y recuperación de claves con respecto a una o varias categorías de certificados, deberá constar, en caso de que esta opción sea posible, en la correspondiente Política de Certificación. En la misma será necesario detallar, al menos, los siguientes aspectos:

a. Quién puede solicitar el depósito y la recuperación de claves
b. Cómo se tramitará la solicitud
c. Los requisitos de confirmación de solicitudes
d. Los mecanismos utilizados para depositar y recuperar claves

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

La Autoridad de Certificación asegura la aplicación y gestión adecuada de los procedimientos administrativos, de conformidad con los estándares reconocidos y, en particular:

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

b. Es responsable de 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. Establece las normas principales en materia de seguridad, mediante un órgano de alto nivel que define la política de seguridad de la información de la Autoridad y da la publicidad necesaria mediante acciones de comunicación interna.

d. 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 en el apartado anterior.

e. Documenta, implanta y mantiene 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, garantiza el mantenimiento del nivel necesario de la seguridad de la información.

5.1. Controles de seguridad física

5.1.1. Áreas seguras

La Autoridad de Certificación 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 el 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

La Autoridad de Certificación 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 antirrobos.
- Conformidad y entrada no autorizada.
- Recuperación del desastre.
- Salida no autorizada de equipamientos, informaciones, apoyos y aplicaciones relativos a componentes utilizados para los servicios de la Autoridad de Certificación.

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 les 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

La Autoridad de Certificación establece niveles de seguridad con restricción de acceso a los diferentes perímetros y barreras físicas definidas.

Para el acceso a las dependencias de la Autoridad de Certificación 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 la Autoridad de Certificación, 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 la Autoridad de Certificación 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

La Autoridad de Certificación 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 la Autoridad de Certificación cuentan con sistemas automáticos de detección y extinción de incendios.

En concreto, los dispositivos criptográficos y apoyos que almacenan claves de las Autoridades 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 uso de soportes extraíbles está minimizado y restringido únicamente al movimiento de archivos entre sistemas mediante dispositivos pendrive USB. Para garantizar tanto la integridad como la confidencialidad los soportes extraíbles se guardarán en una caja fuerte en la misma sala.

5.1.9. Tratamiento de residuos

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, ésta se somete a un tratamiento físico de destrucción.

5.1.10. Copia de seguridad fuera de las instalaciones

Se realizan copias de seguridad de los sistemas de información en dependencias físicamente separadas de aquellas en las cuales se encuentran los equipos.

Las copias de seguridad se harán online en el sistema de contingencia, un CPD alternativo, a través de comunicaciones cifradas.

5.2. Controles de procedimientos

La Autoridad de Certificación garantiza que sus sistemas se operan de forma segura y, por eso, establece e implementa procedimientos para las funciones que afectan la provisión de sus servicios.

El personal al servicio de la Autoridad de Certificación realiza los procedimientos administrativos y de gestión de acuerdo con la política de seguridad de la Autoridad de Certificación.

5.2.1. Funciones fiables

Las personas que ocupan estos lugares son nombradas formalmente por la alta dirección de la Autoridad de Certificación.

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.

Según lo especificado en las normas ETSI EN 319 401 y CEN/TS 419261, los roles mínimos establecidos son:

- Responsable de seguridad (Security Officer): Mantiene la responsabilidad global sobre la administración y la implementación de las políticas y procedimientos de seguridad.
- Operador de RA (Registration Officer): Responsables de aprobar, emitir suspender y revocar los certificados de Entidad final, así como las oportunas verificaciones en certificados de autenticación web.
- Responsable de revocación (Revocation Officers): Responsable de realizar los cambios en el estado de un certificado.
- Administradores del sistema de certificación (System Administrator): Autorizado para realizar cambios en la configuración del sistema, pero sin acceso a los datos del mismo.
- Operadores de sistemas (System Operators): Responsables de la gestión del día a día del sistema (Monitoreo, backup, recovery…)
- Auditor interno (System Auditors): Autorizado a acceder a los logs del sistema y verificar los procedimientos que se realizan sobre el mismo.
- Operador de CA - Operador de Certificación: Responsables de activar las claves de la CA en el entorno Online, o de los procesos de firma de certificados y LRC’s en el entorno Root Offline.

5.2.2. Nombre de personas por tarea

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

5.2.3. Identificación y autenticación para cada función

La Autoridad de Certificación identifica y autentica el personal antes de acceder a la correspondiente función fiable.

5.2.4. Roles que requieren separación de tareas

La Autoridad de Certificación identifica en su política de seguridad, funciones o roles fiables.

Las funciones fiables incluyen:

a. Oficial de Seguridad
b. Operador de registro
c. Administradores 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 descripciones de roles tendrán que realizarse teniendo en cuenta que ha de existir una separación de funciones sensibles, así como una concesión de mínimo privilegio, cuando sea posible. Para determinar la sensibilidad de la función, se tendrán en cuenta los siguientes elementos:

a. Deberes asociados a la función
b. Nivel de acceso
c. Monitorización de la función
d. Formación y concienciación
e. Habilidades requeridas

Las citadas restricciones se aplican en todo caso:

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

5.3. Controles de personal

La Autoridad de Certificación tiene en cuenta y vela porque el personal cumpla con los aspectos siguientes:

- Mantener 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.
- Ser 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 revelar información no pública fuera del ámbito de la infraestructura, ni se extraen apoyos de información a niveles de seguridad inferiores.
- Reportar al Responsable de Seguridad, cualquier incidente que se considere que afecta la seguridad de la infraestructura o limita la calidad del servicio.
- Utilizar los activos de la infraestructura para las finalidades que los han sido encomendadas.
- Exigir manuales o guías de usuario de los sistemas que utiliza, que permiten desarrollar su función correctamente.
- Exigir documentación escrita que marque sus funciones y las medidas de seguridad a que está sometido.
- El responsable de seguridad deberá velar porque el punto anterior sea ejecutado y provee los responsables de área de toda la información que fuera necesaria.
- No instalar, 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 acceder voluntariamente ni 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 la Autoridad de Certificación.
- el Responsable de Seguridad.
- el Responsable de Operaciones.
- el Equipo técnico de administración, operación y explotación.
- los Administradores de la Red y
- los Usuarios de la Autoridad de Certificación.

La Autoridad de Certificación, además, se ve afectada por el siguiente personal:

- quien hace las peticiones de los certificados.

- quien hace la aprobación y la validación de las peticiones de certificados.
- quien hace la generación / personalización de certificados.
- quien custodia las claves o los tokens criptográficos.
- quien custodia las claves o las combinaciones de seguridad de acceso a la sala de operaciones.
- quien 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

La Autoridad de Certificación 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 la Autoridad de Certificación, especialmente en relación con los procedimientos de personal de seguridad.

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

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

La Autoridad de Certificación 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 del entorno del 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.

Adicionalmente, la Autoridad de Certificación, proporciona a todo el personal involucrado en sus operaciones como Autoridad 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 las Autoridades de Registro tiene como requisito imprescindible la asistencia al curso de formación de Autoridades de Registro impartido por el Consorci AOC.

Se realizarán actualizaciones con una frecuencia anual, salvo por modificaciones en la DPC, que serán notificadas a medida que sean aprobadas.

5.3.4. Sanciones por acciones no autorizadas

La Autoridad de Certificación 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.

5.3.5. Requisitos de contratación de profesionales

La Autoridad de Certificación 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 Consorci AOC 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 de la Autoridad de Certificación.

5.3.6. Suministro de documentación al personal

La Autoridad de Certificación suministrará la documentación que necesite estrictamente su personal en cada momento, con el fin de que pueda desarrollar de forma competente sus funciones.

5.4. Procedimientos de auditoría de seguridad

5.4.1. Tipo de eventos registrados

La Autoridad de Certificación 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 Autoridad de Certificación.
- Los intentos no autorizados de acceso a los ficheros del sistema.
- La generación de las claves de la Autoridad de Certificación.
- Los intentos nulos de lectura y escritura en un certificado y en el directorio.
- Acontecimientos relacionados con el ciclo de vida del certificado, como una solicitud, una emisión, una revocación y una renovación de un certificado.
- Acontecimientos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de este.

La Autoridad de Certificación también conserva, 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 Autoridad de Certificación.
- 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 éstos no hayan 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 durante 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 de registro de auditoría diariamente y copias completas semanalmente.

Para conservar correctamente las copias de seguridad realizadas, la Autoridad de Certificación 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 Autoridad 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 Autoridad 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 la Autoridad de Certificación, 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, entre otras razones, por monitorizar las vulnerabilidades del sistema.

Se realizan análisis de vulnerabilidades internas, al menos trimestralmente y externas, al menos anualmente.

5.5. Archivo de informaciones

La Autoridad de Certificación 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

La Autoridad de Certificación guarda todos los acontecimientos que tengan lugar durante el ciclo de vida de un certificado, incluyendo la renovación de este.

La Autoridad de Certificación guarda un registro de lo siguiente:

- Tipo de documento presentado en la solicitud del certificado
- Número de identificación único proporcionado por el documento anterior
- Identidad de la Autoridad de Registro que acepta la solicitud del certificado
- La ubicación de las copias de solicitudes de certificado y del Acuerdo firmado por el suscriptor, en el caso de certificados individuales.

Asimismo, deberá conservar los siguientes 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

La Autoridad de Certificación guardará los registros especificados a la sección 5.5.1 de esta DPC durante, al menos, 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.

5.5.3. Protección del archivo

La Autoridad de Certificación asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas en los casos en que así se requiera.

Adicionalmente, la Autoridad de Certificación pondrá todos los medios a su alcance para garantizar la confidencialidad frente a terceros, durante el proceso de generación, de las claves privadas de firma digital que proporciona.

5.5.4. Procedimientos de copia de seguridad

Un técnico de comunicaciones de la Autoridad de Certificación 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 Autoridad de Registro.

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

También se realizan copias de seguridad de la aplicación KeyOne personalizada para la Autoridad de Certificación. Estas copias las guarda la Autoridad de Certificación en sus instalaciones.

5.5.5. Requisitos de sello de cautela de fecha y hora

La Autoridad de Certificación emite los certificados y las LRC con información de tiempo y hora.

5.5.6. Localización del sistema de archivo

La Autoridad de Certificación tiene un sistema de mantenimiento de datos de archivo fuera de sus propias instalaciones.

5.5.7. Procedimientos de obtención y verificación de información de archivo

Sólo las personas autorizadas por la Autoridad de Certificación tienen acceso a los datos de archivo, ya sea en las instalaciones de la Autoridad de Certificación, como en los archivos de las Autoridades de Registro.

5.6. Renovación de claves

Los certificados de la Autoridad de Certificación que se hayan renovado, se comunican a los usuarios finales, mediante su publicación en el directorio del Consorci AOC.

5.7. Compromiso de claves y recuperación de desastre

5.7.1. Procedimiento de gestión de incidencias y compromisos

La Autoridad de Certificación establece los procedimientos que aplican a la gestión de las incidencias que afectan sus claves y, muy especialmente, a los compromisos de la seguridad de las mismas.

5.7.2. Corrupción de recursos, aplicaciones o datos

Cuando tenga lugar un acontecimiento de corrupción de recursos, aplicaciones o datos, la Autoridad de Certificación inicia las gestiones necesarias, de conformidad con los documentos de 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 Entidad

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

En caso de compromiso, la Autoridad de Certificación, como mínimo:

- Informa todos los suscriptores y verificadores del compromiso.
- Indica que los certificados y la información del estado de revocación entregados usando la clave de la Autoridad de Certificación ya no son válidos.
- Revocar, en el plazo que se pacte con el supervisor nacional, los certificados emitidos por esta CA, aplicando, si procede, alguno de los procedimientos previstos en el Plan de Cese o en el Plan de Continuidad.

5.7.4. Desastre sobre las instalaciones

La Autoridad de Certificación 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 al Plan de Seguridad.

La Autoridad de Certificación 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 La Autoridad de Certificación 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 Autoridad de Certificación tienen las medidas de seguridad físicas especificadas en el Plan de Seguridad.

5.8. Finalización del servicio

5.8.1. La Autoridad de Certificación

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

Antes de acabar sus servicios la Autoridad de Certificación ejecuta, como mínimo, los procedimientos siguientes:

- Informa todos los suscriptores y verificadores (no se requiere que la Autoridad de Certificación tenga alguna relación anterior con terceras partes).
- Acaba las autorizaciones de subcontrataciones que actúen en nombre de la Autoridad de Certificación 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 la Autoridad de Certificación o las retira del uso.

La Autoridad de Certificación declara en su Plan de Cese, las previsiones que tiene que adoptar en caso de finalizar el servicio. Éstas incluyen:

- Notificación a las entidades afectadas con una antelación mínima de 2 meses a la finalización efectiva del servicio.
- El tratamiento del estado de revocación de los certificados emitidos que todavía no han expirado.

La Autoridad de Certificación transfiere los certificados, en los términos previstos en la legislación aplicable en materia de firma electrónica y servicios de confianza digital.

5.8.2. Autoridad de Registro

Sin estipulación adicional.

6. Controles de seguridad técnica

La Autoridad de Certificación 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 Autoridad de Certificación.

6.1.2. Envío de la clave privada al suscriptor

Para los certificados de firma cualificada y los certificados de nivel alto, la clave privada tendrá que ser entregada al poseedor de claves, debidamente protegida mediante una tarjeta inteligente, que cumpla lo establecido en un perfil de protección de dispositivo cualificado de creación de firma electrónica, o bien, almacenada según los términos de la sección 3.2.1. de la presente DPC. Adicionalmente, se tendrán que entregar al poseedor de claves, los mecanismos de acceso a la misma.

6.1.3. Envío de la clave pública al emisor del certificado

El método de envío de la clave pública a la Autoridad de Certificación es PKCS #10, otra prueba equivalente o cualquier otro método aprobado por el Consorci AOC.

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

La clave de la Autoridad de Certificación y las claves de las Autoridades de Certificación anteriores en la jerarquía pública de certificación de Cataluña se comunican a los verificadores, y así se asegura la integridad de la clave y se autentica el origen.

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

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 la Autoridad de Certificación se publica en la web del Consorci AOC: https://www.aoc.cat/catcert.

Los usuarios acceden al directorio para obtener las claves públicas de la Autoridad de Certificación.

6.1.5. Medidas de claves

Las claves de la Autoridad de Certificación son de 2.048 bits.
Las claves de todos los certificados emitidos por la Autoridad de Certificación son de 2.048 bits.

6.1.6. Generación de parámetros de clave pública

Sin estipulación adicional.

6.1.7. Comprobación de calidad 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 pares de claves de la Autoridad de Certificación son generados utilizando hardware criptográfico que cumple los requisitos establecidos por la especificación técnica CEN CWA 141617 o equivalente y de acuerdo con ITSEC, Common Criteria EAL 4+o FIPS 140-2 Nivel 3 o superior nivel de seguridad..

Los pares de claves de los suscriptores de certificados T-CAT de firma cualificada se tienen que generar en tarjetas inteligentes o en dispositivos criptográficos que cumplan los requisitos establecidos por las especificaciones técnicas CEN CWA 14169 y CWA 14170 o equivalente.

El par de claves de los suscriptores de certificados de firma y de certificados de nivel alto tendrán que generarse en tarjetas inteligentes o en dispositivos criptográficos que cumplan los requisitos establecidos en un perfil de protección de dispositivo cualificado de creación de firma electrónica.

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

6.1.9. Propósitos de uso de claves

El Consorci AOC 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 Autoridades de Certificación tendrán que protegerse utilizando un módulo criptográfico que cumpla los requisitos establecidos en un perfil de protección, de acuerdo con Common Criteria EAL 4+ o FIPS 140-2 Nivel 3 o superior nivel de seguridad.

Los pares de claves de los suscriptores de certificados de firma cualificada y de certificados de nivel alto serán protegidos mediante tarjetas inteligentes o en dispositivos criptográficos que cumplan los requisitos establecidos en un perfil de protección de dispositivo cualificado de creación de firma electrónica.

La protección de las claves privadas del resto de certificados podrá realizarse mediante aplicaciones informáticas.

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 Autoridad de Registro Colaboradora o Interna, o bien directamente por el Consorci AOC cuando actúa como Autoridad de Registro Virtual.

Por cada nueva emisión o renovación de los certificados se entrega una tarjeta nueva, es decir, no se cargan 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 entregará en una tarjeta nueva, sin coste adicional para el suscriptor.

6.2.2. Control para más de una persona sobre la clave privada

El acceso a las claves privadas de las Autoridades de Certificación off-line, tendrá que requerir necesariamente del concurso simultáneo de tres (3) dispositivos criptográficos protegidos por una clave de acceso, de entre cinco (5) dispositivos.

Cada uno de estos dispositivos es responsabilidad de una persona concreta, única conocedora de la clave de acceso al mismo. Ninguna persona conoce más de una de las claves de acceso. También se deposita ante Notario un sobre cerrado en el que el responsable de cada dispositivo ha escrito la clave de activación del dispositivo del cual es responsable. Estos sobres sólo pueden ser retirados de la custodia del Notario por el propio responsable o por otra persona debidamente autorizada por este (presentando autorización firmada por él).

Los dispositivos criptográficos quedan almacenados en las dependencias de la Autoridad de Certificación y para su acceso es necesaria una persona adicional.

6.2.3. Depósito de la clave privada

Las claves privadas de la Autoridad de Certificación se almacenan en espacios ignífugos y protegidos por controles de acceso físico doble.

6.2.4. Copia de seguridad de la clave privada

Las claves privadas de la Autoridad de Certificación 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 la Autoridad de Certificación tendrá que contar con una copia de seguridad realizada, almacenada y recuperada en su caso por personal sujeto a la política de confianza del personal. Este personal tiene que estar expresamente autorizado para estas finalidades.

Tendrá que mantenerse y utilizarse protegida por un dispositivo criptográfico que cumpla los requisitos establecidos en un perfil de protección, de acuerdo con Common Criteria EAL 4+, o FIPS 140-2 Nivel 3 o superior nivel de seguridad.

Cuando la clave privada de firma abandone estos tipos de dispositivos, tendrá que hacerlo de forma cifrada.

Los controles de seguridad a aplicar en las copias de apoyo de la Autoridad de Certificación tendrán que ser de igual o superior nivel a las que se aplican a las claves habitualmente en uso.

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

No se almacenarán copias de claves privadas de los certificados, excepto en casos de certificados sobre los que se prevea esta posibilidad conforme a lo establecido en la correspondiente Política de Certificación. Esta clave privada podrá estar almacenada para garantizar la recuperación de datos.

6.2.6. Introducción de la clave privada en el módulo criptográfico

Las claves privadas de la Autoridad de Certificación 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. Almacenamiento 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 las claves privadas de la Autoridad de Certificación.

Para certificados T-CAT en tarjeta, la clave privada del suscriptor se activa mediante la introducción del PIN en la tarjeta inteligente o dispositivo criptográfico.

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

Para certificados personales, la clave privada del suscriptor se activará mediante la introducción del PIN en la tarjeta inteligente o de los datos de activación exigidos para el dispositivo criptográfico o sistema de almacenamiento.

6.2.9. Método de desactivación de la clave privada

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

Para certificados personales que incluyan la política básica de firma cualificada, cuando la tarjeta inteligente se retire del dispositivo lector, o la aplicación que la utilice finalice la sesión, será necesario introducir nuevamente los datos de activación anteriormente indicadas.

Para certificados personales que incluyan la política básica de firma avanzada, cuando la aplicación que utilice el certificado finalice la sesión, será necesario introducir nuevamente los datos de activación de firma (PIN).

6.2.10. Método 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 la Autoridad de Certificación obtienen o superan el nivel EAL 4 de Common Criteria (ISO 15408) con los aumentos que se determinan en la especificación técnica CEN CWA 14167.

Los módulos de la Autoridad de Certificación tienen que encontrarse certificados con el nivel y los aumentos previstos en un perfil de protección, de acuerdo con Common Criteria EAL 4+, o FIPS 140-2 Nivel 3.

Los módulos de los suscriptores de certificados T-CAT en tarjeta 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.

Los módulos de los suscriptores de certificados de firma electrónica reconocida y de certificados de nivel alto tienen que encontrarse certificados con el nivel y aumentos

previstos en un perfil de protección de dispositivo cualificado de creación de firma electrónica.

6.3. Otros aspectos de gestión del par de claves

6.3.1. Archivo de la clave pública

La Autoridad de Certificación archiva sus claves públicas de acuerdo con lo establecido en la sección 5.5.

6.3.2. Períodos de utilización de las claves públicas 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 se puede continuar utilizando hasta después de la expiración del certificado.

6.4. Datos de activación

6.4.1. Generación e instalación de las claves de activación

Si la Autoridad de Certificación facilita al suscriptor un dispositivo cualificado de creación de firma, los datos de activación del dispositivo tendrán que ser generados de forma segura por la Autoridad de Certificación.

6.4.2. Protección de los datos de activación

Para proteger al máximo los datos de activación, la Autoridad de Certificación se encarga de distribuir los elementos de los certificados por dos canales diferentes.

- En primer lugar, el responsable de la Autoridad 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:

- La Autoridad de Certificación 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 Autoridad de Certificación garantiza que el acceso a los sistemas de información y aplicaciones se restringe según 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 Autoridad de Certificación, 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 Autoridad de Certificación se identifica y reconoce antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del certificado.
- El personal de la Autoridad de Certificación 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 la Autoridad de Certificación (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 informáticas de la Autoridad de Certificación y de la Autoridad de Registro son fiables, de acuerdo con las especificaciones técnicas CEN CWA 14167-1 y EN 319 411-2., 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 utilizado 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

La Autoridad de Certificación 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

La Autoridad de Certificación tendrá que mantener un inventario de todos los activos informáticos y realizará 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 auditará de forma periódica, de acuerdo con aquello establecido en la sección correspondiente de esta DPC.

Se realizará un seguimiento de las necesidades de capacidad y se planificarán procedimientos para garantizar suficiente disponibilidad electrónica y de almacenamiento 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 en las diferentes redes de la Autoridad de Certificación 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 las Autoridades de Certificación.

- 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 revocación de certificados

7.1. Perfil de certificado

Los documentos descriptivos de los varios perfiles de certificados digitales que expide la Autoridad de Certificación se publican en la web del Consorci AOC.

Los certificados emitidos por el Consorci AOC y las Autoridades de Certificación adscritas a la jerarquía pública de certificación de Cataluña, tendrán el contenido y los campos descritos en el documento "perfil de certificado" correspondiente, que el Consorci AOC publica en su web.

En todo caso, el perfil de cada certificado incluirá en su estructura, como mínimo, los siguientes datos:

a. Número de serie, que será un código único respecto al nombre distinguido del emisor.
b. Algoritmo de firma, con alguno de los algoritmos identificados en la sección correspondiente de esta DPC.
c. El nombre distinguido del emisor, de acuerdo con la sección correspondiente de esta DPC.
d. Inicio de validez del certificado, en Tiempo Coordinado Universal, codificado conforme al RFC 6818.
e. Fin de validez del certificado, en Tiempo Coordinado Universal, codificado conforme al RFC 6818.
f. Nombre distinguido del sujeto, de acuerdo con la sección correspondiente de esta DPC.
g. Clave pública del sujeto, codificada de acuerdo con el RFC 6818.
h. Firma generada y codificada, de acuerdo con la RFC 6818.

Los certificados serán conformes con las siguientes normas:

1. RFC 6818: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008.
2. ITU-T Recommendation X.509 (1997): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework, June 1997.
3. L'especificació "*Perfiles de Certificados Electrónicos*" elaborada per la *Dirección de Tecnologías de la Información y las Comunicaciones* (DTIC) del *Ministerio de Hacienda y Administraciones Públicas* (MINHAP).

Adicionalmente, los certificados de firma cualificada serán conformes con las siguientes normas:

1. ETSI EN 319 412, partes 1, 2 y 5, en su versión vigente en el momento de la publicación de esta DPC.
2. La especificación "Perfiles de Certificados Electrónicos" elaborada por la Dirección de Tecnologías de la Información y las Comunicaciones (DTIC) del Ministerio de Hacienda y Administraciones Públicas (MINHAP).

3. RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, 2001 (siempre que no entre en conflicto con las anteriores TS 101 862).

Asimismo, los certificados cualificados tendrán que contener los siguientes campos:

a. La indicación que se expiden como certificados cualificados.
b. El código identificativo único del certificado.
c. La identificación del prestador de servicios de certificación que expide el certificado, indicando el nombre o razón social, domicilio, dirección electrónica y número de identificación fiscal.
d. La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
e. La identificación del firmante (el suscriptor, en caso de certificados individuales, o del poseedor de claves, en caso de certificados de organización), por su nombre y apellidos y DNI o equivalente, o a través de un pseudónimo que conste de manera inequívoca.
f. Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.
g. Los límites de uso del certificado, si se prevén.
h. Los límites del valor de las transacciones para las cuales puede utilizarse el certificado, si se establecen.

7.1.1. Número de versión

Todos los certificados contendrán un campo con el número de versión, indicando que se trata de certificados de versión 3.

7.1.2. Extensiones de certificado

Las extensiones 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.

7.1.3. Identificadores de objeto de algoritmos

La Autoridad de Certificación podrá utilizar el siguiente algoritmo de firma:

- sha256WithRSAEncryption OID = {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

7.1.4. Formatos de nombre

La Autoridad de Certificación rellenará los campos de nombres de los certificados con las informaciones establecidas en el perfil correspondiente de certificado, publicado en la web.

7.1.5. Restricciones de nombres

Sin estipulación adicional.

7.1.6. Identificador de objeto de política de certificado

La Autoridad de Certificación rellenará la extensión política del certificado con los identificadores de objeto establecidos en la sección correspondiente de esta DPC, cuando se adhieren directamente a ella misma.

En caso de crear su propia política, en los casos permitidos por esta DPC, incluirá el identificador del objeto específicamente definido al efecto.

7.1.7. Uso de la extensión restricciones de política

Sin estipulación adicional.

7.1.8. Sintaxis y semántica de los cualificadores de política

La Autoridad de Certificación incluirá en los certificados un cualificador de política, con los siguientes elementos:

- CPS Pointer
- Explicit Text

CPS Pointer tendrá que incluir una referencia URI en las condiciones generales de verificación de los certificados emitidos por la Autoridad de Certificación.

Explicit Text tendrá que contener una declaración concisa relativa al certificado.

7.1.9. Semántica del proceso de la extensión crítica de la política de certificado

Sin estipulación adicional.

7.1.10. Especificaciones técnicas para todas las Autoridades de Certificación

Las Autoridades de Certificación tienen que respetar los usos tecnológicos generalmente aceptados y tienen que adaptarse a buenas prácticas y a los requisitos técnicos más avanzados.

Adicionalmente, la renovación de las Autoridades de Certificación inmediatamente posterior a la presente versión de la Declaración de Prácticas de Certificación, respetará las siguientes especificaciones técnicas:

- El algoritmo utilizado tiene que ser renovado cuando exista un riesgo de desencriptación advertido por la comunidad. Las Autoridades de Certificación incorporarán, posteriormente a la emisión de esta Declaración de Prácticas de Certificación, el algoritmo SHA-256.
- Los números de serie de los certificados siempre serán enteros y, en todo caso, positivos.
- Se utilizará la codificación UTF-8.
- Se simplificará la extensión “authorityKeyIdentifier”.

- Se restringirán los OIDs generados por las Autoridades de Certificación intermedias.

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

8. Auditoría de conformidad

La Autoridad de Certificación 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.

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

La Autoridad de Certificación tiene que realizar periódicamente una auditoría de conformidad para probar que cumple, una vez ha empezado a funcionar, los requisitos de seguridad y de operación necesarios para formar parte de la jerarquía pública de certificación de Cataluña.

La Autoridad de Certificación tiene que estar preparada para pasar otras revisiones, no periódicas, que demuestren su confianza:

- Antes de aceptar una nueva Autoridad de Certificación subordinada a la jerarquía, el Consorci AOC tiene que realizar una revisión de sus documentos de seguridad y DPC y PCs para asegurar que cumple los requisitos de seguridad y de operación necesarios para formar parte de la Jerarquía de Autoridades de Certificación del Consorci AOC.
- Si en cualquier momento se sospecha que la Autoridad de Certificación, una vez ha empezado a funcionar, no cumple alguno de los requisitos de seguridad, o si se ha detectado un compromiso de claves -ya sea una sospecha o compromiso real - o cualquier acontecimiento que pueda suponer un peligro para la seguridad o integridad de la Autoridad de Certificación, se llevará a cabo una auditoría interna.

La Autoridad de Certificación puede delegar la ejecución de las auditorías a una tercera entidad, y tiene que cooperar completamente con el personal que lleve a cabo la investigación.

8.1. Frecuencia de la auditoría de conformidad

La Autoridad de Certificación tiene que llevar a cabo una auditoría de conformidad anualmente, además de las auditorías internas que puedan llevar a cabo bajo su propio criterio o en cualquier momento, cuando exista alguna sospecha de incumplimiento de alguna medida de seguridad, o por un compromiso de claves.

8.2. Identificación y calificación del auditor

La Autoridad de Certificación deberá acudir 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 Autoridad de Certificación.

8.4. Relación de elementos objeto de auditoría

Los elementos objeto de auditoría serán los siguientes:

- Proceso de Autoridades de certificación y elementos relacionados
- Sistemas de información
- Protección del centro de proceso
- Documentos

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, la Autoridad de Certificación discute, con la entidad que ha ejecutado la auditoría y con el Consorci AOC, las deficiencias encontradas y desarrolla y ejecuta un plan correctivo que las soluciona.

Si la Autoridad de Certificación, una vez auditado, es incapaz de desarrollar y/o ejecutar el mencionado plan 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 la CA, tal como se describe a la sección 4.9 de esta DPC.
- Acabar el servicio de la CA, 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 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. Importes

9.1.1. Importe de emisión y renovación de certificados

El Consorci AOC establece los importes que aplica la Autoridad de Certificación en la prestación de sus servicios. Los importes se pueden consultar en la web del servicio de certificación digital del Consorci AOC.

9.1.2. Importe de acceso a certificados

No se puede establecer un importe por el acceso a los certificados.

9.1.3. Importe de acceso a información de estado de certificado

No se puede establecer un importe por el acceso a la información de estado de los certificados.

9.1.4. Importes de 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 en la normativa aplicable de firma electrónica y servicios de confianza. Este seguro cubre las actuaciones del Consorci AOC como Prestador de servicios de certificación.

En caso de uso incorrecto o no autorizado de los certificados, el Consorci AOC (o la Autoridad de Certificación correspondiente) 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 la Autoridad de Certificación correspondiente).

9.2.2. Otros activos

Sin estipulación adicional.

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

En caso de uso incorrecto o no autorizado de los certificados, la Autoridad de Certificación 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 la Autoridad de Certificación).

9.3. Confidencialidad

9.3.1. Informaciones confidenciales

Las informaciones siguientes se mantienen de forma confidencial por la Autoridad de Certificación:

a. Información de negocio suministrada por sus proveedores y otras personas con quienes el Consorci AOC o la Autoridad de Certificación 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 Autoridad de Certificación y sus auditores.

d. Planes de continuidad de negocio y de emergencia.

e. Política y planes de seguridad.

f. Documentación de operaciones, como por ejemplo, el archivo, la monitorización y otras operaciones análogas.

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 y las Políticas de Certificación del Consorci AOC.
- La información contenida en los certificados
- Cualquier información cuya publicidad sea impuesta normativamente
- Cualquier otra información identificada como “Pública”.

9.3.3. Responsabilidad para la protección de información confidencial

La Autoridad de Certificación es responsable del establecimiento de las medidas apropiadas de protección de la información confidencial.

Estas medidas incluyen las cláusulas apropiadas de información confidencial a las que estarán sometidas todas las personas involucradas en los procesos de certificación que correspondan.

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 normativa aplicable de protección de datos.

La estructura de los tratamientos 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, dirección 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 los 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.

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, se detallan los requisitos y obligaciones en relación con la obtención y gestión de los datos personales.

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.

9.4.2. Datos de carácter personal no disponibles a terceros

Los datos de carácter personal que tengan que ser incluidos en los certificados y los mecanismos indicados de comprobación del estado de los certificados son considerados datos de carácter público. En este sentido, no serán considerados 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 Autoridad de Certificación.
- Cualquier otro dato de carácter personal que no sea susceptible de consulta, almacenamiento o acceso por terceros.

9.4.3. Datos de carácter personal disponibles a terceros

Los “datos de carácter personal”, se refieren a toda información personal que se incluye en los certificados y el referido mecanismo de comprobación del estado de los certificados, de acuerdo con la sección 3.1 de este documento.

La mencionada información, proporcionada durante la solicitud de certificados en los términos que se prevén en la legislación aplicable, es incluida en sus certificados y el 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 Autoridad 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 en el 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.

j. La información contenida en la parte pública del Registro de la Autoridad 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 la sección 9.15 Conformidad 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 Autoridad de Certificación, en sus instalaciones, comunica inmediatamente por teléfono con el Responsable de la Autoridad 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 de la Autoridad de Certificación o el responsable técnico del proyecto afectado (en este caso, con copia del mensaje al Responsable de la Autoridad 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 Autoridad 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 Autoridad 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 Autoridad de Certificación, protegido convenientemente para que sólo pueda acceder el personal autorizado; así queda garantizado que se hacen copias de seguridad de su contenido.

En el 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 comportan tratamiento de datos personales.

En la expedición de ciertos certificados, estos datos son comunicados por los suscriptores, sin necesidad de consentimiento de los afectados poseedores de claves, de acuerdo con lo establecido por la normativa reguladora de la relación del personal al servicio del suscriptor del certificado u otra normativa que resulte aplicable.

El Consorci AOC informa a los poseedores de claves de la obtención de sus datos personales.

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 obligado 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 en la normativa aplicable de protección de datos de carácter personal.

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

Excepcionalmente, en caso de cese de su actividad por parte de la Autoridad de Certificación, el Consorci AOC cederá los datos personales para el supuesto de transferencia de prestación del servicio.

9.5. Derechos de propiedad

9.5.1. Propiedad de los certificados e información de revocación

El Consorci AOC es la única entidad que disfruta de los derechos de propiedad sobre los certificados que emite.

El Consorci AOC 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 El Consorci AOC y la parte que reproduzca y/o distribuya el certificado.

Las normas anteriores figuran en los instrumentos jurídicos que existen entre El Consorci AOC y los suscriptores y los verificadores.

Adicionalmente, los certificados emitidos por El Consorci AOC 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 sobre la política de certificación de la jerarquía pública de certificación de Cataluña.

El Consorci AOC es propietario 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 a la marca, producto o nombre comercial contenido en el certificado.

El suscriptor (o el poseedor de claves, si procede) es el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en 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. La Autoridad de Certificación

9.6.1.1. Obligaciones y otros compromisos

La Autoridad de Certificación se obliga a cumplir lo siguiente:

- Determina la comunidad de suscriptores y verificadores de la Autoridad de Certificación.
- Aprueba las políticas de certificación y, si procede, las políticas específicas de certificación.
- Aprueba, si procede, la documentación contractual y reguladora de los servicios de certificación en la comunidad de usuarios de la Autoridad de Certificación, 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 en la sección 9.15
- De conformidad con la ley aplicable, antes de la emisión y entrega del certificado, la Autoridad de Certificación informa de los aspectos previstos en 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 la Autoridad de Certificación.
    - La Autoridad de Certificación 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.
- La Autoridad de Certificación 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 en el 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 a terceros, en caso de final de operaciones de la Autoridad de Certificación 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 la Autoridad de Certificación acepta o excluye su responsabilidad.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.

La Autoridad de Certificación identifica al poseedor de claves, de acuerdo con la legislación aplicable y esta DPC. Especialmente, la Autoridad de Certificación 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

La Autoridad de Certificación garantiza al suscriptor, como mínimo:

a. El cumplimiento de sus obligaciones legales como Prestador de servicios de certificación, de acuerdo con la legislación aplicable.
b. Que no hay errores en las informaciones contenidas en 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.
c. Que los certificados cumplen todos los requisitos materiales establecidos en la DPC.
d. Que los servicios de revocación y el uso del directorio cumplen todos los requisitos materiales establecidos en la DPC.
e. Que, en caso de que haya generado las claves privadas, se mantiene la confidencialidad durante el proceso.
f. La responsabilidad de la Autoridad de Certificación, con los límites que se establezcan.

9.6.1.2.2. Garantías ofrecidas a los verificadores

La Autoridad de Certificación 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 lo contrario.

c. En caso de certificados publicados en el 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.

i. La responsabilidad de la Autoridad de Certificación, con los límites que se establezcan.

9.6.2. Autoridades de Registro

9.6.2.1. Obligaciones y otros compromisos

9.6.2.1.1. Obligaciones de las Autoridades de Registro Internas

La Autoridad de Registro Interna se obligará a cumplir lo siguiente:

a. Nombrar como operadores de la autoridad (técnica) de registro a dos o más de sus trabajadores (dependiendo del EC, generalmente cuatro o más) y comunicar al Consorci AOC los datos correspondientes a estas personas para la emisión de los certificados de operador correspondientes. Cuando un operador deje de tener capacidad para actuar como lo que es, bajo el control y la autoridad de la Autoridad de Registro Interna, esta Autoridad de Registro Interna tiene que solicitar de forma inmediata a la Autoridad de Certificación la revocación del certificado de operador correspondiente

b. Validar y aprobar las solicitudes de certificados y generar los certificados para los poseedores de claves, de acuerdo con los procedimientos e instrumentos técnicos establecidos por la Autoridad de Certificación, de acuerdo con la DPC y la documentación de operaciones de la Autoridad de Certificación

c. Si la Autoridad de Registro Interna no dispusiera de información actualizada del poseedor de claves, comprobar la identidad personalmente o de acuerdo con aquello establecido en la legislación aplicable, descrita en el apartado 9.15 Conformidad con la Ley aplicable, y registrar un justificante acreditativo del nombre completo, lugar y fecha de nacimiento, DNI y/o cualquier otra información que pudiera ser utilizada para diferenciar a una persona de otra en el ámbito de la Autoridad de Registro Interna

d. Verificar, cuando sea necesario, cualquier atributo específico del poseedor de claves y registrar un justificante acreditativo de la información

e. Realizar o tramitar las solicitudes de suspensión, habilitación, revocación y renovación de certificados, de acuerdo con los procedimientos y los instrumentos técnicos establecidos por la Autoridad de Certificación, de acuerdo con la Declaración de Prácticas de certificación y la documentación de operaciones de la Autoridad de Certificación

f. Almacenar los registros, ya sea en papel, ya sea de forma electrónica, con las adecuadas medidas de seguridad, autenticidad, integridad y conservación, relativos a la información contenida en el certificado, durante un periodo de 15 años. Estos registros tienen que estar a disposición de la Autoridad de Certificación

g. Almacenar las hojas de entrega de certificado durante un periodo de 15 años. Estos registros tienen que estar a disposición de la Autoridad de Certificación

9.6.2.1.2. Autoridad de Registro Virtual

La Autoridad de Registro Virtual se obligará a cumplir lo siguiente:

a. Aportar la justificación documental necesaria para el registro de usuarios y para la posterior emisión de certificados por parte de la Autoridad de Certificación o la Autoridad de Registro Colaboradora.

b. La justificación documental tendrá que ser realizada por una unidad orgánica de la Autoridad de Registro Virtual facultada legalmente para dar fe de los datos a certificar, que se indicará al Consorci AOC.

9.6.2.1.3. Autoridad de Registro Colaboradora

La Autoridad de Certificación podrá delegar algunas funciones a Autoridades de Registro Colaboradoras, que en este caso quedarán obligadas a su cumplimiento, en iguales condiciones que la Autoridad de Certificación.

La Autoridad de Registro Colaboradora asistirá a los suscriptores de certificados emitidos a LAS INSTITUCIONES con Autoridad de Registro Virtual, y a todos los suscriptores del resto de certificados.

La Autoridad de Registro Colaboradora actuará en su propio nombre, sin perjuicio de la responsabilidad de la Autoridad de Certificación.

La Autoridad de Registro Colaboradora 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 cual se realizarán 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 tienen que incluir la justificación documental aportada por el solicitante y, si la Autoridad de Registro Colaboradora lo considerara necesario, cualquier

otro documento e información relevante, facilitados por el suscriptor, por el poseedor de claves o por terceras personas.

Si la Autoridad de Registro Colaboradora detectara errores en los datos que tienen que ser incluidos en los certificados, o en los documentos que justificaran estos datos, estará 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 supuesto de que la Autoridad de Registro Colaboradora corrija los datos sin gestión previa de la incidencia correspondiente con el suscriptor, quedará obligada a notificar los datos que finalmente se certifiquen al suscriptor en el momento de la entrega.

La Autoridad de Registro Colaboradora 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, y si fuera necesario, del poseedor de claves.

9.6.2.2. Garantías ofrecidas a suscriptor y verificadores

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

El Consorci AOC garantiza que la clave privada de la Autoridad de Certificación utilizada para emitir certificados no ha sido comprometida, salvo que el Consorci AOC hubiera comunicado lo contrario, de conformidad con esta DPC.

El Consorci AOC únicamente garantiza que:

a. Los certificados de firma electrónica contienen toda la información exigida por la Ley aplicable, que se describe en la sección 9.15.

b. No ha originado ni ha introducido declaraciones falsas o erróneas en la información de ningún certificado, ni ha dejado de incluir información necesaria aportada por el suscriptor y validada por el Consorci AOC o por la Autoridad de Registro colaboradora, en el momento de la emisión del certificado.

c. Todos los certificados cumplen los requisitos formales y de contenido de su Política de Certificación y Perfil de Certificado correspondiente.

d. Queda vinculada por los procedimientos operativos, de seguridad y de archivo descritos en la Declaración de prácticas de certificación

9.6.2.2.2. Exclusión de la garantía

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

9.6.3. Suscriptores

9.6.3.1. Obligaciones y otros compromisos

9.6.3.1.1. Requisitos para todos los tipos de certificados

La Autoridad de Certificación obliga al suscriptor de los certificados a:

a. Facilitar a la Autoridad de Certificación la información completa y adecuada conforme a los requisitos de esta DPC, en especial, en aquello 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 en la legislación vigente descrita a la sección 9.15 de esta DPC.

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

e. Notificar a la Autoridad de Certificación, 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 la Autoridad de Certificación 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 en la sección correspondiente.

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

i. No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de la jerarquía pública de certificación de Cataluña sin permiso previo por escrito.

j. No comprometer intencionadamente la seguridad de la jerarquía pública de certificación de Cataluña.

9.6.3.1.2. Requisitos específicos para los certificados de firma electrónica cualificada

La Autoridad de Certificación obligará al suscriptor a:

a. Utilizar el par de claves exclusivamente para firmas electrónicas y conforme a cualquier otra limitación que le sea notificada

b. Ser especialmente diligente en la custodia de su clave privada y de su dispositivo cualificado de creación de firma, con el fin de evitar usos no autorizados

c. Si el suscriptor genera sus propias claves, se obliga a:

    1. Generar sus claves de suscriptor utilizando un algoritmo reconocido como aceptable para la firma electrónica reconocida

    2. Crear las claves dentro del dispositivo cualificado de creación de firma

    3. Utilizar longitudes y algoritmos de clave reconocidos como aceptables para la firma electrónica reconocida

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

9.6.3.2. Garantías ofrecidas por el suscriptor

La Autoridad de Certificación obliga al suscriptor, mediante el correspondiente instrumento jurídico, a garantizar que:

a. Todas las manifestaciones realizadas en la solicitud son correctas.
b. Todas las informaciones suministradas por el suscriptor que se encuentren contenidas en el 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 Autoridad de Certificación y no utiliza la clave privada correspondiente a la clave pública listada en el certificado para firmar ningún certificado (o cualquiera otro formato de clave pública certificada) ni LRC.
f. Ninguna persona no autorizada ha tenido acceso jamás a la clave privada del suscriptor.

9.6.3.3. Protección de la clave privada

La Autoridad de Certificación 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

La Autoridad de Certificación 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 monitorizar, manipular o realizar actos 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 dispositivos cualificados de firma electrónica son firmas electrónicas equivalentes a firmas manuscritas, de acuerdo con el artículo 25.2 del Reglamento (UE) 910/2014..

9.6.4.2. Garantías ofrecidas por el verificador

La Autoridad de Certificación 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 en el 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 se obliga a operar las Autoridades de Certificación a su cargo, incluyendo la Autoridad 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.

9.6.5.2. Garantías ofrecidas a los suscriptores

El Consorci AOC garantiza que la clave privada de las Autoridades de Certificación a su cargo 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 la Autoridad de Certificación y validada por el Consorci AOC o la Autoridad de Registro, en el momento de emisión de los certificados.

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

c. 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 en 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 utilizar de forma diferente ninguna firma digital o certificado digital emitido por el Consorci 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

La Autoridad de Certificación 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

La Autoridad de Certificación 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 la Autoridad de Certificación

La Autoridad de Certificación puede rechazar todas las garantías del servicio que no se encuentren vinculadas a obligaciones establecidas por la legislación aplicable, descrita en 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 la Autoridad de Certificación

La Autoridad de Certificación 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.

La Entidad de Certificación podrá 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 Autoridad de Certificación 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 y finalización

La Autoridad de Certificación 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. Supervivencia

La Autoridad de Certificación establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, cláusulas de supervivencia, en virtud de las cuales se establecen como ciertas obligaciones continúan vigentes después de la finalización de la relación jurídica reguladora del servicio entre las partes.

A tal efecto, la Autoridad de Certificación vela porque, al menos los requisitos contenidos en 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 la Autoridad de Certificación con suscriptores y verificadores.

El Consorci AOC determinará un Plan de Cese de Negocio. Este Plan de Cese 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 tipo, 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

La Autoridad de Certificación 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

El Consorci AOC 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 la Autoridad de Certificación no puede ir en contra de las políticas 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.

9.13. Resolución de conflictos

9.13.1. Resolución extrajudicial de conflictos

La Autoridad de Certificación 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 la Autoridad de Certificación.

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

9.13.2. Jurisdicción competente

La Autoridad de Certificación 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

La Autoridad de Certificación establece, en sus instrumentos jurídicos con suscriptores y verificadores, que la ley aplicable a la prestación de los servicios, incluyendo la Declaración de Prácticas de Certificación y las Políticas de Certificación, es la siguiente:

- En general, la ley española, siempre y cuando la Autoridad de Certificación continúe establecida en el Estado Español, y/o sus servicios de certificación se presten por medio de un establecimiento permanente situado en el Estado Español; y,
- La normativa administrativa correspondiente, estatal y autonómica.

9.15. Conformidad con la ley aplicable

El Consorci AOC será responsable de los daños y perjuicios ocasionados a los usuarios por sus servicios y a otros terceros en los términos establecidos en la legislación vigente y en la presente DPC.

9.16. Cláusulas diversas

9.16.1. Acuerdo íntegro

La Autoridad de Certificación 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 Autoridad 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 Autoridad de Certificación.

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

Los derechos y los deberes asociados a la condición de Autoridad de Certificación Virtual podrán ser objeto, de cambio, de cesión y subrogación, pero estas incidencias tendrán que ser notificadas al Consorci AOC.

9.16.3. Divisibilidad

La Autoridad de Certificación 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 considerarían 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.