



**Consorci
Administració Oberta
de Catalunya**


Política General de Certificación Consorci AOC

Referencia: D1111_E0650_N-PGdC

Versión: 4.2

Fecha: 03/08/2016

Control documental

Estado formal	Elaborado por:		Aprobado por:
	Servei de Certificació Digital –Consorci AOC		Direcció del Consorci AOC
Fecha de creación	27/08/2007		
Control de versiones	Fecha:	03/08/2016	
	Descripción:	Revisión global. Integración de CATCert en Consorci AOC	
Nivel de acceso información	pública		
Título	Política General de Certificación		
Fichero	D1111 E0650 N-PGdC v4r2 CAS		
Control de copias	Sólo las copias disponibles en https://www.aoc.cat/ garantizan la actualización de los documentos. Toda copia impresa o guardada en ubicaciones diferentes se considerarán copias no controladas.		
Derechos de Autor	 Esta obra está sujeta a una licencia Reconocimiento-No Comercial-Sin obras derivadas 3.0 España de Creative Commons. Para ver una copia, visitad http://creativecommons.org/licenses/by-nc-nd/3.0/es/deed.ca o enviad una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.		

Índice

Índice.....	3
1. Introducción.....	11
1.1 ANTECEDENTES	11
1.2 PRESENTACIÓN	12
1.2.1 Términos habituales utilizados en este documento	12
1.2.2 Tipos y clases de certificados	15
1.2.3 Relación entre la política de certificación y otros documentos	20
1.3 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN	21
1.4 COMUNIDAD DE USUARIOS DE CERTIFICADOS	22
1.4.1 Prestadores de servicios de certificación	22
1.4.2 Entidad de Certificación Raíz	22
1.4.3 Entidades de Certificación Vinculadas	23
1.4.4 Entidades de Registro	23
1.4.5 Usuarios finales	24
1.5 USO DE LOS CERTIFICADOS	25
1.5.1 Usos típicos de los certificados	25
1.5.2 Aplicaciones prohibidas	30
1.6 ADMINISTRACIÓN DE LA POLÍTICA	33
1.6.1 Organización que administra la especificación	33
1.6.2 Datos de contacto de la organización	33
1.6.3 Persona que determina la conformidad de una DPC con la política	34
1.6.4 Procedimiento de aprobación	34
2. Publicación de información y directorio de certificados	35
2.1 DIRECTORIO DE CERTIFICADOS	35
2.2 PUBLICACIÓN DE INFORMACIÓN DE LA ENTIDAD DE CERTIFICACIÓN	35
2.3 FRECUENCIA DE PUBLICACIÓN	35
2.4 CONTROL DE ACCESO	36
3. Identificación y autenticación	37
3.1 GESTIÓN DE NOMBRES	37
3.1.1 Tipos de nombres	37
3.1.2 Significado de los nombres	37
3.1.3 Utilización de anónimos y seudónimos	37
3.1.4 Interpretación de formatos de nombres	38
3.1.5 Unicidad de los nombres	38
3.1.6 Resolución de conflictos relativos a nombres	38
3.2 VALIDACIÓN INICIAL DE LA IDENTIDAD	40

3.2.1	Prueba de posesión de clave privada	40
3.2.2	Autenticación de la identidad de una organización	40
3.2.3	Comprobaciones a realizar en el caso de solicitudes de certificados de dispositivo servidor seguro	42
3.2.4	Autenticación de la identidad de una persona física	42
3.2.5	Información de suscriptor no verificada	44
3.3	IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITUDES DE RENOVACIÓN	44
3.3.1	Validación para la renovación rutinaria de certificados9F	44
3.3.2	Validación para la renovación de certificados después de la revocación0F ...	45
3.4	IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SOLICITUD DE REVOCACIÓN1F.....	45
3.5	AUTENTICACIÓN DE UNA PETICIÓN DE SUSPENSIÓN	45
4.	Características de operación del ciclo de vida de los certificados.....	46
4.1	SOLICITUD DE EMISIÓN DE CERTIFICADO	46
4.1.1	Legitimación para solicitar la emisión	46
4.1.2	Procedimiento de alta; Responsabilidades	48
4.2	PROCESAMIENTO DE LA SOLICITUD DE CERTIFICACIÓN	49
4.2.1	Requisitos para todos los tipos de certificados	49
4.2.2	Requisitos específicos para el CIC	49
4.2.3	Requisitos para los certificados personales.....	50
4.2.4	Requisitos para los certificados de entidad.....	51
4.2.5	Requisitos para los certificados de dispositivo.....	51
4.3	EMISIÓN DE CERTIFICADO	52
4.3.1	Acciones de la Entidad de Certificación durante los procesos de emisión y de renovación.....	52
4.3.2	Comunicación de la emisión al suscriptor.....	53
4.4	ACEPTACIÓN DEL CERTIFICADO	53
4.4.1	Responsabilidades de la Entidad de Certificación	53
4.4.2	Conducta que constituye aceptación del certificado	54
4.4.3	Publicación del certificado	54
4.4.4	Comunicación de la emisión a terceros	54
4.5	USO DEL PAR DE CLAVES Y DEL CERTIFICADO	54
4.5.1	Uso por parte de los poseedores de claves.....	55
4.5.2	Uso por el tercero que confía en certificados.....	55
4.6	RENOVACIÓN DE CERTIFICADOS SIN RENOVACIÓN DE CLAVES	55
4.7	RENOVACIÓN DE CERTIFICADO CON RENOVACIÓN DE CLAVES	56
4.8	RENOVACIÓN TELEMÀTICA	56
4.9	MODIFICACIÓN DE CERTIFICADOS.....	56
4.10	REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.....	57

4.10.1	Causas de revocación de certificados	57
4.10.2	Legitimación para solicitar la revocación	59
4.10.3	Procedimientos de solicitud de revocación	60
4.10.4	Plazo temporal de solicitud de revocación	60
4.10.5	Plazo máximo de procesamiento de la solicitud de revocación	60
4.10.6	Obligación de consulta de información de revocación de certificados	61
4.10.7	Frecuencia de emisión de listas de revocación de certificados (LCRs)	61
4.10.8	Periodo máximo de publicación de LCRs	62
4.10.9	Disponibilidad de servicios de comprobación de estado de certificados	62
4.10.10	Obligación de consulta de servicios de comprobación de estado de certificados	62
4.10.11	Otras formas de información de revocación de certificados	62
4.10.12	Requerimientos especiales en caso de compromiso de la clave privada ...	62
4.10.13	Causas de suspensión de certificados	63
4.10.14	Efecto de la suspensión de certificados	63
4.10.15	Quien puede solicitar la suspensión	64
4.10.16	Procedimientos de solicitud de suspensión	64
4.10.17	Plazo máximo de suspensión	65
4.10.18	Habilitación de un certificado suspendido	65
4.11	SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS	65
4.11.1	Características de operación de los servicios	65
4.11.2	Disponibilidad de los servicios	65
4.11.3	Otras funciones de los servicios	65
4.12	FINALIZACIÓN DE LA SUSCRIPCIÓN	66
4.13	DEPÓSITO Y RECUPERACIÓN DE CLAVES	66
4.13.1	Política y prácticas de depósito y recuperación de claves	66
4.13.2	Política y prácticas de encapsulamiento y recuperación de claves de sesión	66
5.	Controles de seguridad física, de gestión y de operaciones	67
5.1	CONTROLES DE SEGURIDAD FÍSICA	67
5.1.1	Localización y construcción de las instalaciones	67
5.1.2	Acceso físico	68
5.1.3	Electricidad y aire acondicionado	68
5.1.4	Exposición al agua	68
5.1.5	Advertencia y protección de incendios	68
5.1.6	Almacenaje de soportes	69
5.1.7	Tratamiento de residuos	69

5.1.8	Copia de seguridad fuera de las instalaciones	69
5.2	CONTROLES DE PROCEDIMIENTOS	69
5.2.1	Funciones fiables	70
5.2.2	Número de personas por tarea	70
5.2.3	Identificación y autenticación para cada función	70
5.2.4	Roles que requieren separación de tareas	70
5.3	CONTROLES DE PERSONAL	71
5.3.1	Requisitos de historial, calificaciones, experiencia y autorización	71
5.3.2	Requisitos de formación	71
5.3.3	Requisitos y frecuencia de actualización formativa	72
5.3.4	Secuencia y frecuencia de rotación laboral	72
5.3.5	Sanciones por acciones no autorizadas	72
5.3.6	Requisitos de contratación de profesionales	72
5.3.7	Suministro de documentación al personal	72
5.4	PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD	73
5.4.1	Tipos de acontecimientos registrados	73
5.4.2	Frecuencia de tratamiento de registros de auditoría	73
5.4.3	Periodo de conservación de registros de auditoría	74
5.4.4	Protección de los registros de auditoría	74
5.4.5	Procedimientos de backup	74
5.4.6	Localización del sistema de acumulación de registros de auditoría	74
5.4.7	Notificación del acontecimiento de auditoría al causante del acontecimiento	74
5.4.8	Análisis de vulnerabilidades	74
5.5	ARCHIVO DE INFORMACIONES	75
5.5.1	Tipos de acontecimientos registrados	75
5.5.2	Periodo de conservación de registros	75
5.5.3	Protección del archivo	75
5.5.4	Procedimientos de copia de soporte	76
5.5.5	Requisitos de sellado de fecha y hora	76
5.5.6	Localización del sistema de archivo	76
5.5.7	Procedimientos de obtención y verificación de información de archivo	76
5.6	RENOVACIÓN DE CLAVES	76
5.7	COMPROMISO DE CLAVES Y RECUPERACIÓN DE DESASTRE	77
5.7.1	Procedimiento de gestión de incidencias y compromisos	77
5.7.2	Corrupción de recursos, aplicaciones o datos	77
5.7.3	Compromiso de la clave privada de la Entidad	77

5.7.4	Desastre sobre las instalaciones.....	77
5.8	FINALIZACIÓN DEL SERVICIO	78
5.8.1	Entidad de Certificación.....	78
5.8.2	Entidad de Registro.....	78
6.	Controles de seguridad técnica	79
6.1	GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES.....	79
6.1.1	Generación del par de claves	79
6.1.2	Envío de la clave privada al suscriptor	79
6.1.3	Envío de la clave pública al emisor del certificado.....	79
6.1.4	Distribución de la clave pública del Prestador de Servicios de Certificación ..	80
6.1.5	Medidas de claves.....	80
6.1.6	Generación de parámetros de clave pública.....	80
6.1.7	Comprobación de calidad de parámetros de clave pública	80
6.1.8	Generación de claves en aplicaciones informáticas o en bienes de equipo...81	
6.1.9	Propósitos de uso de claves.....	81
6.2	PROTECCIÓN DE LA CLAVE PRIVADA.....	81
6.2.1	Módulos de protección de la clave privada	81
6.2.2	Control por más de una persona (n de m) sobre la clave privada	82
6.2.3	Depósito de la clave privada.....	82
6.2.4	Backup de la clave privada.....	82
6.2.5	Archivo de la clave privada.....	83
6.2.6	Introducción de la clave privada en el módulo criptográfico	83
6.2.7	Almacenaje de la clave privada en el módulo criptográfico.....	83
6.2.8	Método de activación de la clave privada	83
6.2.9	Método de desactivación de la clave privada	84
6.2.10	Método de destrucción de la clave privada.....	84
6.2.11	Clasificación de los módulos criptográficos	84
6.3	OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES.....	84
6.3.1	Archivo de la clave pública	84
6.3.2	Periodos de utilización de las claves pública y privada.....	84
6.4	DATOS DE ACTIVACIÓN	85
6.4.1	Generación e instalación de los datos de activación	85
6.4.2	Protección de datos de activación	85
6.4.3	Otros aspectos de los datos de activación.....	85
6.5	CONTROLES DE SEGURIDAD INFORMÁTICA.....	85

6.5.1	Requisitos técnicos específicos de seguridad informática	85
6.5.2	Evaluación del nivel de seguridad informática	86
6.6	CONTROLES TÉCNICOS DEL CICLO DE VIDA	86
6.6.1	Controles de desarrollo de sistemas.....	86
6.6.2	Controles de gestión de seguridad	86
6.6.3	Evaluación del nivel de seguridad del ciclo de vida	87
6.7	CONTROLES DE SEGURIDAD DE RED.....	87
6.8	SELLO DE TIEMPO	87
7.	Perfiles de certificados y listas de certificados revocados	88
7.1	PERFIL DE CERTIFICADO	88
7.1.1	Número de versión	89
7.1.2	Extensiones de certificado.....	89
7.1.3	Identificadores de objeto de algoritmos	89
7.1.4	Formatos de nombres	89
7.1.5	Restricciones de nombres	89
7.1.6	Identificador de objeto de política de certificado	89
7.1.7	Uso de la extensión restricciones de política	90
7.1.8	Sintaxis y semántica de los calificadores de política127F	90
7.1.9	Semántica del proceso de la extensión crítica de la política de certificado	90
7.1.10	Especificaciones técnicas para todas las Entidades de Certificación.....	90
8.	Auditoría de conformidad	91
8.1	FRECUENCIA DE LA AUDITORÍA DE CONFORMIDAD	91
8.2	IDENTIFICACIÓN Y CALIFICACIÓN DEL AUDITOR.....	91
8.3	RELACIÓN DEL AUDITOR CON LA ENTIDAD AUDITADA	91
8.4	RELACIÓN DE ELEMENTOS OBJETO DE AUDITORÍA	92
8.5	ACCIONES A EMPRENDER COMO RESULTADO DE UNA FALTA DE CONFORMIDAD.....	92
8.6	TRATAMIENTO DE LOS INFORMES DE AUDITORÍA	92
9.	Requisitos comerciales y legales.....	93
9.1	TARIFAS.....	93
9.1.1	Tarifa de emisión o renovación de certificados	93
9.1.2	Tarifa de acceso a certificados	93
9.1.3	Tarifa de acceso a información de estado de certificado	93
9.1.4	Tarifas de otros servicios.....	93
9.1.5	Política de reintegro	93
9.2	CAPACIDAD FINANCIERA.....	93
9.2.1	Seguro de responsabilidad civil	93
9.2.2	Otros activos	94

9.2.3	Cobertura de aseguramiento para suscriptores y terceros que confíen en certificados	94
9.3	CONFIDENCIALIDAD	94
9.3.1	Informaciones confidenciales	94
9.3.2	Informaciones no confidenciales	94
9.3.3	Responsabilidad para la protección de información confidencial	94
9.4	PROTECCIÓN DE DATOS PERSONALES.....	95
9.4.1.	Política de Protección de Datos Personales	95
9.4.2.	Datos de carácter personal no disponibles a terceros	96
9.4.3.	Datos de carácter personal disponibles a terceros	97
9.4.4.	Responsabilidad correspondiente a la protección de datos personales.....	97
9.4.5.	Gestión de incidencias relacionadas con los datos de carácter personal.....	98
9.4.6.	Prestación del consentimiento para el tratamiento de los datos personales	99
9.4.7.	Comunicación de datos personales	99
9.5	DERECHOS DE PROPIEDAD INTELECTUAL.....	99
9.5.1	Propiedad de los certificados e información de revocación	99
9.5.2	Propiedad de la política de certificado y Declaración de Prácticas de Certificación.....	100
9.5.3	Propiedad de la información relativa a nombres	100
9.5.4	Propiedad de claves	100
9.6	OBLIGACIONES Y RESPONSABILIDAD CIVIL.....	100
9.6.1	Entidades de Certificación	100
9.6.2	Entidades de Registro	104
9.6.3	Suscriptores	107
9.6.4	Verificadores	109
9.6.5	Otros Participantes	110
9.7	RENUNCIAS DE GARANTÍAS	110
9.7.1	Renuncia de garantías de la Entidad de Certificación.....	110
9.8	LIMITACIONES DE RESPONSABILIDAD	111
9.8.1	Limitaciones de responsabilidad de la Entidad de Certificación.....	111
9.8.2	Caso fortuito y fuerza mayor.....	111
9.9	INDEMNIZACIONES	111
9.9.1	Cláusula de indemnidad de suscriptor	111
9.9.2	Cláusula de indemnidad de verificador	111
9.10	PLAZO Y FINALIZACIÓN	111
9.10.1	Plazo	111

9.10.2	Finalización	112
9.10.3	Supervivencia.....	112
9.11	NOTIFICACIONES	112
9.12	MODIFICACIONES	112
9.12.1	Procedimiento para las modificaciones	112
9.12.2	Periodo y mecanismos para notificaciones.....	113
9.12.3	Circunstancias en las que un OID tiene que ser cambiado.....	113
9.13	RESOLUCIÓN DE CONFLICTOS.....	113
9.13.1	Resolución extrajudicial de conflictos	113
9.13.2	Jurisdicción competente	113
9.14	LEY APLICABLE	114
9.15	CONFORMIDAD CON LA LEY APLICABLE	114
9.16	CLÁUSULAS DIVERSAS	114
9.16.1	Acuerdo íntegro.....	114
9.16.2	Subrogación	114
9.16.3	Divisibilidad	115
9.16.4	Aplicaciones	115
9.16.5	Otras cláusulas.....	115
ANEXO – Control documental		116
CONTROL DE VERSIONES PGDC 1ER SEMESTRE 2016.....		116

1. Introducción

1.1 Antecedentes

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

En cumplimiento de dicho pacto institucional y para desarrollar el programa Catalunya en Xarxa (Cataluña en Red), Localret y la Generalitat de Catalunya acordaron la creación del Consorci per a l'Administració Oberta Electrónica de Catalunya (Consortio para la Administración Abierta Electrónica de Catalunya), con la finalidad de desarrollar políticas públicas en materia de servicios electrónicos a las administraciones públicas y de ejercer la condición de autoridad (técnica) de certificación de firma electrónica para garantizar el secreto, la integridad, la identidad y la autenticidad en las comunicaciones y documentos electrónicos que se producen en el ámbito de las administraciones públicas catalanas.

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

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

Por tanto, la Agencia Catalana de Certificació se constituyó en la entidad principal del sistema público catalán de certificación que regulaba la emisión y la gestión de los certificados que se emitieran para las instituciones de autogobierno de Catalunya, las instituciones que integran el mundo local, y el resto de entidades públicas y privadas que integran el sector público catalán; así como la admisión y el uso de los certificados emitidos a ciudadanos y empresas por otros prestadores de servicios de certificación y que solicitaran la correspondiente clasificación.

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

En fecha 2 de agosto de 2011, el Gobierno de la Generalitat de Catalunya aprobó el acuerdo sobre medidas de racionalización y simplificación de la estructura del sector público de Catalunya, en el marco de las cuales se instaba a los departamentos competentes a formular e implantar estrategias de reordenación de su sector público que

incidieran especialmente en la mejora de la eficiencia organizativa de la que cual se ha de derivar una eficiencia económica.

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

En consecuencia, la Comisión Ejecutiva del Consorcio AOC acordó la reversión al Consorcio de los servicios gestionados hasta la fecha por CATCert, con la incorporación a aquel de los medios materiales, económicos y humanos correspondientes, así como la gestión directa del servicio de certificación digital y todas las funciones generales del conjunto de la organización.

De manera que ahora el Consorci Administració Oberta de Catalunya es el prestador de los servicios de certificación (TSP) públicos de Catalunya y el propietario de la infraestructura de clave pública (PKI) que antes era titularidad de CATCert.

1.2 Presentación

Uno de los elementos más importantes de la jerarquía pública de certificación de Cataluña es la redacción y la publicación de una política general de certificación – contenida en este documento – que, en forma de requisitos y condiciones, será aplicable a todos los certificados que se emitan a personas físicas y jurídicas por las diferentes entidades de certificación que se vinculen a la jerarquía. Asimismo, los requisitos y condiciones establecidos en esta política han de ayudar a la homologación de las políticas de certificados de terceros prestadores, a efectos de la oportuna clasificación y admisión por las administraciones públicas catalanas de dichos certificados.

La aparición de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, implicó el reconocimiento de las especificidades de la firma electrónica de las administraciones públicas, con la regulación de los certificados digitales correspondientes en la sede electrónica, el sello de actuación administrativa automatizada y la firma electrónica del personal al servicio de las administraciones públicas, reforzando la aproximación inicialmente adoptada por CATCert para la prestación de sus servicios. Asimismo, la regulación propuesta exigió la revisión de los contenidos de la política general de certificación en relación con estos tipos de certificados, sin afectar al resto del modelo de certificación del sistema público catalán.

Más allá, el servicio de certificación digital del Consorci AOC cumple con la versión actual de las pautas del CA/Browser Forum para la emisión y la gestión de certificados de validación extendida (*extended validation*) publicadas en: <http://www.cabforum.org>.

1.2.1 Términos habituales utilizados en este documento

A continuación, se aportan breves explicaciones del significado que algunos términos tienen en el ámbito de este documento:

Certificado	Documento electrónico firmado por una entidad de certificación, que vincula unos datos de verificación de firma electrónica a una persona (física o jurídica) y confirma su identidad.
Declaración de prácticas de certificación	Documento exigido por la Ley de firma electrónica, que detalla los requisitos que cumple el prestador de servicios de certificación cuando emite certificados.
Entidad de certificación	Persona física o jurídica que emite certificados, de acuerdo con la Ley de firma electrónica. Con frecuencia se trata como un sinónimo de autoridad de certificación, que es un componente técnico del servicio.
Entidad de certificación raíz	Entidad de certificación superior de la jerarquía de certificación, que garantiza legalmente todos los certificados emitidos por las entidades de certificación vinculadas a la jerarquía.
Entidad de certificación vinculada	Entidad de certificación que ha sido vinculada a una jerarquía de certificación, de forma que la entidad de certificación raíz garantiza los certificados emitidos por la entidad vinculada.
Entidad de certificación virtual	Entidad de certificación que ha delegado todas las operaciones técnicas para la emisión de los certificados al Consorci AOC, en su calidad de prestador de servicios de certificación.
Entidad de registro	Persona jurídica que ejecuta los procedimientos de comprobación de la identidad y del resto de circunstancias de los suscriptores y de los poseedores de claves de los certificados. A veces se trata como un sinónimo de autoridad de registro, que es un componente técnico del servicio.
Entidad de registro colaboradora	Entidad de registro que colabora con las entidades de certificación en la emisión de los certificados a los suscriptores.
Entidad de registro interna	Entidad de registro de una administración suscriptora de certificados, que registra a sus poseedores de claves.

Entidad de registro virtual	Entidad de registro interna que ha delegado en la entidad de certificación o en una entidad de registro colaboradora los trabajos técnicos del procedimiento de comprobación de la identidad y del resto de circunstancias personales de los suscriptores y de los poseedores de los certificados.
Jerarquía pública de certificación de Cataluña	Conjunto de entidades públicas catalanas de certificación, entidades de registro y otras que emiten certificados, organizadas en un sistema público controlado y garantizado por el Consorci AOC, que actúa como entidad de certificación raíz por delegación de las instituciones de autogobierno de Cataluña, y de las administraciones públicas catalanas.
Lista de revocación de certificados	Documento electrónico firmado por una entidad de certificación que detalla los certificados que, temporalmente o definitivamente, no son válidos.
Perfil de certificado	Documento que detalla los contenidos de los certificados, sintáctica y semánticamente.
Poseedor de claves	Persona física que recibe un certificado emitido a un suscriptor (que será una entidad, cuando se trate de certificados corporativos, o la propia persona física, cuando se trate de certificados individuales), y que lo utiliza bajo la responsabilidad de dicho suscriptor.
Prestador de servicios de certificación	Persona jurídica que actúa legalmente como entidad de certificación i/o que presta servicios de certificación a terceros, por delegación de una entidad de certificación.
Sello electrónico	De acuerdo con la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, se trata de un sistema de firma electrónica para la actuación administrativa automatizada, basada en certificado electrónico.
Sede Electrónica	De acuerdo con la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, es la dirección electrónica disponible para los ciudadanos a través de las redes de telecomunicaciones la titularidad, gestión y

	administración de la cual corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.
Sistema público catalán de certificación	Conjunto de todas las entidades, públicas y privadas, catalanas, nacionales e internacionales, de certificación, entidades de registro y otras que emitan certificados, organizadas en un sistema público controlado y garantizado por la Agència Catalana de Certificació, que actúa como entidad de clasificación por delegación de las instituciones de autogobierno de Cataluña, y de las administraciones públicas catalanas.
Suscriptor de certificados electrónicos	Es su titular. En certificados expedidos a personas físicas, que actúan individualmente, es la persona física que solicita su certificado y que custodiará los datos de creación de firma (la clave privada). En el caso de certificados corporativos, el suscriptor es la persona jurídica a la cual está vinculado el poseedor de claves.

1.2.2 Tipos y clases de certificados

El Consorci AOC presta sus servicios de certificación con el fin de expedir certificados digitales para diversos usos y diferentes usuarios finales.

Para ello se definieron y se emiten diferentes tipos y clases de certificados digitales, que son los que se describen a continuación. En primer lugar, dentro de la jerarquía pública de certificación de Cataluña, se expiden certificados a otras Entidades de Certificación, que de esta forma quedan vinculadas a la jerarquía. Estos certificados se denominan Certificados de Infraestructura de Entidad de Certificación (CIC), y permiten que las entidades de certificación suscriptoras de los certificados CIC puedan expedir certificados a otras Entidades de Certificación o a usuarios finales.

Los CIC se expiden para ofrecer servicios a una comunidad de usuarios concreta (por ejemplo, el personal de la Generalitat de Catalunya, o de las entidades que integran la Administración local, los ciudadanos, o los docentes y alumnos universitarios, entre otros ejemplos) dentro de la jerarquía pública de certificación de Cataluña, pudiendo ser de diferentes niveles (1, 2 o sucesivos).

Con los certificados CIC, las Entidades de Certificación pueden emitir certificados a usuarios finales o a otras Entidades de Certificación dentro de su propia comunidad de usuarios, en función de las necesidades concretas y siempre que técnicamente no afecte al funcionamiento, en las plataformas, sistemas y aplicaciones habitualmente empleados por los usuarios finales.

Cada certificado CIC recibirá un nivel, adecuado al período de duración de dicho certificado, que se empleará para la programación de la renovación periódica de la infraestructura de certificación.

Los certificados de usuarios finales se dividen en:

- 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 entidad, caracterizados por el hecho que el suscriptor del certificado y, de acuerdo con la ley, firmante, es una persona jurídica, que actúa por medio de un poseedor de claves (también llamado, para estos certificados, “responsable de custodia”)
- Certificados de dispositivo, caracterizados por el hecho que el poseedor de la clave privada es un dispositivo informático que realiza las operaciones de firma y descifrado de forma automática, bajo la responsabilidad de una persona física o jurídica (denominado suscriptor o titular del certificado).

Los certificados de usuario final se emiten en dos modalidades:

- Los certificados de Clase 1 son certificados corporativos, caracterizados por el hecho que el poseedor de la clave privada está vinculado al suscriptor o titular del certificado, que es una organización del sector público. Además, en certificados de entidad, el poseedor de la clave privada ha sido facultado, de acuerdo con la ley de atribuciones aplicable, para la obtención del certificado. La persona física poseedora de la clave privada estará identificada en el certificado. En circunstancias excepcionales, motivadas por la necesidad de garantizar la seguridad de la persona que se identifica o firma, se prevé la posibilidad de utilizar seudónimos en casos especiales como pueden ser certificados de cuerpos de seguridad o de personal vinculado a la administración de justicia, entre otros, de conformidad con lo establecido en el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los Servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. En estos supuestos, se identificará al poseedor de claves de forma indirecta mediante un identificador que permita la identificación de la persona actuante, bajo requerimiento expreso de la autoridad competente a tal fin.

El registro de los datos para la emisión de los certificados de clase 1 lo realiza la entidad suscriptora de dicho certificado, actuando como entidad de registro interna.

- El resto de certificados serán certificados de Clase 2, emitidos en concurrencia con el libre mercado, y habitualmente en régimen de actuación subsidiaria, cuando no existan prestadores que ofrezcan el servicio o el número de los mismos resulte insuficiente para garantizar su distribución efectiva a los usuarios finales (ciudadanos, empresas, profesionales).

El registro de los datos para la emisión de los certificados de clase 2 lo realiza una entidad de registro, bajo la responsabilidad de la Entidad de Certificación.

Los certificados de clase 2 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 mediante un seudónimo en las condiciones descritas para los certificados de clase 1).

De este modo, las Entidades de Certificación de la jerarquía pública de certificación de Cataluña podrán, en función de sus necesidades y de la situación coyuntural del mercado de servicios de certificación, emitir los siguientes grupos de certificados:

- Certificados de entidad de certificación de nivel 2.
- Certificados personales de clase 1 y de clase 2.
- Certificados de entidad de clase 1 y de clase 2.
- Certificados de dispositivos de clase 1 y de clase 2.

Por su parte, resulta competencia exclusiva del Consorci AOC emitir los certificados de entidad de certificación de nivel 1 a nuevas Entidades de Certificación.

A continuación se detallan las diferentes políticas de certificados de infraestructura, personales, de entidad, de dispositivo y de objeto, tanto de clase 1 como de clase 2, que se ofrecen a las Entidades de Certificación y a la comunidad de usuarios, así como las posibles combinaciones y ampliaciones para usos concretos de las mismas.

1.2.2.1 Certificados de infraestructura

Podrán existir los siguientes tipos de certificados de infraestructura:

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

Las Entidades de Certificación vinculadas pueden, a su vez, emitir certificados de infraestructura o certificados de entidad final (personales, de entidad y de dispositivo), según la clase del certificado CIC que posean, desde el momento en el que hayan obtenido un certificado CIC válido, y mientras dicho certificado se encuentre vigente.

- 2) Certificado de infraestructura personal de firma electrónica reconocida de operadores (CIPISR), que se utiliza para autorizar operaciones relacionadas con los servicios de certificación, como la aprobación de solicitudes de certificación.
- 3) Certificado de infraestructura de dispositivo servidor seguro (CIDS), que es utilizado para una aplicación informática servidor de SSL o de TLS de infraestructura para identificarse ante las aplicaciones cliente que se conecten y para proteger el secreto de las comunicaciones entre el cliente y el servidor, como por ejemplo los servidores de las entidades de certificación.
- 4) Certificado de infraestructura de dispositivo de aplicación digitalmente asegurada (CIDA), que es utilizado para aplicaciones informáticas de la infraestructura que se identifiquen digitalmente, firmen electrónicamente *webservices* u otros protocolos y que reciban documentos y mensajes cifrados, como por ejemplo las aplicaciones de notificación de mensajes de las entidades de certificación.
- 5) Certificado de infraestructura de servidor de estado de certificados en línea (CIO), que es utilizado por un servidor *OCSP Responder* para firmar sus respuestas sobre el estado de validez de los certificados.

- 6) Certificado de infraestructura de entidad de sellos de tiempo (CIT), que es utilizado por una entidad para firmar los sellos de tiempo que emite.
- 7) Certificado de infraestructura de entidad de validación (CIV), que es utilizado por un servidor de entidad de validación para firmar sus informes.

1.2.2.2 Certificados personales

Podrán existir las siguientes políticas de certificados personales:

- 1) Certificados personales de firma electrónica reconocida (CPSR), de acuerdo con lo establecido en el artículo 6 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, que permiten que personas físicas, a título individual o por razón de su vinculación con una institución jurídico-pública o privada (cargo, atribución, apoderamiento) firmen documentos con dispositivo seguro de creación de firma.
- 2) Certificados personales de firma electrónica avanzada (CPSA), de acuerdo con lo establecido en el artículo 6 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, que permiten que personas físicas, a título individual o por razón de su vinculación con una institución jurídico-pública o privada (cargo, atribución, apoderamiento) firmen documentos sin dispositivo seguro de creación de firma.
- 3) Certificados personales de identificación (CPI), que se utilizan para firmar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos.
- 4) Certificados personales de cifrado (CPX), que se utilizan para producir o recibir documentos o mensajes confidenciales.

Las anteriores políticas permiten combinaciones entre ellas, dependiendo de las necesidades de los usuarios, de forma que un único certificado puede dar cumplimiento a más de una política. Por ejemplo, resulta frecuente combinar las políticas de firma reconocida y de identificación, dando lugar a certificados de tipo CPISR; o incluso combinar las políticas de identificación, cifrado y firma avanzada, que dan como resultado certificados de tipo CPIXSA.

Adicionalmente, en función de los requisitos técnicos y las necesidades de los usuarios, es posible que dichos tipos de certificado puedan incorporar otras funcionalidades que, en todo caso, serán identificadas en una política específica de certificación, que deberá ser desarrollada o aprobada por el Consorci AOC.

1.2.2.3 Certificados de entidad

Podrán existir cuatro tipos de certificados de entidad:

- 1) Certificados de entidad de firma electrónica reconocida (CESR), de acuerdo con lo establecido en el artículo 7 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, que permiten que instituciones públicas y privada, corporaciones de derecho público y personas jurídico-públicas (colectivamente llamadas “entidades”) firmen documentos con dispositivo seguro de creación de firma.
- 2) Certificados de entidad de firma electrónica avanzada (CESA), según la definición del punto 2 del artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica y de acuerdo con lo establecido en el artículo 7 de la misma ley; que permiten que instituciones públicas y privada, corporaciones de derecho público y

personas jurídico-públicas (colectivamente llamadas “entidades”) firmen documentos sin dispositivo seguro de creación de firma.

- 3) Certificados de entidad para identificación (CEI) que se utilizan para firmar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos
- 4) Certificados de entidad de cifrado (CEX), de acuerdo con lo establecido en el artículo 7 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, que permiten que instituciones públicas y privadas, corporaciones de derecho público y personas jurídico-públicas (colectivamente llamadas “entidades”) puedan producir y recibir documentos confidenciales.

Las anteriores políticas permiten combinaciones entre ellas, dependiendo de las necesidades de los usuarios, de forma que un único certificado puede dar cumplimiento a más de una política. Por ejemplo, resulta frecuente combinar las políticas de firma reconocida y de identificación, dando lugar a certificados de tipo CEISR; o incluso combinar las políticas de identificación, cifrado y firma avanzada, que dan como resultado certificados de tipo CEIXSA.

Adicionalmente, en función de los requisitos técnicos y las necesidades de los usuarios, es posible que dichos tipos de certificado puedan incorporar otras funcionalidades que, en todo caso, serán identificadas en una política específica de certificación, que deberá ser desarrollada o aprobada por el Consorci AOC.

1.2.2.4 Certificados de dispositivo

Podrán existir cuatro tipos de certificado de dispositivo:

- 1) Certificado de firma de aplicaciones informáticas (CDP), que se utiliza para firmar digitalmente aplicaciones informáticas a transmitir por medio de redes.
- 2) Certificado de dispositivo servidor seguro (CDS), que es ocupado por una aplicación informática servidor de SSL o de TLS para identificarse ante las aplicaciones cliente que se conecten y para proteger el secreto de las comunicaciones entre el cliente y el servidor.
- 3) Certificado de dispositivo servidor seguro controlador de dominio (CDSCD), que es ocupado por una aplicación informática servidor de SSL o de TLS para identificar en una red Windows a los usuarios que pertenecen a un determinado dominio, mediante un certificado digital de firma con tarjeta criptográfica.
- 4) Certificado de dispositivo servidor seguro Extended Validation (CDS EV), que es ocupado por una aplicación informática servidor de SSL o de TLS para identificarse ante las aplicaciones cliente que se conecten, y para proteger el secreto de las comunicaciones entre el cliente y el servidor, y que permite la validación automática, de conformidad con las normas establecidas por el CAB Forum.
- 5) Certificado de dispositivo de aplicación digitalmente asegurada (CDA), que es utilizado para aplicaciones informáticas que se identifican digitalmente, firman electrónicamente *webservices* u otros protocolos y que reciban documentos y mensajes cifrados.
- 6) Certificado de dispositivo servidor seguro sede electrónica Extended Validation (CDS Sede Electrónica EV) que es ocupado por una aplicación informática de SSL o de TLS que tanga la consideración de sede electrónica, de conformidad con lo

establecido en la legislación administrativa vigente; este certificado permitirá a la sede electrónica identificarse ante las aplicaciones cliente que se conecten, y protegerá el secreto de las comunicaciones, entre el cliente y el servidor.

- 7) Certificado de dispositivo de aplicación digitalment assegurada sello electrónico (CDA Sello electrónico), que es utilizado para aplicaciones informáticas que realicen actividad administrativa automatitzadade acuerdo con la legislación administrativa vigente, que se identifican digitalmente, firman electrónicamente *webservices* u otros protocolos y que reciban documentos y mensajes cifrados.

Adicionalmente, en función de los requisitos técnicos y las necesidades de los usuarios, es posible que dichos tipos de certificado puedan incorporar otras funcionalidades que, en todo caso, serán identificadas en una política específica de certificación, que deberá ser desarrollada o aprobada por el Consorci AOC.

1.2.2.5 Certificados de pruebas

De cualquiera de los tipos de certificados que recoge la presente política se pueden emitir, bajo determinadas circunstancias, certificados de prueba.

1.2.3 Relación entre la política de certificación y otros documentos

Este documento contiene la política general de certificación del Consorci AOC. Una política de certificación es un conjunto de principios y reglas relativos a la emisión y gestión de certificados digitales, con soporte de claves públicas, que pueden utilizarse en diferentes servicios, como la autenticación de la identidad, la integridad y la autenticidad documental o el secreto de los datos, documentos y transmisiones.

La política de certificación establece las reglas mínimas que se tienen que cumplir por parte de las Entidades de Certificación, los suscriptores y otros usuarios de los certificados emitidos por la jerarquía de certificación del Consorci AOC.

Por otro lado, cada Entidad de Certificación debe disponer de una Declaración de Prácticas de Certificación con los procedimientos que aplica en la prestación de sus servicios, en cumplimiento de lo establecido en el artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, indicando el grado de aplicación de los requisitos establecidos por las políticas de certificados que gestiona y detallando sus prácticas profesionales en relación con la provisión de los servicios de certificación.

La Entidad de Certificación raíz EC-ACC aplicará las normas y principios de la presente Política General de Certificación quecumplirá, en este caso, las funciones de Declaración de Prácticas de Certificación.

Esta documentación se relaciona con documentación auxiliar, entre la que se encuentran los instrumentos jurídicos reguladores de la prestación del servicio (documentación jurídica auxiliar), documentación de seguridad y documentación de operaciones.

1.3 Nombre del documento e identificación

Este documento de políticas de certificación de la jerarquía se denomina “Política General de Certificación – Consorci AOC”-

Esta Política General de Certificación se identifica con el siguiente OID:

1.3.6.1.4.1.15096.1.2.1

Cada política de certificado (básica, resultante de una combinación de políticas o de una política específica de certificado de aplicación general) recibe su propio OID, y que se debe incluir dentro del certificado, en el campo “Información de política” (*Policy Information*), excepto cuando no resulte posible técnicamente.

Cada Entidad de Certificación Vinculada, antes de empezar a emitir certificados, podrá establecer su propia política de certificado para cada tipo y clase de certificado, a partir de lo establecido en este documento, concretando o estableciendo nuevas normas de certificación, con absoluto respeto a las normas de esta política.

Las políticas específicas pueden ser de dos tipos:

- a) Políticas que definen normas aplicables a toda la comunidad de usuarios, con independencia de la Entidad de Certificación que emita el certificado, por ejemplo, la creación de un tipo específico de certificado CPSR, incluyendo el cargo, política que puede ser aplicable a otras Entidades de Certificación.
- b) Políticas que definan o adapten normas aplicables a una parte de la comunidad de usuarios, generalmente dependiendo de una Entidad de Certificación concreta, por ejemplo la adaptación de un CPSR a las necesidades concretas de una Entidad de Certificación, que puede no tener sentido para otras Entidades de Certificación.

Para determinadas políticas se introduce el concepto de “nivel”, en referencia a la robustez criptográfica de las claves, a su generación y su custodia y aplicación. Podrán existir dos niveles en relación con el tipo de certificado:

- a) Nivel alto: la generación, custodia y aplicación de la clave privada debe realizarse:
 - a. Para los certificados personales y de entidad, en dispositivo seguro de creación de firma, de acuerdo con la Ley 59/2003.
 - b. Para los certificados de dispositivo, en maquinaria criptográfica que cumple los requisitos establecidos a cualquier perfil de protección o *security target*, escrito de acuerdo con CC EAL 3 o o FIPS 140-1 o -2 nivel 2, que incorpore los requisitos del CEN *Workshop Agreement* CWA14167-1 para certificados no cualificados (reconocidos) o de conformidad con otros esquemas de certificación (ITSEC), que incorpora los requisitos de CEN *Workshop Agreement* CWA14167-1 para certificados no cualificados(reconocidos).
- b) Nivel medio: la generación, custodia y aplicación de la clave privada puede realizarse en módulos criptográficos en programario y los algoritmos y sus parámetros serán los comúnmente utilizados.

Cada política básica de certificado, cada combinación de políticas de certificado, y cada política específica de certificado dispondrá de su propio OID, que se especificará en la Declaración de Prácticas de Certificación correspondiente.

Este OID será asignado por el Consorci AOC, dentro de su rama de OIDs 1.3.6.1.4.1.15096.1.3.1. De esta manera se declarará la conformidad del tipo de certificado con esta política general¹

1.4 Comunidad de usuarios de certificados

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

Los certificados de clase 1 se expiden a las instituciones de autogobierno de Cataluña, las instituciones que integran el mundo local, y el resto de entidades que integran el Sector Público de Cataluña (en adelante, “las instituciones”); los reciben y los utilizan su personal, sus entidades y sus dispositivos.

Los certificados de clase 2 pueden expedirse, en libre concurrencia con otros prestadores de servicios de certificación, a personas físicas y jurídicas, incluidas aquellas sujetas a una relación administrativa de sujeción especial – como la de los estudiantes universitarios con la universidad pública en la que cursan sus estudios superiores, o la de las empresas privadas cuando contratan con la Administración pública.

1.4.1 Prestadores de servicios de certificación

De acuerdo con la Ley 59/2003, de 19 de diciembre, de firma electrónica, 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.

El Consorci AOC es el prestador de servicios de certificación público de Cataluña.

Conforme a esta función, el Consorci AOC ofrece servicios a diversas entidades de certificación de entidades del Sector Público de Cataluña, mediante sistemas técnicos de autoridad de certificación diferenciados y vinculados a la jerarquía pública de certificación de Cataluña. Y es responsable por la actuación de estos sistemas ante sus usuarios finales y ante los terceros verificadores de los certificados digitales emitidos.

1.4.2 Entidad de Certificación Raíz

La Entidad de Certificación Raíz dispone de un sistema técnico de autoridad de certificación principal, que tiene la finalidad de integrar otras entidades de certificación en el sistema público catalán de certificación mediante la vinculación técnica de las autoridades de certificación correspondientes a la jerarquía pública de certificación de Cataluña.

Esta vinculación técnica se consigue mediante la emisión de certificados CIC, de nivel 1 y de nivel 2, de acuerdo con lo establecido en esta Política General de Certificación.

¹ TS 101 456: 8.4; TS 102042: 8.3

1.4.3 Entidades de Certificación Vinculadas

Las Entidades de Certificación Vinculadas son las entidades del Sector Público de Cataluña a las que el Consorci AOC, en calidad de prestador de servicios de certificación, presta los servicios de expedición y gestión de los certificados para sus autoridades de certificación.

Las Entidades de Certificación Vinculadas se encuentran inscritas en la jerarquía pública de certificación de Cataluña.

Mediante una Entidad de Certificación Vinculada, la entidad emite certificados a usuarios finales..

Cuando una entidad del Sector Público de Cataluña encarga al Consorci AOC la operación técnica de la entidad de certificación vinculada y de los correspondientes sistemas técnicos de autoridad de certificación, la institución permanece responsable de la organización y las decisiones de gestión referidas a la entidad de certificación. Esta función, que no puede ser objeto de delegación, se llama Entidad de Certificación Virtual.

Cuando no exista una institución única responsable de una comunidad de usuarios que precisen certificados, el Consorci AOC puede crear sistemas técnicos de autoridad de certificación de su propia titularidad, vinculados a la jerarquía pública de certificación de Cataluña.

En el caso que una entidad de certificación sea operada directamente por una entidad del Sector Público de Cataluña, constituida ésta como prestador de servicios de certificación, con su propio sistema técnico de autoridad de certificación, esta entidad de certificación podrá integrarse en el sistema público catalán de certificación mediante la vinculación técnica de dicho sistema de autoridad de certificación en la jerarquía pública de certificación de Cataluña – según lo descrito en el apartado 1.4.2

1.4.4 Entidades de Registro

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.

Existen los siguientes tipos de Entidades de Registro:

- 1) Las Entidades de Registro Internas, operadas por una institución suscriptora de certificados de clase 1.
- 2) Las Entidades de Registro Colaboradoras, que colaboran con Entidades de Certificación Vinculadas en el proceso de emisión de los certificados.

La constitución de una Entidad se regula mediante los instrumentos jurídicos correspondientes.

El Consorci AOC es responsable del proceso de creación de entidades de registro: verifica que la Entidad de Registro cuenta con los recursos materiales y humanos necesarios; y que ha designado y al formado al personal que será responsable de la emisión de certificados (los denominados operadores de la entidad de registro). Asimismo, es responsable, de la emisión de los certificados de operador que éstos necesitaran para poder operar (típicamente, serán CIPISR); 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 la Declaración de Prácticas de Certificación.

Las instituciones, para ser Entidades de Registro Internas, 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 programario y al ciclo de vida de los certificados que emitan. Estos componentes y procedimientos serán previamente aprobados por el Consorci AOC.

1.4.5 Usuarios finales

Los usuarios finales son las personas que obtienen y utilizan certificados personales, de entidad, de dispositivos y de objetos emitidos por las Entidades de Certificación, y, en concreto, podemos distinguir los siguientes usuarios finales:

- a) Los solicitantes de certificados
- b) Los suscriptores o titulares de certificados
- c) Los poseedores de claves
- d) Los verificadores de firmas, sellos y certificados

1.4.5.1 Solicitantes de certificados

Todo certificado tiene que ser solicitado por una persona, bien sea en su propio nombre, o en nombre de otra persona - física o jurídica.

Pueden ser solicitantes:

- a) De certificados personales: la persona que será el futuro poseedor de claves.
- b) De certificados corporativos: una persona autorizada al efecto por la futura entidad suscriptora.
- c) Una persona autorizada por la Entidad de Certificación – típicamente, el Consorci AOC actuando de oficio.

La autorización del solicitante podrá realizarse tanto de forma expresa como tácita, si bien, en aquellos casos en los que la entidad de certificación lo considere conveniente, se formalizará documentalmente.

1.4.5.2 Suscriptores de certificados

Los suscriptores son las personas, físicas o jurídicas (las entidades) así identificadas en el campo "Subject" del certificado.

Cuando se trata de certificados corporativos de persona física o jurídica, la entidad suscriptora del certificado actúa a través de un poseedor de claves, debidamente autorizado, y que figura identificado en el certificado.

El suscriptor tiene licencia de uso del certificado.

1.4.5.3 Poseedores de claves

Los poseedores de claves son las personas físicas que poseen de forma exclusiva las claves de generación de firma digital de certificados personales o de entidad, de clase 1 o de clase 2, que se encuentran debidamente autorizadas para esto por el suscriptor y que han sido debidamente identificadas en el certificado mediante su nombre y apellidos o mediante un seudónimo.

En los certificados de entidad, además, los poseedores de claves hanque tener en cuenta lo establecido en el artículo 7 de la Ley 59/2003, de 19 de diciembre.

También existen poseedores de claves de descifrado, en certificados CPX y CEX, con la peculiaridad que la clave de descifrado, a diferencia de la clave de firma, puede ser recuperada, en ciertos casos y condiciones, por la Entidad de Certificación, según disponga la correspondiente Declaración de Prácticas de Certificación.

1.4.5.4 Verificadores de certificados

Los verificadores son las personas (físicas o jurídicas) que reciben firmas digitales, sellos electrónicos y certificados digitales y tienen que verificarlos, como paso previo a confiar en las mismas.

1.5 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.

1.5.1 Usos típicos de los certificados

1.5.1.1 Requisitos específicos para el CIC

Los certificados de entidad de certificación (CIC) son emitidos por la Entidad de Certificación Raíz, a organizaciones que operan una Entidad de Certificación dentro de su jerarquía, para diferentes usos, según su clase: Firma de peticiones de renovación, suspensión y revocación de certificados CIC

- Emisión y firma de certificados de infraestructura, personales, de entidad y de dispositivo (CPISR, CIO, CIV, CIT, CPSR, CPSA, CPISR, CPISA, CPIXSA, CPI, CPX, CESR, CEX, CDS, o CDA, entre otros).
- Emisión y firma de listas de revocación de certificados (LCR).

Los CIC se obtienen después de un proceso de admisión de la Entidad de Certificación Vinculada a los servicios de certificación de la Agència Catalana de Certificació.

1.5.1.2 Requisitos específicos para el CIPISR

Los certificados de infraestructura personal de identificación y firma reconocida (CIPISR) son emitidos a operadores de Entidades de Registro, para los trabajos de emisión y gestión del ciclo de vida de certificados de una Entidad de Certificación.

1.5.1.3 Requisitos específicos para el CIDS

Los certificados de infraestructura de dispositivo servidor seguro (CIDS) se emiten a Entidades de Certificación, 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

Los certificados CIDS son certificados ordinarios, y que garantizan la identidad de la Entidad de Certificación y del servidor concreto donde funcionan.

1.5.1.4 Requisitos específicos para el CIDA

Los certificados de infraestructura de dispositivo de aplicación digitalmente asegurada (CIDA) se emiten a Entidades de Certificación responsables de la operación de aplicaciones informáticas que se identifican digitalmente, firman electrónicamente webservices u otros protocolos y que reciben documentos y mensajes cifrados.

Los certificados CIDA son certificados ordinarios, y garantizan la identidad de la Entidad de Certificación y la integridad y la autenticidad de los datos firmados. También permiten la recepción de información cifrada.

1.5.1.5 Requisitos específicos para el CIO

Los certificados de infraestructura de servidor de estado de certificados en línea (CIO) se emiten a entidades responsables de la operación de un servidor *OCSP Responder*, para firmar sus respuestas sobre el estado de validez de los certificados.

Los certificados CIO son certificados ordinarios, que garantizan la identidad del servidor *OCSP Responder*, de la entidad responsable de este servicio, así como garantizan la integridad y la autenticidad de los datos firmados por éste.

1.5.1.6 Requisitos específicos para el CIT

Los certificados de infraestructura de entidad de sellos de tiempos (CIT) se emiten a entidades responsables de la operación de servicio de sellado de tiempo, para firmar los sellos de tiempos que emiten.

Los certificados CIT son certificados ordinarios, que garantizan la identidad del servidor de firma de sellos de tiempos, de la entidad responsable de este servicio, así como garantizan la integridad y la autenticidad de los datos firmados por éste.

1.5.1.7 291BRequisitos específicos para el CIV

Los certificados de infraestructura de entidad de validación (CIV) se emiten a entidades responsables de la operación de un servicio de validación de firmas y certificadis digitales, para firmar sus informes de validación.

Los certificados CIV son certificados ordinarios, que garantizan la identidad del servicio de validación, de la entidad responsable de este servicio, así como garantizan la integridad y la autenticidad de los datos firmados.

1.5.1.8 Requisitos específicos para el CPSR

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

Los CPSR son certificados reconocidos que funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3, de la Ley 59/2003, de 19 de diciembre.

Por este motivo, los CPSR garantizan la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permiten la generación de la “firma electrónica reconocida”; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha estado generada utilizando un dispositivo seguro, por lo cual, de acuerdo con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita para efecto legal, sin necesidad de cumplir ningún otro requerimiento adicional.

Los certificados CPSR, cuando lo prevé una política específica, pueden incluir una manifestación relativa a la categoría de personal y cargo del poseedor de claves, que han sidocomprobados antes de emitir el certificado, y son correctos.

Los certificados CPSR podran emitirse para su uso con seudónimo, garantizando la seguridad y el anonimato del poseedor de claves, debiéndose indicar esta circunstancia en el certificado en el campo que describa su tipología.

1.5.1.9 Requisitos específicos para el CPSA

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

Los CPSA no funcionan necesariamente con dispositivo seguro de creación de firma electrónica de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Los CPSA garantizan la identidad del suscriptor y, en su caso, del poseedor de la clave de firma, resultando idóneos para ofrecer soporte a la firma electrónica avanzada.

Aunque la firma electrónica avanzada no se equipara directamente a la firma escrita, esta equiparación se puede producir igualmente en virtud de un contrato de firma electrónica o de una norma jurídica específica, que establecerá las condiciones adicionales necesarias para que se produzca dicha equiparación.

1.5.1.10 Requisitos específicos para el CPI

Los certificados personales de identidad (CPI) se pueden utilizar para diversos usos, entre los que se pueden indicar los siguientes:

- Identificación remota, basada en presentación de la credencial
- Autenticación en sistemas de control de acceso, de sistemas operativos o centralizados.

Los CPI son certificados ordinarios, y garantizan la identidad del suscriptor y, en su caso, la del poseedor de la clave de firma.

1.5.1.11 Requisitos específicos para el CPX

Los certificados personales de cifrado (CPX) se pueden utilizar exclusivamente para recibir mensajes de datos confidenciales, en cualquier formato, protegidos mediante el cifrado del texto del mensaje, por parte del remitente del mensaje, utilizando la clave pública del suscriptor indicada en el CPX.

El poseedor de la clave privada la utilizará para descifrar el mensaje.

Los CPX garantizan la identidad del suscriptor, pero no permiten la firma electrónica de mensajes de datos.

La clave privada del CPX no podrá ser archivada por la entidad de certificación..

1.5.1.12 Requisitos específicos para el CESR

Los certificados de entidad de firma reconocida (CESR) son certificados reconocidos, no emitidos al público, que se expiden a entidades subscriptoras, de acuerdo con lo establecido en el artículo 11.1, con el contenido prescrito por el artículo 11.2, y emitidos siguiendo las prescripciones de los artículos 7, 12, 13 y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y que dan cumplimiento a lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones identificada con la referencia TS 101 456.

Los CESR corresponden a certificados reconocidos con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Por este motivo, los CESR garantizan la identidad del suscriptor y del responsable de la custodia de la clave privada de firma, resultando idóneos para ofrecer soporte a la firma electrónica reconocida de la entidad; esto es, la firma electrónica avanzada que se basa en certificado reconocido y que ha estado generada utilizando un dispositivo seguro, por el que, de acuerdo con el artículo 3.4 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma manuscrita para efecto legal, sin necesidad de cumplir ningún requisito adicional más.

1.5.1.13 Requisitos específicos para el CESA

Los certificados de entidad de firma avanzada son certificados reconocidos, de acuerdo con lo establecido en el artículo 11.1, con el contenido prescrito por el artículo 11.2, y emitidos siguiendo las prescripciones de los artículos 7, 12, 13 y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y que dan cumplimiento a lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones identificada con la referencia TS 101 456.

Los CESA no funcionan necesariamente con dispositivo seguro de creación de firma electrónica de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Los CESA garantizan la identidad del suscriptor y del responsable de la custodia de la clave privada de firma, resultando idóneos para ofrecer soporte a la firma electrónica avanzada.

Aunque la firma electrónica avanzada no se equipara directamente a la firma escrita, esta equiparación se puede producir igualmente en virtud de un contrato de firma electrónica o de una norma jurídica específica, que establecerá las condiciones adicionales necesarias para que se produzca dicha equiparación.

1.5.1.14 Requisitos específicos para el CEI

Los certificados de entidad para identificación (CEI) se pueden utilizar para varios usos, entre los cuales se pueden indicar los siguientes:

- Identificación remota, basada en presentación de la credencial.
- Autenticación en sistemas de control de acceso, de sistemas operativos o centralizados.

Los CEI son certificados reconocidos, y garantizan la identidad del suscriptor y, en su caso, del poseedor de la clave de firma.

1.5.1.15 Requisitos específicos para el CEX

Los certificados de entidad de cifrado (CEX) son certificados reconocidos, no emitidos al público, que se expiden a entidades suscriptoras y se pueden utilizar exclusivamente para cifrar o recibir mensajes de datos confidenciales, en cualquier formato, protegidos mediante el cifrado del texto del mensaje, utilizando la clave pública del suscriptor indicada en el CEX.

El poseedor de la clave privada la utilizará para descifrar los mensajes.

La clave privada del CEX podrá estar archivada por la entidad de certificación de manera que, en ciertas circunstancias, pueda recuperarse y acceder a la información cifrada.

1.5.1.16 Requisitos específicos para el CDS

Los certificados de dispositivo servidor seguro (CDS) se emiten a personas físicas o personas jurídicas, 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

Los certificados CDS son certificados ordinarios, y que garantizan la identidad de la persona responsable y del servidor concreto donde funcionan.

Los certificados CDS-1 Sede electrónica sólo se pueden suministrar a las administraciones públicas, órganos o entidades administrativas, de acuerdo con el artículo 10 de la Ley 11/2007, y deben cumplir los requisitos del artículo 17 de la Ley 11/2007.

1.5.1.17 Requisitos específicos para el CDP

Los certificados de firma de software (CDP) se emiten a personas jurídicas responsables de la edición, publicación o distribución digital de software informático, para la firma del software, de forma que éste pueda ser instalado o ejecutado remotamente.

Los certificados CDP son certificados ordinarios, y que garantizan la identidad de la entidad responsable del software firmado, así como garantizan su origen e integridad.

1.5.1.18 Requisitos específicos para el CDA

Los certificados de dispositivo de aplicación digitalmente asegurada se emiten a personas jurídicas responsables de la operación de aplicaciones informáticas que se identifican digitalmente, firman electrónicamente webservices u otros protocolos y que reciben documentos y mensajes cifrados.

Los certificados CDA son certificados ordinarios, y garantizan la identidad de la entidad responsable, así como garantizan la integridad y la autenticidad de los datos firmados. También permiten la recepción de información cifrada.

Los certificados CDA-1 Sello electrónico sólo se pueden suministrar a las administraciones públicas, órganos o entidades administrativas, para el ejercicio de la competencia administrativa de forma automatizada, y han de cumplir los requisitos del artículo 18 de la Ley 11/2007.

1.5.2 Aplicaciones prohibidas

1.5.2.1 Prohibiciones generales

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 requieran actuaciones a prueba de errores, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un error pudiera directamente comportar la muerte, lesiones personales o daños medioambientales severos.

Los certificados de entidades finales no se pueden utilizar para firmar peticiones de emisión, renovación, suspensión, habilitación o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LCR).

Los certificados de firma no se pueden utilizar para firmar mensajes de autenticación incomprensibles para el firmante, en particular desafíos de cliente SSL o TLS, excepto cuando se combinen con un certificado de identidad y tampoco se pueden utilizar para recibir mensajes cifrados, excepto cuando se combinen con un certificado de cifrado y no se almacene la clave privada.

1.5.2.2 Certificados de infraestructura

Requisitos específicos para el CIC

Los certificados CIC se atenderán a lo dispuesto en esta política y, en todo caso, las limitaciones estarán delimitadas por la clase del certificado CIC, así como se especifica en dicho punto y, en su caso, por la política de certificado concreta.

Requisitos específicos para el CIO

Los CIO no se pueden utilizar en sistemas diferentes de los de la Entidad de Certificación.

Requisitos específicos para el CIT

Los CIT no se pueden utilizar en sistemas diferentes de los de la Entidad de Certificación.

Requisitos específicos para el CIV

Los CIV no se pueden utilizar en sistemas diferentes de los de una Entidad de Validación.

306B Requisitos específicos para el CIDS

Los CIDS no se pueden utilizar en sistemas diferentes al de la Entidad de Certificación.

307B Requisitos específicos para el CIDA

Los CIDA no se pueden utilizar en sistemas diferentes al de la Entidad de Certificación.

Requisitos específicos para el CIPISR

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

1.5.2.3 Certificados personales

Requisitos específicos para el CPSR

Los CPSR no pueden utilizarse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LCR).

Los CPSR tampoco pueden utilizarse para firmar mensajes de autenticación incomprensibles para el firmante, en particular desafíos de cliente SSL o TLS, excepto cuando se combinen con un CPI, y tampoco se pueden utilizar para recibir mensajes cifrados, excepto cuando se combinen con un CPX y no se almacene la clave privada.

Requisitos específicos para el CPSA

Los CPSA no pueden utilizarse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LCR).

Los CPSA tampoco pueden utilizarse para firmar mensajes de autenticación incomprensibles para el firmante, en particular desafíos de cliente SSL o TLS, excepto cuando se combinen con un CPI, y tampoco se pueden utilizar para recibir mensajes cifrados, excepto cuando se combinen con un CPX y no se almacene la clave privada.

Requisitos específicos para el CPI

Los CPI no pueden utilizarse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados CIC, certificados de ningún tipo, o listas de revocación de certificados (LCR), y tampoco se pueden utilizar para recibir mensajes cifrados, excepto cuando se combinan con un CPX.

Requisitos específicos para el CPX

Los CPX no se pueden usar para generar firmas digitales de ningún tipo de mensaje de datos, excepto cuando se combinen con un CPSR –si la clave privada no se almacena-, CPS o CPI.

1.5.2.4 Certificados de entidad

Requisitos específicos para el CESR y CESA

Los CESR y los CESA no pueden utilizarse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados CIC, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LCR).

Los CESR y los CESA tampoco pueden usarse para firmar mensajes de autenticación incomprensibles para el firmante, en particular desafíos de cliente SSL o TLS, excepto cuando se combinan con un CEI, y tampoco se pueden usar para recibir mensajes cifrados, excepto cuando se combinan con un CEX y no se almacene la clave privada.

Requisitos específicos para el CEX

Los CEX no pueden utilizarse para generar firmas digitales de ningún tipo de mensaje de datos.

1.5.2.5 Certificados de dispositivo

Requisitos específicos para el CDS

Los CDS no pueden utilizarse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados CIC, certificados de ningún tipo, o listas de revocación de certificados (LCR).

Requisitos específicos para el CDA

Los CDA no pueden utilizarse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados CIC, certificados de ningún tipo, o listas de revocación de certificados (LCR).

Tampoco pueden utilizarse para asegurar aplicaciones diferentes a la identificada en el certificado.

1.6 Administración de la política

1.6.1 Organización que administra la especificación

Consorci Administració Oberta de Catalunya – Consorci AOC

1.6.2 Datos de contacto de la organización

Consorci Administració Oberta de Catalunya – Consorci AOC

Domicili social: Via Laietana, 26 – 08003 Barcelona

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

Web del Consorci AOC: www.aoc.cat

Web del Servicio de Certificación Digital del Consorci AOC:

www.aoc.cat/Inici/SERVEIS/Signatura-electronica-i-seguretat/CATCert

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

1.6.3 Persona que determina la conformidad de una DPC con la política

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

1.6.4 Procedimiento de aprobación

El sistema documental y de organización de la Entidad de Certificación garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de la política 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 las Declaraciones 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 las Declaraciones de prácticas

Las modificaciones finales de la política tendrán que ser aprobadas por el Comitè de Direcció del Consorci AOC.

2. Publicación de información y directorio de certificados

2.1 Directorio de certificados

El servicios de directorio de certificados estará disponible durante las 24 horas de los 365 días del año; y en caso de fallo del sistema fuera de control de la Entidad de Certificación, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección correspondiente de la DPC aplicable.

2.2 Publicación de información de la Entidad de Certificación

La Entidad de Certificación publicará las siguientes informaciones², en su web:

- a. Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- b. La política general de certificación.
- c. Los perfiles de los certificados.
- d. La Declaración de Prácticas de Certificación.
- e. Los instrumentos jurídicos vinculantes con suscriptores y verificadores.

Todo cambio en las especificaciones o condiciones del servicio será comunicado a los usuarios por la Entidad de Certificación a través de su web y, cuando sea oportuno, a través de la dirección de correo electrónico proporcionada al efecto por el poseedor de las claves.

En todos los casos se hará una referencia explícita a los cambios en la página principal del Web del servicio.No se retirará la versión anterior del documento objeto del cambio, pero se indicará que ha sido substituido por la versión nueva.Al cabo de 15 (quince) días desde la publicación de la nueva versión, se podrá retirar la referencia al cambio de la página principal.

Las versiones antiguas de la documentación serán conservadas, por un periodo de 15 (quince) años por la Entidad de Certificación, pudiendo ser consultadas, por causa razonada por los interesados.

2.3 Frecuencia de publicación

La información de la Entidad de Certificación se publicará cuando se encuentre disponible y en especial, de forma inmediata cuando se emitan las menciones relativas a la vigencia de los certificados.

Los cambios en la DPC se registrarán por lo establecido en la sección correspondiente de la DPC.

² TS 101 456: 7.3.5; TS 102042: 7.3.5

La información de estado de revocación de certificados emitidos por la Entidad de Certificación se publicará de acuerdo con lo establecido en las secciones correspondientes de esta política.

2.4 Control de acceso

La Entidad de certificación no limita el acceso de lectura a la información de estado de revocación de los certificados emitidos por ella,

La Entidad de Certificación protege la integridad y la autenticidad de la información de estado de revocación de los certificados³

También establece controles para mantener la integridad del directorio de los certificados expedidos. Más concretamente, utiliza sistemas fiables para el Directorio, de manera tal que⁴:

- Se pueda comprobar la autenticidad de los certificados.
- Las personas no autorizadas no puedan alterar los datos.
- Los certificados solamente estén accesibles en los supuestos o para la personas autorizadas
- Se pueda detectar cualquier cambio técnico que afecte a los requisitos de seguridad.

³ TS 101 456: 7.3.6 j); TS 102042: 7.3.6 j)

⁴ Ley 59/2003: 20.1g)

3. Identificación y autenticación

3.1 Gestión de nombres⁵

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

3.1.1 Tipos de nombres

Todos los certificados contendrán un nombre diferenciado X.501 en el campo *Subject*, incluyendo un componente *Common Name* (CN=).

La estructura sintáctica y el contenido de los campos de cada certificado, así como su significado semántico se encuentra descrito en el documento “perfil de certificado” correspondiente, que el Consorci AOC publica en su web.

3.1.2 Significado de los nombres

En certificados correspondientes a personas físicas la identificación del firmante estará formada por su nombre y apellidos, más su DNI, o en su caso, un seudónimo que conste como tal de manera inequívoca⁶.

En certificados correspondientes a personas jurídicas, esta identificación se realizará por medio de su denominación o razón social, y su CIF.⁷

3.1.3 Utilización de anónimos y seudónimos

No se pueden utilizar seudónimos para identificar una organización.

Los certificados personales, tanto los individuales como los corporativos, y también los de entidad pueden indicar seudónimos en lugar del nombre verdadero del poseedor de la clave del certificado.

El seudónimo constará como tal de manera inequívoca, y se indicará esta naturaleza en la descripción del tipo de certificado.⁸

⁵ TS 101 456: 7.3.1

⁶ Artículo 11.2.e) Ley 59/2003; Artículo 32 Reglamento (UE) N° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los Servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

⁷ Artículo 11.2.e) Ley 59/2003

⁸ Artículo 11.2.e) Ley 59/2003 Artículo 32 Reglamento (UE) N° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los Servicios de

El seudónimo 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 seudónimo garantizará, en la fase de registro, la disponibilidad de la identificación real del poseedor de claves, que solo 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

Los nombres de los poseedores de claves de certificados serán únicos, en el ámbito del servicio de generación de certificados prestado por una Entidad de Certificación Vinculada y para cada tipo (perfil) de certificado. Es decir, una persona podrá tener a su nombre certificados de perfiles diferentes expedidos por la misma Entidad de Certificación Vinculada; también podrá tener certificados a su nombre del mismo perfil expedidos por diferentes Entidades de Certificación Vinculadas.

No se podrá volver a asignar el nombre de un poseedor de claves que ya haya sido ocupado, a un usuario diferente⁹.

3.1.6 Resolución de conflictos relativos a nombres

En **certificados individuales**, los conflictos de nombres de poseedores de claves que aparezcan identificados en los certificados con su nombre real se solucionan mediante la inclusión, en el nombre diferenciado (*distinguished name*) del certificado, de:

- En caso de nacionales españoles, el número de DNI del suscriptor.
V.gr.: (C) = ES; (SN) = #DNI
- En caso de extranjeros con algún tipo de vinculación con España, como puede ser la residencia en territorio español, el número de NIE del suscriptor.
V.gr.: francés (C) = ES; (SN) = #NIE
V.gr.: argentino (C) = ES; (SN) = #NIE
- En caso de extranjeros nacionales de Estados que son parte del Acuerdo Schengen y que carecen de NIE, el número de documento nacional de identidad del país de origen o de procedencia o pasaporte vigente del suscriptor. También se podrá consignar, antes del número del documento identificador citado, el código del país del que el suscriptor es nacional, de conformidad con los parámetros establecidos por la norma ISO 3166 Codes (Countries), separado por un guión.
V.gr.: italiano (C) = IT; (SN) = #Documento nacional de identidad

confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

⁹ TS 101 456: 7.3.3 d); TS 102042: 7.3.3 d)

V.gr.: italiano (C) = IT; (SN) = IT-#Documento nacional de identidad

- En caso de extranjeros nacionales de Estados que no son parte del Acuerdo Schengen y que carecen de NIE, el número de Pasaporte ordinario, diplomático, oficial o de servicio, del suscriptor válidamente expedido y en vigor. También se podrá consignar, antes del número del documento identificador citado, el código del país del que el suscriptor es nacional, de conformidad con los parámetros establecidos por la norma ISO 3166 Codes (Countries), separado por un guión.

V.gr.: chino (C) = CN; (SN) = #Pasaporte

V.gr.: chino (C) = CN; (SN) = CN-#Pasaporte

En **certificados corporativos**, los conflictos de nombres de poseedores de claves que aparezcan identificados en los certificados con su nombre real se solucionan mediante la inclusión, en el nombre diferenciado del certificado, de:

- En caso que la “Organization” del campo “Subject” (esto es, la entidad suscriptora) esté sometida a Derecho español:

- En caso de nacionales españoles, el número de DNI del poseedor de claves.

V.gr.: (C) = ES; (SN) = #DNI

- En caso de extranjeros, con algún tipo de vinculación con España, como puede ser la residencia en territorio español, el número de NIE del poseedor de claves.

V.gr.: francés (C) = ES; (SN) = #NIE

V.gr.: argentino (C) = ES; (SN) = #NIE

- En caso de extranjeros nacionales de Estados parte del Acuerdo Schengen y que carecen de NIE, el número de documento nacional de identidad del país de origen o de procedencia o pasaporte vigente del poseedor de claves. También se podrá consignar, antes del número del documento identificador citado, el código del país del que el poseedor de claves es nacional, de conformidad con los parámetros establecidos por la norma ISO 3166 Codes (Countries), separado por un guión.

V.gr.: italiano (C) = ES; (SN) = #Documento nacional de identidad

V.gr.: italiano (C) = ES; (SN) = IT-#Documento nacional de identidad

- En el caso de extranjeros nacionales de Estados que no son parte del Acuerdo Schengen y que carecen de NIE, el número de Pasaporte ordinario, diplomático, oficial o de servicio del poseedor de claves válidamente expedido y en vigor. También se podrá consignar, antes del número del documento identificador citado, el código del país del que el poseedor de claves es nacional, de conformidad con los parámetros establecidos por la norma ISO 3166 Codes (Countries), separado por un guión.

V.gr.: chino (C) = ES; (SN) = #Pasaporte

V.gr.: chino (C) = ES; (SN) = CN-#Pasaporte

- Cualquier otro número de identificador asignado al poseedor de claves por el suscriptor.

V.gr.: un número de colegiado.

- En caso de que la “Organizational Unit” del “Subject” (esto es, la entidad suscriptora) no esté sometida a Derecho español, la semántica del “SerialNumber” dependerá de la normativa aplicable conforme al “countryName” de la Entidad.

En **certificados de entidad**, los conflictos de nombres de los responsables de la custodia de claves que aparezcan identificados en los certificados con su nombre real se solucionan mediante la inclusión del número de DNI o de NIE del responsable de la custodia de claves, siguiendo criterios similares a los descritos para los certificados individuales.

En caso de que el nombre a incluir en el certificado sea excesivamente largo, se procederá a abreviar alguno de los nombres y nunca el primer apellido.

La Entidad de Certificación se reserva el derecho de rehusar una solicitud de certificado por causa de conflicto de nombre.

3.2 Validación inicial de la identidad

3.2.1 Prueba de posesión de clave privada

Debe asegurarse que únicamente el suscriptor de certificados individuales (o bien el poseedor de claves de certificados corporativos o de certificados de entidad) tiene la clave de privada (que permite la generación de firmas o el descifrado de datos, según el tipo de certificado de que se trate).

Esta sección describe los métodos a utilizar para demostrar que se posee la clave privada correspondiente a la clave pública objeto de certificación.¹⁰

Este requisito no se aplica cuando el par de claves es generado por la Entidad de Registro Colaboradora, durante el proceso de generación del certificado – típicamente en un dispositivo seguro de creación de firma que se entregará al poseedor de las claves. En este caso, la posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del dispositivo seguro y del correspondiente certificado y par de claves almacenadas en su interior.

En general, el método de demostración de posesión de la clave privada será la aportación, por parte del poseedor de la clave privada, de un fichero de formato PKCS #10, si bien el consorcio AOC puede aceptar otra prueba criptográfica equivalente o cualquier otro método aprobado por él.

3.2.2 Autenticación de la identidad de una organización

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

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

¹⁰ TS 101456: 7.3.1.j); TS 102042: 7.3.1.n)

3.2.2.1 Entidades de Registro

La Entidad de Certificación tiene que autenticar la identidad de la organización responsable de la Entidad de Registro así como la de sus operadores, junto a otros datos establecidos en la sección correspondiente, con carácter previo a la emisión y entrega de certificados para cualquiera de los componentes de una Entidad de Registro o para sus operadores.

Paratodo esto, la Entidad de Certificación podrá utilizar los siguientes métodos:

- 1) Obtención de información sobre la organización, de un proveedor externo de servicios de esta naturaleza
- 2) Comprobación de documentación justificativa aportada por el solicitante. En este caso, se requerirá la formalización del instrumento jurídico pertinente.

3.2.2.2 Suscriptores de certificados

Requisitos para certificados de clase 1

No se requiere realizar procedimiento de autenticación de la organización titular del certificado en certificados de clase 1, ya que se trata de certificados corporativos, en los que la organización suscriptora del certificado y la Entidad de Registro Interna coinciden.

Requisitos para certificados de clase 2

La Entidad de Certificación tiene que autenticar, con carácter previo a la emisión y entrega de un certificado corporativo de clase 2, la identidad del suscriptor y la del poseedor de claves privadas y otros datos, establecidos en la sección correspondiente para certificados corporativos.

La Entidad de Certificación podrá utilizar Entidades de Registro para esta tarea.

Para esto, la Entidad de Certificación o la Entidad de Registro podrán utilizar los siguientes métodos:

- 1) Obtención de información sobre la organización, de un proveedor externo de servicios de esta naturaleza, a discreción de la Entidad de Certificación, que previamente tendrá que aprobar al proveedor externo.
- 2) Comprobación de documentación justificativa aportada por el solicitante, sobre los siguientes extremos¹¹ :
 - a) Nombre legal completo de la organización
 - b) Estado legal de la organización
 - c) Número de identificación fiscal
 - d) Datos de identificación registral

¹¹ TS 101 456: 7.3.1 e); TS 102 042: 7.3.1 g)

3.2.3 Comprobaciones a realizar en el caso de solicitudes de certificados de dispositivo servidor seguro

En el caso de solicitudes de certificados de dispositivo, adicionalmente a la comprobación que tenga que hacerse de la organización responsable, se comprobará:

- 1) La existencia del servidor
- 2) La titularidad del nombre de dominio proveniente del registro correspondiente
- 3) La autorización de la organización responsable del servidor para la emisión del certificado al servidor.

3.2.4 Autenticación de la identidad de una persona física

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

3.2.4.1 Elementos de identificación requeridos¹²

La Entidad de Certificación establecerá el número y los tipos de documentos que sean suficientes para acreditar la identidad del poseedor de la clave, pudiendo utilizar los siguientes:

- A. Documento Nacional de Identidad o Número de Identificación de extranjeros o, de forma equivalente, justificante de renovación o reemisión de DNI (o NIE) más otro documento acreditativo de la identidad con fotografía
- B. Pasaporte
- C. Cualquier otro de los admitidos en derecho, siempre que contenga, al menos, la siguiente información¹³:
 - a) Nombre y apellidos de la persona
 - b) Lugar y fecha de nacimiento
 - c) Número de identidad reconocido legalmente
 - d) Otros atributos de la persona que tengan que constar en el certificado
 - e) Fotografía

3.2.4.2 Validación de los elementos de identificación¹⁴

Requisitos para certificados de Clase 1

La información de identificación de poseedores de claves de certificados de clase 1 se validará comparando la información de la solicitud con los registros internos de la Entidad de Registro Interna que, tratándose de certificados de clase 1, corporativos, coincide con la

¹² Artículo 13.1 Ley 59/2003

¹³ TS 101 456:7.3.1 d); TS 102 042: 7.3.1 f)

¹⁴ TS 101 456:7.3.1 c); TS 102 042: 7.3.1 d)

organización suscriptora del certificado. Ésta debe, por tanto, asegurarse de la corrección de la información que certifica y adjunta a la solicitud de los certificados.

Esta tarea la podrá realizar un proveedor corporativo de información de recursos humanos.

Requisitos para certificados de Clase 2

La información de identificación de suscriptores de certificados individuales, así como de poseedores de claves de certificados corporativos, se realiza contrastando la información de la solicitud con la documentación acreditativa aportada, electrónicamente o en soporte físico.

3.2.4.3 Necesidad de presencia personal¹⁵

La identificación de la persona física que tenga que obtener un certificado reconocido (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 reconocido, la Entidad de Certificación – mediante la intervención de una Entidad de Registro -tendrá que comprobarla identidad del poseedor de claves mediante la personación de éste.

El acto de personación puede diferirse al momento de entrega y aceptación del certificado, aprovechándolo 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 sido autenticada mediante el uso de un certificado electrónico de firma reconocida clasificado por el Consorci AOC, siempre que se encuentre vigente y no hayan transcurrido más de cinco años desde la identificación con presencia personal.

Se podría prescindir de la personación si la firma contenida en la solicitud de expedición de un certificado ha sido legitimada notarialmente¹⁶, y en los casos previstos por el artículo 13.4 de la Ley 59/2003, de 19 de diciembre. Pero esta política no da soporte a este mecanismo por la inexistencia de un procedimiento al efecto por parte de los notarios.

Requisitos específicos para los CPSR y CESR

Antes de la emisión y entrega de un certificado CPSR o CESR, la Entidad de Certificación – mediante la intervención de una Entidad de Registro - tendrá que comprobar la identidad del poseedor de claves mediante la personación de éste.

¹⁵ TS 101 456: 7.3.1 c)

¹⁶ Article 13.1 Llei 59/2003

El acto de personación de estos perfiles de certificados se difiere al momento de entrega y aceptación del certificado, aprovechándolo 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 sido autenticada mediante el uso de un certificado electrónico de firma reconocida clasificado por el Consorci AOC, siempre que se encuentre vigente y no hayan transcurrido más de cinco años desde la identificación con presencia personal.

3.2.4.4 Vinculación de la persona física con una organización

Requisitos para certificados de clase 1

Como se trata de certificados corporativos de clase 1, dado que la Entidad de Registro y el suscriptor son la misma entidad, no es necesario obtener una justificación documental específica de la vinculación del poseedor de la clave con la Entidad de Registro, sino que se podrían utilizar los registros internos de la institución. Si bien lo habitual y preferible es que se adjunte a la solicitud un certificado, emitido por una persona de la entidad competente al efecto, que garantice la veracidad y exactitud de los datos consignados en la solicitud, referentes a la entidad suscriptora y/o a los poseedores de claves indicados.

Requisitos para certificados de clase 2

Cuando se expidan certificados corporativos, la Entidad de Certificación – 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.¹⁷.

3.2.5 Información de suscriptor no verificada

No estipulado en este documento. A concretar por cada Entidad de Certificación en su Declaración de Prácticas de Certificación (DPC).

3.3 Identificación y autenticación de solicitudes de renovación

3.3.1 Validación para la renovación rutinaria de certificados¹⁸

Antes de renovar un certificado, la Entidad de Certificación 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.

¹⁷ TS 101 456: 7.3.1 e); TS 102 042: 7.3.1 g)

¹⁸ TS 101 456: 7.3.2; TS 102 042: 7.3.2

Si cualquier información del suscriptor o del poseedor de la clave ha cambiado, se registrará adecuadamente la nueva información, de acuerdo con lo establecido en la sección correspondiente.

3.3.2 Validación para la renovación de certificados después de la revocación¹⁹

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

3.4 Identificación y autenticación de la solicitud de revocación²⁰

Cada Entidad de Certificación tendrá que autenticar las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una fuente autorizada.

Dichas peticiones e informes serán confirmados cumpliendo los procedimientos establecidos en la Declaración de Prácticas de Certificación de la Entidad de Certificación.

3.5 Autenticación de una petición de suspensión

El suscriptor se identifica telefónicamente ante el Consorci AOC, dando un número que lo identifique (NIF) y contestando correctamente a la pregunta de desafío.

En el caso de los certificados individuales, esta pregunta de desafío la fija el poseedor de las claves en el momento de entrega del certificado.

En el caso de los certificados corporativos, el código de suspensión es generado aleatoriamente por la Autoridad de Certificación y se comunica al poseedor de las claves por escrito, en la hoja de entrega del certificado que éste recibe en el acto de entrega y aceptación del certificado.

¹⁹ TS 101 456: 7.3.2; TS 102 042: 7.3.2

²⁰ TS 101 456: 7.3.6 c); TS 102 042: 7.3.6 c)

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

Los siguientes requisitos de operación del ciclo de vida de los certificados no son aplicables para los certificados de pruebas, que se regirán por lo estipulado en la DPC de la Entidad de Certificación Vinculada que los emita.

4.1 Solicitud de emisión de certificado

Podrán existir los siguientes tipos de solicitudes:

1. Solicitud de certificado de oficio (no contiene clave pública)
2. Solicitud electrónica de certificado por parte del interesado (el poseedor de la clave, en el caso de certificados individuales o la persona designada al efecto por la entidad suscriptora, en el caso de certificados corporativos) sin generación previa de claves (no aporta clave pública, y va firmada digitalmente).
3. Solicitud electrónica de certificado por parte del interesado (el poseedor de la clave, en el caso de certificados individuales o la persona designada al efecto por la entidad suscriptora, en el caso de certificados corporativos) con generación previa de claves y aportación de prueba de posesión de la correspondiente clave privada (PKCS#10 o mecanismo similar, de acuerdo con la sección “Prueba de posesión de clave privada” de la presente política).

4.1.1 Legitimación para solicitar la emisión

4.1.1.1 Requisitos para todos los tipos de certificados

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

En el caso de certificados individuales, el solicitante será el propio suscriptor quien, a su vez, será también el poseedor de las claves privadas.

En el caso de certificados corporativos de clase 1, el solicitante será la persona autorizada al efecto por la entidad suscriptora.

En el caso de certificados corporativos de clase 2, el solicitante y el suscriptor pueden ser entidades diferentes. De ser así, debe existir una autorización de la Entidad de Certificación para realizar la solicitud, que se instrumentará jurídicamente.

Por tanto, podrán existir los siguientes tipos de autorizaciones:

- Clase 1: la Entidad de Registro autoriza a personal propio, ante la Entidad de Certificación.
- Clase 2: la Entidad de Registro autoriza, ante la Entidad de Certificación, que la emisión de certificados la solicite personal relacionado con el suscriptor (puede ser un trabajador del suscriptor, o un representante externo, o incluso una entidad diferente).

4.1.1.2 Requisitos específicos del CIC

La futura Entidad de Certificación no podrá solicitar el certificado hasta que haya completado favorablemente el procedimiento de admisión en la Jerarquía de Entidades de Certificación del Consorci AOC.

4.1.1.3 Requisitos para certificados personales, de entidad y de dispositivo

Requisitos específicos para certificados de Clase 1

Adicionalmente a lo establecido anteriormente, la Entidad de Certificación Vinculada tendrá que recibir solicitudes de certificados, de acuerdo con uno de los siguientes casos:

- 1) La solicitud es realizada por una persona que ha sido autorizada por la Entidad de Certificación Vinculada, por indicación de la entidad suscriptora.

En este caso debe haber un documento, en soporte papel o electrónico, firmado por la entidad suscriptora, que incluirá la indicación de la persona o personas a autorizar, por parte de la Entidad de Certificación Vinculada, para realizar peticiones. Dicha autorización se lleva a cabo mediante la configuración de los permisos necesarios para poder tramitar solicitudes de los tipos de certificados indicados, en el sistema de tramitación correspondiente, a favor del usuario/usuarios indicado/s en el documento.

Los datos del usuario final necesarios para realizar la solicitud podrán provenir de una base de datos de la organización o bien ser introducidas manualmente por el solicitante.

- 2) La solicitud es realizada por el futuro poseedor de claves. En este caso deben concurrir las siguientes circunstancias:
 - Debe existir el documento, en soporte papel o electrónico, de la solicitud del certificado.
 - Respecto al par de claves criptográficas: el solicitante puede generar su par de claves o acordar que le serán generadas. En caso que las haya generado él mismo, tiene que adjuntar a la solicitud la clave pública para que sea certificada y también la prueba de posesión de la correspondiente clave privada.
 - El solicitante debe aceptar un acuerdo de suscriptor, que pueden tener la forma de Condiciones de uso.

Para solicitar un certificado puede usarse otro vigente, de acuerdo con lo establecido en el art. 13.4.b de la Ley 59/2003.

Requisitos específicos para certificados de Clase 2

Adicionalmente a lo establecido anteriormente, la Entidad de Certificación Vinculada tendrá que recibir solicitudes de certificados, cuando menos de acuerdo con uno de los siguientes casos:

- 1) En el caso de certificados corporativos: la solicitud es realizada por una persona que ha sido autorizada por la Entidad de Certificación Vinculada en lugar del suscriptor.

En este caso debe haber un documento, en soporte papel o electrónico, firmado por la futura entidad suscriptora, que incluirá la indicación de la persona o personas a autorizar, por parte de la Entidad de Certificación Vinculada, para realizar peticiones.

Los datos del usuario final necesarios para realizar la solicitud serán introducidos por el solicitante.

- 2) En el caso de certificados individuales: la solicitud es realizada por el poseedor de claves.

En este caso debe haber un documento, en soporte papel o electrónico, firmado por la Entidad de Registro, que incluirá la indicación de la persona o personas a autorizar, por parte de la Entidad de Certificación Vinculada, para realizar peticiones.

Los datos del usuario final necesarios para realizar la solicitud serán introducidos por el solicitante.

- 3) La solicitud es realizada por el futuro suscriptor: en este caso deben concurrir las siguientes circunstancias:
- Debe existir el documento, en soporte papel o electrónico, de la solicitud del certificado.
 - Respecto al par de claves criptográficas: el solicitante puede generar su par de claves o acordar que le sean generadas. En caso que las haya generado él mismo, tiene que adjuntar a la solicitud la clave pública para que sea certificada y también la prueba de posesión de la correspondiente clave privada.
 - El solicitante debe aceptar un acuerdo de suscriptor, que pueden tener la forma de Condiciones de uso.

4.1.2 Procedimiento de alta; Responsabilidades

La Entidad de Certificación Vinculada tiene que asegurarse que las solicitudes de certificados son completas, precisas y están debidamente autorizadas²¹.

Antes de la entrega del certificado, la Entidad de Certificación Vinculada informará al poseedor de claves de los términos y condiciones aplicables al certificado.²²

En certificados de organización, este requisito se cumplirá entregando una hoja de entrega al poseedor de claves que incluya esta información.

Dicha información se comunicará en soporte perdurable, en papel o electrónicamente y en lenguaje fácilmente comprensible.²³

A la solicitud se podrá acompañar documentación justificativa de la identidad del suscriptor y otras circunstancias, en caso de certificados individuales, o del poseedor de claves, en

²¹ TS 101 456: 7.3.1; TS 102 042: 7.3.1

²² TS 101 456: 7.3.1 a); TS 102 042: 7.3.1 a)

²³ TS 101 456: 7.3.1 b); TS 102 042: 7.3.1 c)

caso de certificados de organización o de entidad, de acuerdo con lo establecido en la sección correspondiente de esta política de certificados.

También se podrá acompañar una dirección física, u otros datos, que permitan contactar con el suscriptor, en caso de certificados individuales, o al poseedor de claves, en caso de certificados de organización o de entidad²⁴.

4.2 Procesamiento de la solicitud de certificación

4.2.1 Requisitos para todos los tipos de certificados

Cuando recibe una petición de certificado, la Entidad de Certificación tiene que verificar la información proporcionada, conforme a la sección correspondiente de esta política.

Si la información no es correcta, la Entidad de Certificación tiene que denegar la petición. En caso contrario, la Entidad de Certificación aprobará la generación del certificado.

4.2.2 Requisitos específicos para el CIC

Cuando la Entidad de Certificación que solicita ser vinculada a la jerarquía pública de certificación de Cataluña no esté operada por el Consorci AOC, se comprobará, antes de emitir el certificado, que el prestador de servicios de certificación correspondiente pueda demostrar la necesaria fiabilidad de sus servicios.²⁵

El Consorci AOC comprobará, en el proceso de admisión de la Entidad de Certificación, los siguientes aspectos:

- Que las políticas y procedimientos operados por la Entidad de Certificación no son discriminatorios.²⁶
- Que la Entidad de Certificación ofrecerá sus servicios a todos los solicitantes cuyas actividades entren en el ámbito de operación declarado²⁷ en su DPC, de acuerdo con lo establecido en la sección 1.3 de esta política.
- Que la Entidad de Certificación es una entidad legal²⁸, de acuerdo con lo establecido en la sección 1.3.1 de esta política, dato que será autenticado de acuerdo con lo establecido en la sección correspondiente de esta política.
- Que la Entidad de Certificación dispone de sistemas de gestión de la calidad y la seguridad adecuados para la prestación del servicio²⁹, dato que será comprobado en la auditoría de conformidad prevista en la sección 8 de esta política.

²⁴ TS 101 456: 7.3.1 f); TS 102 042: 7.3.1 j)

²⁵ Ley 59/2003: Artículo 20.1 a); TS 101 456: 7.5; TS 102 042: 7.5

²⁶ TS 101 456: 7.5 a); TS 102 042: 7.5 a)

²⁷ TS 101 456: 7.5 b); TS 102 042: 7.5 b)

²⁸ TS 101 456: 7.5 c); TS 102 042: 7.5 c)

²⁹ TS 101 456: 7.5 d); TS 102 042: 7.5 d)

- Que la Entidad de Certificación utiliza personal calificado y con la experiencia necesaria para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos adecuados de seguridad y de gestión.³⁰.
- Que la Entidad de Certificación cumple los requisitos de capacidad financiera establecidos en la sección 9.2 de esta política³¹.
- Que la Entidad de Certificación cumple los requisitos relativos a los procedimientos de resolución de disputas, establecidos en la sección 9.13 de esta política³².
- Que la Entidad de Certificación ha documentado adecuadamente las relaciones jurídicas en virtud de las que externaliza parte o la totalidad de sus servicios.³³.

4.2.3 Requisitos para los certificados personales

La Entidad de Certificación tendrá que:

- Utilizar un procedimiento de generación de certificados que vincule de forma segura el certificado con la información de registro, incluyendo la clave pública certificada³⁴.
- En caso que la Entidad de Certificación genere el par de claves, utilizar un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves, y que la clave privada sea entregada de forma segura al poseedor de claves³⁵.
- Proteger la integridad de los datos de registro, especialmente en caso que sean intercambiados con el suscriptor, en caso de certificados individuales, con el poseedor de claves, en caso de certificados de organización o de entidad, o con el tercer solicitante, en su caso.³⁶.

4.2.3.1 Requisitos específicos para los certificados personales

Adicionalmente, la Entidad de Certificación tendrá que:

- Incluir en el certificado las informaciones establecidas en el artículo 11 de la Ley 59/2003, de acuerdo con lo establecido en la sección 7 de esta política.
- Garantizar la fecha y la hora en que se expidió un certificado³⁷

³⁰ Ley 59/2003: Artículo 20.1 c); TS 101 456: 7.5 g); TS 102 042: 7.5 g)

³¹ TS 101 456: 7.5 f); TS 102 042: 7.5 f)

³² TS 101 456: 7.5 h); TS 102 042: 7.5 h)

³³ TS 101 456: 7.5 i); TS 102 042: 7.5 i)

³⁴ TS 101 456: 7.3.3 b); TS 102042: 7.3.3 b)

³⁵ TS 101 456: 7.3.3 c); TS 102042: 7.3.3 c)

³⁶ TS 101 456: 7.3.3 e); TS 102042: 7.3.3 e)

³⁷ Ley 59/2003: Art. 20.1 b)

- En caso que la Entidad de Certificación aporte su dispositivo seguro de creación de firma, utilizar un procedimiento de gestión de dispositivos seguros de creación de firma que asegure que dicho dispositivo es entregado de forma segura al poseedor de claves³⁸.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte³⁹.
- Asegurarse que el certificado es emitido por sistemas que utilicen protección contra falsificación y, en caso que la Entidad de Certificación genere claves privadas, que garanticen el secreto de las claves durante el proceso de generación de dichas claves⁴⁰.

4.2.4 Requisitos para los certificados de entidad.

Adicionalmente, la Entidad de Certificación tendrá que:

- Incluir en el certificado las informaciones establecidas en el artículo 11.2 de la Ley 59/2003, de acuerdo con lo establecido en la sección 7 de esta política.
- Garantizar la fecha y la hora en que se expidió un certificado⁴¹.
- En caso que la Entidad de Certificación aporte el dispositivo seguro de creación de firma, utilizar un procedimiento de gestión de dispositivos seguros de creación de firma que asegure que dicho dispositivo es entregado de forma segura al poseedor de las claves⁴².
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte⁴³.
- Asegurarse que el certificado es emitido por sistemas que utilicen protección contra falsificación y, en caso que la Entidad de Certificación genere claves privadas, que garanticen el secreto de las claves durante el proceso de generación de dichas claves⁴⁴.

4.2.5 Requisitos para los certificados de dispositivo

La Entidad de Certificación, o la Entidad de Registro Colaboradora autorizada, antes de aprobar una solicitud de certificado de dispositivo que lleve adjunta la clave pública a certificar y la prueba de posesión de la correspondiente clave privada, debe comprobar dicha prueba de posesión.

³⁸ TS 101 456: 7.3.3 c); TS 102042: 7.3.3 c)

³⁹ Ley 59/2003: Art. 20.1 d)

⁴⁰ TS 101 456: 7.3.3, con referencia a D 99/93: Anexo II g);

⁴¹ Ley 59/2003: Art. 20.1 b)

⁴² TS 101 456: 7.3.3 c); TS 102042: 7.3.3 c)

⁴³ Ley 59/2003: Art. 20.1 d)

⁴⁴ TS 101 456: 7.3.3, con referencia a D 99/93: Anexo II g);

En caso que la comprobación de la prueba de posesión de la clave privada sea satisfactoria, se procederá a la emisión del certificado, conforme a lo que se estipula a continuación.

4.3 Emisión de certificado

4.3.1 Acciones de la Entidad de Certificación durante los procesos de emisión y de renovación

Después de la aprobación de la solicitud de certificación se procederá a la emisión del certificado, de forma segura⁴⁵ y se pondrá el certificado a disposición del poseedor de claves, de acuerdo con lo establecido en la sección correspondiente⁴⁶.

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

La Entidad de Certificación tendrá que:

- a. Utilizar un procedimiento de generación de certificados que vincule de forma segura el certificado con la información de registro, incluyendo la clave pública certificada⁴⁷
- b. En caso que la Entidad de Certificación genere el par de claves, utilizar un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves. Y entregar de forma segura la clave privada al poseedor correspondiente.⁴⁸
- c. Proteger la integridad de los datos de registro, especialmente en caso de que sean intercambiados con el suscriptor⁴⁹.

Adicionalmente a lo establecido en la sección correspondiente, la Entidad de Certificación tendrá que:

- a. Incluir en el certificado las informaciones establecidas en el artículo 11.2 de la Ley 59/2003, de acuerdo con lo establecido en la sección correspondiente de esta política.
- b. Indicar la fecha y la hora en las que se expidió un certificado.⁵⁰
- c. En caso de que la Entidad de Certificación aporte el dispositivo seguro de creación de firma, utilizar un procedimiento de gestión de dispositivos seguros de creación de firma que asegure que este dispositivo es entregado de forma segura al poseedor de claves⁵¹.

⁴⁵ TS 101 456: 7.3.3

⁴⁶ TS 101 456: 7.3.5 a)

⁴⁷ TS 101 456: 7.3.3 b)

⁴⁸ TS 101 456: 7.3.3 c)

⁴⁹ TS 101 456: 7.3.3 e)

⁵⁰ Art. 20,1,b) Ley 59/2003

⁵¹ TS 101 456: 7.3.3 c)

- d. Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.⁵²
- e. Tomar medidas contra la falsificación de certificados y, en caso que la Entidad de Certificación Vinculada genere claves privadas, que garanticen el secreto de las claves durante el proceso de generación de estas claves.⁵³

4.3.2 Comunicación de la emisión al suscriptor

La Entidad de Certificación tendrá que comunicarle al solicitante la aprobación o denegación de la solicitud.

También se comunicará al futuro poseedor de claves que se ha creado el certificado, se encuentra disponible y la forma de obtenerlo.

4.4 Aceptación del certificado

4.4.1 Responsabilidades de la Entidad de Certificación

La Entidad de Certificación tendrá que:

- Si no lo ha hecho antes, y cuando resulte necesario, acreditar la identidad del poseedor de claves, de acuerdo con lo establecido en la sección 3.2 de esta política.
- Proporcionar al futuro poseedor de claves, acceso al certificado⁵⁴.
- Cuando el certificado en cuestión se encuentre en un dispositivo criptográfico de generación de firma:
 - o Entregar, al poseedor de claves, dicho dispositivo
 - o Entregarle también una hoja de entrega del certificado, con los siguientes contenidos mínimos:
 - Información básica sobre la política y las condiciones de uso del certificado, incluyendo especialmente información sobre la Entidad de Certificación Vinculada y la Declaración de Prácticas de Certificación aplicable, así como sus obligaciones, facultades y responsabilidades.
 - Información sobre el certificado y el dispositivo criptográfico.
 - Obligaciones del poseedor de claves
 - Responsabilidad de poseedor de claves
 - Método de imputación exclusiva al poseedor de la clave privada, de los datos de activación del certificado y, en su caso, del dispositivo criptográfico, de acuerdo con lo establecido en las secciones correspondientes de esta política.

⁵² Ley 59/2003: 20.1.d)

⁵³ TS 101 456: 7.3.3, en referencia a D 99/93: Anexo II g); Art. 20,1,e) Ley 59/2003

⁵⁴ TS 101 456: 7.3.5 a); TS 102042: 7.3.5 a)

- La fecha del acto de entrega y aceptación.
- Recabar, del poseedor de claves, la aceptación del certificado; y, en su caso, el reconocimiento de recibir el dispositivo criptográfico. Esto se materializa mediante la firma, manuscrita y por parte del poseedor de claves, de los siguientes documentos - los cuales incluyen mención explícita a estos reconocimientos:
 - Cuando el certificado se entrega almacenado en un dispositivo criptográfico: el poseedor de las claves firma una hoja de entrega del certificado.
 - Cuando el certificado se genera en soporte software y el mecanismo de entrega consiste en su descarga, desde una página web, por parte del poseedor de las claves (como ocurre con los certificados idCAT, por ejemplo): éste firma la solicitud de emisión del certificado.

Un ejemplar de estos documentos serán guardados durante 15 años por la Entidad de Certificación – mediante la participación de las Entidades de Registro; otro, se entregará al poseedor de claves.

4.4.2 Conducta que constituye aceptación del certificado

El certificado se podrá aceptar mediante la firma de la hoja de entrega o de la solicitud de emisión del certificado, descritos anteriormente.

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

4.4.3 Publicación del certificado

Los certificados de clase 1 se podrán publicar en todo caso, sin el consentimiento previo de los poseedores de claves, mientras que la publicación de los certificados de clase 2 requerirá siempre el consentimiento de los suscriptores⁵⁵.

4.4.4 Comunicación de la emisión a terceros

No aplicable.

4.5 Uso del par de claves y del certificado

Los certificados deben utilizarse de acuerdo con su función propia y finalidad establecida, y no deben utilizarse en otras funciones y con otras finalidades; especialmente no se han diseñado, no se pueden destinar y no se autoriza su uso para aquellas funciones prohibidas explícitamente por esta política en el apartado “Aplicaciones prohibidas”.

Los certificados tendrán que utilizarse únicamente de acuerdo con la ley aplicable.

⁵⁵ Ley 59/2003: Art. 17.2

La extensión Key Usage se utilizará para establecer límites técnicos a los usos que puede darse a una clave privada correspondiente a una clave pública contenida en un certificado X.509v3. Aunque hay que considerar que la efectividad de las limitaciones basadas en extensiones de certificados depende en ocasiones del tratamiento que de éstas hagan aplicaciones informáticas que no han sido fabricadas ni pueden estar controladas por las Entidades de Certificación.

4.5.1 Uso por parte de los poseedores de claves

Son las siguientes:

Utilizar el par de claves exclusivamente para generar firmas electrónicas y/o descifrar información, y de acuerdo con cualesquiera otras limitaciones que le sean notificadas.⁵⁶

Ser especialmente diligente en la custodia de su clave privada y de su dispositivo seguro de creación de firma, con la finalidad de evitar usos no autorizados.⁵⁷

Si el poseedor de claves genera sus propias claves, se obliga a:

- Generar sus claves utilizando un algoritmo reconocido como aceptable para la firma electrónica reconocida.⁵⁸
- Crear las claves dentro del dispositivo seguro de creación de firma.⁵⁹
- Utilizar longitudes y algoritmos de clave reconocidos como aceptables para la firma electrónica reconocida.⁶⁰

4.5.2 Uso por el tercero que confía en certificados

Son las siguientes:

Utilizar el certificado digital exclusivamente para validar firmas electrónicas y/o cifrar información para otro usuario, y de acuerdo con cualesquiera otras limitaciones que le sean notificadas.

Comprobar la validez del certificado digital (vigencia y estado) antes de confiar en éste.

4.6 Renovación de certificados sin renovación de claves

No recomendado por las mejores prácticas del sector y no soportado por el actual sistema de certificación implantado. No se permite la renovación de certificados sin renovación de claves.

⁵⁶ TS 101456: 6.2.b)

⁵⁷ TS 101456: 6.2.c), más estricto, y extensión al dispositivo seguro de creación de firma.

⁵⁸ TS 101456: 6.2.d) primero

⁵⁹ TS 101456: 6.2.f)

⁶⁰ TS 101456: 6.2.d) segundo

4.7 Renovación de certificado con renovación de claves

La renovación de un certificado se inicia dos meses antes de la fecha de expiración del certificado, cuando el suscriptor recibe un correo electrónico donde se le informa de los pasos a seguir para ejecutar la renovación del certificado. Este correo se vuelve a enviar 30 días antes de la expiración.

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 Entidad de Registro Interna tendrá que verificar que los datos de registro continúan siendo válidos y, si algún dato ha cambiado, éste debe ser verificado, se debe guardar evidencia de dicha comprobación y el suscriptor tiene que estar de acuerdo con la modificación, tal como se especifica en la sección correspondiente de esta política⁶¹.

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

La Entidad 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.⁶²

Para certificados individuales en soporte llavero, el suscriptor deberá personarse en las oficinas de la Entidad de Registro, puesto que las nuevas claves se generarán en dicho dispositivo.

4.8 Renovación telemática

El Consorci AOC 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 éste), 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 Entidad 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 para introducir las modificaciones necesarias, incluyendo la revocación del certificado vigente. En ciertos casos, en función de la

⁶¹ TS 101 456: 7.3.2 a) y c); TS 102 042: 7.3.2 a) y c)

⁶² TS 101 456: 7.3.2 b); TS 102 042: 7.3.2 b)

información a modificar, esta revocación podrá hacerse en fecha posterior a la emisión del certificado con los datos actualizados.

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

4.10 Revocación y suspensión de certificados

La Entidad de Certificación tendrá que detallar en su Declaración de Prácticas de Certificación los siguientes aspectos⁶³ :

- a. Quien puede solicitar la revocación
- b. Como se remitirá la solicitud
- c. Los requisitos de confirmación de solicitudes de revocación
- d. Si se pueden suspender certificados, y las causas de suspensión
- e. Los mecanismos utilizados para distribuir información de estado de revocación
- f. El máximo retraso entre la recepción de la solicitud y la disponibilidad para verificadores del cambio del estado de revocación, que no podrá superar en ningún caso el plazo de un día.

4.10.1 Causas de revocación de certificados

Una Entidad de Certificación podrá revocar un certificado por la concurrencia de las siguientes causas:

1. Circunstancias que afecten la información contenida en el certificado⁶⁴
 - Modificación de alguno de los datos contenidos en el certificado.
 - Descubrimiento de que alguno de los datos aportados en la solicitud del certificado es incorrecto, 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 la seguridad de la clave o del certificado
 - Compromiso de la clave privada o de la infraestructura o sistemas de la Entidad de Certificación que emitió el certificado, siempre que afecte la fiabilidad de los certificados emitidos a partir de este incidente.
 - Infracción, por la Entidad de Certificación, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en la DPC de la Entidad de Certificación.

⁶³ TS 101 456: 7.3.6 a); TS 102042: 7.3.6 a)

⁶⁴ Ley 59/2003: Art. 8.1.g)

- Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del poseedor de claves⁶⁵.
- Acceso o utilización no autorizadas, por un tercero, de la clave privada del poseedor de claves⁶⁶.
- El uso irregular del certificado por el poseedor de claves, o falta de diligencia en la custodia de la clave privada.

3. Circunstancias que afectan 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 Entidad de Certificación Vinculada y el poseedor de claves.
- Modificación o extinción de la relación jurídica subyacente o de la causa que motivó la emisión del certificado al poseedor de claves.
- Infracción, por parte del solicitante del certificado, de los requisitos preestablecidos para la solicitud de éste.
- 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 Entidad de Certificación Vinculada que le emitió el certificado.
- La incapacidad sobrevenida o la muerte del poseedor de claves⁶⁷.
- En caso de certificados corporativos, la extinción de la persona jurídica suscriptora del certificado⁶⁸, 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 política.

5. Circunstancias relativas a los certificados Extended Validation:

- Solicitud del suscriptor de revocación del certificado.
- La Entidad de Certificación obtiene pruebas razonables de que la clave privada del suscriptor se ha visto comprometida o de que el certificado ha sido usurpado por un tercero.

⁶⁵ Ley 59/2003: Art. 8.1.c)

⁶⁶ Ley 59/2003: Art. 8.1 c)

⁶⁷ Ley 59/2003: Art. 8.1 e)

⁶⁸ Ley 59/2003: Art. 8.1 e)

- La Entidad 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 Entidad de Certificación tiene conocimiento del incumplimiento de las Condiciones Generales de Uso o de otras especificaciones establecidas en la documentación jurídica u operativa.
- La Entidad de Certificación cesa actividades que dan soporte a la revocación de certificados Extended Validation o pierde el derecho de emitir certificados Extended Validation. Si la Entidad de Certificación puede garantizar el mantenimiento de los servicios de validación CRL y OCSP, la revocación no es necesaria.
- Compromiso o sospecha de compromiso de las claves de cualquier Entidad 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 por un periodo superior a 120 días.
- La finalización del servicio de la Entidad de Certificación Vinculada.
- La finalización de la prestación de servicios por parte de el Consorci AOC.
- Resolución judicial o administrativa que lo ordene (Art. 8.1 de la Ley 59/2003, de firma electrónica).
- La Entidad de Certificación Vinculada tiene conocimiento de que los certificados CDP han realizado firmas sobre código hostil.

El instrumento jurídico que vincula a la Entidad de Certificación Vinculada 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 Entidad de Certificación Vinculada 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 por la entidad suscriptora; en ocasiones, a instancia del poseedor de claves.
- En caso de certificados de entidad, la persona autorizada al efecto por la entidad suscriptora; en ocasiones, a instancia del responsable de la custodia de las claves.

- La Entidad de Registro que solicitó la emisión del certificado.

4.10.3 Procedimientos de solicitud de revocación

La revocación de un certificado debe solicitarse a la Entidad de Certificación Vinculada, a través de la Entidad de Registro que aprobó la solicitud de certificación; por tanto, debe dirigirse a ésta – presencialmente o por medios electrónicos.

Las Entidades de Registro atienden 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, cuyo horario de atención es 24x365.

La solicitud de revocación debe incluir la siguiente información:

- Fecha de solicitud de la revocación
- Identidad del poseedor de claves
- Razón detallada para la petición de revocación
- Nombre y cargo de la persona que pide la revocación
- Información de contacto de la persona que pide la revocación

Una vez revocados, los certificados no podrán ser reactivados. La revocación no podrá levantarse ni anularse de ninguna forma; es un estado definitivo del certificado⁶⁹.

4.10.4 Plazo temporal de solicitud de revocación

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

Fuera del horario de atención de las Entidades de Registro, el suscriptor puede solicitar la suspensión cautelar del certificado a través del Servicio de Atención al Usuario del Consorci AOC.

4.10.5 Plazo máximo de procesamiento de la solicitud de revocación

Cuando una Entidad de Registro o una Entidad de Certificación Vinculada reciban una solicitud de revocación, ésta será procesada en el mínimo plazo posible, dentro de los horarios de oficina de la Entidad de Certificación.^{70 71}

Antes de proceder a la revocación efectiva de un certificado, el destinatario de la solicitud debe autenticarla, de acuerdo con los requisitos establecidos en la sección correspondiente de esta política.⁷²

⁶⁹ TS 101 456: 7.3.6. f); TS 102042: 7.3.6 f)

⁷⁰ Ley 59/2003: Art. 10

⁷¹ TS 101 456: 7.3.6. b); TS 102042: 7.3.6 b)

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

Se deberá informar sobre el cambio de estado del certificado que se ha revocado al poseedor de claves y también, cuando se trate de certificados corporativos, al suscriptor⁷³.

4.10.6 Obligación de consulta de información de revocación de certificados

Los verificadores deben comprobar el estado de los certificados antes de confiar en ellos.

Para verificar el estado de los certificados debe consultarse la lista de certificados revocados (CRL o LCR) vigente emitida por el Entidad de Certificación que emitió dicho 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 Entidades 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 que se publica dicha información (listas CRL y servicios OCSP) se indican entre el contenido de los certificados que emiten.

4.10.7 Frecuencia de emisión de listas de revocación de certificados (LCRs)

4.10.7.1 Requisitos específicos del CIC

La Entidad de Certificación Raíz o entidad de certificación que expida certificados de entidad de certificación tendrá que emitir una LCR inmediatamente después de la revocación de una Entidad de Certificación de la jerarquía.

Y, en todo caso, emitirá una LCR anualmente⁷⁴.

4.10.7.2 Requisitos para los certificados personales, de entidad y de dispositivo

La Entidad de Certificación Vinculada tendrá que emitir una LCR al menos cada 24 horas⁷⁵.

En la LCR se indicará el momento programado de emisión de una nueva LCR, si bien se podrá emitir una LCR antes de dicho momento, por necesidades del servicio (esto es, si se ha revocado algún certificado)⁷⁶.

⁷² TS 101 456: 7.3.6. c); TS 102042: 7.3.6 c)

⁷³ TS 101 456: 7.3.6. e); TS 102042: 7.3.6 e)

⁷⁴ CAFB BR 4.9.7

⁷⁵ TS 101 456: 7.3.6 g); TS 102042: 7.3.6 g)

⁷⁶ TS 101 456: 7.3.6 g); TS 102042: 7.3.6 h)

Se retirarán del contenido de la LCR las referencias a certificados que hayan superado el periodo de validez previsto en el momento de su emisión.

4.10.8 Periodo máximo de publicación de LCRs

Una vez generadas, las nuevas versiones de las LCRs serán publicadas inmediatamente en la webdel Consorci AOC y en 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 un servicio en línea que responda sobre el estado de certificados (servicio *OCSP responder* u otros servicios de validación de certificados) operado por un prestador de servicios de validación en el que se confía.

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

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

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

Los verificadores deben 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 dicho estado.

4.10.11 Otras formas de información de revocación de certificados

Se podrán establecer otras formas para informar sobre la revocación de los certificados, que se tendrán que detallar en la DPC de la Entidad de Certificación Vinculada.

4.10.12 Requerimientos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de una Entidad de Certificación Vinculada 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 LCR pertinente de la referencia al certificado digital de dicha Entidad de Certificación.

4.10.13 Causas de suspensión de certificados

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

- Cuando lo solicite el poseedor de claves o el suscriptor o un tercero autorizado (art. 9.1.a de la Ley 59/2003).
- En los casos legalmente previstos en el artículo 9.1 de la Ley de Firma electrónica, esto es, en el caso de que una resolución judicial o administrativa lo ordene.
- Cuando la documentación requerida en la solicitud de revocación sea suficiente pero no se pueda identificar razonablemente al poseedor de claves.
- Cuando la documentación requerida en la solicitud de revocación no sea suficiente, aunque se pueda identificar razonablemente al poseedor de claves
- Cuando la documentación requerida en la solicitud de revocación no sea suficiente y tampoco permitan 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 éste sea confirmado. En este caso, la Entidad de Certificación Vinculada tiene que asegurarse que el certificado no está suspendido durante más tiempo del necesario para confirmar su compromiso.

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 se 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 deberá personarse ante la Entidad de Registro que aprobó la solicitud de emisión de dicho certificado y presentar el documento acreditativo de su identidad, para que ésta pueda comprobarla.

Todo cambio de estado de un certificado (suspensión, habilitación, etc) se deberá informar al poseedor de claves y también, cuando se trate de certificados corporativos, al suscriptor⁷⁷

⁷⁷ TS 101 456: 7.3.6. e); TS 102042: 7.3.6 e)

4.10.15 Quien puede solicitar la suspensión

Podrán solicitar la suspensión de un certificado:

- En caso de certificados individuales: el poseedor de claves o la entidad de registro que solicitó la emisión del certificado, actuando en nombre de éste.
- En caso de certificados corporativos: un representante autorizado por la entidad suscriptora, la entidad 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 formas 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 del Consorci AOC.
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 del Consorci AOC.
3. La suspensión puede ser solicitada por la Entidad de Registro. En caso de que la Entidad de Registro disponga de autorización del Consorci AOC, puede realizar ella misma el proceso de suspensión. En caso contrario, realiza la tramitación de la suspensión a través del Consorci AOC.

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 debe suspender el certificado digital.
- DNI del poseedor de claves a quien se le debe suspender el certificado digital.
- Número de serie (serial number) 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 trate 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 pide 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 de que el plazo máximo de la misma será de 120 días (arts. 10.2 y 10.4 de la Ley 59/2003).

4.10.17 Plazo máximo de suspensión

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

4.10.18 Habilitación de un certificado suspendido

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

4.11 Servicios de comprobación de estado de certificados

4.11.1 Características de operación de los servicios

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

De forma alternativa, los verificadores podrán consultar los certificados publicados en el directorio de la Entidad de Certificación Vinculada.

4.11.2 Disponibilidad de los servicios

Los sistemas de distribución de LCRs y de consulta en línea del estado de los certificados tendrán que estar disponibles las 24 horas de los 7 días de la semana.⁷⁸

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de la Entidad de Certificación, esta tendrá que realizar sus mejores esfuerzos para asegurar que este servicio se mantiene inactivo el mínimo tiempo posible. La Entidad de Certificación detallará en su DPC el periodo máximo de tiempo en el que el servicio tendrá que volver a operar.⁷⁹

La Entidad de Certificación tendrá que suministrar información a los verificadores sobre el funcionamiento del servicio de información de estado de certificados.

4.11.3 Otras funciones de los servicios

Sin estipulación adicional.

⁷⁸ TS 101 456: 7.3.6 i); TS 102042: 7.3.6 i)

⁷⁹ TS 101 456: 7.3.6 i); TS 102042: 7.3.6 i)

4.12 Finalización de la suscripción

La finalización de la suscripción no implicará la revocación de los certificados que hayan estado 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 Entidad de Certificación tendrá que detallar en su DPC los siguientes aspectos:

- a. Quién puede solicitar el depósito y la recuperación de claves
- b. Cómo se remitirá 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 encapsulamiento y recuperación de claves de sesión

Sin estipulación adicional.

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

5.1 Controles de seguridad física

La Entidad de Certificación tiene que disponer de instalaciones que protejan físicamente la prestación, al menos, de los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos.⁸⁰

La protección física se conseguirá mediante la creación de perímetros de seguridad claramente definidos alrededor de los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación. La parte de las instalaciones compartida con otras organizaciones tiene que encontrarse fuera de estos perímetros.⁸¹

La Entidad de Certificación establecerá controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentren los sistemas, así como 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 establecerá prescripciones para las siguientes contingencias⁸²:

- Controles de acceso físico
- Protección ante desastres naturales
- Medidas de protección ante incendios
- Fallo de los sistemas de soporte (energía eléctrica, telecomunicaciones, etc)
- Derribo de la estructura
- Inundaciones
- Protección antirrobo
- Conformidad y entrada no autorizada
- Recuperación del desastre
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativas a componentes utilizados para los servicios de la Entidad de Certificación.⁸³

5.1.1 Localización y construcción de las instalaciones

La localización de las instalaciones tiene que permitir la presencia de fuerzas de seguridad en un plazo de tiempo razonablemente inmediato desde que una incidencia les sea notificada (en el caso de no contar con presencia física permanente de personal de seguridad de la Entidad de Certificación).

⁸⁰ TS 101 456: 7.4.4 d); TS 102 042: 7.4.4 d)

⁸¹ TS 101 456: 7.4.4 e) ; TS 102 042: 7.4.4 e)

⁸² TS 101 456: 7.4.4 f) ; TS 102 042: 7.4.4 f)

⁸³ TS 101 456: 7.4.4 g) ; TS 102 042: 7.4.4 g)

La calidad y solidez de los materiales de construcción de las instalaciones tendrá que garantizar unos adecuados niveles de protección ante intrusiones por fuerza bruta.

5.1.2 Acceso físico

La Entidad de Certificación tendrá que establecer niveles de seguridad con restricción de acceso a los diferentes perímetros y barreras físicas definidas.

Para el acceso a las dependencias de la Entidad de Certificación donde se lleven a cabo procesos relacionados con el ciclo de vida del certificado, será necesaria la autorización previa, identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.⁸⁴

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

La generación de claves criptográficas de las Entidades de Certificación, así como su almacenaje, tendrá que realizarse en dependencias específicas para estas finalidades, y requerirán de acceso y permanencia dobles.

5.1.3 Electricidad y aire acondicionado

Los equipos informáticos de la Entidad de Certificación tendrán que estar convenientemente protegidos ante fluctuaciones o cortes de suministro eléctrico, que puedan dañarlos o interrumpir el servicio.

Las instalaciones contarán 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 tendrán que estar ubicados en un entorno donde se garantice una climatización (temperatura y humedad) adecuada a sus condiciones óptimas de trabajo.

5.1.4 Exposición al agua

La Entidad de Certificación tendrá que disponer de sistemas de detección de inundaciones adecuados para proteger los equipos y activos ante tal eventualidad, en el caso que las condiciones de ubicación de las instalaciones lo hicieran necesario.

5.1.5 Advertencia y protección de incendios

Todas las instalaciones y activos de la Entidad de Certificación tienen que contar con sistemas automáticos de detección y extinción de incendios.

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

⁸⁴ TS 101 456: 7.4.4 a) y d); ; TS 102 042: 7.4.4 a) y d)

5.1.6 Almacenaje de soportes

El almacenaje en soportes de información tiene que realizarse de forma que se garantice tanto su integridad como su confidencialidad, de acuerdo con la clasificación de la información que se haya establecido.⁸⁵

Tendrá que contar para ellos con dependencias o armarios ignífugos.

El acceso a estos soportes, incluso para su eliminación, tendrá que estar restringido a personas específicamente autorizadas.

Cabe tener en cuenta que las Entidades de Registro se quedan con una copia firmada por el poseedor de claves de la hoja de entrega o de la hoja de solicitud de emisión de certificados. Esta copia es guardada durante 15 años por la Entidad de Registro, aplicándosele las indicaciones de la legislación catalana de archivos, en relación con la guarda y custodia de documentación.

5.1.7 Tratamiento de residuos

La eliminación de soportes, tanto papel como magnéticos, se tendrá que realizar mediante mecanismos que garanticen la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se procederá al formateo, borrado permanente, o destrucción física del soporte.

En el caso de documentación en papel, éste tendrá que someterse a un tratamiento físico de destrucción.

5.1.8 Copia de seguridad fuera de las instalaciones

Periódicamente, la Entidad de Certificación almacenará un backup de los sistemas de información, en dependencias físicamente separadas de aquellas en las que se encuentren los equipos.

Se realizará una copia de seguridad incremental diaria y una copia de seguridad semanal.

En el momento de realizar una salida de información de las dependencias, se deben adoptar medidas adecuadas para impedir cualquier recuperación indebida de la mencionada información (como por ejemplo la utilización de carteras con dispositivos seguros de claves o combinaciones o la utilización de ficheros cifrados).

5.2 Controles de procedimientos

Las Entidades de Certificación tienen que garantizar que sus sistemas se operen de forma segura⁸⁶, y por esto tendrán que establecer e implantar procedimientos para las funciones que afecten a la provisión de sus servicios.⁸⁷

⁸⁵ TS 101 456: 7.4.5 c) e i); TS 102 042: 7.4.5 c) e i)

⁸⁶ Art. 20, 1, d) Ley 59/2003; TS 101 456: 7.4.5; TS 102 042: 7.4.5

⁸⁷ TS 101 456: 7.4.5 d); TS 102 042: 7.4.5 d)

El personal al servicio de la Entidad de Certificación realizará los procedimientos administrativos y de gestión de acuerdo con la política de seguridad de la Entidad de Certificación.⁸⁸

5.2.1 Funciones fiables

Las personas que tengan que ocupar estos sitios tendrán que ser formalmente nominados por la alta dirección de la Entidad de Certificación⁸⁹.

Las funciones fiables tendrán que incluir⁹⁰:

- a. Personal responsable de la seguridad
- b. Administradores del sistema
- c. Operadores del sistema
- d. Auditores del sistema
- e. Cualquier otra persona con acceso a datos de carácter personal, como los operadores de registro.

Las funciones y obligaciones fiables tendrán que definirse y documentarse en la Declaración de Prácticas de Certificación de la Entidad de Certificación⁹¹

5.2.2 Número de personas por tarea

Las funciones fiables identificadas en la política de seguridad de la Entidad de Certificación Vinculada, y sus responsabilidades asociadas, serán documentadas en descripciones de lugares de trabajo⁹².

5.2.3 Identificación y autenticación para cada función

La Entidad de Certificación tendrá que identificar y autenticar el personal antes de acceder a la correspondiente función fiable.⁹³

5.2.4 Roles que requieren separación de tareas

La Entidad de Certificación tendrá que identificar, en su política de seguridad, funciones o roles fiables.⁹⁴

Dichas descripciones tendrán que realizarse teniendo en cuenta que tiene que existir una separación de funciones sensibles, así como una concesión de mínimo privilegio, cuando

⁸⁸ TS 101 456: 7.4.3 d) ; TS 102 042: 7.4.5 d)

⁸⁹ TS 101 456: 7.4.3 h); TS 102 042: 7.4.3 h)

⁹⁰ TS 101 456: 7.4.3 g); TS 102 042: 7.4.3 g)

⁹¹ RD 994/99: Art. 9.1

⁹² TS 101 456: 7.4.3 b); TS 102 042: 7.4.3 b)

⁹³ TS 101 456: 7.4.6 e); TS 102 042: 7.4.3 e)

⁹⁴ TS 101 456: 7.4.3 b); TS 102 042: 7.4.3 b)

sea posible. Para determinar la sensibilidad de la función, se tendrán en cuenta los siguientes elementos⁹⁵:

- 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

5.3.1 Requisitos de historial, calificaciones, experiencia y autorización

El Consorci AOC 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 del Consorci AOC, especialmente en relación con procedimientos de personal de seguridad.

La calificación y la experiencia pueden suplirse mediante una formación y entrenamiento apropiados.

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

5.3.2 Requisitos de formación

La Entidad de Certificación tendrá que formar al personal en lugares fiables y de gestión, hasta que logren la calificación necesaria, de acuerdo con lo establecido en la sección correspondiente de esta política.

La formación tendrá que incluir los siguientes contenidos:

- a. Principios y mecanismos de seguridad de la jerarquía pública de certificación de Cataluña, así como el entorno de usuario de la persona a formar.
- b. Versiones de maquinaria y aplicaciones en uso
- c. Tareas que tiene que realizar la persona
- d. Gestión y tramitación de incidentes y compromisos de seguridad

⁹⁵ TS 101 456: 7.4.3 c); TS 102 042: 7.4.3 c)

- e. Procedimientos de continuidad de negocio y emergencia
- f. Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.⁹⁶

5.3.3 Requisitos y frecuencia de actualización formativa

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

5.3.4 Secuencia y frecuencia de rotación laboral

Sin estipulación adicional.

5.3.5 Sanciones por acciones no autorizadas

La Entidad de Certificación tendrá que disponer de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas.

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

5.3.6 Requisitos de contratación de profesionales

La Entidad de Certificación podrá contratar profesionales para cualquier función, incluso para un lugar fiable, caso en el que se tendrá que someter a los mismos controles que los empleados restantes.

En el caso que el profesional no tenga que someterse a estos controles, tendrá que estar constantemente acompañado por un empleado fiable.

En el caso que todos o una parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección 5, o en otras partes de la política de certificado o de la DPC, serán aplicados y completados por el tercero que realice las funciones de operación de los servicios de certificación, la entidad de certificación será responsable en todo caso de la efectiva ejecución.

Estos aspectos tendrán que quedar concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por el tercero diferente a la entidad de certificación.

5.3.7 Suministro de documentación al personal

La Entidad de Certificación suministrará la documentación que estrictamente necesite su personal en cada momento, con el fin que sea suficientemente competente de acuerdo con lo establecido en la sección correspondiente de esta política.

⁹⁶ RD 994/99: Art. 9.2

5.4 Procedimientos de auditoría de seguridad

5.4.1 Tipos de acontecimientos registrados

La Entidad de Certificación tiene que guardar registro, como mínimo, de los siguientes acontecimientos relacionados con la seguridad de la entidad:

- Encendido y apagado de los sistemas
- Inicio y finalización de la aplicación de Autoridad (técnica) de certificación
- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema
- Cambios en las claves de la Autoridad (técnica) de certificado
- Cambios en las políticas de emisión de certificados
- Intentos de entrada y salida del sistema
- Intentos no autorizados de entrada en la red de la Entidad de Certificación
- Intentos no autorizados de acceso a los ficheros del sistema
- Generación de las claves de la Entidad de Certificación y de las Entidades de Certificación vinculadas
- 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, emisión, revocación y renovación de un certificado
- Acontecimientos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de éste

La Entidad de Certificación también tiene que guardar, ya sea manual o electrónicamente, la siguiente información:

- 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, en caso de certificados individuales, o del poseedor de claves, en caso de certificados de organización, o del responsable de la custodia de claves, en caso de certificados de entidad
- Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Certificación
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.

5.4.2 Frecuencia de tratamiento de registros de auditoría

Los registros de auditoría se examinarán al menos una vez a la semana en búsqueda de actividad sospechosa o no habitual

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

5.4.3 Periodo de conservación de registros de auditoría

Los registros de auditoría se retienen durante al menos dos meses después de procesarlos y a partir de ese momento se archivan de acuerdo con la sección correspondiente de esta política

5.4.4 Protección de los registros de auditoría

Los ficheros de registro, tanto manuales como electrónicos, tienen que protegerse de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada usando controles de acceso lógico y físico.

5.4.5 Procedimientos de backup

Se tendrán que generar copias de soporte incrementales de registro de auditoría diariamente y copias completas semanalmente.

5.4.6 Localización del sistema de acumulación de registros de auditoría

El sistema de acumulación de registros de auditoría tendrá que ser, al menos, un sistema interno de la Entidad de Certificación, compuesto por los registros de la aplicación, por los registros de red y por los registros del sistema operativo, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado.

5.4.7 Notificación del acontecimiento de auditoría al causante del acontecimiento

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

Se podrá comunicar 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 tendrán que ser guardados, en parte, para monitorizar las vulnerabilidades del sistema.

Las análisis de vulnerabilidad tienen que ser ejecutadas, repasadas y revisadas por medio de un examen de estos acontecimientos monitorizados

Estos análisis tienen que ser ejecutados diariamente, mensualmente y anualmente de acuerdo con su definición en el Plan de Auditoría de la Entidad de Certificación.

5.5 Archivo de informaciones

La Entidad de Certificación tiene que garantizar que toda la información relativa a los certificados se guarda durante un periodo de tiempo apropiado⁹⁷, según lo establecido en la sección correspondiente de esta política.

5.5.1 Tipos de acontecimientos registrados

La Entidad de Certificación tiene que guardar todos los acontecimientos que tengan lugar durante el ciclo de vida de un certificado, incluyendo la renovación de éste.⁹⁸

La Entidad de Certificación tiene que guardar 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 Entidad de Registro que acepta la solicitud de certificado.⁹⁹
- La ubicación de las copias de solicitudes de certificados y del acuerdo firmado por el suscriptor, en caso de certificados individuales o del poseedor de las claves en caso de certificados de organización o de entidad.¹⁰⁰

5.5.2 Periodo de conservación de registros

5.5.2.1 Requisitos para todos los tipos de certificados

La Entidad de Certificación tiene que guardar los registros especificados en la sección correspondiente de esta política durante 5 años, contados desde el momento de la expedición del certificado.

5.5.2.2 Requisitos específicos para los certificados reconocidos

La Entidad de Certificación tiene que guardar los registros especificados en la sección correspondiente de esta política durante 15 años, contados desde el momento de la expedición del certificado.

5.5.2.3 Requisitos para los certificados CIC

Para los certificados CIC los registros se guardarán indefinidamente.

5.5.3 Protección del archivo

La Entidad de Certificación tiene que:

- Mantener la integridad y la confidencialidad del archivo que contiene los datos referentes a los certificados emitidos.¹⁰¹
- Archivar los datos indicados anteriormente de forma completa y confidencial.¹⁰²

⁹⁷ TS 101 456: 7.4.11; TS 102 042: 7.4.11

⁹⁸ TS 101 456: 7.4.11 h) ; TS 102 042: 7.4.11 h)

⁹⁹ TS 101 456: 7.4.11 i) ; TS 102 042: 7.4.11 i)

¹⁰⁰ TS 101 456: 7.4.11 i) ; TS 102 042: 7.4.11 i)

¹⁰¹ TS 101 456: 7.4.11 a) ; TS 102 042: 7.4.11 a)

- Mantener la privacidad de los datos de registro del suscriptor, en caso de certificados individuales, o del poseedor de las claves, en caso de certificados de organización o de entidad.¹⁰³

5.5.4 Procedimientos de copia de soporte

5.5.4.1 Requisitos para todos los tipos de certificados

La Entidad de Certificación tiene que realizar copias de soporte incrementales diarias de todos sus documentos electrónicos, según esta política. Tiene, además, que realizar copias de soporte completas semanalmente para casos de recuperación de datos, de acuerdo con la sección correspondiente de esta política.

5.5.4.2 Requisitos específicos para los certificados personales y de identidad

La Entidad de Certificación tiene que guardar los documentos en papel, según la sección correspondiente, en un lugar fuera de las instalaciones de la misma Entidad de Certificación para casos de recuperación de datos, de acuerdo con la sección correspondiente de esta política.

5.5.5 Requisitos de sellado de fecha y hora

La Entidad de Certificación tiene que emitir los certificados y las LCR con información de tiempo y hora. No es necesario que esta información se encuentre firmada.

5.5.6 Localización del sistema de archivo

La Entidad de Certificación debe de tener un sistema de mantenimiento de datos de archivo fuera de sus propias instalaciones, así como se especifica en la sección correspondiente de esta política.

5.5.7 Procedimientos de obtención y verificación de información de archivo

Solamente personas autorizadas por la Entidad de Certificación podrán tener acceso a los datos de archivo, sea en las mismas instalaciones de la Entidad de Certificación o en su ubicación externa.

5.6 Renovación de claves

Para la renovación de certificados CIC, la Entidad de Certificación emisora comprobará que se continúan cumpliendo los requisitos que determinaron la emisión de este certificado.

La solicitud del nuevo certificado será firmada con la clave privada del certificado CIC a renovar, siempre que este se encuentre vigente.

Los certificados CIC renovados se comunicaran a los usuarios finales, mediante su publicación en el Registro de el Consorci AOC.

¹⁰² TS 101 456: 7.4.11 b) ; TS 102 042: 7.4.11 b)

¹⁰³ TS 101 456: 7.4.11 j) ; TS 102 042: 7.4.11 j)

5.7 Compromiso de claves y recuperación de desastre

5.7.1 Procedimiento de gestión de incidencias y compromisos

La Entidad de Certificación establecerá en su DPC los procedimientos que aplica en la gestión de las incidencias que afecten sus claves y, muy especialmente, en los compromisos de la seguridad de las claves.

5.7.2 Corrupción de recursos, aplicaciones o datos

Cuando tenga lugar un acontecimiento de corrupción de recursos, aplicaciones o datos la Entidad de Certificación tiene que iniciar las gestiones necesarias, según los documentos Plan de Seguridad, Plan de Emergencia y Plan de Auditoría, para hacer que el sistema vuelva a su estado normal de funcionamiento.

5.7.3 Compromiso de la clave privada de la Entidad

El plan de continuidad de negocio de la Entidad de Certificación (o plan de recuperación de desastres) tiene que considerar el compromiso o sospecha de compromiso de la clave privada de la Entidad de Certificación como un desastre.

En caso de compromiso la Entidad de Certificación tiene que proporcionar como mínimo lo siguiente:

- Informar a todos los suscriptores y verificadores del compromiso.
- Indicar que los certificados y la información del estado de revocación entregados usando la clave de esta Entidad de Certificación ya no son válidos.¹⁰⁴

5.7.4 Desastre sobre las instalaciones.

La Entidad de Certificación tiene que desarrollar, mantener, testar y, si es necesario, ejecutar un plan de emergencia en el caso de desastre, ya sea por causas naturales o causado por el hombre, sobre las instalaciones, que indique como restaurar los servicios de los Sistemas de Información. La ubicación de los sistemas de recuperación de desastre tiene que disponer de las protecciones físicas de seguridad detalladas en el Plan de Seguridad.

La Entidad de Certificación tiene que ser 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 la Entidad de Certificación tiene que estar 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 Entidad de Certificación deben de tener las medidas de seguridad físicas especificadas en el Plan de Seguridad.

¹⁰⁴ TS 101 456: 7.4.8 c); TS 102 042: 7.4.8 c)

5.8 Finalización del servicio

5.8.1 Entidad de Certificación

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

Antes de acabar sus servicios la Entidad de Certificación tiene que ejecutar, como mínimo, los siguientes procedimientos:

- Informar a todos los suscriptores y verificadores (no se requiere que la Entidad de Certificación tenga alguna relación anterior con terceras partes).
- Terminar toda autorización de subcontrataciones que actúen en nombre de la Entidad de Certificación en el proceso de emisión de certificados.
- Ejecutar 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 tiempo respectivos indicados al suscriptor y a los verificadores.
- Destruir las claves privadas de la Entidad de Certificación o retirarlas del uso.

La Entidad de Certificación tiene que declarar en sus prácticas las previsiones que tiene para el caso de finalización del servicio. Estas tienen que incluir:

- Notificación a las entidades afectadas
- Transferencia de las obligaciones de la Entidad de Certificación a otras personas
- Como se tratará el estado de revocación de los certificados emitidos que aún no han expirado¹⁰⁵.

La Entidad de Certificación podrá transferir los certificados, en los términos previstos en la Ley 59/2003, de 19 de diciembre.

5.8.2 Entidad de Registro

Sin estipulación adicional.

¹⁰⁵ TS 101 456: 7.4.9; TS 102 042: 7.4.9

6. Controles de seguridad técnica

La Entidad de Certificación tendrá que utilizar sistemas y productos fiables, que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.¹⁰⁶

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 Requisitos específicos para el CIC

El Consorci AOC procederá a la generación de las claves de Entidad de Certificación de acuerdo con la Ceremonia de Claves, dentro del perímetro de alta seguridad destinado específicamente a esta tarea.

6.1.1.3 Requisitos específicos para los certificados de cifrado

Las claves de los certificados de cifrado serán creadas por la Entidad de Registro y, en su caso, almacenadas para su posterior recuperación.

6.1.2 Envío de la clave privada al suscriptor

Para los certificados de firma reconocida y 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 seguro de creación de firma electrónica de entidad final normalizado, de acuerdo con Common Criteria, EAL 4+, o FIPS 140-2 Nivel 3 o superior nivel de seguridad.

6.1.3 Envío de la clave pública al emisor del certificado

Cuando el par de claves haya sido generado por el poseedor de claves, el método de envío de la clave pública a la Entidad de Certificación será mediante un fichero PKCS #10, o mediante otra prueba criptográfica equivalente o cualquier otro método aprobado por el Consorci AOC al efecto.

¹⁰⁶ Ley 59/2003: Art. 20.1 d); TS 101 456: 7.4.7; TS 102 042: 7.4.7

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

Las claves de Entidades de Certificación deben ser comunicadas a los verificadores, asegurando la integridad de la clave y autenticando el origen.¹⁰⁷

La clave pública de la entidad de certificación raíz (*root CA*) de la jerarquía de certificación del Consorci AOC se publicará en el directorio de dicha Entidad de Certificación, en forma de certificado auto firmado, junto a una declaración referente a que la clave permite autenticar a la Entidad de Certificación.

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

Las claves públicas de las Entidades de Certificación Vinculadas se publicarán en el web del Consorci AOC, en forma de certificado CIC firmado por la entidad de certificación superior en la jerarquía de certificación del Consorci AOC. También se publican, con el mismo formato, en el directorio de cada Entidad de Certificación.

Adicionalmente, en aplicaciones S/MIME, el mensaje de datos podrá contener una cadena de certificados, incluyendo certificados CIC con las claves públicas de las Entidades de Certificación de la jerarquía, que de esta forma son distribuidas a los usuarios.

6.1.5 Medidas de claves

El Consorci AOC gestiona de manera diligente la jerarquía pública de certificación, esforzándose por mantenerla conforme a las novedades que se introduzcan en las especificaciones técnicas aplicables.

Concretamente, en relación a las medidas de las claves de las Entidades de Certificación Vinculadas: serán al menos de 2.048 bits.

Las claves de todos los certificados emitidos por les Entidades de Certificación Vinculadas 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 realizará de acuerdo con el informe especial del ETSI TS 001 276, que indica la calidad de los algoritmos de firma electrónica.

¹⁰⁷ TS 101 456: 7.2.3 a); TS 102 042: 7.2.3 a)

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

Los pares de claves de las Entidades de Certificación (tanto del Consorci AOC como de las Entidades de Certificación Vinculadas) tendrán que estar generados utilizando hardware criptográfico que cumpla los requisitos establecidos en un perfil de protección de dispositivo seguro de creación de firma electrónica de autoridad de certificación normalizado, 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 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 seguro de creación de firma electrónica de entidad final normalizado, de acuerdo con Common Criteria EAL 4+ o FIPS 140-2 Nivel 3 o superior nivel de seguridad.

La generación de claves para el resto de certificados podrá realizarse mediante aplicaciones informáticas.

6.1.9 Propósitos de uso de claves

La Entidad de Certificación tendrá que incluir 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 módulos criptográficos¹⁰⁸

Las claves privadas de las Entidades de Certificación (tanto del Consorci AOC como de las Entidades de Certificación Vinculadas) tendrán que protegerse utilizando hardware criptográfico que cumpla los requisitos establecidos en un perfil de protección de dispositivo seguro de creación de firma electrónica de autoridad de certificación normalizado, 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 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 seguro de creación de firma electrónica de entidad final normalizado, de acuerdo con Common Criteria EAL 4+ o FIPS 140-2 Nivel 3 o superior nivel de seguridad.

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

¹⁰⁸ TS 101 456: 7.2.2

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

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

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

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

El acceso a las claves privadas de las Entidades de Certificación off-line, tendrá que requerir necesariamente del concurso simultaneo de tres (3) dispositivos criptográficos protegidos por una clave de acceso, de entre cinco (5) dispositivos. El resto de Entidades de Certificación Vinculadas requerirá del concurso de dos (2) dispositivos criptográficos de cinco (5) posibles.

Cada uno de estos dispositivos es responsabilidad de una persona concreta, única conocedora de la clave de activación del mismo. La clave de activación será conocida únicamente por la persona responsable de este dispositivo; ninguna de ellas conocerá más que 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. Dichos sobres solo 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 quedarán almacenados en las dependencias de la Entidad de Certificación Vinculada.

6.2.3 Depósito de la clave privada

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

Las claves privadas de los certificados de firma, personales (individuales y corporativos) y de entidad, no se podrán almacenar en la Entidad de Certificación; sí, en cambio, se pueden almacenar las claves privadas de certificados de cifrado.

6.2.4 Backup de la clave privada

Tendrá que existir backup, en dependencia independiente de aquella donde se almacena habitualmente, de la clave privada de la Entidad de Certificación Vinculada, así como de los medios necesarios para acceder a ella..

6.2.5 Archivo de la clave privada¹⁰⁹

La clave privada de la Entidad de Certificación tendrá que contar con una copia de soporte 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, y tiene que limitarse a aquel que necesite hacerlo en las prácticas de la Entidad de Certificación.

Tendrá que mantenerse y utilizarse protegidas por un dispositivo criptográfico que cumpla los requisitos establecidos en un perfil de protección de dispositivo seguro de creación de firma electrónica de autoridad de certificación normalizado, 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 este tipo de dispositivos, tendrá que hacerlo de forma cifrada.

Los controles de seguridad a aplicar a las copias de soporte de la Entidad de Certificación tendrán que ser de igual o superior nivel a las que se apliquen a la claves habitualmente en uso.

Cuando las claves se almacenen en un módulo hardware 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 de cifrado de datos, en que según, disponga la DPC de la Entidad 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 las Entidades de Certificación quedarán almacenadas en ficheros cifrados con claves fragmentadas y en tarjetas inteligentes (de las que no podrán ser extraídas).

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

6.2.7 Almacenaje de la clave privada en el módulo criptográfico

Las claves privadas se generarán directamente en los módulos criptográficos.

6.2.8 Método de activación de la clave privada

Para certificados CIC, se requerirán al menos dos personas para activar la clave privada.

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

¹⁰⁹ TS 101 456: 7.2.2

6.2.9 Método de desactivación de la clave privada

Para certificados personales y de entidad que incluyan la política básica de firma reconocida, 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 indicados.

Para certificados personales y de entidad 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 serán destruidas en una forma que impida su robo, modificación, divulgación no autorizada o uso no autorizado.

6.2.11 Clasificación de los módulos criptográficos

Los módulos de las Entidades de Certificación Vinculada deben hallarse certificados con el nivel y aumentos previstos en un perfil de protección de dispositivo seguro de creación de firma electrónica de autoridad de certificación normalizado, de acuerdo con Common Criteria EAL 4+, o FIPS 140-2 Nivel 3.

Los módulos de los suscriptores de certificados de firma electrónica reconocida y de certificados de nivel alto deben hallarse certificados con el nivel y aumentos previstos en un perfil de protección de dispositivo seguro de creación de firma electrónica de entidad final normalizado, de acuerdo con Common Criteria EAL 4+, o FIPS 140-2 nivel 3.

6.3 Otros aspectos de gestión del par de claves

6.3.1 Archivo de la clave pública

La Entidad de Certificación archivará sus claves públicas, de acuerdo con lo establecido en la sección correspondiente de esta política.

6.3.2 Periodos de utilización de las claves pública y privada¹¹⁰

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

Como excepción, la clave privada de descifrado podrá continuar utilizándose más allá de la expiración del certificado.

¹¹⁰ TS 101 456: 7.2.6; TS 102 042: 7.2.6

6.4 Datos de activación

6.4.1 Generación e instalación de los datos de activación

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

6.4.2 Protección de datos de activación

Si la Entidad de Certificación facilita al suscriptor un dispositivo seguro de creación de firma, los datos de activación del dispositivo deberán ser distribuidos separadamente del dispositivo de creación de firma (por ejemplo, entregándose en momentos diferentes, o por rutas o canales diferentes).

Como excepción, cuando el poseedor de claves reciba presencialmente un dispositivo, de una Entidad de Registro, podrá seleccionar e introducir los datos de activación, de forma que los conozca únicamente él.

6.4.3 Otros aspectos de los datos de activación

Sin estipulación

6.5 Controles de seguridad informática

6.5.1 Requisitos técnicos específicos de seguridad informática¹¹¹

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

- La Entidad de Certificación tiene que garantizar 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 Entidad de Certificación tiene que garantizar que el acceso a los sistemas de información y aplicaciones se restringe de acuerdo a lo establecido en la política de control de acceso, así como que los sistemas proporcionan los controles de seguridad suficientes para implementar la segregación de funciones identificada en las prácticas de la Entidad, 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 estará restringido y estrechamente controlado.
- El personal de la Entidad tendrá que estar identificado y reconocido antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del certificado.

¹¹¹ TS 101 456: 7.4.6; TS 101 456: 7.4.6

- El personal de la Entidad será responsable y tendrá que poder justificar sus actividades, por ejemplo mediante un archivo de acontecimientos.
- Tendrá que evitarse la posibilidad de revelación de datos sensibles mediante la reutilización de objetos de almacenaje (por ejemplo ficheros borrados) que queden accesibles a usuarios no autorizados.
- Los sistemas de seguridad y monitorización tienen que permitir una rápida detección, registro y actuación ante intentos irregulares de acceso o no autorizados a sus recursos (por ejemplo, mediante un sistema de detección de intrusiones, monitorización y alarma).
- El acceso a los depósitos públicos de la información de la Entidad (por ejemplo, certificados o información de estado de revocación) tendrá que contar con un control de accesos para modificaciones o borrado de datos.

6.5.2 Evaluación del nivel de seguridad informática

Las aplicaciones de CA y RA tendrán que ser fiables, de acuerdo con la especificación técnica CEN CWA 14167-1.

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Se tendrá que realizar un análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente utilizada en las aplicaciones de Autoridad (técnica) de certificación y de Autoridad (técnica) de Registro, para garantizar que los sistemas son seguros.¹¹²

Se utilizarán procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.¹¹³

6.6.2 Controles de gestión de seguridad

La Entidad 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.¹¹⁴

La configuración de los sistemas se auditará de forma periódica, de acuerdo con lo establecido en la sección correspondiente de esta política.¹¹⁵

¹¹² TS 101 456: 7.4.7 a)

¹¹³ TS 101 456: 7.4.7 b)

¹¹⁴ TS 101 456: 7.4.2 a)

¹¹⁵ TS 101 456: 7.4.6 h)

Se realizará un seguimiento de las necesidades de capacidad, y se planificarán procedimientos para garantizar suficiente disponibilidad electrónica y de almacenaje para los activos informativos.¹¹⁶

6.6.3 Evaluación del nivel de seguridad del ciclo de vida

Sin estipulación.

6.7 Controles de seguridad de red¹¹⁷

Se tendrá que garantizar que el acceso a las diferentes redes de la Entidad de Certificación está limitado a individuos debidamente autorizados. En particular:

- Tienen que implementarse controles (como por ejemplo cortafuegos) para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos tendrán que configurarse de forma que se impidan accesos y protocolos que no sean necesarios para la operación de la Entidad de Certificación.
- Los datos sensibles tendrán que protegerse cuando se intercambien a través de redes no seguras (incluyendo los datos de registro del suscriptor).
- Se tiene que garantizar que los componentes locales de red (como direccionadores) se encuentren ubicados en entornos seguros, así como la auditoría periódica de sus configuraciones.

6.8 Sello de tiempo

Sin estipulación adicional.

¹¹⁶ TS 101 456: 7.4.5 f)

¹¹⁷ TS 101 456: 7.4.6

7. Perfiles de certificados y listas de certificados revocados

7.1 Perfil de certificado

Los certificados emitidos por el Consorci AOC y las Entidades 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 política.
- c. El nombre distinguido del emisor, de acuerdo con la sección correspondiente de esta política.
- d. Inicio de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 5280.
- e. Fin de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 5280.
- f. Nombre distinguido del sujeto, de acuerdo con la sección correspondiente de esta política.
- g. Clave pública del sujeto, codificada de acuerdo con RFC 5280
- h. Firma, generada y codificada de acuerdo con RFC 5280

Los certificados serán conformes con las siguientes normas:

1. RFC 5280: 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

Adicionalmente, los certificados CPSR y de entidad serán conformes con las siguientes normas:

1. ETSI TS 101 862 v1.2.1 (2001-06): Qualified Certificate Profile, 2001
2. RFC 3039: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, 2001 (siempre que no entre en conflicto con TS 101 862)

Asimismo, los certificados reconocidos tendrán que contener los siguientes campos.¹¹⁸

- a. La indicación que se expiden como certificados reconocidos
- b. El código identificativo único del certificado

¹¹⁸ Ley 59/2003: Art. 11.2

- 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 o de entidad), por su nombre y apellidos y DNI o equivalente, o a través de un seudónimo 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. El comienzo y el final del periodo de validez del certificado.
- h. Los límites de uso del certificado, si se prevén.
- i. Los límites del valor de las transacciones para las que 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 encuentra descrito en el documento “perfil de certificado” correspondiente, que el Consorci AOC publica en su web.

7.1.3 Identificadores de objeto de algoritmos

La Entidad de Certificación podrá utilizar los siguientes algoritmos de firma:

- sha-1WithRSAEncryption OID = {iso (1) member-body (2) us (840) rsadsi (113549) pkcs (1) pkcs-1 (1) 5}
- sha256WithRSAEncryption OID = {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

7.1.4 Formatos de nombres

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

7.1.5 Restricciones de nombres

Sin estipulación.

7.1.6 Identificador de objeto de política de certificado

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

En caso de crear su propia política, en los casos permitidos por esta política de certificados, incluirá el identificador de 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 calificadores de política¹¹⁹

La Entidad de Certificación incluirá en los certificados un calificador de política, con los siguientes elementos:

- CPS Pointer
- explicit Text

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

explicit Text tendrá que contener una declaración concisa relativa al certificado¹²⁰.

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 Entidades de Certificación

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

Adicionalmente, la renovación de las Entidades de Certificación inmediatamente posterior a la presente versión de la Política General respetará las siguientes especificaciones técnicas:

- El algoritmo utilizado ha de ser renovado cuando exista un riesgo de descryptación advertido por la comunidad. Las Entidades de Certificación incorporarán, posteriormente a la emisión de esta Política General, 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 entidades de certificación intermedias.

¹¹⁹ RFC 2459: 4.2.1.5

¹²⁰ Véase sección correspondiente 5

8. Auditoría de conformidad

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

Además de la auditoría de conformidad, la Entidad de Certificación Vinculada tiene que estar preparada para pasar otras revisiones, no periódicas, que demuestren su confianza:

- Antes de aceptar una nueva Entidad de Certificación subordinada a la jerarquía, el Consorci AOC tiene que realizar una revisión de sus documentos de seguridad y DPC y PdC para asegurar que cumple los requisitos de seguridad y de operación necesarios para formar parte de la Jerarquía de Entidades de Certificación d.
- Si en cualquier momento se sospecha que la Entidad de Certificación Vinculada, 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 Entidad de Certificación Vinculada, se llevará a término una auditoría interna.

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

8.1 Frecuencia de la auditoría de conformidad

La Entidad de Certificación Vinculada tiene que llevar a término una auditoría de conformidad anualmente, además de las auditorías internas que pueda llevar a término bajo su propio criterio o en cualquier momento, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de claves.

8.2 Identificación y calificación del auditor

Si la Entidad de Certificación Vinculada dispone de un departamento de auditoría interna, éste podrá encargarse de llevar a término la auditoría de conformidad.

En el caso de no poseer este departamento, la Entidad de Certificación Vinculada podrá acudir a un auditor independiente externo, el cual tiene que demostrar experiencia en seguridad informática, en seguridad de Sistemas de Información y en auditorías de conformidad de Autoridades de Certificación y los elementos relacionados.

8.3 Relación del auditor con la entidad auditada

Las auditorías de conformidad ejecutadas por terceros tienen que ser llevadas a cabo por una entidad independiente de la Entidad de Certificación Vinculada auditada. En caso de auditoría interna, el auditor no debe tener ningún conflicto de intereses que afecte negativamente a su capacidad de llevar a cabo servicios de auditoría.

8.4 Relación de elementos objeto de auditoría

Los elementos objeto de auditoría serán los siguientes:

- Procesos 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 se obtiene el informe de la auditoría de cumplimiento llevada a término, la Entidad de Certificación Vinculada tiene que discutir, con la entidad que ha ejecutado la auditoría y con el Consorci AOC, las deficiencias encontrada y desarrollar y ejecutar un plan correctivo que solucione dichas deficiencias.

Si la Entidad de Certificación Vinculada auditada es incapaz de desarrollar y/o ejecutar dicho plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema tendrá que realizarse una de las siguientes acciones:

- Revocar la clave de la Entidad de Certificación Vinculada, de la forma como se describe en las secciones correspondientes de esta política.
- Acabar el servicio de la Entidad de Certificación Vinculada, de la forma como se describe en la sección correspondiente de esta política.

8.6 Tratamiento de los informes de auditoría

Los informes de resultados de las auditorías serán entregados al Consorci AOC, en un plazo máximo de 15 días tras la ejecución de la auditoría, en tanto que es el Prestador de Servicios de Certificación.

9. Requisitos comerciales y legales

9.1 Tarifas

9.1.1 Tarifa de emisión o renovación de certificados

El Consorci AOC establecerá las tarifas que aplicarán todas las Entidades de Certificación Vinculadas, a la prestación de sus servicios.

Estas tarifas pueden encontrarse en la web del Consorci AOC.

9.1.2 Tarifa de acceso a certificados

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

9.1.3 Tarifa de acceso a información de estado de certificado

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

9.1.4 Tarifas de 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, como prestador de servicios de certificación, dispone de una garantía suficiente de cobertura de su responsabilidad civil, en los términos previstos en el artículo 20.2 de la Ley 59/2003, de 19 de diciembre, excepto cuando se encuentre eximida por Ley de esta obligación.

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

9.2.2 Otros activos

Sin estipulación adicional.

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

Sin estipulación adicional.

9.3 Confidencialidad

9.3.1 Informaciones confidenciales

Las siguientes informaciones serán mantenidas confidenciales por la Entidad de Certificación:

- a. Información de negocio suministrada por sus proveedores y otras personas con las que el Consorci AOC o la Entidad de Certificación Vinculada tenga una obligación de guardar secreto, establecida legal 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 Entidad de Certificación Vinculada y sus auditores.
- d. Planes de continuidad de negocio y de emergencia.
- e. Política y planes de seguridad
- f. Documentación de operaciones y restantes planes de operación, como ahora archivo, monitorización y otros de análogos.
- g. Toda otra información identificada como "Confidencial".

9.3.2 Informaciones no confidenciales

Las siguientes informaciones no tendrán carácter confidencial:

- a. Las Declaraciones de Prácticas de Certificación de todas las Entidades de Certificación
- b. Toda otra información identificada como "Pública"

9.3.3 Responsabilidad para la protección de información confidencial

La Entidad de Certificación Vinculada será responsable del establecimiento de las medidas apropiadas de protección de la información confidencial.

Estas medidas incluirán las apropiadas cláusulas de información confidenciales en los instrumentos jurídicos con todas las personas.

9.4 Protección de datos personales

9.4.1. Política de Protección de Datos Personales

El Consorci AOC desarrolla una política de protección de datos personales, de acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y la normativa reglamentaria de aplicación en materia de protección de datos de carácter personal.

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

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

SUSCRIPTORES DE CERTIFICADOS:

- Datos identificativos del colectivo suscriptor: nombre de la entidad o del organismo que solicita los certificados, CIF, 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 cuya inclusión sea solicitada para la persona autorizada, como el código CIP de la Tarjeta Individual Sanitaria, así como el código identificativo o usuario en el caso de certificados con seudónimo
- 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 (sólo en caso de certificados de clase 1 y clase 2 de colectivo).
- Denominación de la entidad CIF, área de adscripción política, orgánica, laboral o profesional.

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

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

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

- a. Ámbito de aplicación del documento de seguridad con especificación detallada de los recursos protegidos (artículo 88 del RD 1720/2007) – sección 6.1.
- b. Medidas, normas, procedimientos, regla y estándares que garantizan el nivel e seguridad exigido por el RD 1720/2007 –sección 6.1 y, en general, todos los controles técnicos de las secciones 5 y 6 de la Política General de Certificación.
- c. Funciones y obligaciones del personal (artículo 89 del RD 1720/2007) – sección 5.3.
- d. Registro de incidencias (artículo 90 del RD 1720/2007), procedimiento de notificación, gestión y respuesta ante las incidencias - sección 9.4.5.
- e. Control de acceso (artículo 91 del RD 1720/2007) – secciones 5 i 6.
- f. Gestión de soportes (artículo 92 del RD 1720/2007) – sección 5.
- g. Identificación i autenticación (artículo 93 del RD 1720/2007) – sección 5.2.
- h. Procedimientos de copia de seguridad i recuperación de datos (artículo 94 del RD 1720/2007) - sección 5.5.

9.4.2.Datos de carácter personal no disponibles a terceros

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

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

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

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

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

9.4.3. Datos de carácter personal disponibles a terceros

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

Esta información, proporcionada en la solicitud de certificados en los términos previstos en el artículo 17.2 de la Ley 59/2003, de la Ley 59/2003, de 19 de diciembre, de firma electrónica, se incluye en sus certificados y en el mecanismo de comprobación del estado de los certificados.

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

En todo caso, se considera no confidencial la siguiente información:

- a. Los certificados emitidos o en trámite de emisión.
- b. La sujeción de suscriptor a un certificado emitido por la Entidad de Certificación.
- c. El nombre y los apellidos del suscriptor del certificado, así como cualquier otra circunstancia o dato personal del titular en el supuesto de que sean significativos 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 de 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 (LCRs), así como la resta de informaciones de estado de revocación.
- j. La información contenida en la parte pública del Registro de la Entidad de Certificación.

9.4.4. Responsabilidad correspondiente a la protección de datos personales

El Consorci AOC, como mínimo, garantiza el cumplimiento de sus obligaciones legales como prestador de servicios de certificación, de conformidad con la Ley 59/2003, de 19 de diciembre, y en virtud de esto, y de acuerdo con el artículo 22 de la citada Ley, responde por los daños y perjuicios que cause en el ejercicio de la actividad que le es propia, en el caso de incumplir, en lo que aquí interesa, las obligaciones contenidas en el artículo 17 de la Ley 59/2003, relativas a 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 comunicación, gestión y respuesta ante las incidencias relacionadas con los datos personales.

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

Si durante la gestión de la incidencia es necesario hacer modificaciones en el programario 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 del Área Técnica o el responsable técnico del proyecto afectado (en este caso, con copia del mensaje al Responsable del Área Técnica).

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 del Área Técnica 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 del Área Técnica mantiene copia de los formularios correspondientes a las incidencias registradas durante los 12 últimos meses sobre los ficheros que contienen datos de carácter personal. Estos se guardan en un directorio dedicado dentro del servidor que comparten los usuarios de la Entidad de Certificación, protegido convenientemente para que sólo pueda acceder el personal del Área Técnica; 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 certificados de clase 1, 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, como prevé el artículo 6 LOPD.

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

9.4.7. Comunicación de datos personales

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

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

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

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

9.5 Derechos de propiedad intelectual

9.5.1 Propiedad de los certificados e información de revocación

La Entidad de Certificación Vinculada será la única entidad que disfrutará de los derechos de propiedad intelectual sobre los certificados que emita.

La Entidad de Certificación Vinculada tendrá que conceder licencia no exclusiva para reproducir, distribuir, verificar y utilizar los certificados, sin ningún coste, en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de aplicación de esta política, de acuerdo con el correspondiente instrumento vinculante entre la Entidad de Certificación Vinculada y la parte que reproduzca y/o distribuya el certificado.

Las anteriores normas figurarán en los instrumentos jurídicos que existan entre la Entidad de Certificación Vinculada y los suscriptores y los verificadores.

Adicionalmente, los certificados emitidos por la Entidad de Certificación Vinculada tienen que contener un aviso legal relativo a la propiedad de éstos.

Esta normativa resultará de aplicación en el uso de información de revocación de certificados.

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

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

Cada Entidad de Certificación Vinculada será propietaria de su Declaración de Prácticas de Certificación.

9.5.3 Propiedad de la información relativa a nombres

El suscriptor y, en su caso, el poseedor de claves, conservará cualquier derecho, de existir este, relativo a la marca, producto o nombre comercial contenido en el certificado.

El suscriptor, o en su caso, el poseedor de claves, será el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección correspondiente de esta política.

9.5.4 Propiedad de claves

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

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

9.6 Obligaciones y responsabilidad civil

9.6.1 Entidades de Certificación

9.6.1.1 Obligaciones y otros compromisos

Obligaciones del Consorci AOC

El Consorci AOC tiene las siguientes obligaciones

- a. Operar la Entidad de Certificación Raíz diligentemente, de acuerdo con las políticas, prácticas y normativa de la jerarquía pública de certificación de Cataluña.
- b. Operar sus Entidades de Certificación Vinculadas, propias o que den servicios a las Entidades de Certificación Virtuales, de acuerdo con aquello dispuesto por el apartado 9.6.1.1.2.
- c. Garantizar la equivalencia de la seguridad de la operación de las Entidades de Certificación Vinculadas de terceros prestadores de servicios de certificación, y especialmente, velar porque estas cumplan las obligaciones previstas por el apartado 9.6.1.1.2.

Obligaciones de las Entidades de Certificación Vinculadas

Las Entidades de Certificación Vinculadas se obligarán a cumplir lo siguiente:

- a. La Entidad de Certificación Vinculada tiene que garantizar bajo su plena responsabilidad, que cumple con todos los requisitos establecidos en esta política de certificación.¹²¹.
- b. La Entidad de Certificación Vinculada será la única entidad responsable del cumplimiento de los procedimientos descritos en esta política, incluido cuando una parte o la totalidad de las operaciones sean subcontratadas externamente.¹²².
- c. La Entidad de Certificación Vinculada tiene que prestar sus servicios de certificación de acuerdo con su Declaración de Prácticas de Certificación vigente.¹²³, en la que se detallarán al menos los contenidos previstos en el artículo 19 de la Ley 59/2003.
- d. Antes de la emisión y entrega del certificado al suscriptor, la Entidad de Certificación Vinculada tendrá que informarlo de los aspectos previstos en el artículo 18.b) de la Ley 59/2003.¹²⁴, y de los siguientes aspectos:
 - a) Indicación de la política aplicable, con indicación de si los certificados se expiden al público y de la necesidad de utilización de dispositivo seguro de creación de firma.¹²⁵
 - b) Forma en que se garantiza la responsabilidad patrimonial de la Entidad de Certificación.¹²⁶
 - c) Si la Entidad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema. En concreto, la certificación del prestador de servicios de certificación.¹²⁷ y la certificación de los productos de firma electrónica utilizados.¹²⁸.
- e. Este requisito se cumplirá mediante un “Texto divulgativo de la política de certificado” aplicable, que podrá ser transmitida electrónicamente, utilizando un medio de comunicación que dure en el tiempo, y lenguaje comprensible.¹²⁹.
- f. La Entidad de Certificación Vinculada tiene que obligar a los suscriptores, a los poseedores de claves y a los verificadores mediante instrumentos jurídicos apropiados en cada situación.
- g. Estos instrumentos jurídicos podrán ser transmitidos electrónicamente, tendrán que estar en lenguaje escrito y comprensible, y deben de tener los siguientes contenidos mínimos.¹³⁰:

¹²¹ TS 101456: 6.1 primero; TS 102042: 6.1 primero

¹²² TS 101456: 6.1 segundo; TS 102042: 6.1 segundo

¹²³ TS 101456: 6.1 cuarto; TS 102042: 6.1 tercero

¹²⁴ TS 101456: 7.3.1 a) y b); TS 102042: 7.3.1 a) y c)

¹²⁵ TS 101456: 7.3.4

¹²⁶ Ley 59/2003: Art. 26

¹²⁷ Ley 59/2003: Art. 26

¹²⁸ Ley 59/2003: Art. 27

¹²⁹; TS 101456: 7.3.1 a) y b); TS 102042: 7.3.1 a) y c)

¹³⁰ TS 101456: 7.3.4; TS 102 042: 7.3.4

- a) Prescripciones para dar cumplimiento a lo establecido en la presente política de certificación.
 - b) Indicación de la política aplicable, con indicación de si los certificados se expiden al público y de la necesidad de uso del dispositivo seguro de creación de firma.
 - c) Manifestación que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.¹³¹.
 - d) Consentimiento para la publicación del certificado en el directorio y acceso por terceros al mismo.¹³².
 - e) Consentimiento para el almacenaje de la información utilizada para el registro del suscriptor y del poseedor de claves, para la provisión del dispositivo seguro de creación de firma y para la cesión de dicha información a terceros, en caso de finalización de operaciones de la Entidad de Certificación Vinculada.¹³³ sin revocación de certificados válidos.
 - f) Límites de uso del certificado, incluyendo las establecidas en la sección 4.5 de esta política.
 - g) Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las que se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como verificador.
 - h) Limitaciones de responsabilidad aplicables, incluyendo los usos por los que la Entidad de Certificación Vinculada acepta o excluye su responsabilidad.
 - i) Procedimientos aplicables de resolución de disputas.
 - j) Ley aplicable y jurisdicción competente.
- h. La Entidad de Certificación Vinculada tiene que identificar al suscriptor del certificado, de acuerdo con los artículos 12 y 13 de la Ley 59/2003 y la presente política de certificado y, en concreto:
- a) La Entidad de Certificación Vinculada tiene que comprobar por si misma o por medio de una Entidad de Registro, la identidad y cualquier otra circunstancia personal de los solicitantes de los certificados, de acuerdo con lo establecido en el artículo 13 de la Ley 59/2003.
 - b) En caso que el suscriptor del certificado de persona física (certificado de clase 1 o certificado de clase 2 de colectivo) sea una persona jurídica, la Entidad de Certificación Vinculada tiene que comprobar que el poseedor de la clave se encuentra debidamente autorizado por el suscriptor.
- i. La Entidad de Certificación Vinculada tiene que cumplir el resto de obligaciones contenidas en el artículo 12 de la Ley 59/2003.

Requisitos específicos para los certificados personales y de entidad.

¹³¹ TS 101456: 7.3.1 h) quinto; TS 102 042: 7.3.1 l) quinto

¹³² TS 101456: 7.3.1 h) cuarto; TS 102042: 7.3.1 l) cuarto

¹³³ TS 101456: 7.3.1 h) tercero; TS 102042: 7.3.1 l) tercero

La Entidad de Certificación tiene que asumir otras obligaciones incorporadas directamente en el certificado o incorporadas por referencia.¹³⁴

Nota: La incorporación por referencia se consigue incluyendo en el certificado un identificador de objeto u otra forma de enlace a un documento, que se considera incluido de forma íntegra en la presente política de certificado.

Adicionalmente a lo establecido en la sección correspondiente, el instrumento jurídico que vincula la Entidad de Certificación Vinculada y el suscriptor tendrá que estar en lenguaje escrito y comprensible, y debe de tener los siguientes contenidos mínimos:

- a. Indicación de la política aplicable, con indicación si los certificados se expiden al público o a una comunidad cerrada de usuarios y de la necesidad de uso de dispositivo seguro de creación de firma.¹³⁵
- b. Certificación de servicios de la Entidad de Certificación Vinculada.¹³⁶
- c. Forma en que se garantiza la responsabilidad patrimonial de la Entidad de Certificación Vinculada.¹³⁷

Requisitos específicos para el CDS, CDSCD y CDS-1 de Sede electrónica

La Entidad de Certificación tiene que comprobar el nombre de dominio, y otros datos técnicos, como la IP, que tengan que figurar en el certificado.

Obligaciones de la Entidad de Certificación Virtual

Las Entidades de Certificación Virtual se obligarán a cumplir lo siguiente:

- a. Determinar la comunidad de suscriptores y verificadores de la Entidad de Certificación Vinculada.
- b. Aprobar las políticas de certificación y, si es necesario, las políticas específicas de certificación.
- c. Aprobar, si es necesario, la Declaración de Prácticas de Certificación.
- d. Aprobar la documentación contractual y reguladora de los servicios de certificación en la comunidad de usuarios de la Entidad de Certificación Vinculada.
- e. Notificar puntualmente a la Entidad de Certificación Vinculada de todas las informaciones relativas a los cambios a realizar, incidencias en los servicios, reclamaciones, denuncias e inspecciones del servicio.

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

9.6.1.2 Garantías ofrecidas a suscriptores y verificadores

La Entidad de Certificación Vinculada, como mínimo, garantizará al suscriptor:

¹³⁴ TS 101 456: 6.1 tercero

¹³⁵ TS 101 456: 7.3.4

¹³⁶ Ley 59/2003: Art. 26

¹³⁷ Ley 59/2003: Art. 20.2

- a. El cumplimiento de sus obligaciones legales como prestador de servicios de certificación, de acuerdo con la Ley 59/2003, de 19 de diciembre.
- b. Que no haya errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Entidad de Certificación Vinculada y, en su caso, por la Entidad de Registro.
- c. Que no haya errores de hecho en las informaciones contenidas en los certificados, debidos a falta de diligencia en la gestión de la solicitud de certificado o a la creación de éste.
- d. Que los certificados cumplan todos los requisitos materiales establecidos en la DPC.
- e. Que los servicios de revocación y el uso del directorio cumplan todos los requisitos materiales establecidos en la DPC.

La Entidad de Certificación Vinculada, como mínimo, garantizará al verificador:

- a. El cumplimiento de sus obligaciones legales como prestador de servicios de certificación, de acuerdo con la Ley 59/2003, de 19 de diciembre.
- b. Que la información contenido o incorporada por referencia al certificado es correcta, excepto cuando se indique lo contrario.
- c. En caso de certificados publicados en el directorio, que el certificado ha sido emitido al suscriptor identificado en éste y que el certificado ha sido aceptado, de acuerdo con la sección correspondiente de la presente política de certificación.
- 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 la DPC.
- e. La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación

Adicionalmente, la Entidad de Certificación garantizará al suscriptor y al verificador:

- a. Que el certificado contiene las informaciones que tiene que contener un certificado reconocido, de acuerdo con el artículo 11.2 de la Ley 59/2003, de 19 de diciembre.
- b. Que, en el caso que genere las claves privadas del suscriptor o, en su caso, el poseedor de claves, se mantiene su confidencialidad durante el proceso¹³⁸.
- c. La responsabilidad de la Entidad de Certificación, con los límites que se establezcan.

9.6.2 Entidades de Registro

9.6.2.1 Obligaciones y otros compromisos

Obligaciones de las Entidades de Registro Internas

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

¹³⁸ Ley 59/2003: Art. 20.1.e)

- a. Actuar exclusivamente en relación con personas vinculadas a la Entidad de Registro Interna.
- b. Nombrar como operadores de la autoridad (técnica) de registro, a dos o más de sus trabajadores (dependiendo de la EC, generalmente cuatro o más), y comunicar a el 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 Entidad de Registro Interna, esta Entidad de Registro Interna tiene que solicitar de forma inmediata a la Entidad de Certificación Vinculada la revocación del certificado de operador correspondiente.
- c. 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 Entidad de Certificación Vinculada, de acuerdo con la DPC y la documentación de operaciones de la Entidad de Certificación Vinculada.
- d. Si la Entidad de Registro Interna no dispusiera de información actualizada del poseedor de claves, comprobar la identidad personalmente o de acuerdo con lo establecido en el artículo 13.4 de la Ley 59/2003, 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 una persona respecto otra en el ámbito de la Entidad de Registro Interna.
- e. Verificar, cuando sea necesario, cualquier atributo específico del poseedor de claves, y registrar un justificante acreditativo de la información.
- f. Realizar o tramitar las solicitudes de suspensión, habilitación, revocación y renovación de certificados, de acuerdo con los procedimientos y los instrumentos técnicos establecidos para la Entidad de Certificación Vinculada, de acuerdo con la Declaración de Prácticas de Certificación, y la documentación de operaciones de la Entidad de Certificación Vinculada.
- g. Almacenar los registros, ya sean en papel, ya sean 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 Entidad de Certificación Vinculada.
- h. 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.

Entidad de Registro Virtual

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

Entidad de Registro Colaboradora

La Entidad de Certificación podrá delegar algunas funciones a Entidades de Registro Colaboradoras,¹³⁹ que en este caso quedarán obligadas a su cumplimiento, en las mismas condiciones que la Entidad de Certificación.

La Entidad de Registro Colaboradora asistirá a los suscriptores de certificados de clase 1 con Entidad de Registro Virtual, y a todos los suscriptores de certificados de clase 2.

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

La Entidad 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 que realizará 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 Entidad de Registro Colaboradora lo considerase necesario, cualquier otro documento e información relevante, facilitados por el suscriptor, por el poseedor de claves o por terceras personas.

Si la Entidad de Registro Colaboradora detectase errores en los datos que tienen que ser incluidos en los certificados, o en los documentos que justificasen 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 caso que la Entidad 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 Entidad 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

Garantía del Consorci AOC por los servicios de certificación digital

El Consorci AOC garantiza que la clave privada de la entidad de certificación utilizada para emitir certificados no ha sido comprometida, a excepción de que el Consorci AOC no hubiere comunicado lo contrario mediante el registro de certificación del Consorci AOC, de conformidad con la Declaración de prácticas de certificación.

El Consorci AOC únicamente garantiza que:

a) Los certificados de firma electrónica contienen toda la información exigida por la Ley 59/2003, de 19 de diciembre.

¹³⁹ Art 13.5. Ley 59/2003

- 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 entidad de registro colaboradora, en el momento de la emisión del certificado.
- c) Todos los certificados cumplen los requisitos formales y de contenido de su Declaración de prácticas de certificación.
- d) Queda vinculada por los procedimientos operativos, de seguridad y de archivo descritos en la Declaración de prácticas de certificación.

Exclusión de la garantía

El Consorci AOC no garantiza software alguna utilizado por el suscriptor o por cualquier otra persona, para generar, verificar o no utilizar de forma distinta firma digital alguna 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

Requisitos para todos los tipos de certificados

La Entidad de Certificación Vinculada obligará¹⁴⁰ al suscriptor a:

- a. Facilitar a la Entidad de Certificación Vinculada información completa y adecuada, conforme a los requerimientos de esta política de certificación, en especial por lo que respecta al procedimiento de registro.¹⁴¹
- b. Manifestar su consentimiento previo a la emisión y entra de un certificado.
- c. Cumplir las obligaciones que se establecen para el suscriptor en la presente política de certificación y en el artículo 23.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.
- d. Utilizar el certificado de acuerdo con lo establecido en la sección correspondiente.
- e. Notificar a la Entidad de Certificación Vinculada, sin retrasos injustificables, la pérdida, la alteración, el uso no autorizado, el robo o el compromiso de su dispositivo seguro de creación de firma.
- f. Notificar a la Entidad de Certificación Vinculada y cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:¹⁴²
 - a) La pérdida, el robo o el compromiso potencial de su clave privada.

¹⁴⁰ No se establece ningún requisito sobre la manera en la que se tendría que cumplir este requisito: podrá ser mediante contrato o mediante otro instrumento jurídico.

¹⁴¹ TS 101 456: 6.2.a) se considera una obligación que tiene que ser genérica para todos los tipos de certificados solicitados por suscriptores.

¹⁴² TS 101 456: 6.2.g)

- b) La pérdida de control sobre su clave privada, a causa del compromiso de los datos de activación (por ejemplo, el código PIN del dispositivo seguro 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 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, sin permiso previo por escrito.
- j. No comprometer intencionadamente la seguridad de la jerarquía pública de certificación de Cataluña.

Requisitos específicos para los certificados de firma electrónica reconocida

La Entidad de Certificación Vinculada obligará al suscriptor a:

- a. Utilizar el par de claves exclusivamente para firmas electrónicas y conforme a cualquier otra limitación que le sea notificada.¹⁴³
- b. Reconocer que estas firmas electrónicas son firmas electrónicas equivalentes a firmas manuscritas, de acuerdo con el artículo 3.4 de la Ley 59/2003, de 19 de diciembre.
- c. Ser especialmente diligente en la custodia de su clave privada y de su dispositivo seguro de creación de firma, con el fin de evitar usos no autorizados¹⁴⁴.
- d. 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.¹⁴⁵
 - 2. Crear las claves dentro del dispositivo seguro de creación de firma.¹⁴⁶
 - 3. Utilizar longitudes y algoritmos de clave reconocidos como aceptables para la firma electrónica reconocida.¹⁴⁷
- e. Notificar a la EC, sin retrasos injustificables, la pérdida, la alteración, el uso no autorizado, el robo o el compromiso de su dispositivo seguro de creación de firma.

¹⁴³ TS 101 456: 6.2.b)

¹⁴⁴ TS 101 456: 6.2.c), más estricto, y extensión al dispositivo seguro de creación de signatura.

¹⁴⁵ TS 101 456: 6.2.d) primero

¹⁴⁶ TS 101 456: 6.2.f)

¹⁴⁷ TS 101 456: 6.2.d) segundo

9.6.3.2 Garantías ofrecidas por el suscriptor

La Entidad de Certificación Vinculada tendrá que obligar al suscriptor, mediante el correspondiente instrumento jurídico, a garantizar:

- a. En caso que el suscriptor fuera el solicitante del certificado, que todas las manifestaciones realizadas en la solicitud son correctas.
- b. Que todas las informaciones suministradas por el suscriptor que se encuentre contenidas en el certificado son correctas.
- c. Que el certificado se utiliza exclusivamente para usos legales y autorizados, de acuerdo con la DPC de la Entidad de Certificación Vinculada.
- d. Que cada firma digital creada con la clave privada correspondiente a la clave pública listada en el certificado es la firma digital del suscriptor o poseedor de claves 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. Que el suscriptor es una entidad final y no una Entidad de Certificación, y no utilizará la clave privada correspondiente a la clave pública listada en el certificado para firmar ningún certificado (o cualquier otro formato de clave pública certificada), ni LRC.
- f. Que ninguna persona no autorizada ha tenido nunca acceso a la clave privada del suscriptor.

9.6.3.3 Protección de la clave privada

La Entidad de Certificación Vinculada tendrá que obligar al suscriptor, mediante el correspondiente instrumento jurídico, a garantizar que el suscriptor 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 Entidad de Certificación Vinculada tiene que obligar al usuario de certificados¹⁴⁸ 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 que utilizará información sobre el estado de los certificados.¹⁴⁹
- 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.¹⁵⁰

¹⁴⁸ Típicamente, mediante unas condiciones generales de uso del certificado.

¹⁴⁹ TS 101 456: 6.3 a); TS 102 042: 6.3 a)

¹⁵⁰ TS 101 456: 6.3 b); TS 102 042: 6.3 b)

- e. Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.¹⁵¹
- 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 certificados reconocidos de firma reconocida, son firmas electrónicas equivalentes a firmas escritas, de acuerdo con el artículo 3.4 de la Ley 59/2003, de 19 de diciembre.

9.6.4.2 Garantías ofrecidas por el verificador

La Entidad de Certificación tendrá que obligar al verificador, mediante el correspondiente instrumento jurídico, a manifestar:

- a. Que dispone de suficiente información para tomar una decisión informada para confiar o no en el certificado.
- b. Que es el único responsable de confiar o no en la información contenida en el certificado.
- c. Que será el único responsable si incumple sus obligaciones como verificador.

9.6.5 Otros Participantes

9.6.5.1 Obligaciones y garantías del directorio

La Entidad de Certificación Vinculada podrá delegar algunas funciones en el directorio, que en este caso estará obligado a su cumplimiento, en las mismas condiciones que la Entidad de Certificación.

Las funciones, obligaciones y deberes del directorio se establecerán detalladamente en la Declaración de Prácticas de Certificación de la Entidad de Certificación Vinculada, así como en la documentación jurídica auxiliar, especialmente la entregada a suscriptores, poseedores de claves y verificadores.

9.6.5.2 Garantías ofrecidas por el directorio

La Entidad de Certificación Vinculada tiene que establecer en su DPC la responsabilidad civil del directorio, cuando sea operado por una tercera entidad.

9.7 Renuncias de garantías

9.7.1 Renuncia de garantías de la Entidad de Certificación

La Entidad de Certificación Vinculada podrá rechazar todas las garantías del servicio que no se encuentren vinculadas a obligaciones establecidas por la Ley 59/2003, de 19 de

¹⁵¹ TS 101 456: 6.3 c); TS 102 042: 6.3 c)

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 la Entidad de Certificación

La Entidad de Certificación Vinculada limitará 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) suministrado por la Entidad de Certificación.

La Entidad de Certificación Vinculada podrá limitar su responsabilidad mediante la inclusión de límites de uso del certificado,¹⁵² y límites de valor de las transacciones para las que puede utilizarse el certificado.¹⁵³

9.8.2 Caso fortuito y fuerza mayor

La Entidad de Certificación Vinculada incluirá 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 Cláusula de indemnidad de suscriptor

No se establecerá cláusula de indemnidad del suscriptor.

9.9.2 Cláusula de indemnidad de verificador

No se establecerá cláusula de indemnidad del verificador.

9.10 Plazo y finalización

9.10.1 Plazo

La Entidad de Certificación Vinculada tendrá que establecer, en sus instrumentos jurídicos con los suscriptores, una cláusula que determine el período de vigencia de la relación jurídica en virtud de la cual les suministra certificados.

¹⁵² Ley 59/2003: 11.2.h)

¹⁵³ Ley 59/2003: 11.2.i)

9.10.2 Finalización

La Entidad de Certificación Vinculada tendrá que establecer, en sus instrumentos jurídicos con los suscriptores, una cláusula que determine las consecuencias de la finalización de la relación jurídica en virtud de la cual les suministra certificados.

9.10.3 Supervivencia

La Entidad de Certificación Vinculada tendrá que establecer, en sus instrumentos jurídicos con los suscriptores, cláusulas de supervivencia, en virtud de la cual ciertas reglas continuaran vigentes después de la finalización de la relación jurídica reguladora del servicio entre las partes.

A este efecto, la Entidad de Certificación Vinculada velará 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 Entidad de Certificación con suscriptores.

El Consorci AOC determinará un Plan de Continuidad de Negocio. Este Plan de Continuidad de Negocio determinará las obligaciones que asume el Consorci AOC en caso de cesación 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 soporte en el que han sido generados o almacenados. A tal efecto, el Consorci AOC se asegura de que se genera una copia de seguridad con periodicidad suficiente, como previsión complementaria de la actividad corriente y del aseguramiento de la continuidad de negocio.

9.11 Notificaciones

La Entidad de Certificación Vinculada tendrá que establecer cláusulas de notificación en sus instrumentos jurídicos vinculantes con suscriptores y verificadores.

En virtud de estas cláusulas, se establecerá el procedimiento por el que las partes se notifiquen hechos mutuamente.

9.12 Modificaciones

9.12.1 Procedimiento para las modificaciones

Las Entidades de Certificación Vinculadas podrán modificar, de forma unilateral, la política de certificación, siempre que procedan según el siguiente procedimiento:

- La modificación tendrá que estar justificada desde el punto de vista técnico, legal o comercial.
- La modificación propuesta por una Entidad de Certificación Vinculada no podrá ir en contra de la política de certificación establecida por el Consorci AOC.

- Se establecerá un control de modificaciones, para garantizar, en todo caso, que las especificaciones resultantes cumplen los requisitos que se intentaban cumplir y que dieron pie al cambio.
- Se establecerán las implicaciones que el cambio de especificaciones tiene sobre el usuario, y se preverá la necesidad de notificarle dichas modificaciones.
- La nueva política tendrá que ser aprobada por el Consorci AOC.

9.12.2 Periodo y mecanismos para notificaciones

Las modificaciones de la política se notificarán al Consorci AOC, para su posterior aprobación.

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

La Entidad de Certificación Vinculada tendrá que establecer, en sus instrumentos jurídicos con suscriptores y verificadores, los procedimientos de mediación y resolución de conflictos aplicables¹⁵⁴.

Con esta finalidad, se tendrá en cuenta la consideración como Administración Pública de la Entidad de Certificación Vinculada.

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

9.13.2 Jurisdicción competente

La Entidad de Certificación Vinculada tendrá que establecer, en sus instrumentos jurídicos vinculantes con suscriptores y verificadores, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles.

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

Cuando la Entidad de Certificación Vinculada tenga la consideración de Administración Pública se tendrá en cuenta la legislación administrativa que resulte aplicable.

¹⁵⁴ TS 101 456: 7.5.1 h); TS 102042: 7.5.1 h)

9.14 Ley aplicable

La Entidad de Certificación Vinculada tendrá que establecer, en sus instrumentos jurídicos con suscriptores y verificadores, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación es la siguiente:

- En general, la ley española, siempre y cuando la Entidad de Certificación Vinculada esté establecida en el Estado Español, y/o sus servicios de certificación se presten por medio de un establecimiento permanente situado en el Estado Español.¹⁵⁵
- Para las Entidades de Certificación Vinculadas a la jerarquía con la consideración de Administración Pública, la normativa administrativa correspondiente, estatal y autonómica.

9.15 Conformidad con la ley aplicable

La Entidad de Certificación Vinculada tendrá que manifestar el cumplimiento de la Ley 59/2003, de 19 de diciembre, de firma electrónica y la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico, en su DPC y con los instrumentos jurídicos con suscriptores y verificadores.

9.16 Cláusulas diversas

9.16.1 Acuerdo íntegro

La Entidad de Certificación tendrá que establecer, en sus instrumentos jurídicos vinculantes con suscriptores y verificadores, cláusulas de acuerdo íntegro.

En virtud de la cláusula de acuerdo íntegro se entenderá que el instrumento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.

9.16.2 Subrogación

Los derechos y los deberes asociados a la condición de Entidad de Certificación Vinculada no podrán ser objeto de cesión a terceros de ningún tipo, ni ninguna tercera entidad podrá subrogarse en la posición jurídica de una Entidad de Certificación.

En caso de producirse una cesión o subrogación, se procederá a la finalización de la Entidad de Certificación Vinculada.

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

¹⁵⁵ Ley 59/2003: 1.2

9.16.3 Divisibilidad

La Entidad de Certificación tendrá que establecer, sus instrumentos jurídicos vinculantes con suscriptores y verificadores, cláusulas de divisibilidad.

En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.

Para el caso que, como causa en los artículos 7 y 8 de la Ley 7/1998 sobre condiciones generales de la contratación, se considerasen no incorporadas al contrato, o nulas algunas o cualquiera de las cláusulas indicadas, la referida no incorporación o nulidad no determinará la ineficacia total del contrato, si este pudiera subsistir sin las cláusulas indicadas.¹⁵⁶.

9.16.4 Aplicaciones

Sin estipulación adicional.

9.16.5 Otras cláusulas

Sin estipulación adicional.

¹⁵⁶ Ley 7/1998: Art. 10

ANEXO – Control documental

Control de versiones PGdC 1er semestre 2016

Proyecto:	Informe modificación del documento PGdC
Entidad de destino:	Consorci AOC
Código de referencia:	Revisión 1er semestre 2016
Versión:	Cambios de la v4.1 a la v4.2 en catalán y en castellano
Fecha de edición:	03/08/2016

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
4.2	Todo el documento	Revisión global 1er trimestre 2016.	Servei de Certificació Digital – Consorci AOC	03/08/2016