Consorci
Administració Oberta
de Catalunya

Declaración de Prácticas de Certificación
Entidad de Certificación Sector Públic
(EC-SECTORPUBLIC)

Referencia:	D1111_E0650_N-DPC EC-SECTORPUBLIC
Versión:	2.0
Fecha:	09/05/2018

Índex

1. Introducción

1.1. Presentación

1.1.1. Tipos y clases de certificados

El Consorci AOC ha definido una tipología de servicios de certificación que permiten, a EC-SECTORPUBLIC, emitir certificados digitales para varios usos y usuarios finales diferentes.

Los perfiles recogidos en este documento, se han creado para cumplir con los requerimientos previstos a la ley aplicable, que se describe en el apartado 9.15 Conformidad con la ley aplicable

Los certificados de usuarios finales se dividen en:

- Certificados de infraestructura, caracterizados por el hecho que el poseedor de la clave privada es un operador de una infraestructura, y que se utiliza para autorizar operaciones relacionadas con los servicios de certificación, como la aprobación de solicitudes de certificación
- Certificados personales, caracterizados por el hecho que el poseedor de la clave privada es una persona física, que actúa en nombre y representación del suscriptor o titular del certificado (que puede ser él mismo o una persona jurídica a la cual esté vinculado)
- Certificados de dispositivo, caracterizados por el hecho que el poseedor de la clave privada es un dispositivo informático que realiza operaciones de firma y descifrado de forma automática, bajo la responsabilidad de una persona física o jurídica (denominada suscriptor o titular del certificado)

Cuando los certificados se expiden a LAS INSTITUCIONES, se requiere realizar procedimiento de autenticación de la organización titular del certificado, puesto que se trata de certificados corporativos, en los cuales la organización suscriptora del certificado y la Entidad de Registro coinciden.

En circunstancias excepcionales, motivadas por la necesidad de garantizar la seguridad de la persona que se identifica o firma, se prevé la posibilidad de usar pseudónimos en casos especiales como pueden ser certificados de cuerpos de seguridad o de personal vinculado a la administración de justicia, entre otros, en conformidad con aquello establecido al Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los Servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CEa la ley aplicable, que se describe en el apartado 9.15 Conformidad con la ley aplicable.

En estos supuestos, se identificará el poseedor de claves de forma indirecta mediante un identificador que permita la identificación de la persona actuando, bajo requerimiento expreso de la autoridad competente con cuyo objeto.

Para el resto de casos la Entidad de Certificación tiene que autenticar, con carácter previo a la emisión y entrega de un certificado, la identidad del suscriptor y la del poseedor de claves privadas y otros datos, establecidas en la sección correspondiente para certificados corporativos. Pueden ser individuales (cuando se expiden a una persona física, actuando en su propio nombre - como por ejemplo, a los ciudadanos para relacionarse por medios electrónicos con las entidades del sector público de Cataluña) o corporativos (de organización del sector privado o del sector público fuera de Cataluña - cuando se expiden a una organización, que actúa por medio de una persona física, identificada en el certificado aunque sea intermediando un pseudónimo).

1.1.1.1. Certificados de infraestructura

EC-SECTORPUBLIC podrá emitir los siguientes tipos de certificados de infraestructura:

- Certificados de infraestructura personales de identificación y firma electrónica cualificada de operadores (CIPISQ), que se usa para autorizar operaciones relacionadas con los servicios de certificación, como la aprobación de solicitudes de certificación
- Certificado de infraestructura de servidor de estado de certificados en linea (CIO), que es utilizado por un servidor OCSP Responder para firmar sus respuestas sobre el estado de validez de los certificados

1.1.1.2. Certificados personales

EC-SECTORPUBLIC podrá emitir los siguientes tipos de certificados personales:

- Certificado electrónico de trabajador público de nivel alto de autenticación: es un certificado cualificado. Funciona con dispositivo cualificado de creación de firma electrónica. Garantizan la identidad del suscriptor y del poseedor de la clave privada de identificación y firma;. Se pueden utilizar en aplicaciones que no requieran la firma electrónica equivalente a la firma manuscrita, sino solamente la identificación del poseedor de claves, en nombre de los suscriptores.
- Certificado cualificado de firma de trabajador público de nivel alto: es un certificado cualificado. Funciona con dispositivo cualificado de creación de firma electrónica. Garantizan la identidad del suscriptor y del poseedor de la clave privada de firma, y permiten la generación de la "firma electrónica cualificada"escrita por efecto legal, sin necesidad de cumplimiento de ningún requisito adicional.
- Certificado electrónico de persona vinculada de nivel alto: es un certificado cualificado. Funciona con dispositivo cualificado de creación de firma electrónica. Garantizan la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permiten la autenticación y la generación de la "firma electrónica cualificada".
- Certificado electrónico de persona vinculada de nivel alto: es un certificado cualificado. Funciona con dispositivo cualificado de creación de firma electrónica. Garantizan la identidad del suscriptor y del poseedor de la clave privada de

identificación y firma, y permiten la autenticación y la generación de la "firma electrónica cualificada".

- Certificado cualificado de firma de trabajador público con pseudónimo de nivel alto: es un certificado cualificado de acuerdo con aquello establecido a la ley aplicable, que se describe en el apartado 9.15 Conformidad con la ley aplicable. Funciona con dispositivo cualificado de creación de firma electrónica. Garantizan, de forma indirecta, la identidad del suscriptor y del poseedor de la clave privada de firma, y permiten la generación de la "firma electrónica cualificada".
- Certificado electrónico de representante ante las AAPP de nivel alto: es un certificado cualificado de acuerdo con aquello establecido a la ley aplicable, que se describe en el apartado 9.15 Conformidad con la ley aplicable. Funciona con dispositivo cualificado de creación de firma electrónica. Garantizan la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permiten la generación de la "firma electrónica cualificada"; También se puede utilizar en aplicaciones que no requieran la firma electrónica equivalente a la firma manuscrita, sino solamente la identificación del poseedor de claves, en nombre de los suscriptores
- Certificado electrónico de trabajador público, y también de persona vinculada, de nivel medio: es un certificado cualificado de acuerdo con aquello establecido a la legislación aplicable, que se describe en el apartado 9.15 Conformidad con la ley aplicable. Garantiza la identidad del suscriptor y del poseedor de la clave privada de identificación y firma y permite la generación de la “firma electrónica avanzada”

1.1.1.3. Certificados de dispositivo

EC-SECTORPUBLIC emite los siguientes tipos de certificados de dispositivo:

- Certificado de dispositivo servidor seguro (CDS-1), que se utiliza por una aplicación informática, servidor de SSL o de TLS, para identificarse ante las aplicaciones cliente que se conectan y para proteger el secreto de las comunicaciones entre el cliente y el servidor
- Certificado de dispositivo servidor seguro de Extended Validation (CDS-1 EV), que se utiliza por una aplicación informática, servidor de SSL o de TLS, porque se identifique ante las aplicaciones cliente que se conectan y para proteger el secreto de las comunicaciones entre el cliente y el servidor, ofreciendo la validación automática en el navegador

  Certificado de dispositivo de sede electrónica nivel medio de (CDS-1 SENM), que sirve para identificar y garantizar una comunicación segura con la sede electrónica de un ente.

  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, entre otros.

  El certificado de nivel medio es recomendable para la mayoría de las administraciones públicas con previsión de los siguientes riesgos: infracción de seguridad (por ejemplo, robo de la identidad), pérdidas económicas moderadas, pérdida de información sensible o crítica, o refutación de una transacción con impacto económico significativo

- Certificado de dispositivo aplicación (CDA-1), que almacenado en un servidor y requerido por una aplicación, firma documentos o mensajes

  Certificado de dispositivo de sello electrónico de Administración, órgano o entidad de derecho público nivel medio de 1 (CDA-1 SENM), se utiliza para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada.

  Este certificado puede utilizarse para el intercambio de datos entre administraciones, la identificación y autenticación de un sistema, servicio web o aplicación, el archivo electrónico automatizado, las compulsas y copias electrónicas, entre otros

  El certificado de nivel medio es recomendable para la mayoría de las administraciones públicas que pueden tener los siguientes riesgos: infracción de seguridad (por ejemplo robo de la identidad), pérdidas económicas moderadas, pérdida de información sensible o crítica, o refutación de una transacción con impacto económico significativo.

1.1.1.4. Certificados de pruebas

De cualquier de los tipos de certificados que recoge la presente política se pueden emitir, en determinadas circunstancias, certificados de pruebas.

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

Este documento contiene la declaración de prácticas de certificación de EC-SECTOR PUBLIC.

EC-SECTORPUBLIC emite certificados dentro de la jerarquía de certificación operada por el Consorci AOC, por lo tanto tiene que disponer de una declaración de prácticas de certificación, de acuerdo con la política general de certificación del Consorci AOC.

Esta Declaración de Prácticas de Certificación (DPC) incluye los procedimientos que aplica EC-SECTORPUBLIC en la prestación de sus servicios, en cumplimiento de los requisitos establecidos por las políticas que gestiona y la legislación aplicable.

Esta DPC es coherente con aquello establecido en la Política General de Certificación y, incluso, incluye múltiples referencias en esta, para evitar duplicidades allá donde la DPC no introduce información adicional.

1.2. Nombre del documento e identificación

1.2.1. Nombre del documento e identificación

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

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

```
1.3.6.1.4.1.15096.1.2.10
```

1.2.2. Identificación de políticas de certificación cubiertas por esta DPC

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

Certificados personales:

- **CPI-1** – Certificado electrónico de trabajador público de nivel alto de autenticación, emitido por EC-SECTORPUBLIC

  OID: 1.3.6.1.4.1.15096.1.3.2.7.1.2

- **CPSQ-1** – Certificado cualificado de firma de trabajador público de nivel alto

  OID: 1.3.6.1.4.1.15096.1.3.2.7.1.1

- **CPISQ-2** – Certificado electrónico de persona vinculada de nivel alto

  OID: 1.3.6.1.4.1.15096.1.3.2.82.1

- **CPISA** – Certificado electrónico de nivel medio, emitido por EC-SECTORPUBLIC

  Trabajador público – CPISA-1 - OID: 1.3.6.1.4.1.15096.1.3.2.7.3.1

  Persona vinculada – CPISA-2 - OID: 1.3.6.1.4.1.15096.1.3.2.86.1

- **CPPI-1** – Certificado electrónico de trabajador público público con pseudónimo de nivel alto de autenticación, emitido por EC-SECTORPUBLIC

  OID: 1.3.6.1.4.1.15096.1.3.2.4.1.2

- **CPPSQ-1** – Certificado cualificado de firma de trabajador público con pseudónimo de nivel alto, emitido por EC-SECTORPUBLIC

  OID: 1.3.6.1.4.1.15096.1.3.2.4.1.1

- **CPRISQ-1** – Certificado electrónico de representante ante las AAPP de nivel alto, emitido por EC-SECTORPUBLIC

  OID: 1.3.6.1.4.1.15096.1.3.2.8.1.1

Certificados de dispositivo:

- **CDS-1** – Certificado de dispositivo SSL, emitido por EC-SECTORPUBLIC

  OID: 1.3.6.1.4.1.15096.1.3.2.51.1

- **CDSQ-1** - Certificado de dispositivo SSL EV, emitido por EC-SECTORPUBLIC. Estos certificados no se podrán emitir a partir de la entrada en vigor de la versión 2.0 de este documento.

  OID: 1.3.6.1.4.1.15096.1.3.1.51.2

- **CDSQ-1** -Certificado de dispositivo SSL EV, emitido por EC-SECTORPUBLIC y adaptado por eIDAS

  OID: 1.3.6.1.4.1.15096.1.3.2.51.2

- **CDS-1 SENM -** Certificado de sede electrónica de nivel medio, emitido por EC-SECTORPUBLIC

  OID: 1.3.6.1.4.1.15096.1.3.2.5.2

- **CDA-1** – Certificado de aplicación, emitido por EC-SECTORPUBLIC

  OID: 1.3.6.1.4.1.15096.1.3.2.91.1

- **CDA-1 SGNM -** Certificado de sello electrónico de nivel medio, emitido por EC-SECTORPUBLIC

  OID: 1.3.6.1.4.1.15096.1.3.2.6.2

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

1.3. Comunidad de usuarios de certificados

Esta declaración de prácticas de certificación regula una comunidad de usuarios que obtienen certificados para poder llevar a cabo relaciones administrativas por medios electrónicos, de acuerdo con la Ley aplicable y la normativa administrativa correspondiente, que se recogen en el apartado 9.15 Conformidad con la ley aplicable

Los certificados dEC-SECTORPUBLIC no se expiden al público, sino a las entidades, al personal y a los dispositivos de las entidades que integran el Sector Público de Cataluña.

1.3.1. Prestadores de servicios de certificación

Un prestador de servicios de certificación es una persona física o jurídica que produce certificados y presta otros servicios en relación con la firma electrónica, de acuerdo con la Ley aplicable, descrita en el apartado 9.15 Conformidad con la ley aplicable.

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

Conforme a esta función, el Consorci AOC será responsable por la actuación de EC-SECTORPUBLIC, ante los usuarios finales y los terceros verificadores de certificados y firmas electrónicas.

1.3.2. Entidad de Certificación Raíz

El Consorci AOC dispone de una autoridad de certificación principal, que es la raíz de la jerarquía pública de certificación de Cataluña: el EC-ACC, la finalidad de la cual es integrar otras entidades de certificación en el sistema público catalán de certificación mediante la vinculación técnica de las autoridades de certificación correspondientes.

1.3.3. EC-SECTORPUBLIC

EC-SECTORPUBLIC es la Entidad de Certificación para dotar de certificados digitales a las entidades, al personal y a los dispositivos de los Organismos, Departamentos y Empresas Públicas que integran el Sector Público de Cataluña.

EC-SECTORPUBLIC está vinculada a la jerarquía de entidades de certificación de las entidades públicas de Cataluña y emite los certificados indicados en el punto 1.1.1.

1.3.4. Entidades de Registro

Conforme a aquello establecido en la Política General de Certificación, las Entidades de Registro asisten a las Entidades de Certificación Vinculadas 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.

El Consorci AOC es responsable del proceso de creación de entidades de registro dEC-SECTORPUBLIC: verifica que la Entidad de Registro cuenta con los recursos materiales y humanos necesarios; y que ha designado y ha formado al personal que será responsable de la emisión de certificados (los llamados operadores de la entidad de registro). Así mismo, es responsable de la emisión de los certificados de operador que estos necesitarán para poder operar (típicamente, serán CIPISQ); el Consorci AOC validará las peticiones de certificados para operadores de las Entidades de Registro examinando la solicitud y haciendo las comprobaciones necesarias para el cumplimiento de la Política General de Certificación y de esta Declaración de Prácticas de Certificación.

Existen los siguientes tipos de Entidades de Registro dEC-SECTORPUBLIC:

1) Los entes suscriptor , operadas por una entidad suscriptora de certificados
2) Las Entidades de Registro, que colaboran con EC-SECTORPUBLIC en el proceso de emisión de los certificados

Para ser Entidades de Registro, las entidades tendrán que diseñar e implantar los correspondientes componentes y procedimientos técnicos, jurídicos y de seguridad, referentes al ciclo de vida de los dispositivos seguros de creación de firma o, en su caso, de cifrado, al ciclo de vida de las claves en apoyo software y al ciclo de vida de los certificados que emitan. Estos componentes y procedimientos serán previamente aprobados por el Consorci AOC.

1.3.5. Usuarios finales

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

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

1.3.5.1. Solicitantes de certificados

Conforme a aquello establecido en la Política General de Certificación. Más concretamente, pueden ser solicitantes de certificados dEC-SECTORPUBLIC:

a) De certificados corporativos: una persona autorizada al efecto por la futura entidad suscriptora
b) Una persona autorizada por la Entidad de Certificación – típicamente, el Consorci AOC actuando de oficio

La autorización se formalizará documentalmente.

1.3.5.2. Suscriptores de certificados

Conforme a aquello establecido en la Política General de Certificación.

1.3.5.3. Poseedores de claves

Conforme a aquello establecido en la Política General de Certificación.

1.3.5.4. Usuarios de certificados

Conforme a aquello establecido en la Política General de Certificación.

1.3.5.5. Verificadores de certificados

Conforme a aquello establecido en la Política General de Certificación.

1.4. Uso de los certificados

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

1.4.1. Uso de los certificados

1.4.1.1. Certificados de infraestructura

1.4.1.1.1. Certificado personal de Infraestructura personal de identificación y firma cualificada (CIPISQ)

Conforme a aquello establecido en la Política General de Certificación.

1.4.1.1.2. Requisitos específicos para el CIC

Conforme a aquello establecido en la Política General de Certificación.

1.4.1.1.3. Requisitos específicos para el CIO

Conforme a aquello establecido en la Política General de Certificación.

1.4.1.2. Requisitos específicos por los Certificados personales

1.4.1.2.1. Certificado electrónico de trabajador público de nivel alto de autenticación

Permiten la autenticación de los usuarios.

1.4.1.2.2. Certificado cualificado de firma de trabajador público de nivel alto

Permiten los trabajadores públicos la creación de firma electrónica cualificada .

1.4.1.2.3. Certificado electrónico de persona vinculada de nivel alto

Permiten a personas vinculadas autenticarse, y la creación de firma electrónica cualificada.

1.4.1.2.4. Certificado electrónico de trabajador público de nivel medio

Permiten los trabajadores públicos la autenticación y creación de firma electrónica avanzada.

1.4.1.2.5. Certificado electrónico de persona vinculada de nivel medio

Permiten las personas vinculadas la autenticación y creación de firma electrónica avanzada.

1.4.1.2.6. Certificado electrónico de trabajador público con pseudónimo de nivel alto de autenticación

Permiten la autenticación trabajadores públicos identificados con pseudónimo

1.4.1.2.7. Certificado cualificado de firma de trabajador público con pseudónimo de nivel alto

Permiten a trabajadores públicos identificados con pseudónimo generar firmas cualificadas.

1.4.1.2.8. Certificado electrónico de representante ante las AAPP de nivel alto

Permiten a trabajadores públicos autenticarse con atribuciones de representación de entidades públicas, y también la generación de firma electrónica cualificada.

1.4.1.3. Certificados de Dispositivo

1.4.1.3.1. Certificados de dispositivo SSL (CDS-1)

EC-SECTORPUBLIC los podrá emitir certificados a las entidades integrantes del Sector Público de Cataluña que sean responsables de la operación de servidores seguros SSL o TLS, con los siguientes usos:

- Autenticación de servidor
- Cifrado de las comunicaciones entre cliente y servidor

Son certificados ordinarios; y garantizan el origen de la comunicación (la identidad del servidor concreto donde funcionen), así como la de la entidad responsable de este.

1.4.1.3.2. Certificados de dispositivo SSL EV (CDS-1 EV)

EC-SECTORPUBLIC los podrá emitir certificados a las entidades responsables de la operación de servidores seguros SSL o TLS, con los siguientes usos:

- Autenticación de servidor
- Cifrado de las comunicaciones entre cliente y servidor
- Validación automática del certificado mediante los navegadores web adheridos a CAV Forum.

Son certificados ordinarios; y garantizan el origen de la comunicación (la identidad del servidor concreto donde funcionen), así como la de la entidad responsable de este.

1.4.1.3.3. Certificado de sede electrónica de nivel medio (CDS-1 SENM)

EC-SECTORPUBLIC los podrá emitir certificados a entidades integrantes del Sector Público de Cataluña que sean responsables de la operación de servidores seguros SSL o TLS destinados a identificar y garantizar la comunicación segura con la sede electrónica de estas entidades. Se trata de certificados cualificados que pueden utilizarse para garantizar la autenticación de un sitio web oficial (esto es, el origen de las conexiones web establecidas por un ciudadano con una sede electrónica) y la conexión segura con este, el alojamiento de registros electrónicos de entrada/salida, la consulta y la autorización de registros de representación, etc.

1.4.1.3.4. Certificado de aplicación (CDA-1)

EC-SECTORPUBLIC los podrá emitir 1 a entidades integrantes del Sector Público de Cataluña que sean responsables de la operación de aplicaciones informáticas que se identifican digitalmente, que firman electrónicamente webservices u otros protocolos y que reciben documentos y mensajes cifrados.

Son certificados ordinarios que garantizan la integridad y la autenticidad de los datos firmados. También garantizan la identidad de la entidad responsable.

1.4.1.3.5. Certificado de sello electrónico nivel medio (CDA-1 SGNM)

EC-SECTORPUBLIC los podrá emitir c a entidades integrantes del Sector Público de Cataluña, para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada.

Este certificado puede utilizarse para el intercambio de datos entre administraciones, la identificación y la autenticación de un sistema, servicio web o aplicación, para implementar sistemas de archivo electrónico automatizado o de compulsas y copias electrónicas, entre otras.

1.4.2. Aplicaciones prohibidas

1.4.2.1. Informaciones para todos los tipos de certificados

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

1.4.2.2. Certificados de infraestructura

Los certificados de infraestructura emitidos por EC-SECTORPUBLIC – los perfiles de los cuales se relacionan en el apartado 1.2.2 Identificación de políticas de certificación

cubiertas por esta DPC – no podrán utilizarse para los fines descritos en la Política General de Certificación, apartado Aplicaciones prohibidas.

1.4.2.3. Certificados personales

Los certificados personales emitidos por EC-SECTORPUBLIC – los perfiles de los cuales se relacionan a la apartado Identificación de políticas de certificación cubiertas por esta DPC – no podrán utilizarse para los fines descritos en la Política General de Certificación, apartado Aplicaciones prohibidas.

1.4.2.4. Certificados de dispositivo

Los certificados de dispositivo emitidos por EC-SECTORPUBLIC – los perfiles de los cuales se relacionan a la apartado Identificación de políticas de certificación cubiertas por esta DPC – no podrán utilizarse para los fines descritos en la Política General de Certificación, apartado Aplicaciones prohibidas.

1.5. Administración de la Declaración de Prácticas

1.5.1. Organización que administra la especificació

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`

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

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

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

1.5.4. Procedimiento de aprobación

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

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

La versión inicial de esta Declaración de prácticas es aprobada por la Comisión Ejecutiva del Consorci AOC, que es el órgano colegiado de dirección ejecutiva del Consorci.

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

Conforme a aquello establecido en la Política General de Certificación.

2.2. Publicación de información de EC-SECTORPUBLIC

Conforme a aquello establecido en la Política General de Certificación.

2.3. Frecuencia de publicación

La información de EC-SECTORPUBLIC 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 aquello establecido a la sección 9.12.1 Procedimiento para las modificaciones.

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

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

La información de estado de revocación de certificados se publica de acuerdo con aquello establecido a la sección 4.10.7 Frecuencia de emisión de listas de revocación de certificados (CRL's).

2.4. Control de acceso

Conforme a aquello establecido en la Política General de Certificación.

3. Identificación y autenticación

3.1. Gestión de nombre

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

3.1.1. Tipo de nombres

Conforme a aquello establecido en la Política General de Certificación.

3.1.2. Significado de los nombres

Conforme a aquello establecido en la Política General de Certificación.

3.1.3. Utilización de anónimos y pseudónimos

No se pueden usar pseudónimos para identificar una organización.

Los certificados personales, así los individuales como los corporativos, podrán indicar pseudónimos en vez del nombre verdadero del poseedor de la clave del certificado.

El pseudónimo constará como tal de forma inequívoca, y se indicará esta naturaleza a la descripción del tipo de certificado.

El pseudónimo se hará constar mediante un campo Pseudonym del certificado, y estará vinculado a una dirección de correo electrónico, mediante un campo de carácter obligatorio.

En cualquier caso, la emisión de certificados con pseudónimo garantizará, en la fase de registro, la disponibilidad de la identificación real del poseïdor de claves, que sólo podrá ser revelada previa solicitud de la autoridad competente

3.1.4. Interpretación de formatos de nombres

Sin estipulación adicional.

3.1.5. Unicidad de los nombres

Conforme a aquello establecido en la Política General de Certificación.

3.1.6. Resolución de conflictos relativos a nombres

Conforme a aquello establecido en la Política General de Certificación.

Referent al tractament de marques registrades, veure l'apartat 9.5.3.

3.2. Validación inicial de la identidad

3.2.1. Prueba de posesión de clave privada

Conforme a aquello establecido en la Política General de Certificación.

3.2.2. Autenticación de la identidad de una organización

Aquesta secció conté els requisits per a la comprovació de la identitat d'una organització identificada en el certificat.

En general, l'EC-SECTORPUBLIC no haurà de determinar que un sol·licitant de certificats té dret sobre el nom que apareix en una sol·licitud de certificat. Tampoc actuarà com àrbitre o mediador, ni haurà de resoldre cap disputa concernent a la propietat de noms de persones o organitzacions, noms de domini, marques o noms comercials (per exemple, relatius a direccions electròniques).

3.2.2.1. Entidades de Registro

Conforme a aquello establecido en la Política General de Certificación.

3.2.2.2. Las entidades suscriptoras de certificados corporativos

No es requereix realitzar procediment d'autenticació de les entitats suscriptores (titular del certificat) en certificats emesos a LES INSTITUCIONS, ja que es tracta de certificats corporatius, en els que l'organització suscriptora del certificat i l'Entitat de Registre Interna coincideixen.

3.2.2.3. Otras entidades suscriptoras

3.2.2.3.1. Requisitos para certificados de persona vinculada

Conforme a aquello establecido en la Política General de Certificación.

3.2.2.3.2.Requisitos específicos para los certificados de dispositivo

Conforme a aquello establecido en la Política General de Certificación.

3.2.3. Autenticación de la identidad de una persona física

Aquesta secció conté informacions per a la comprovació de la identitat d'una persona física identificada en un certificat.

3.2.3.1. Elementos de identificación

El número i tipus de documents necessaris per a acreditar la identitat del posseïdor de claus són els que admet cada organització suscriptora, tal com es recull en la seva normativa reguladora.

En tot cas, aquests documents identificatius contindran com a mínim:

- Nom i cognoms de la persona
- Número d'identitat reconegut legalment (DNI, NIF o NIE dels països signants de l'Acord de Schengen; passaport en el cas dels certificats d'estranger)
- Qualsevol altra informació que pugui ser utilitzada per a diferenciar a una persona d'altra, dintre de l'àmbit de la Institució (per exemple: fotografia, correo-e, categoria, càrrec, etc.).

3.2.3.2. Validación de los elementos de identificación

Conforme a aquello establecido en la Política General de Certificación.

3.2.3.3. Validación de los elementos de identificación

Conforme a aquello establecido en la Política General de Certificación.

3.2.3.4. Vinculación de la persona física con la organización

Para los certificados de trabajador público: cómo se trata de certificados corporativos, en que la Entidad de Registro y el suscriptor coinciden, no es necesario obtener una justificación documental específica de la vinculación del poseedor de la clave con la Entidad de Registro, sino que se utilizan los registros internos de la entidad.

Para los certificados de persona vinculada: EC-SECTORPUBLIC – mediante la intervención de una Entidad de Registro – tiene que obtener una justificación documental de la vinculación de la persona física que será poseedora de la clave privada con la organización, mediante cualquier medio admitido en derecho.

3.2.4. Información no verificada

La entidad suscriptora del certificado se responsabiliza 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).

3.3. Identificación y autenticación de solicitudes de renovación

3.3.1. Validación para la renovación de certificados

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

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

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

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

4.1. Solicitud de emisión de certificado

La solicitud es el primer paso que tiene que hacer el suscriptor para conseguir los certificados para su personal.

En el caso de las Administraciones Públicas, la solicitud se enviará:

- A través de sus Entidades de Registre T-CAT
- Directamente al Consorci AOC, de forma supletoria en caso de que el ente no tenga ninguna entidad de registro asignada. En este caso el Consorci AOC actuará como Entidad de Registre T-Cat

Esta solicitud requiere el envío de un documento con la información exacta y comprobada (certificada) de las personas, entidades o dispositivos para las cuales se pide el certificado. Esta tiene que ir firmada por la persona autorizada al efecto por la entidad suscriptora; y tiene que traer adjunto el certificado de esta información.

También se puede confirmar una dirección física u otros datos que permitan establecer contacto directo con el futuro poseedor de claves.

Toda la documentación se entrega a la Entidad de Registro, por medios electrónicos. Podrá ser remitida en apoyo papel o mediante correo electrónico, excepcionalmente, por los siguientes motivos:

- Que la entidad suscriptora, por razón de su naturaleza jurídica, no pueda ser usuario del aplicativo informático usado para remitir las solicitudes (actualmente, EACAT)
- Que sea una entidad que solicite certificados digitales por primera vez, de forma que no disponga de ningún certificado digital con el que llevar a cabo la tramitación de la solicitud por medios electrónicos

4.1.1. Legitimación para solicitar la emisión

Conforme a aquello establecido en la Política General de Certificación en relación a la solicitud de certificados de infraestructura; a la solicitud de los certificados corporativos, personales y a la solicitud de los certificados de dispositivo.

4.1.2. Procedimiento de alta; Responsabilidades

No aplicable.

4.2. Procedimiento de solicitud de certificación

4.2.1. Requisitos generales para todos los certificados

El procedimiento ordinario para solicitar certificados digitales es el siguiente:

1. Entrega de la Ficha del suscriptor

Para que una entidad integrada en el Sector Público de Cataluña pueda solicitar certificados, previamente tiene que remitir la Ficha del suscriptor, debidamente cumplimentada, al Consorci AOC porque este pueda darla de alta en el sistema y configurar las necesarias autorizaciones del personal indicado por la entidad.

Esta remisión se hará, de manera ordinaria, por medios electrónicos, cuando todos los roles que intervienen en el proceso de solicitud (solicitante, certificador y responsable del servicio) dispongan de certificados digitales.

Alternativamente, podrá solicitarlos, conforme a los motivos descritos en el apartado 4.1 Solicitud de emisión de certificado, a través del siguiente procedimiento alternativo:

- Descarga de la Ficha del suscriptor desde el web del Consorci AOC
- Envío de la Ficha, debidamente agasajada y firmada digitalmente, a la dirección: scd@aoc.cat; o bien, envío de la Ficha, debidamente agasajada y firmada manuscritamente, por correo ordinario a la dirección que se recoge a la sección 1.5.2 Datos de contacto de la organización de este documento

La entrega de esta documentación se hará junto con la primera solicitud de certificados, o cuando sea necesario actualizar la información confirmada en ella.

2. Obtención de los certificados

Cuando la solicitud se realiza por medios electrónicos, una vez agasajada, tiene que ser firmada digitalmente por el solicitante y, cuando tenga que adjuntarse un certificado de datos, este tendrá que ser firmado digitalmente por el certificador:

- Primero, cuando el solicitante firma la solicitud, el sistema envía automáticamente un correo electrónico al certificador de la entidad avisándolo que tiene que verificar los datos de la solicitud del certificado
- El certificador es la persona del ente con capacidad para justificar documentalmente los datos del titular del certificado a emitir, por ejemplo, lo/la secretario/aria, lo/la responsable de recursos humanos, etc. El certificador de la entidad abre la solicitud en cuestión y, una vez ha comprobado que los datos son correctos, la firma digitalmente finalizando así el proceso de solicitud
- En este momento se hace automáticamente el asentamiento del registro de salida de la entidad y el asentamiento del registro de entrada a la Entidad de Registre T-CAT que corresponda a la entidad

EC-SECTORPUBLIC recibe los datos de la solicitud y las carga a la aplicación de generación de certificados, donde quedan a disposición de la Entidad de Registro correspondiente.

Una vez el certificado ha sido generado por esta Entidad de Registro, se envía a la entidad suscriptora.

Si la solicitud se realiza por medios electrónicos, se tienen que solicitar por el siguiente procedimiento alternativo:

- Descarga del modelo de solicitud y el certificado de datos correspondiente
- Envío de los documentos, debidamente agasajados y firmados digitalmente, a la dirección: scd@aoc.cat; o bien, envío de los documentos, debidamente agasajados y firmados manuscritamente, por correo ordinario a la dirección que se recoge en la sección 1.5.2 Datos de contacto de la organización de este documento

4.3. Emisión de certificado

Las solicitudes recibidas son procesadas y validadas.

En caso de que todo sea correcto, se envía la solicitud a la Entidad de Registro que corresponda a la entidad solicitante.

Seguidamente, y de manera automática, se envía al solicitante un mensaje informando del resultado positivo o negativo de la operación y, en este último caso, detallando el tipo de error detectado.

4.3.1. Acciones de EC-SECTORPUBLIC durante el proceso de emisión

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 nuevo certificado.

Para cada solicitud de certificado enviada, EC-SECTORPUBLIC actuará conforme a aquello establecido al efecto en la Política General de Certificación – apartado 4.3.1 Acciones de la Entidad de Certificación durante los procesos de emisión y renovación.

4.3.2. Comunicación de la emisión al suscriptor

EC-SECTORPUBLIC comunicará al solicitante la aprobación o denegación de la solicitud.

En caso de que haya sido aprobada, también comunicará – cuando corresponda - al futuro poseedor de claves que se ha creado el certificado, que se encuentra disponible y la forma de obtenerlo.

4.4. Acceptación del certificado

Para determinados perfiles de certificados, EC-SECTORPUBLIC es responsable de crear el par de claves criptográficas; y, para todos los perfiles de certificados, es responsable de generar el certificado digital correspondiente.

Para los perfiles de certificados para los cuales se genera el par de claves y se almacena en tarjetas criptográficas, EC-SECTORPUBLIC también es responsable de crear los correspondientes códigos PIN y PUK de estas tarjetas. Estos códigos se envían directamente al poseedor de las claves, de manera ordinaria por correo electrónico dirigido a este o, de manera extraordinaria, por correo postal en sobre ciego. El poseedor de las claves podrá, en cualquier momento, recuperar estos códigos a través de la aplicación telemática al efecto.

Paralelamente, la tarjeta con el certificado solicitado se envía por correo postal a la atención del responsable de la entidad de registro interna de la entidad suscriptora.

EC-SECTORPUBLIC generará la hoja de entrega y aceptación del certificado para el poseedor de claves; en el cual se lo indican los contenidos descritos en la Política General de Certificación.

4.4.1. Responsabilidades del Ente subcriptor

4.4.1.1. Para Certificados personales

EC-SECTORPUBLIC delega en los entes suscriptores (más concretamente, en la figura del responsable) algunas de sus responsabilidades, referentes al proceso de entrega y aceptación de los certificados digitales que emite.

Concretamente, el responsable de la entidad de registro tendrá que:

- informar al poseedor de las claves de sus obligaciones y responsabilidades en relación al certificado que le entrega
- requerir del poseedor de las claves el reconocimiento de recibir el certificado y, en su caso, el dispositivo criptográfico correspondiente, así como el reconocimiento de la aceptación de estos elementos, mediante la firma de la hoja de entrega y aceptación del certificado
- En el caso de aquellos perfiles que requieren tarjeta criptográfica, entregar-al poseedor de las claves en persona, una vez este haya firmado la hoja de entrega y aceptación del certificado; así como también un ejemplar de la hoja de entrega y aceptación del certificado

4.4.1.2. Para certificados de dispositivo

Los certificados de dispositivo se entregarán mediante un fichero que tendrá que descargar el responsable del ente suscriptor.

4.4.2. Conducta que constituye aceptación del certificado

El certificado se acepta mediante la firma, por parte del poseedor de claves, de la hoja de entrega y aceptación del certificado.

También se considera la posibilidad de aceptar el certificado mediante un mecanismo telemático de activación del certificado.

4.4.3. Publicación del certificado

Conforme a aquello establecido en la Política General de Certificación.

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

Conforme a aquello establecido en la Política General de Certificación.

4.5.2. Uso por el tercero que confía en certificados

Conforme a aquello establecido en la Política General de Certificación.

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

Conforme a aquello establecido en la Política General de Certificación.

4.8. Renovación telemática

Conforme a aquello establecido en la Política General de Certificación.

4.9. Modificación de certificados

Conforme a aquello establecido en la Política General de Certificación.

Más allá, en determinadas circunstancias (como por ejemplo, en momentos de cambios organizativos, como el inicio de una nueva legislatura, cuando algunos departamentos desaparecen y sus funciones se integran en otro departamento, o simplemente cambian de nombre), y de manera transitoria, los datos no identificativos que sobre el poseedor de las claves constan en el certificado (como son: la dirección de correo-e, el departamento al cual está adscrito, etc.) pueden no ajustarse a las nuevas circunstancias. En estos casos, la organización tendrá que planificar la renovación de los certificados de sus usuarios, lo cual podrá demorarse razonablemente atendiendo a motivos económicos y/u organizativos, sin que suponga un incumplimiento de la responsabilidad atribuida.

4.10. Revocación y suspensión de certificados

4.10.1. Causas de revocación de certificados

Conforme a aquello establecido en la Política General de Certificación.

4.10.2. Legitimación para solicitar la revocación

Conforme a aquello establecido en la Política General de Certificación.

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. Tiene que incluirse la información suficiente para poder identificar razonablemente, en criterio de EC-SECTORPUBLIC, por un lado, el certificado que se solicita revocar y, por otra, la autenticidad y autoridad del solicitante.

Esta información suficiente tiene que estar formada por los datos de contacto del poseedor de claves, incluido su DNI o equivalente y de la entidad que pide la revocación, la fecha y la razón de la petición, así como el número de serie del certificado.

Quién haga la solicitud de revocación puede pedir a la Entidad de Registro más información sobre este procedimiento.

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

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

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

- Certificado de dispositivo SSL
- Certificado de dispositivo SSL EV
- Certificado de sede electrónica de nivel medio

La acción de revocación la lleva a cabo uno de los operadores de la Entidad de Registro, quien accede a la aplicación web al efecto, autenticándose intermediando un certificado digital de operador (CIPISQ) emitido por EC-SECTORPUBLIC.

Una vez registrado el cambio de estado del certificado en el sistema de EC-SECTORPUBLIC, de forma automática y en la mayor brevedad posible, se genera y publica una nueva Lista de Certificados Revocados (LCR o CRL) en la cual constará la referencia de este certificado.

Se informa al suscriptor y, en su caso, al poseedor de claves, sobre el cambio de estado del certificado, de acuerdo con el artículo 10.2 de la Ley de firma electrónica.

4.10.4. Plazo temporal de solicitud de revocación

Conforme a aquello establecido en la Política General de Certificación.

4.10.5. Plazo máximo de procesamiento de la solicitud de revocación

Conforme a aquello establecido en la Política General de Certificación.

4.10.6. Obligación de consulta de información de revocación de certificados

Conforme a aquello establecido en la Política General de Certificación.

4.10.7. Frecuencia de emisión de listas de revocación de certificados (CRL's)

Conforme a aquello establecido en la Política General de Certificación.

4.10.8. Periodo máximo de publicación de CRL'

Conforme a aquello establecido en la Política General de Certificación.

4.10.9. Disponibilidad de servicios de comprobación de estado de certificados

Conforme a aquello establecido en la Política General de Certificación.

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

Conforme a aquello establecido en la Política General de Certificación.

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

Conforme a aquello establecido en la Política General de Certificación.

4.10.13. Causas de suspensión de certificados

Conforme a aquello establecido en la Política General de Certificación.

4.10.14. Efecto de la suspensión de certificados

Conforme a aquello establecido en la Política General de Certificación.

4.10.15. Quién puede solicitar la suspensión

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

4.10.16. Procedimientos de solicitud de suspensión

Conforme a aquello establecido en la Política General de Certificación.

4.10.17. Periodo máximo de suspensión

Conforme a aquello establecido en la Política General de Certificación.

4.10.18. Habilitación de un certificado suspenso

Conforme a aquello establecido en la Política General de Certificación.

4.11. Servicios de comprobación de estado de certificados

4.11.1. Características de operación de los servicios

Las CRL's 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 dEC-SECTORPUBLIC.

4.11.2. Disponibilidad de los servicios

Conforme a aquello establecido en la Política General de Certificación.

4.11.3. Otras funciones de los servicios

Sin estipulación adicional.

4.12. Finalización de la suscripción

Conforme a aquello establecido en la Política General de Certificación.

4.13. Depósito y recuperación de claves

4.13.1. Política y prácticas de depósito y recuperación de claves

No se practica recuperación de claves para los certificados emitidos por EC-SECTORPUBLIC.

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

Sin estipulación adicional.

4.14. Notificación de problemas con certificados de autenticación de sitio web

Para notificar cualquier problema relacionada con el uso, corrección, seguridad u otro, relativo en cualquier clase de certificado de autenticación de sitio web o certificado SSL emitido por el Consorci Administració Oberta de Catalunya, a saber:

- Certificado de dispositivo SSL
- Certificado de dispositivo SSL EV
- Certificado de sede electrónica de nivel medio

por favor contacte con el Consorci AOC a través de los Datos de contacto de la organización o en la dirección electrónica siguiente:

incident_pki@aoc.cat,

proporcionando, si es posible:

- Fecha y hora
- Número de serie del certificado
- URL a la que se está accediendo
- dirección IP desde la que se está intentando acceder a la URL

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

5.1. Controles de seguridad física

Conforme a aquello establecido en la Política General de Certificación.

5.1.1. Localización y construcción de las instalaciones

Conforme a aquello establecido en la Política General de Certificación.

5.1.2. Acces físico

Conforme a aquello establecido en la Política General de Certificación.

5.1.3. Electricidad y aire acondicionado

Conforme a aquello establecido en la Política General de Certificación.

5.1.4. Exposición al agua

Conforme a aquello establecido en la Política General de Certificación.

5.1.5. Advertencia y protección de incendios

Conforme a aquello establecido en la Política General de Certificación.

5.1.6. Almacenamiento de soportes

Conforme a aquello establecido en la Política General de Certificación.

5.1.7. Tratamiento de residuos

Conforme a aquello establecido en la Política General de Certificación.

5.1.8. Copia de seguridad fuera de las instalaciones

Conforme a aquello establecido en la Política General de Certificación.

5.2. Controles de procedimientos

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

El personal al servicio de EC-SECTORPUBLIC realiza los procedimientos administrativos y de gestión de acuerdo con la política de seguridad de EC-SECTORPUBLIC. Esta política de seguridad ofrece apoyo a roles con diferentes privilegios.

5.2.1. Funciones fiables

Conforme a aquello establecido en la Política General de Certificación.

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

5.2.2. Número de personas por tarea

Conforme a aquello establecido en la Política General de Certificación.

5.2.3. Identificación y autenticación para cada función

Conforme a aquello establecido en la Política General de Certificación.

5.2.4. Roles que requieren separación de tareas

Conforme a aquello establecido en la Política General de Certificación.

5.3. Controles de personal

EC-SECTORPUBLIC tiene en cuenta los siguientes aspectos:

- Se mantiene la 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, mantenimiento y custodia de los activos de la infraestructura identificados en la política, en los planes de seguridad o en este documento
- No se revela información no pública fuera del ámbito de la infraestructura, ni se extraen apoyos de información a niveles de seguridad inferiores
- Se reporta al Responsable de Seguridad, el más bien posible, cualquier incidente que se considere que afecta a la seguridad de la infraestructura, o limitar la calidad del servicio
- Se utilizan los activos de la infraestructura para las finalidades que los han sido encomendadas
- Se exigen manuales o guías de usuario de los sistemas que utiliza, que permiten desarrollar su función correctamente
- Se exige documentación escrita que marque sus funciones y medidas de seguridad a las cuales está sometido
- El responsable de seguridad vela porque el punto anterior sea ejecutado, proveyendo a los responsables de área toda la información que fuera necesaria
- No se instalan en ninguno de los sistemas de la infraestructura, software o hardware que no sea expresamente autorizado por escrito por el responsable de sistemas de información.
- No se accede voluntariamente, ni se elimina o altera información no destinada a su persona o perfil profesional

El personal afectado por esta normativa es:

- el Responsable del Servicio de Certificación Digital
- el Responsable dEC-SECTORPUBLIC
- el Responsable de Seguridad
- el Responsable de Operaciones
- el Operador de Ceremonias de Claves

- el Equipo técnico de administración, operación y explotación
- los Administradores de la Red
- los Operadores de la Entidades de Registro

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

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

5.3.1. Requisitos de historial, calificaciones, experiencia y autorización

Conforme a aquello establecido en la Política General de Certificación.

5.3.2. Requisitos de formación

Conforme a aquello establecido en la Política General de Certificación.

El Consorci AOC, además, proporciona a todo el personal involucrado en las operaciones de las Entidades de Registro dEC-SECTORPUBLIC, una información adecuada, que incluye los procedimientos de trabajo y los de seguridad.

También se realiza instrucción periódica en normas de seguridad, planes de contingencia y gestión de incidencias al personal interno.

5.3.3. Requisitos y frecuencia de actualización formativa

Conforme a aquello establecido en la Política General de Certificación.

5.3.4. Secuencia y frecuencia de rotación laboral

Sin estipulación adicional.

5.3.5. Sanciones por acciones no autorizadas

Conforme a aquello establecido en la Política General de Certificación.

5.3.6. Requisitos de contratación de profesionales

Conforme a aquello establecido en la Política General de Certificación.

5.3.7. Suministro de documentación al personal

Conforme a aquello establecido en la Política General de Certificación.

5.4. Procedimientos de auditoría de seguridad

5.4.1. Tipo de acontecimientos registrados

Conforme a aquello establecido en la Política General de Certificación.

5.4.2. Frecuencia de tratamiento de registros de auditoría

Conforme a aquello establecido en la Política General de Certificación.

5.4.3. Periodo de conservación de registros de auditoría

Conforme a aquello establecido en la Política General de Certificación.

5.4.4. Protección de los registros de auditoría

Conforme a aquello establecido en la Política General de Certificación.

5.4.5. Procedimientos de copias de seguridad

Conforme a aquello establecido en la Política General de Certificación.

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

- Se guardan en armarios ignífugues
- Solamente personas autorizadas disponen de acceso a las copias de seguridad
- Las copias están identificadas
- Si un material ha contenido copias de seguridad (usb, dvd's...) y se quieren reutilizar, se asegura que los datos que ha contenido sean totalmente borradas haciendo imposible su recuperación

- Se autoriza expresamente la extracción de las copias de seguridad fuera de la Entidad de Registro, rellenando una ficha al respeto y anotando el correspondiente detalle en un libro de registro
- Se procura ir depositando copias de seguridad periódicamente fuera de la Entidad de Registro

5.4.6. Localización del sistema de acumulación de registros de auditoría

Conforme a aquello establecido en la Política General de Certificación.

5.4.7. Notificación del acontecimiento de auditoría al causante del acontecimiento

Conforme a aquello establecido en la Política General de Certificación.

5.4.8. Análisis de vulnerabilidades

Conforme a aquello establecido en la Política General de Certificación.

5.5. Archivo de informaciones

Conforme a aquello establecido en la Política General de Certificación.

5.5.1. Tipo de acontecimientos registrados

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

EC-SECTORPUBLIC guarda registro del siguiente:

- Documentos originales:
    - Formulario de solicitud de certificados
    - Certificado de datos
    - Hoja de entrega de suscriptor de certificados

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

- *LOG* y pistas de auditoría
- Documentación relativa a peticiones, verificaciones y revocaciones de certificados Extended Validation

5.5.2. Periodo de conservación de registros

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

EC-SECTORPUBLIC guarda los registros especificados a la sección 5.5.1 en relación con los certificados Extended Validation por un periodo de 7 años, contados desde el momento de la expedición del certificado.

5.5.3. Protección del archivo

Conforme a aquello establecido en la Política General de Certificación.

5.5.4. Procedimientos de copia apoyo

Se hacen copias de seguridad de los logs de acceso lógico al sistema operativo de la LRA. Se encarga un técnico de comunicaciones del Consorci AOC.

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

5.5.5. Requisitos de sellado de fecha y hora

Conforme a aquello establecido en la Política General de Certificación.

5.5.6. Localización del sistema de archivo

EC-SECTORPUBLIC tiene un sistema de almacenamiento de datos de archivo fuera de sus propias instalaciones, así como se especifica a la sección 5.1.8.

5.5.7. Procedimientos de obtención y verificación de información de archivo

Conforme a aquello establecido en la Política General de Certificación.

5.6. Renovación de claves

Los certificados dEC-SECTORPUBLIC renovados se comunican a los usuarios finales, mediante su publicación en la página web del Servicio SCD del Consorci AOC.

5.7. Compromiso de claves y recuperación de desastre

5.7.1. Procedimiento de gestión de incidencias y compromisos

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

5.7.2. Corrupción de recursos, aplicaciones o datos

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

5.7.3. Compromiso de la clave privada de la Entidad

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

En caso de compromiso, EC-SECTORPUBLIC:

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

5.7.4. Desastre sobre las instalaciones

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

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

- Revocación de certificados
- Publicación de información de revocación

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

5.8. Finalización del servicio

5.8.1. EC-SECTORPUBLIC

Conforme a aquello establecido en la Política General de Certificación.

5.8.2. Entidad de Registro

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

6. Controles de seguridad técnica

EC-SECTORPUBLIC 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

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

6.1.1.2. Información para los certificados CPI, CPSQ, CPPI, CPPSQ Y CPRISQ

Las claves pública y privada de los certificados CPI, CPSQ, CPPI, CPPSQ y CPRISQ las genera el Consorci AOC dentro de un dispositivo cualificado de creación de firma electrónica..

6.1.1.3. Información para los certificados CPISA

Las claves pública y privada de los certificados CPISA las puede generar el Consorci AOC y son enviadas al poseedor de claves de forma segura. También pueden ser generadas por el futuro poseedor de claves, quienes remitirá la correspondiente prueba de posesión de clave privada (PKCS#10) a EC-SECTORPUBLIC.

6.1.1.4. Información para los certificados CDS-1, CDS-1 EV, CDS-1 SENM, CDA-1, CDA-1 SENM

El par de claves de los certificados CDS-1, CDS-1 EV, CDS-1 SENM, CDA-1, CDA-1 SENM, lo genera la entidad que solicita el certificado, el suscriptor, que remitirá la correspondiente prueba de posesión de clave privada (PKCS#10) a EC-SECTORPUBLIC.

6.1.2. Envío de la clave privada al suscriptor

6.1.2.1. Conforme a aquello establecido en la Política General de Certificación.

6.1.3. Envío de la clave pública al emisor del certificado

Conforme a aquello establecido en la Política General de Certificación.

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

La clave de EC-SECTORPUBLIC y las claves de las Entidades de Certificación anteriores en la jerarquía pública de certificación de Cataluña son comunicadas a los verificadores, garantizando la integridad de la clave y autenticando el origen.

La clave pública de EC-SECTORPUBLIC se publica en el directorio de EC-SECTORPUBLIC, en forma de certificado CIC firmado por el EC-ACC. Los usuarios pueden acceder al directorio para obtener las claves públicas de EC-SECTORPUBLIC.

Este mismo certificado también se publica en la web del Consorci AOC.

Adicionalmente, en aplicaciones S/MIME, el mensaje de datos contiene una cadena de certificados, incluyendo los certificados CIC con las claves públicas de las Entidades de Certificación de la jerarquía (en este caso, de EC-SECTORPUBLIC y del EC-ACC), que de este modo son distribuidas a los usuarios.

6.1.5. Medidas de claves

Las claves de EC-SECTORPUBLIC son de mínimo de 2.048 bits.

Las claves de todos los certificados emitidos por EC-SECTORPUBLIC son de mínimo 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

Conforme a aquello establecido en la Política General de Certificación.

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

Conforme a aquello establecido en la Política General de Certificación.

6.1.9. Propósitos de uso de claves

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

6.2. Protección de la clave privada

6.2.1. Módulos de protección de la clave privada

6.2.1.1. Estándares de los módulos criptográficos

Conforme a aquello establecido en la Política General de Certificación.

6.2.1.2. Ciclo de vida de las tarjetas con circuito integrado

Conforme a aquello establecido en la Política General de Certificación.

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

Conforme a aquello establecido en la Política General de Certificación.

6.2.3. Depósito de la clave privada

Conforme a aquello establecido en la Política General de Certificación.

6.2.4. Copia de seguridad de la clave privada

Conforme a aquello establecido en la Política General de Certificación.

6.2.5. Archivo de la clave privada

Conforme a aquello establecido en la Política General de Certificación.

6.2.6. Introducción de la clave privada en el módulo criptográfico

Conforme a aquello establecido en la Política General de Certificación.

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

Conforme a aquello establecido en la Política General de Certificación.

6.2.8. Método de activación de la clave privada

Se requieren al menos dos personas para activar la clave privada de EC-SECTORPUBLIC.

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

6.2.9. Método de desactivación de la clave privada

Conforme a aquello establecido en la Política General de Certificación.

6.2.10. Método de destrucción de la clave privada

Conforme a aquello establecido en la Política General de Certificación.

6.2.11. Clasificación de los módulos criptográficos

Conforme a aquello establecido en la Política General de Certificación.

6.3. Otros aspectos de gestión del par de claves

6.3.1. Archivo de la clave pública

EC-SECTORPUBLIC archiiva sus claves públicas, de acuerdo con aquello establecido en la sección 6.2.

6.3.2. Periodos de utilización de las claves pública y privada

Conforme a aquello establecido en la Política General de Certificación.

6.4. Datos de activación

6.4.1. Generación e instalación de los datos de activación

Conforme a aquello establecido en la Política General de Certificación.

6.4.2. Protección de los datos de activación

Conforme a aquello establecido en la Política General de Certificación.

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

Conforme a aquello establecido en la Política General de Certificación.

6.5.2. Evaluación del nivel de seguridad informática

La aplicación de autoridad de certificación, mediante la cual opera EC-SECTORPUBLIC (EJBCA Enterprise Edition) es fiable, dado que obtuvo la certificación Common Criteria EAL 4+.

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

Conforme a aquello establecido en la Política General de Certificación.

6.6.2. Controles de gestión de seguridad

Conforme a aquello establecido en la Política General de Certificación.

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

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

6.6.3. Evaluación del nivel de seguridad del ciclo de vida

Sin estipulación adicional.

6.7. Controles de seguridad de red

Se garantiza que el acceso en las diferentes redes de EC-SECTORPUBLIC 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 EC-SECTORPUBLIC
- Los datos sensibles (incluyendo los datos de registro del suscriptor) se protegen cuando se intercambian a través de redes no seguras
- Se garantiza que los componentes locales de red (como enrutadores/routers) se encuentran ubicados en entornos seguros; también se garantiza la auditoría periódica de sus configuraciones.

6.8. Sello de tiempo

Sin estipulación adicional.

7. Perfiles de certificados y listas de certificados revocados

7.1. Perfil de certificado

Conforme a aquello establecido en la Política General de Certificación.

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

7.2. Perfil de la lista de revocación de certificados

Conforme a aquello establecido en la Política General de Certificación.

8. Auditoría de conformidad

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

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

8.1. Frecuencia de la auditoría de conformidad

Conforme a aquello establecido en la Política General de Certificación.

8.2. Identificación y cualificación del auditor

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

8.3. Relación del auditor con la entidad auditada

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

8.4. Relación de elementos objeto de auditoría

Conforme a aquello establecido en la Política General de Certificación.

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

Conforme a aquello establecido en la Política General de Certificación.

8.6. Tratamiento de los informes de auditoría

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

9. Requisitos comerciales y legales

9.1. Tarifas

9.1.1. Tarifa de emisión o renovación de certificados

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

9.1.2. Tarifa de acceso a certificados

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

9.1.3. Tarifa de acceso a información de estado de certificado

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

9.1.4. Tarifas otros servicios

Sin estipulación adicional.

9.1.5. Política de reintegro

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

9.2. Capacidad financiera

9.2.1. Seguro de responsabilidad civil

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

9.2.2. Otros activos

Sin estipulación adicional.

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

En caso de uso incorrecto o no autorizado de los certificados, el Consorci AOC (o EC-SECTORPUBLIC) no actuará como agente fiduciario ante suscriptores y terceras personas, que tendrán que dirigirse contra el infractor de las condiciones de uso de los certificados establecidas por el Consorci AOC (o EC-SECTORPUBLIC).

9.3. Confidencialidad

9.3.1. Informaciones confidenciales

Conforme a aquello establecido en la Política General de Certificación.

9.3.2. Informaciones no confidenciales

Conforme a aquello establecido en la Política General de Certificación.

9.3.3. Responsabilidad para la protección de información confidencial

Conforme a aquello establecido en la Política General de Certificación.

9.4. Protección de datos personales

9.4.1. Política de Protección de Datos Personales

Conforme a aquello establecido en la Política General de Certificación.

9.4.2. Datos de carácter personal no disponibles a terceros

Conforme a aquello establecido en la Política General de Certificación.

9.4.3. Datos de carácter personal disponibles a terceros

Conforme a aquello establecido en la Política General de Certificación.

9.4.4. Responsabilidad correspondiente a la protección de datos personales

Conforme a aquello establecido en la Política General de Certificación.

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

Conforme a aquello establecido en la Política General de Certificación.

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

Conforme a aquello establecido en la Política General de Certificación.

9.4.7. Comunicación de datos personales

Conforme a aquello establecido en la Política General de Certificación.

9.5. Derechos de propiedad intelectual

9.5.1. Propiedad de los certificados e información de revocación

Conforme a aquello establecido en la Política General de Certificación.

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

Conforme a aquello establecido en la Política General de Certificación.

9.5.3. Propiedad de la información relativa a nombres

Conforme a aquello establecido en la Política General de Certificación.

9.5.4. Propiedad de claves

Conforme a aquello establecido en la Política General de Certificación.

9.6. Obligaciones y responsabilidad civil

9.6.1. Entidades de Certificación

9.6.1.1. Obligaciones generales de EC-SECTORPUBLIC

Conforme a aquello establecido en la Política General de Certificación.

9.6.1.2. Requisitos específicos para los certificados personales

Conforme a aquello establecido en la Política General de Certificación.

9.6.1.3. Información adicional para el CDS-1, CDS-1 EV, y CDS-1 Sede electrónica

Conforme a aquello establecido en la Política General de Certificación.

Las obligaciones allá establecidas se ejercitan dentro del marco de las políticas, prácticas y normativas generales de la jerarquía pública de certificación de Cataluña.

9.6.1.4. Garantías ofrecidas a suscriptores y verificadores

Conforme a aquello establecido en la Política General de Certificación.

9.6.2. Obligaciones y otros compromisos de las Entidades de Registro

9.6.2.1. Obligaciones y otros compromisos

Conforme a aquello establecido en la Política General de Certificación.. Exceptuando la obligación de almacenar las hojas de entrega de certificado durante un periodo de 15 años, que es asumida por las entidades suscriptoras de los certificados corporativos que emite EC-SECTORPUBLIC.

En en cuanto al número de operadores de la autoridad de registro que esta tiene que nombrar: para EC-SECTORPUBLIC tendrán que ser cuatro o más de los empleados que trabajen para ella.

9.6.3. Obligaciones y otros compromisos de las entidades suscriptoras de los certificados corporativos emitidos por EC-SECTORPUBLIC

Las entidades suscriptoras de los certificados emitidos por EC-SECTORPUBLIC se obligan a almacenar las hojas de entrega de certificado durante un periodo de 15 años.

Estos registros tienen que estar a disposición de la Entidad de Certificación Vinculada.

9.6.4. Garantías ofrecidas a suscriptor y verificadores

9.6.4.1. Garantía del Consorci AOC por los servicios de certificación digital

Conforme a aquello establecido en la Política General de Certificación.

9.6.4.2. Exclusión de la garantía

Conforme a aquello establecido en la Política General de Certificación.

9.6.5. Suscriptores

9.6.5.1. Obligaciones y otros compromisos

9.6.5.1.1. Informaciones para todos los tipos de certificados

Conforme a aquello establecido en la Política General de Certificación.

9.6.5.1.2. Informaciones específicas para los certificados de firma electrónica cualificada

Conforme a aquello establecido en la Política General de Certificación.

9.6.5.2. Garantías ofrecidas por el suscriptor

Conforme a aquello establecido en la Política General de Certificación.

9.6.5.3. Protección de la clave privada

Conforme a aquello establecido en la Política General de Certificación.

9.6.6. Verificadores

9.6.6.1. Obligaciones y otros compromisos

Conforme a aquello establecido en la Política General de Certificación.

9.6.6.2. Garantías ofrecidas por el verificador

Conforme a aquello establecido en la Política General de Certificación.

9.6.7. Otros participantes

9.6.7.1. Obligaciones y garantías del directorio

Conforme a aquello establecido en la Política General de Certificación.

9.6.7.2. Garantías ofrecidas por el directorio

EC-SECTORPUBLIC tiene la responsabilidad civil del directorio de certificación.

9.7. Renuncias de garantías

9.7.1. Rechazo de garantías de EC-SECTORPUBLIC

EC-SECTORPUBLIC puede rechazar todas las garantías del servicio que no se encuentren vinculadas a obligaciones establecidas por la Ley 59/2003, de 19 de diciembre, incluyendo especialmente la garantía de adaptación para un propósito particular o garantía de uso mercantil del certificado.

9.8. Limitaciones de responsabilidad

9.8.1. Limitaciones de responsabilidad de EC-SECTORPUBLIC

Más allá de las limitaciones de los prestadores de servicios de certificación establecidas al artículo 23 de la Ley 59/2003, de 19 de diciembre, EC-SECTORPUBLIC 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).

Y, para determinados tipo de certificados, EC-SECTORPUBLIC limita 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

EC-SECTORPUBLIC incluye cláusulas para limitar su responsabilidad en caso fortuito y en caso de fuerza mayor, en los instrumentos jurídicos con los suscriptores.

9.9. Indemnizaciones

9.9.1. Clàusula de indemnización de suscriptor

No se establecerá cláusula de indemnización al suscriptor.

9.9.2. Cláusula de indemnización de verificador

No se establecerá cláusula de indemnización del verificador.

9.10. Plazo y finalización

9.10.1. Plazo

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

9.10.2. Finalización

EC-SECTORPUBLIC establece, en sus instrumentos jurídicos con los suscriptores, una cláusula que determina las consecuencias de la finalización de la relación jurídica en virtud de la cual los suministra certificados.

9.10.3. Supervivencia

Conforme a aquello establecido en la Política General de Certificación.

9.11. Notificaciones

Conforme a aquello establecido en la Política General de Certificación.

9.12. Modificaciones

9.12.1. Procedimiento para las modificaciones

Conforme a aquello establecido en la Política General de Certificación.

9.12.2. Plazo y mecanismos para notificaciones

Les modificacions d'aquest document seran aprovades pel Consorci AOC, conforme s'estableix a l'apartat 1.5.

9.12.3. Circunstancias en las que un OID tiene que ser cambiado

Sin estipulación adicional.

9.13. Resolución de conflictos

9.13.1. Resolución extrajudicial de conflictos

Conforme a aquello establecido en la Política General de Certificación.

9.13.2. Jurisdicción competente

Conforme a aquello establecido en la Política General de Certificación.

9.14. Ley aplicable

Conforme a aquello establecido en la Política General de Certificación.

9.15. Conformidad con la ley aplicable

Conforme a aquello establecido en la Política General de Certificación.

9.16. Cláusulas diversas

9.16.1. Acuerdo íntegro

Conforme a aquello establecido en la Política General de Certificación.

9.16.2. Subrogación

Conforme a aquello establecido en la Política General de Certificación.

9.16.3. Divisibilidad

Conforme a aquello establecido en la Política General de Certificación.

9.16.4. Aplicaciones

Sin estipulación adicional.

9.16.5. Otras cláusulas

Sin estipulación adicional.

10. ANEXO – Control documental

Proyecto:	**Informe creació del document DPC EC-SECTORPUBLIC**
Entidad de destino:	**Servicio SCD - Consorci AOC**
Código de referencia:	**Revisión 1er trimestre 2018**
Versión:	**Versión inicial**
Fecha de la edición:	**09/05/2018**

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Todo el documento	Redacción inicial de la Declaración de Prácticas de Certificación de EC-SECTORPUBLIC	Servicio CATCert del Consorci AOC	08/2015
2.0	Todo el documento	Adaptación a requisitos eIDAS	Servicio SCD del Consorci AOC	09/05/2018