Agencia de Tecnología y Certificación Electrónica

Política de Certificación de Certificados Cualificados de Representante de Entidad Jurídica en dispositivo seguro

Fecha: 07/02/2025	**Versión:** 3.0.3
Estado: APROBADO	**Nº de páginas:** 49
OID: 1.3.6.1.4.1.8149.3.29.3.0	**Clasificación: PUBLICO**
Archivo: ACCV-CP-29V3.0.3-ES-2025.odt	
Preparado por: Agencia de Tecnología y Certificación Electrónica - ACCV	

Este documento es propiedad de la Agencia de Tecnología y Certificación Electrónica – ACCV.
Licenciado bajo Creative Commons Attribuion-NoDerivatives 4.0 (CC BY-ND 4.0)

Cambios

Versión	Autor	Fecha	Observaciones
1.0.1	ACCV	03/05/2017	Cambios de adaptación RFC3647
1.0.2	ACCV	16/02/2020	Cambio de vigencia
1.0.3	ACCV	20/03/2021	Cambio de Sede y Policy Notice
2.0.1	ACCV	20/03/2022	Se elimina correo y EKU S/MIME
2.0.2	ACCV	09/01/2023	Se cambian los dispositivos QSCD homologados
3.0.1	ACCV	06/10/2023	Nueva jerarquía
3.0.2	ACCV	12/02/2024	Dejar sólo la nueva jerarquía
3.0.3	ACCV	07/02/2025	Revisión y correcciones menores

Tabla de Contenido

1 INTRODUCCIÓN....11

1.1 PRESENTACIÓN....11
1.2 IDENTIFICACIÓN....11
1.3 COMUNIDAD DE USUARIOS Y ÁMBITO DE APLICACIÓN....12
1.3.1 Autoridades de Certificación....12
1.3.2 Autoridades de Registro....12
1.3.3 Suscriptores....12
1.3.4 Partes confiantes....12
1.3.5 Otros participantes....12
1.4 USO DE LOS CERTIFICADOS....13
1.4.1 Usos Permitidos....13
1.4.2 Usos Prohibidos....13
1.5 POLÍTICA DE ADMINISTRACIÓN DE LA ACCV....13
1.5.1 Especificación de la Organización Administradora....13
1.5.2 Persona de Contacto....13
1.5.3 Competencia para determinar la adecuación de la CPS a la Políticas....13
1.5.4 Procedimiento de aprobación....13
1.6 DEFINICIONES Y ACRÓNIMOS....13
1.6.1 Definiciones....13
1.6.2 Acrónimos....13

2 PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS....14

2.1 REPOSITORIO DE CERTIFICADOS....14
2.2 PUBLICACIÓN....14
2.3 FRECUENCIA DE ACTUALIZACIONES....14
2.4 CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS....14

3 IDENTIFICACIÓN Y AUTENTICACIÓN....15

3.1 REGISTRO DE NOMBRES....15
3.1.1 Tipos de nombres....15
3.1.2 Significado de los nombres....15
3.1.3 Interpretación de formatos de nombres....15
3.1.4 Unicidad de los nombres....15
3.1.5 Resolución de conflictos relativos a nombres....15
3.1.6 Reconocimiento, autenticación y función de las marcas registradas....15

3.2 VALIDACIÓN INICIAL DE LA IDENTIDAD....15
3.2.1 Métodos de prueba de posesión de la clave privada....15
3.2.2 Autenticación de la identidad de una organización....15
3.2.3 Autenticación de la identidad de un individuo....16
3.2.4 Información no verificada del subscriptor....16
3.2.5 Validación de la representación....16
3.2.6 Criterio para la interoperación....16
3.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DE LA CLAVE....16
3.3.1 Identificación y autenticación de las solicitudes de renovación rutinarias....16
3.3.2 Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida....16
3.4 IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DE LA CLAVE....17
4 EL CICLO DE VIDA DE LOS CERTIFICADOS....18
4.1 SOLICITUD DE CERTIFICADOS....18
4.1.1 Legitimación de la solicitud....18
4.1.2 Procedimiento de alta y responsabilidades....18
4.2 TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADOS....18
4.2.1 Ejecución de las funciones de identificación y autenticación....18
4.2.2 Aprobación o rechazo de la solicitud....18
4.2.3 Plazo para resolver la solicitud....19
4.3 EMISIÓN DE CERTIFICADOS....19
4.3.1 Acciones de la CA durante el proceso de emisión....19
4.3.2 Notificación de la emisión al suscriptor....19
4.4 ACEPTACIÓN DE CERTIFICADOS....19
4.4.1 Conducta que constituye aceptación del certificado....19
4.4.2 Publicación del certificado por la CA....20
4.4.3 Notificación de la emisión a terceros....20
4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO....20
4.5.1 Uso del certificado y la clave privada del suscriptor....20
4.5.2 Uso de la clave pública y del certificado por la parte que confía....20
4.6 RENOVACIÓN DE CERTIFICADOS....20
4.6.1 Circunstancia para la renovación del certificado....20
4.6.2 Quién puede solicitar renovación....20
4.6.3 Procesamiento de solicitudes de renovación de certificados....20
4.6.4 Notificación de nueva emisión de certificado al suscriptor....20
4.6.5 Conducta que constituye la aceptación de un certificado de renovación....20
4.6.6 Publicación del certificado de renovación por la CA....20

4.6.7 Notificación de emisión de certificado por la CA a otras entidades *21*
4.7 RENOVACIÓN DE CLAVES 21
4.7.1 Circunstancias para la renovación con regeneración de claves *21*
4.7.2 Circunstancias para la renovación con regeneración de claves *21*
4.7.3 Procesamiento de solicitudes de renovación con regeneración de claves *21*
4.7.4 Notificación de la renovación con regeneración de claves *21*
4.7.5 Conducta que constituye la aceptación de la renovación con regeneración de claves *21*
4.7.6 Publicación del certificado renovado *21*
4.7.7 Notificación de la renovación con regeneración de claves a otras entidades *21*
4.8 MODIFICACIÓN DE CERTIFICADOS 21
4.8.1 Circunstancia para la modificación del certificado *21*
4.8.2 Quién puede solicitar la modificación del certificado *21*
4.8.3 Procesamiento de solicitudes de modificación de certificados *21*
4.8.4 Notificación de nueva emisión de certificado al suscriptor *22*
4.8.5 Conducta que constituye la aceptación de un certificado modificado *22*
4.8.6 Publicación del certificado modificado por la CA *22*
4.8.7 Notificación de emisión de certificado por la CA a otras entidades *22*
4.9 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS 22
4.9.1 Circunstancias para la revocación *22*
4.9.2 Entidad que puede solicitar la revocación *22*
4.9.3 Procedimiento de solicitud de revocación *22*
4.9.3.1 Presencial 22
4.9.3.2 Telemático 22
4.9.4 Periodo de gracia de la solicitud de revocación *22*
4.9.5 Tiempo dentro del cual la CA puede procesar la solicitud de revocación *22*
4.9.6 Requisitos de comprobación de CRLs *22*
4.9.7 Frecuencia de emisión de CRLs *23*
4.9.8 Máxima latencia de CRL *23*
4.9.9 Disponibilidad de comprobación on-line de la revocación *23*
4.9.10 Requisitos de la comprobación on-line de la revocación *23*
4.9.11 Otras formas de divulgación de información de revocación disponibles *23*
4.9.12 Requisitos especiales de revocación por compromiso de las claves *23*
4.9.13 Circunstancias para la suspensión *23*
4.9.14 Entidad que puede solicitar la suspensión *23*
4.9.15 Procedimiento para la solicitud de suspensión *23*
4.9.16 Límites del período de suspensión *23*
4.10 SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS 23
4.10.1 Características operacionales *23*

4.10.2 Disponibilidad del servicio 23
4.10.3 Características opcionales 23
4.11 FINALIZACIÓN DE LA SUSCRIPCIÓN 24
4.12 DEPÓSITO Y RECUPERACIÓN DE CLAVES 24
4.12.1 Política y prácticas clave de custodia y recuperación 24
4.12.2 Política y prácticas de encapsulado y recuperación de claves de sesión 24
5 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES 25
5.1 CONTROLES DE SEGURIDAD FÍSICA 25
5.1.1 Ubicación y construcción 25
5.1.2 Acceso físico 25
5.1.3 Alimentación eléctrica y aire acondicionado 25
5.1.4 Exposición al agua 25
5.1.5 Protección y prevención de incendios 25
5.1.6 Sistema de almacenamiento 25
5.1.7 Eliminación de residuos 25
5.1.8 Backup remoto 25
5.2 CONTROLES DE PROCEDIMIENTOS 25
5.2.1 Papeles de confianza 25
5.2.2 Número de personas requeridas por tarea 25
5.2.3 Identificación y autenticación para cada papel 26
5.3 CONTROLES DE SEGURIDAD DE PERSONAL 26
5.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación 26
5.3.2 Procedimientos de comprobación de antecedentes 26
5.3.3 Requerimientos de formación 26
5.3.4 Requerimientos y frecuencia de actualización de la formación 26
5.3.5 Frecuencia y secuencia de rotación de tareas 26
5.3.6 Sanciones por acciones no autorizadas 26
5.3.7 Requerimientos de contratación de personal 26
5.3.8 Documentación proporcionada al personal 26
5.3.9 Controles periódicos de cumplimiento 26
5.3.10 Finalización de los contratos 26
5.4 PROCEDIMIENTOS DE CONTROL DE SEGURIDAD 27
5.4.1 Tipos de eventos registrados 27
5.4.2 Frecuencia de procesado de logs 27
5.4.3 Periodo de retención para los logs de auditoría 27
5.4.4 Protección de los logs de auditoría 27
5.4.5 Procedimientos de backup de los logs de auditoría 27

5.4.6 Sistema de recogida de información de auditoría (interno vs externo) 27
5.4.7 Notificación al sujeto causa del evento 27
5.4.8 Análisis de vulnerabilidades 27
5.5 ARCHIVO DE INFORMACIONES Y REGISTROS 27
5.5.1 Tipo de informaciones y eventos registrados 27
5.5.2 Periodo de retención para el archivo 27
5.5.3 Protección del archivo 27
5.5.4 Procedimientos de backup del archivo 27
5.5.5 Requerimientos para el sellado de tiempo de los registros 28
5.5.6 Sistema de recogida de información de auditoría (interno vs externo) 28
5.5.7 Procedimientos para obtener y verificar información archivada 28
5.6 CAMBIO DE CLAVE 28
5.7 RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O DE DESASTRE 28
5.7.1 Procedimientos de gestión de incidencias y compromisos 28
5.7.2 Corrupción de recursos, aplicaciones o datos 28
5.7.3 Compromiso de la clave privada de la entidad 28
5.7.4 Continuidad del negocio después de un desastre 28
5.8 CESE DE UNA CA 28
6 CONTROLES DE SEGURIDAD TÉCNICA 29
6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES 29
6.1.1 Generación del par de claves 29
6.1.2 Entrega de la clave privada a la entidad 29
6.1.3 Entrega de la clave pública al emisor del certificado 29
6.1.4 Entrega de la clave pública de la CA a los usuarios 29
6.1.5 Tamaño de las claves 29
6.1.6 Parámetros de generación de la clave pública y verificación de la calidad 29
6.1.7 Propósitos de uso de claves 30
6.2 PROTECCIÓN DE LA CLAVE PRIVADA 30
6.2.1 Estándares para los módulos criptográficos 30
6.2.2 Control multipersona de la clave privada 30
6.2.3 Custodia de la clave privada 30
6.2.4 Copia de seguridad de la clave privada 31
6.2.5 Archivo de la clave privada 31
6.2.6 Introducción de la clave privada en el módulo criptográfico 31
6.2.7 Almacenamiento de clave privada en el módulo criptográfico 31
6.2.8 Método de activación de la clave privada 31
6.2.9 Método de desactivación de la clave privada 31

6.2.10 Método de destrucción de la clave privada *31*
6.2.11 Calificación del módulo criptográfico *31*
Ver la sección 6.2.1 de la presente política *31*
6.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES 31
6.3.1 Archivo de la clave pública *31*
6.3.2 Periodo de uso para las claves públicas y privadas *31*
6.4 DATOS DE ACTIVACIÓN 32
6.4.1 Generación y activación de los datos de activación *32*
6.4.2 Protección de los datos de activación *32*
6.4.3 Otros aspectos de los datos de activación *32*
6.5 CONTROLES DE SEGURIDAD INFORMÁTICA 32
6.5.1 Requisitos técnicos específicos de seguridad informática *32*
6.5.2 Evaluación del nivel de seguridad informática *32*
6.6 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA 32
6.6.1 Controles de desarrollo de sistemas *32*
6.6.2 Controles de gestión de la seguridad *32*
6.6.3 Controles de seguridad del ciclo de vida *32*
6.7 CONTROLES DE SEGURIDAD DE LA RED 33
6.8 FUENTES DE TIEMPO 33
7 PERFILES DE CERTIFICADO, CRL Y OCSP 34
7.1 PERFIL DE CERTIFICADO 34
7.1.1 Número de versión *34*
7.1.2 Extensiones del certificado *34*
7.1.3 Identificadores de objeto (OID) de los algoritmos *36*
7.1.4 Formatos de nombres *36*
7.1.5 Restricciones de los nombres *37*
7.1.6 Identificador de objeto (OID) de la Política de Certificación *37*
7.1.7 Uso de la extensión "Policy Constraints" *38*
7.1.8 Sintaxis y semántica de los cualificadores de política *38*
7.1.9 Tratamiento semántico para la extensión "Certificate Policy" *38*
7.2 PERFIL DE CRL 38
7.2.1 Número de versión *38*
7.2.2 CRL y extensiones *38*
7.3 PERFIL DE OCSP 38
7.3.1 Número de versión *38*
7.3.2 Extensiones *38*

8 AUDITORÍA DE CONFORMIDAD 39

8.1 FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD PARA CADA ENTIDAD 39
8.2 IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR 39
8.3 RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA 39
8.4 TÓPICOS CUBIERTOS POR EL CONTROL DE CONFORMIDAD 39
8.5 ACCIONES A TOMAR COMO RESULTADO DE UNA DEFICIENCIA 39
8.6 COMUNICACIÓN DE RESULTADOS 39

9 REQUISITOS COMERCIALES Y LEGALES 40

9.1 TARIFAS 40
9.1.1 Tarifas de emisión de certificado o renovación 40
9.1.2 Tarifas de acceso a los certificados 40
9.1.3 Tarifas de acceso a la información de estado o revocación 40
9.1.4 Tarifas de otros servicios como información de políticas 40
9.1.5 Política de reintegros 40
9.2 CAPACIDAD FINANCIERA 40
9.2.1 Indemnización a los terceros que confían en los certificados emitidos por la ACCV 40
9.2.2 Relaciones fiduciarias 40
9.2.3 Procesos administrativos 40
9.3 POLÍTICA DE CONFIDENCIALIDAD 40
9.3.1 Información confidencial 40
9.3.2 Información no confidencial 41
9.3.3 Divulgación de información de revocación /suspensión de certificados 41
9.4 PROTECCIÓN DE DATOS PERSONALES 41
9.4.1 Plan de Protección de Datos Personales 41
9.4.2 Información considerada privada 41
9.4.3 Información no considerada privada 41
9.4.4 Responsabilidades 41
9.4.5 Prestación del consentimiento en el uso de los datos personales 41
9.4.6 Comunicación de la información a autoridades administrativas y/o judiciales 41
9.4.7 Otros supuestos de divulgación de la información 41
9.5 DERECHOS DE PROPIEDAD INTELECTUAL 41
9.6 OBLIGACIONES Y RESPONSABILIDAD CIVIL 42
9.6.1 Obligaciones de la Entidad de Certificación 42
9.6.2 Obligaciones de la Autoridad de Registro 42
9.6.3 Obligaciones de los suscriptores 42
9.6.4 Obligaciones de los terceros confiantes en los certificados emitidos por la ACCV 42

9.6.5 Obligaciones del repositorio ... *42*
9.7 RENUNCIAS DE GARANTÍAS ... 42
9.8 LIMITACIONES DE RESPONSABILIDAD ... 42
9.8.1 Garantías y limitaciones de garantías ... *42*
9.8.2 Deslinde de responsabilidades ... *42*
9.8.3 Limitaciones de pérdidas ... *42*
9.9 INDEMNIZACIONES ... 42
9.10 PLAZO Y FINALIZACIÓN ... 42
9.10.1 Plazo ... *42*
9.10.2 Finalización ... *43*
9.10.3 Supervivencia ... *43*
9.11 NOTIFICACIONES ... 43
9.12 MODIFICACIONES ... 43
9.12.1 Procedimientos de especificación de cambios ... *43*
9.12.2 Procedimientos de publicación y notificación ... *43*
9.12.3 Procedimientos de aprobación de la Declaración de Prácticas de Certificación ... *43*
9.13 RESOLUCIÓN DE CONFLICTOS ... 43
9.13.1 Resolución extrajudicial de conflictos ... *43*
9.13.2 Jurisdicción competente ... *43*
9.14 LEGISLACIÓN APLICABLE ... 43
9.15 CONFORMIDAD CON LA LEY APLICABLE ... 43
9.16 CLÁUSULAS DIVERSAS ... 44
9.16.1 Acuerdo integro ... *44*
9.16.2 Asignación ... *44*
9.16.3 Severabilidad ... *44*
9.16.4 Cumplimiento (honorarios de los abogados y renuncia a los derechos) ... *44*
9.16.5 Fuerza Mayor ... *44*
9.17 OTRAS ESTIPULACIONES ... 44
10 ANEXO I ... 45
11 ANEXO II – FORMULARIO DE SOLICITUD DE REVOCACIÓN DE CERTIFICADO ... 48

1 INTRODUCCIÓN

1.1 Presentación

El presente documento es la Política de Certificación asociada a los Certificados Cualificados de Representante de Entidad Jurídica en dispositivo seguro, que contiene las reglas a las que se sujeta el uso de los certificados definidos en esta política. Se describen los papeles, responsabilidades y relaciones entre el usuario final y la Agencia de Tecnología y Certificación Electrónica y las reglas de solicitud, adquisición gestión y uso de los certificados. Este documento matiza y complementa a la *Declaración de Prácticas de Certificación (CPS)* de la Agencia de Tecnología y Certificación Electrónica.

La Política de Certificación referida en este documento se utilizará para la emisión de certificados cualificados en dispositivo seguro para representantes de entidades o empresas con personalidad jurídica, según la legislación vigente.

La presente Declaración de Prácticas de Certificación está redactada siguiendo las especificaciones del RFC 3647 *"Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*" propuesto por *Network Working Group* para este tipo de documentos, al igual que la Declaración de Prácticas de Certificación, para facilitar la lectura o comparación con documentos homólogos.

Esta Política de Certificación asume que el lector conoce los conceptos básicos de Infraestructura de Clave Pública, certificado y firma digital, en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

1.2 Identificación

Nombre de la política	Política de Certificación de Certificados Cualificados de Representante de Entidad Jurídica en dispositivo seguro
Calificador de la política	`Certificado cualificado de Repr. en dispositivo seguro expedido por la ACCV (Pol. Ademuz, s/n. Burjassot, CP 46100, ESPAÑA. CIF A40573396)`
Versión de la política	3.0.3
Estado de la política	APROBADO
Referencia de la política / OID (Object Identifier)	1.3.6.1.4.1.8149.3.29.3.0
Fecha de emisión	7 de febrero 2025
Fecha de expiración	No aplicable.
CPS relacionada	Declaración de Prácticas de Certificación (CPS) de la ACCV. Versión 5.0. OID: 1.3.6.1.4.1.8149.2.5.0 Disponible en `http://www.accv.es/pdf-politicas`
Localización	Esta Política de Certificación se puede encontrar en: http://www.accv.es/legislacion_c.htm

1.3 Comunidad de usuarios y ámbito de aplicación

1.3.1 Autoridades de Certificación

Las CAs que pueden emitir certificados acordes con esta política son ACCV RSA1 PROFESIONALES y ACCV ECC1 PROFESIONALES pertenecientes a la Agencia de Tecnología y Certificación Electrónica, cuya función es la emisión de certificados de entidad final para los suscriptores de ACCV. La elección de una u otra CA dependerá del tipo de claves utilizados para la emisión de los certificados finales: RSA o ECDSA.

Los certificados de ACCV RSA1 PROFESIONALES y ACCV ECC1 PROFESIONALES son válidos desde el día 25 de julio de 2023 hasta el 19 de julio de 2047.

1.3.2 Autoridades de Registro

La lista de Autoridades de Registro (Puntos de Registro de Usuario) que gestionan las solicitudes presenciales de certificados definidos en esta política se encuentra en la URL http://www.accv.es

1.3.3 Suscriptores

El grupo de usuarios que pueden solicitar certificados definidos por esta política está compuesto por los administradores de la Entidad, sus representantes legales y voluntarios con poder bastante a estos efectos.

La custodia de los datos de creación de firma asociados a cada certificado electrónico de representante de persona jurídica será responsabilidad del representante solicitante, cuya identificación se incluirá en el certificado electrónico.

Los soportes de claves y certificados pueden ser de los tipos:

- Tarjeta criptográfica ChipDoc V2 ON JCOP 3 P60 in SSCD configuration, version V7b4_2
- Tarjeta criptográfica ChipDoc v3.2 on JCOP 4 P71 in SSCD configuration version 3.2.0.52

En caso de acreditarse otros dispositivos criptográficos serán recogidos en el presente documento, en su punto 6.2.1.

1.3.4 Partes confiantes

Se limita el derecho a confiar en los certificados emitidos conforme a la presente política a:

- Las aplicaciones y servicios pertenecientes a las Administraciones Públicas españolas o europeas. entidades u organizaciones.
- Las aplicaciones y servicios que, sin pertenecer al ámbito de la Administración Pública, requieran de sistemas de identificación y/o firma seguros, de acuerdo con la legislación española de firma electrónica o con la normativa europea..
- Los actos y las contrataciones de bienes o servicios que sean propios o concernientes al giro o tráfico ordinario de la persona jurídica y su representación.

1.3.5 Otros participantes

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.4 Uso de los certificados

1.4.1 Usos Permitidos

Los certificados emitidos por la Agencia de Tecnología y Certificación Electrónica bajo esta Política de Certificación, pueden utilizarse para la firma electrónica y cifrado de cualquier información o documento. Asimismo, pueden utilizarse como mecanismo de identificación ante servicios y aplicaciones informáticas.

1.4.2 Usos Prohibidos

Los certificados se utilizarán únicamente conforme a la función y finalidad que tengan establecida en la presente Política de Certificación, y con arreglo a la normativa vigente.

1.5 Política de Administración de la ACCV

1.5.1 Especificación de la Organización Administradora

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.5.2 Persona de Contacto

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.5.3 Competencia para determinar la adecuación de la CPS a la Políticas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.5.4Procedimiento de aprobación.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.6 Definiciones y Acrónimos

1.6.1Definiciones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.6.2Acrónimos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

2 Publicación de información y repositorio de certificados

2.1 Repositorio de certificados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

2.2 Publicación

La Agencia de Tecnología y Certificación Electrónica (ACCV) se ajusta a la versión actual del documento "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", publicada en https://www.cabforum.org/. En el caso de cualquier incompatibilidad entre esta Política de Certificación y los requisitos del CAB Forum, dichos requisitos prevalecerán sobre el presente documento.

2.3 Frecuencia de actualizaciones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

2.4 Controles de acceso al repositorio de certificados.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3 Identificación y Autenticación

3.1 Registro de nombres

3.1.1 Tipos de nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.1.2 Significado de los nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.1.3 Interpretación de formatos de nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.1.4 Unicidad de los nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.1.5 Resolución de conflictos relativos a nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.1.6 Reconocimiento, autenticación y función de las marcas registradas.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.2 Validación Inicial de la Identidad

3.2.1 Métodos de prueba de posesión de la clave privada.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.2.2 Autenticación de la identidad de una organización.

La autenticación de la identidad de una organización o entidad se realizará mediante la identificación del solicitante del certificado de representante de entidad (administrador, o el representante legal o voluntario con poder bastante) ante la Autoridad de Registro correspondiente habilitada para la emisión de este tipo de certificados, acreditando su identidad personal y aportando la documentación que se establece a continuación:

- La solicitud del certificado electrónico de representante de entidad para una Administración Pública (estatal, autonómica o local) deberá realizarla la persona responsable y con autoridad en la entidad a nivel de Director General, Gerente, Alcalde, Teniente Alcalde o Secretario, Presidente o Vicepresidente de la Diputación, acompañado del Diario o Boletín Oficial donde conste la publicación de su nombramiento.
- Para solicitar certificado electrónico de representante de una sociedad mercantil o cualquier sociedad de inscripción obligatoria en el Registro Mercantil (Sociedad Anónima, Sociedad de Responsabilidad Limitada, Sociedad Laboral, Sociedad Deportiva, Sociedades Colectivas, Comanditarias o Cooperativas, Agrupaciones de Interés Económico, UTE, otras..), se deberá aportar certificado del Registro Mercantil relativo a la constitución, personalidad jurídica y nombramiento y vigencia del cargo de administrador o representante legal. Si no se aportara

se entiende que presta el consentimiento a la ACCV para la consulta en registro público donde consten inscritos los documentos de constitución y apoderamiento. Si la representación es voluntaria, se sustituirá el certificado de nombramiento y vigencia del cargo por el poder notarial bastante, con la cláusula especial para poder solicitar el Certificado de Representante de Persona Jurídica.

La ACCV guardará copia de la documentación presentada por el solicitante o de la consultada en el Registro Mercantil.

3.2.3 Autenticación de la identidad de un individuo.

La autenticación de la identidad del solicitante de un certificado de representante de persona jurídica se realizará mediante su identificación ante la Autoridad de Registro correspondiente. En el caso de personarse ante el Operador del Punto de Registro habilitado para la emisión de este tipo de certificado, debe acreditarse la identidad mediante presentación del Documento Nacional de Identidad (DNI), pasaporte español, o el Número de Identificación de Extranjeros (NIE) del solicitante. Podrá prescindirse de la personación si su firma en la solicitud de expedición de un certificado cualificado ha sido legitimada en presencia notarial. En el caso de identificación no presencial frente a la Autoridad de registro, el usuario debe presentar un certificado cualificado personal de la ACCV o el DNIe. Previamente se debe haber registrado la solicitud y confirmado la documentación necesaria para identificar la identidad de la organización y la vinculación del solicitante con la misma.

Tras producirse todas las comprobaciones el solicitante dispondrá de un máximo de 30 días para generar el certificado.

3.2.4 Información no verificada del subscriptor

Toda la información suministrada es verificada.

3.2.5 Validación de la representación

La capacidad del solicitante del certificado de realizar la solicitud de certificados en nombre de terceros se verifica durante la validación de la identidad del solicitante. Como se establece por ley es necesario un poder especial especifico para realizar esta operación.

3.2.6 Criterio para la interoperación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.3 Identificación y autenticación de las solicitudes de renovación de la clave.

3.3.1 Identificación y autenticación de las solicitudes de renovación rutinarias.

La identificación y autenticación para la renovación del certificado se realizará utilizando las técnicas y procedimientos recogidos en el punto 3.*2 Validación Inicial de la Identidad*.

3.3.2 Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida.

La política de identificación y autenticación para la renovación de un certificado después de una revocación sin compromiso de la clave será la misma que para el registro inicial, o bien se empleará

algún método electrónico que garantice de manera fiable e inequívoca la identidad del solicitante y la autenticidad de la solicitud.

3.4 Identificación y autenticación de las solicitudes de revocación de la clave

Para la revocación presencial del certificado de Representante de Entidad deberá personarse el solicitante del certificado u otra persona con poder bastante para representar a la Entidad (administrador o el representante legal o voluntario de la Entidad). La identificación de la persona y determinación del poder se llevará a cabo como se recoge en el punto 3.2. *Validación Inicial del la Identidad*

Telemática. Mediante la solicitud de revocación del solicitante del certificado firmado electrónicamente el formulario de revocación ubicado en el Área Personal de Servicios de Certificación (APSC) en http://www.accv.es.

ACCV o cualquiera de las entidades que la componen pueden solicitar de oficio la revocación de un certificado si tuvieran el conocimiento o sospecha del compromiso de la clave privada del subscriptor, o cualquier otro hecho que recomendará emprender dicha acción.

4 El ciclo de vida de los certificados.

Las especificaciones contenidas en este apartado complementan estipulaciones previstas la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.1 Solicitud de certificados

4.1.1 Legitimación de la solicitud

Los suscriptores enumerados en el punto 1.3.3 pueden presentar una solicitud de certificado.

4.1.2 Procedimiento de alta y responsabilidades

El solicitante del certificado que desee que le sea emitido un certificado de Representante de Entidad de acuerdo con esta política de certificación deberá presentarse para solicitarlo en una Autoridad de Registro de la Agencia de Tecnología y Certificación Electrónica, aportando previamente la documentación que se exige en el punto 3.2.2 *Autenticación de la identidad de una organización* utilizando los medios telemáticos que la ACCV pone a disposición del solicitante en https://www.accv.es. Si la presentación es presencial, debe hacerse en un Punto de Registro Autorizado de la Agencia de Tecnología y Certificación Electrónica con su Documento Nacional de Identidad (DNI), pasaporte español o Número de Identificación de Extranjero (NIE) en vigor. Si la presentación es telemática, debe identificarse frente a la Autoridad de Registro con un certificado cualificado personal de la ACCV o bien con el DNIe, en vigor en ambos casos.

Asimismo, en el caso de solicitud de certificado a través de medios remotos sin identificación interactiva de la identidad, se exigirá un periodo de tiempo inferior a cinco años desde la identificación presencial.

El listado de Puntos de registro autorizados para la emisión de este tipo de certificados se encuentra en la URL http://www.accv.es.

4.2 Tramitación de la solicitud de certificados.

Compete a la Autoridad o Entidad de Registro la comprobación de la identidad del solicitante, la verificación de la documentación y la constatación de que el solicitante ha firmado el contrato de certificación. Una vez completa la solicitud, la Autoridad de Registro la remitirá a la Autoridad de Certificación de la ACCV.

4.2.1 Ejecución de las funciones de identificación y autenticación

La autentificación de la identidad del solicitante de un certificado se realizará mediante la identificación ante la Autoridad de Registro correspondiente utilizando los mecanismos descritos en el apartado 3.2.3 Autentificación de la identidad individual. El Operador de la Autoridad de Registro comprueba la documentación y valida los datos utilizando registros de acceso público para dicha verificación.

4.2.2 Aprobación o rechazo de la solicitud

En caso de aceptación, la Autoridad de Registro notificará al solicitante a través de un correo electrónico a la dirección de correo electrónico que figura en la solicitud.

En las solicitudes presenciales, la Autoridad de Registro informará al usuario de la aceptación o el rechazo directamente.

En las solicitudes remotas el solicitante deberá acceder al Área Personal de Servicios de Certificación (Autoridad de Registro remota) con un certificado personal o el DNIe. Si el solicitante puede realizar la solicitud, se mostrará la opción correspondiente.

En caso de rechazo la Autoridad de Registro informará al solicitante mediante los mecanismos correspondientes. En las solicitudes presenciales el Operador informará directamente al usuario del rechazo y el motivo del mismo, interrumpiendo el proceso en ese momento y cancelando la solicitud en la plataforma. En las solicitudes remotas la Autoridad de Registro informará al usuario en la aplicación impidiendo la continuación del proceso.

La ACCV utilizará esta información para decidir sobre nuevas solicitudes.

4.2.3 Plazo para resolver la solicitud

El tiempo máximo para resolver la solicitud es de cinco días laborables.

4.3 Emisión de certificados

ACCV no es responsable de la monitorización, investigación o confirmación de la exactitud de la información contenida en el certificado con posterioridad a su emisión. En el caso de recibir información sobre la inexactitud o la no aplicabilidad actual de la información contenida en el certificado, este puede ser revocado.

4.3.1 Acciones de la CA durante el proceso de emisión

La emisión del certificado tendrá lugar una vez que ACCV haya llevado a cabo las verificaciones necesarias para validar la solicitud de certificación y en presencia del solicitante. El mecanismo por el que determina la naturaleza y la forma de realizar dichas comprobaciones es esta Política de Certificación.

La CA recibe una solicitud de certificado en formato PKCS10, bien del punto de registro, bien del equipo del usuario. Todos los datos que la componen ya ha sido verificados en pasos anteriores. La CA firma esa solicitud y la devuelve a la RA para su procesamiento posterior.

Cuando la CA de ACCV emita un certificado de acuerdo con una solicitud de certificación válida, enviará una copia del mismo a la RA que remitió la solicitud y otra al repositorio de ACCV

4.3.2 Notificación de la emisión al suscriptor

Es tarea de la RA notificar al subscriptor de un certificado la emisión del mismo y proporcionarle una copia, o en su defecto, informarle del modo en que puede conseguirla.

ACCV notifica al suscriptor sobre la emisión del certificado, a través de un correo electrónico a la dirección de correo proporcionada en el proceso de solicitud.

4.4 Aceptación de certificados

4.4.1 Conducta que constituye aceptación del certificado

La aceptación de los certificados por parte de los firmantes se produce en el momento de la firma del contrato de certificación asociado a la Política de Certificación. La aceptación del contrato implica el conocimiento y aceptación por parte del suscriptor de la Política de Certificación asociada.

El Contrato de Certificación es un documento que debe ser firmado por el solicitante y, en el caso de solicitud presencial, por la persona adscrita al Registro de usuarios, y cuyo fin es vincular a la persona a certificar con la acción de la solicitud, con el conocimiento de las normas de uso y con la veracidad

de los datos presentados. El formulario del Contrato de Certificación se recoge en el Anexo I de esta Política de Certificación.

El usuario debe aceptar el contrato antes de la emisión del certificado.

4.4.2 Publicación del certificado por la CA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.4.3 Notificación de la emisión a terceros

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.5 Uso del par de claves y del certificado.

4.5.1 Uso del certificado y la clave privada del suscriptor

Los usos de la clave vienen definidos en el contenido del certificado en las extensiones: keyUsage, extendedKeyUsage y basicConstraints. Estas extensiones se detallan en el apartado *7.1.2 Extensiones del certificado*.

4.5.2 Uso de la clave pública y del certificado por la parte que confía

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6 Renovación de certificados.

La renovación de certificados debe ser realizada utilizando los mismos procedimientos y métodos de identificación que los establecidos para realizar la solicitud inicial.

4.6.1 Circunstancia para la renovación del certificado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.2 Quién puede solicitar renovación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.3 Procesamiento de solicitudes de renovación de certificados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.4 Notificación de nueva emisión de certificado al suscriptor

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.5 Conducta que constituye la aceptación de un certificado de renovación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.6 Publicación del certificado de renovación por la CA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.7 Notificación de emisión de certificado por la CA a otras entidades

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7 Renovación de claves

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.1 Circunstancias para la renovación con regeneración de claves

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.2 Circunstancias para la renovación con regeneración de claves

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.3 Procesamiento de solicitudes de renovación con regeneración de claves

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.4 Notificación de la renovación con regeneración de claves

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.5 Conducta que constituye la aceptación de la renovación con regeneración de claves

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.6 Publicación del certificado renovado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.7 Notificación de la renovación con regeneración de claves a otras entidades

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8 Modificación de certificados.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.1Circunstancia para la modificación del certificado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.2 Quién puede solicitar la modificación del certificado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.3 Procesamiento de solicitudes de modificación de certificados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.4 Notificación de nueva emisión de certificado al suscriptor

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.5 Conducta que constituye la aceptación de un certificado modificado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.6 Publicación del certificado modificado por la CA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.7 Notificación de emisión de certificado por la CA a otras entidades

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9 Revocación y suspensión de certificados.

4.9.1 Circunstancias para la revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.2 Entidad que puede solicitar la revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.3 Procedimiento de solicitud de revocación

La Agencia de Tecnología y Certificación Electrónica acepta solicitudes de revocación por los siguientes procedimientos

4.9.3.1 Presencial

Mediante la presentación e identificación del solicitante del certificado, o persona con poderes para representar a la Entidad de la cual es representante el suscriptor del certificado, en un Punto de Registro de Usuario y la cumplimentación y firma, por parte del mismo, del “Formulario de Solicitud de Revocación” que se le proporcionará y del que se adjunta copia en el anexo II

4.9.3.2 Telemático

El solicitante del certificado podrá solicitar la revocación de certificados, en la web de ACCV, en la URL http://www.accv.es, dentro del Área Personal de Servicios de Certificación, tras identificarse con su certificado personal o de entidad que haya sido solicitado por él mismo.

4.9.4 Periodo de gracia de la solicitud de revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.5 Tiempo dentro del cual la CA puede procesar la solicitud de revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.6 Requisitos de comprobación de CRLs

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.7 Frecuencia de emisión de CRLs
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.8 Máxima latencia de CRL
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.9 Disponibilidad de comprobación on-line de la revocación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.10Requisitos de la comprobación on-line de la revocación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.11Otras formas de divulgación de información de revocación disponibles
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.12 Requisitos especiales de revocación por compromiso de las claves
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.13 Circunstancias para la suspensión
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.14 Entidad que puede solicitar la suspensión
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.15 Procedimiento para la solicitud de suspensión
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.16 Límites del período de suspensión
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.10 Servicios de comprobación de estado de certificados.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.10.1Características operacionales
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.10.2 Disponibilidad del servicio
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.10.3 Características opcionales
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.11 Finalización de la suscripción.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

ACCV informará al firmante, mediante correo electrónico, en un momento previo anterior a la publicación del certificado en la Lista de Certificados Revocados, acerca de la revocación de su certificado, especificando los motivos, la fecha y la hora en que su certificado quedará sin efecto, y comunicándole que no debe continuar utilizándolo

4.12 Depósito y recuperación de claves.

4.12.1 Política y prácticas clave de custodia y recuperación

ACCV no realiza el depósito de certificados y claves de ningún tipo asociadas a este tipo de certificados.

4.12.2 Política y prácticas de encapsulado y recuperación de claves de sesión

La recuperación de las claves de sesión no esta soportado.

5 Controles de seguridad física, de gestión y de operaciones

5.1 Controles de Seguridad Física

5.1.1Ubicación y construcción

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.2 Acceso físico

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.3 Alimentación eléctrica y aire acondicionado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.4 Exposición al agua

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.5 Protección y prevención de incendios

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.6 Sistema de almacenamiento

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.7 Eliminación de residuos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.8 Backup remoto

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.2 Controles de procedimientos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.2.1 Papeles de confianza

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.2.2 Número de personas requeridas por tarea

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.2.3 Identificación y autenticación para cada papel
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3 Controles de seguridad de personal
Este apartado refleja el contenido del documento *Controles de Seguridad del Personal* de ACCV.

5.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.2 Procedimientos de comprobación de antecedentes
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.3 Requerimientos de formación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.4 Requerimientos y frecuencia de actualización de la formación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.5 Frecuencia y secuencia de rotación de tareas
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.6 Sanciones por acciones no autorizadas
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.7 Requerimientos de contratación de personal
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.8 Documentación proporcionada al personal
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.9 Controles periódicos de cumplimiento
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.10 Finalización de los contratos
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4 Procedimientos de Control de Seguridad

5.4.1 Tipos de eventos registrados
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.2 Frecuencia de procesado de logs
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.3 Periodo de retención para los logs de auditoría
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.4 Protección de los logs de auditoría
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.5 Procedimientos de backup de los logs de auditoría
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.6 Sistema de recogida de información de auditoría (interno vs externo)
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.7 Notificación al sujeto causa del evento
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.8 Análisis de vulnerabilidades
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5 Archivo de informaciones y registros

5.5.1 Tipo de informaciones y eventos registrados
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.2 Periodo de retención para el archivo.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.3 Protección del archivo.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.4 Procedimientos de backup del archivo.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.5 Requerimientos para el sellado de tiempo de los registros.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.6 Sistema de recogida de información de auditoría (interno vs externo).
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.7 Procedimientos para obtener y verificar información archivada
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.6 Cambio de Clave
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7 Recuperación en caso de compromiso de una clave o de desastre
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7.1Procedimientos de gestión de incidencias y compromisos
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7.2Corrupción de recursos, aplicaciones o datos
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7.3Compromiso de la clave privada de la entidad
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7.4Continuidad del negocio después de un desastre
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.8 Cese de una CA
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6 Controles de seguridad técnica

6.1 Generación e Instalación del Par de Claves

En este punto se hace siempre referencia a las claves generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación. La información sobre las claves de las entidades que componen la Autoridad de Certificación se encuentra en el punto 6.1 de la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.1.1Generación del par de claves

El par de claves para el certificado emitido bajo el ámbito de la presente Política de Certificación se generan en tarjeta criptográfica del usuario y nunca abandonan la misma.

6.1.2 Entrega de la clave privada a la entidad

La clave privada para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentra contenida en la tarjeta criptográfica que se entrega al suscriptor con su certificado en el momento de su registro.

6.1.3 Entrega de la clave pública al emisor del certificado

La clave pública a ser certificada es generada en el interior de la tarjeta criptográfica y es entregada a la Autoridad de Certificación por la Autoridad de Registro mediante el envío de una solicitud de certificación en formato PKCS#10, firmada digitalmente por el Operador de la Autoridad de Registro.

6.1.4 Entrega de la clave pública de la CA a los usuarios

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.1.5 Tamaño de las claves

El tamaño de las claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación es:

- Para las claves RSA de al menos 2048 bits.
- Para las claves ECDSA de al menos NIST ECC P-256.

6.1.6 Parámetros de generación de la clave pública y verificación de la calidad

Se utilizan los parámetros definidos en el documento ETSI TS 119 312 “Electronic Signatures and Infraestructures (ESI); Cryptographic Suites”.

Los parámetros utilizados son los siguientes:

Signature Suite	**Hash Function**	**Padding Method**	**Signature algorithm**
sha256-with-rsa	sha256	emsa-pkcs1-v1.5	rsa
ecdsa-with-SHA256	sha256		ecdsa

ACCV lleva a cabo la validación de las claves ECC siguiendo el procedimiento definido en NIST SP 800-89

6.1.7Propósitos de uso de claves

Los certificados emitidos bajo la presente política contienen los atributos

"KEY USAGE" y "EXTENDED KEY USAGE", tal como se define en el estándar X.509v3.

Las claves definidas por la presente política se utilizarán para usos descritos en el punto de este documento 1.3 Comunidad de usuarios y ámbito de aplicación.

La definición detallada del perfil de certificado y los usos de las claves se encuentra en el apartado 7 de este documento *"Perfiles de certificado, CRL y OCSP"*.

6.2 Protección de la Clave Privada

En este punto se hace siempre referencia a las claves generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación. La información sobre las claves de las entidades que componen la Autoridad de Certificación se encuentra en el punto 6.2 de la Declaración de Prácticas de Certificación (CPS) de la Agencia de Tecnología y Certificación Electrónica.

Los sistemas donde se almacenan las claves privadas deben cumplir una serie de requisitos relacionados con la seguridad física y lógica de las mismas. ACCV puede solicitar al organismo suscriptor que evidencie los mecanismos que se utilizan para el cumplimiento de dichos requisitos, de manera discrecional. Se recomienda seguir las directrices generadas por el CCN (Centro Nacional de Criptografía) dentro de su serie CNN-STIC, específicamente orientadas a garantizar los sistemas informáticos y las comunicaciones de la Administración.

6.2.1 Estándares para los módulos criptográficos

Los dispositivos criptográficos con certificados cualificados de firma electrónica, aptos como dispositivos cualificados de creación de firma (DSCF), cumplen con los requisitos de nivel de seguridad CC EAL4+, aunque también se aceptan certificaciones que cumplan con un mínimo de criterios de seguridad ITSEC E3 o FIPS 140-2 Nivel 2 o equivalente. La norma europea de referencia para los dispositivos de abonado utilizados es la Decisión de Ejecución (UE) 2016/650 de la Comisión, de 25 de abril de 2016. Estos dispositivos deben aparecer en la lista recopilada de Dispositivos Cualificados de Creación de Firma Electrónica (QSigCDs) según la definición del punto 23 del artículo 3 del Reglamento 910/2014, Dispositivos Cualificados de Creación de Sellos Electrónicos (QSealCDs) según la definición del punto 32 del artículo 3 del Reglamento 910/2014, y Dispositivos Seguros de Creación de Firma (SSCDs) que se benefician de la medida transitoria establecida en el artículo 51.1 del Reglamento 910/2014.

Los dispositivos cualificados de creación de firma (DSCF) que pueden dar soporte a este tipo de certificados son los siguientes:

• BIT4ID Smart Cards:

- ChipDoc V2 ON JCOP 3 P60 in SSCD configuration, version V7b4_2
- ChipDoc v3.2 on JCOP 4 P71 in SSCD configuration version 3.2.0.52

6.2.2 Control multipersona de la clave privada

Las claves privadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentran bajo el control exclusivo de los suscriptores de los mismos.

6.2.3 Custodia de la clave privada

No se custodian claves privadas de los suscriptores de los certificados definidos por la presente política.

6.2.4 Copia de seguridad de la clave privada

No se custodian claves privadas de los suscriptores de los certificados definidos por la presente política.

6.2.5 Archivo de la clave privada.

No se archivan claves privadas de los suscriptores de los certificados definidos por la presente política.

6.2.6 Introducción de la clave privada en el módulo criptográfico.

La generación de las claves vinculadas al certificado se realiza en tarjeta criptográfica por el propio chip criptográfico de la misma y nunca la abandonan.

6.2.7 Almacenamiento de clave privada en el módulo criptográfico..

La generación de las claves vinculadas al certificado se realiza en tarjeta criptográfica por el propio chip criptográfico de la misma y nunca la abandonan.

6.2.8 Método de activación de la clave privada.

La clave privada del suscriptor se activa mediante la introducción del PIN de la tarjeta que la contiene.

6.2.9 Método de desactivación de la clave privada

La desactivación de la clave privada del suscriptor se consigue mediante la extracción de la tarjeta que la contiene del lector PC/SC.

6.2.10 Método de destrucción de la clave privada

La destrucción debe ir siempre precedida de la revocación del certificado asociado a la clave privada, si ésta sigue activa.

La destrucción del Token puede producirse cuando la información impresa en él pierde su validez y hay que emitir una nueva tarjeta.

La tarea a realizar consiste en la Destrucción Segura del Token de carácter físico.

6.2.11 Calificación del módulo criptográfico

Ver la sección 6.2.1 de la presente política.

6.3 Otros Aspectos de la Gestión del par de Claves.

6.3.1 Archivo de la clave pública

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.3.2 Periodo de uso para las claves públicas y privadas

Los certificados emitidos al amparo de la presente política tienen una validez de tres (3) años.

El par de claves utilizado para la emisión de los certificados se crea para cada emisión, y por tanto también tienen una validez de tres (3) años.

Los certificados de ACCV RSA1 PROFESIONALES y ACCV ECC1 PROFESIONALES son válidos desde el día 25 de julio de 2023 hasta el 19 de julio de 2047.

6.4 Datos de activación

6.4.1 Generación y activación de los datos de activación

Los datos de activación de la clave privada consisten en el PIN de la tarjeta que la contiene y que se proporciona al suscriptor del certificado con el mismo.

La generación del PIN de la tarjeta se realiza en el momento de la inicialización de la misma. El PIN, junto con el código de desbloqueo –PUK–, se entregará al suscriptor.

Es responsabilidad y obligación del suscriptor la custodia de ese PIN (y PUK). Se aconseja al suscriptor el cambio de ese PIN preconfigurado por uno de su exclusivo conocimiento.

6.4.2 Protección de los datos de activación

El suscriptor del certificado es el responsable de la protección de los datos de activación de su clave privada.

6.4.3 Otros aspectos de los datos de activación

No hay otros aspectos a considerar.

6.5 Controles de Seguridad Informática

6.5.1 Requisitos técnicos específicos de seguridad informática

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.5.2 Evaluación del nivel de seguridad informática

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.6 Controles de Seguridad del Ciclo de Vida.

6.6.1Controles de desarrollo de sistemas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.6.2 Controles de gestión de la seguridad

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.6.3 Controles de seguridad del ciclo de vida

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.7 Controles de Seguridad de la Red

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.8 Fuentes de tiempo

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7 PERFILES DE CERTIFICADO, CRL Y OCSP

7.1 Perfil de Certificado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.1.1 Número de versión

Ademas de lo establecido en la Declaración de Prácticas de Certificación (CPS) de la ACCV, esta política de certificación especifica la emisión de un certificado con los usos de firma digital, autenticación y cifrado de claves.

7.1.2 Extensiones del certificado

El perfil del certificado emitido bajo la presente política es el siguiente:

Campo	**Valor**
Subject	
SerialNumber	número DNI/NIE Opcionalmente se podrá utilizar la semántica propuesta por la norma ETSI EN319 412-1
GivenName	Nombre del representante , tal como aparece en el DNI
SurName	Apellidos del representante, tal como aparece en el DNI
CommonName	Ver apartado 7.1.2
OrganizationIdentifier (2.5.4.97)	NIF de la entidad, tal como figura en los registros oficiales. Codificado según la Norma Europea ETSI EN 319 412-1
Description (2.5.4.13)	Codificación del documento público que acredita las facultades del firmante o los datos registrales. Ver posibles descripciones en el apartado 7.1.2
Organization	Razón Social, tal como figura en los registros oficiales.
Country	ES
Version	V3
SerialNumber	Identificador único del certificado. Menor de 32 caracteres hexadecimales.
Algoritmo de firma	ACCV_RSA1_PROFESIONALES: sha256withRSAEncryption ACCV_ECC1_PROFESIONALES: ecdsa-with-SHA256
Issuer (Emisor)	DN de la CA que emite el certificado (ver punto 7.1.4)
Válido desde	Fecha de Emisión
Válido hasta	Fecha de Caducidad
Clave Pública	Octet String conteniendo la clave pública del suscriptor

Extended Key Usage		
	Client Authentication Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)	
CRL Distribution Point	ACCV_RSA1_PROFESIONALES: http://www.accv.es/gestcert/accv_rsa1_profesionales.crl ACCV_ECC1_PROFESIONALES: http://www.accv.es/gestcert/accv_ecc1_profesionales.crl	
SubjectAlternativeName		
DirectoryName		
	CN=Nombre del representante|Apellido1 del representante|Apellido2 del representante	
	UID=NIF del representante	
Certificate Policy Extensions		
Policy OID	2.16.724.1.3.5.8	
Policy Notice	Certificado de representante de persona jurídica	
Policy OID	QCP-n-qscd: certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD; Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)	
Policy OID	1.3.6.1.4.1.8149.3.29.3.0	Política de Certificación de Certificados Cualificados de Representante de Entidad en Dispositivo Seguro
Policy CPS Location	http://www.accv.es/legislacion_c.htm	
Policy Notice	`Certificado cualificado de Repr. en dispositivo seguro expedido por la ACCV (Pol. Ademuz, s/n. Burjassot, CP 46100, ESPAÑA. CIF A40573396)`	
Authority Information Access		
Access Method	Id-ad-ocsp	
Access Location	http://ocsp.accv.es	
Access Method	Id-ad-calssuers	
Access Location	ACCV_RSA1_PROFESIONALES: http://www.accv.es/gestcert/accv_rsa1_profesionales.crt ACCV_ECC1_PROFESIONALES:	

	http://www.accv.es/gestcert/accv_ecc1_profesionales.crt	
Fingerprint issuer	Fingerprint del certificado de la CA que emite el certificado (ver CPS)	
Algoritmo de hash	SHA-256	
KeyUsage (críticos)		
	RSA Digital Signature Content Commintment Key Encipherment	**ECC** Digital Signature Content Commintment Key agreement
QcStatement	**Campos QC (Qualified Certificate)**	
QcCompliance		El certificado es cualificado
QcSSCD		La clave privada esta en un dispositivo seguro
QcType	eSign	Tipo particular de certificado cualificado
QcRetentionPeriod	15y	Periodo de retención de la información material
QcPDS	https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-V1.1-EN.pdf	Ubicación de PKI Disclosure Statement

7.1.3 Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

- SHA1withRSA (1.2.840.113549.1.1.5)
- SHA256withRSA (1.2.840.113549.1.1.11)
- ecdsa-with-SHA256 (1.2.840.10045.4.3.2)

7.1.4Formatos de nombres

Los certificados emitidos por ACCV contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

Los Issuer names admitidos para certificados emitidos bajo esta politica son:

- cn=ACCV RSA1 PROFESIONALES.2.5.4.97=VATES-A40573396,o=ISTEC,l=BURJASSOT,s=VALENCIA,c=ES
- cn=ACCV ECC1 PROFESIONALES.2.5.4.97=VATES-A40573396,o=ISTEC,l=BURJASSOT,s=VALENCIA,c=ES

SubjectAlternativeName contiene al menos el nombre y apellidos del suscriptor separados por el caracter "|" (DirectoryName).

Subject name: serialNumber=*DNI NIE*, givenName=*Nombre del representante*, surname=*Apellido1 del representante Apellido2 del representante*, cn=<DEFINIDO A CONTINUACIÓN>, Description=<DEFINIDO A CONTINUACIÓN>, OrganizationIdentifier=NIF, o=Razón Social, c=ES

El campo cn tiene un tamaño máximo de 64 caracteres según la RFC 5280, y debe tener la siguiente forma:.

Campo	Contenido	Ejemplo	tamaño *
NIF	número DNI/NIE	12345678Z	10
Nombre	Tal y como figura en el DNI/NIE	Pedro Antonio	
Apellido 1	Tal y como figura en el DNI/NIE	López	
Literal	(R:		4
NIF de la empresa	NIF de la entidad, tal como figura en los registros oficiales.	B0085974Z	9
Literal	)		2

*(contando espacio en blanco posterior)

El campo ***Description*** (2.5.4.13) se codifica el documento publico que acredita las facultades del firmante o los datos registrales. Ademas de las taxonomias recogidas, podrá utilizarse texto libre si la información que acredita la representación no se ajusta a uno de los tipos preestablecidos.

- Registro mercantil o similar

R: XXX /Hoja /Tomo /Sección /Libro /Folio /Fecha (dd-mm-aaaa) /Inscripción

- Documento notarial

N: Nombre Apellido1 Apellido2 /Núm Protocolo /Fecha Otorgamiento (dd-mm-aaaa)

- Boletín oficial

B: XXX/Fecha (dd-mm-aaaa) /Numero resolución

- Otros

Texto libre detallando la fuente de datos que acredita la representación

Todos los campos del certificado del Subject y del Subject Alternative Name, exceptuando los que se refieren a nombre DNS o direcciones de correo, se cumplimentan obligatoriamente en mayúsculas, prescindiendo de acentos.

7.1.5 Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500, únicos y no ambiguos.

El resto de campos que se incluyen en el certificado son los estrictamente necesarios que se marcan en el RFC-3739 para la obtención de un perfil de certificado cualificado.

7.1.6 Identificador de objeto (OID) de la Política de Certificación

El identificador de objeto definido por la ACCV para identificar la presente política es el siguiente:

1.3.6.1.4.1.8149.3.29.3.0

En este caso se añade un OID para identificar el tipo de entidad que se representa según la definición de los perfiles por la Administración General del Estado.

2.16.724.1.3.5.8	**Certificado de representante de persona jurídica**

En este caso se añade un OID para identificar el tipo de entidad que se representa según la normativa ETSI TS 119 411-2

0.4.0.194112.1.2	**Política de certificación para certificados cualificados EU emitidos a personas físicas en dispositivo seguro**

7.1.7 Uso de la extensión “Policy Constraints”

No se hace uso de la extensión “*Policy Constraints*” en los certificados emitidos bajo la presente Política de Certificación.

7.1.8 Sintaxis y semántica de los cualificadores de política

La extensión de las Políticas de Certificación puede incluir dos campos de Calificación de Políticas(ambos opcionales):

- CPS Pointer: contiene la URL donde se publican las Políticas de Certificación
- User Notice: contiene un texto de descripción

7.1.9 Tratamiento semántico para la extensión “Certificate Policy”

La extensión “*Certificate Policy*” identifica la política que define las prácticas que ACCV asocia explícitamente con el certificado. Adicionalmente la extensión puede contener un cualificador de la política.

7.2 Perfil de CRL

7.2.1Número de versión

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.2.2CRL y extensiones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.3Perfil de OCSP

7.3.1Número de versión

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.3.2Extensiones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8 Auditoría de conformidad

8.1 Frecuencia de los controles de conformidad para cada entidad

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8.2 Identificación/cualificación del auditor

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8.3 Relación entre el auditor y la entidad auditada

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8.4 Tópicos cubiertos por el control de conformidad

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8.5 Acciones a tomar como resultado de una deficiencia.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8.6 Comunicación de resultados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9 Requisitos comerciales y legales

9.1 Tarifas

9.1.1 Tarifas de emisión de certificado o renovación

Los precios para la emisión inicial y la renovación de los certificados a los que se refiere la presente política de certificación se recogen en la Lista de Tarifas de la Agencia de Tecnología y Certificación Electrónica. Esta Lista se publica en la página web de la ACCV www.accv.es

9.1.2 Tarifas de acceso a los certificados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.1.3 Tarifas de acceso a la información de estado o revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.1.4 Tarifas de otros servicios como información de políticas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.1.5 Política de reintegros

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.2 Capacidad financiera

9.2.1 Indemnización a los terceros que confían en los certificados emitidos por la ACCV.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.2.2 Relaciones fiduciarias

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.2.3 Procesos administrativos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.3 Política de Confidencialidad

9.3.1 Información confidencial.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.3.2 Información no confidencial
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.3.3 Divulgación de información de revocación /suspensión de certificados
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4 Protección de datos personales

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.1 Plan de Protección de Datos Personales.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.2 Información considerada privada.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.3 Información no considerada privada.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.4 Responsabilidades.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.5 Prestación del consentimiento en el uso de los datos personales.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.6 Comunicación de la información a autoridades administrativas y/o judiciales.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.7 Otros supuestos de divulgación de la información.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.5 Derechos de propiedad Intelectual
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV..

9.6 Obligaciones y Responsabilidad Civil

9.6.1 Obligaciones de la Entidad de Certificación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.6.2 Obligaciones de la Autoridad de Registro

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.6.3 Obligaciones de los suscriptores

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.6.4 Obligaciones de los terceros confiantes en los certificados emitidos por la ACCV

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.6.5 Obligaciones del repositorio

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.7 Renuncias de garantías

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.8 Limitaciones de responsabilidad

9.8.1 Garantías y limitaciones de garantías

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.8.2 Deslinde de responsabilidades

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.8.3 Limitaciones de pérdidas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.9Indemnizaciones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.10 Plazo y finalización.

9.10.1 Plazo.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.10.2 Finalización.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.10.3 Supervivencia.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.11 Notificaciones.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.12 Modificaciones.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.12.1 Procedimientos de especificación de cambios
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.12.2 Procedimientos de publicación y notificación.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.12.3 Procedimientos de aprobación de la Declaración de Prácticas de Certificación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.13 Resolución de conflictos.

9.13.1 Resolución extrajudicial de conflictos.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.13.2 Jurisdicción competente.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.14 Legislación aplicable
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.15 Conformidad con la Ley aplicable.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.16 Cláusulas diversas.

9.16.1Acuerdo integro
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.16.2Asignación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.16.3Severabilidad
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.16.4Cumplimiento (honorarios de los abogados y renuncia a los derechos)
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.16.5Fuerza Mayor
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.17Otras estipulaciones
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

10 Anexo I

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.29

Secció 1 – Dades del subscriptor / Sección 2 – Datos del suscriptor

Cognoms/*Apellidos*:

Nom/*Nombre*:

DNI/NIF: Tel.:

Adreça de correu electrònic/*Dirección correo electrónico*:

Adreça postal/Dirección postal:

Població/Población: Província/Provincia:

Secció 2 – Dades de l'Entitat / *Sección 1 – Datos de la Entidad*

Raó Social/Razón Social::

CIF de l'Entitat/*CIFde la Entidad*:

Domicili Fiscal/Domicilio Fiscal::

Població/Población: Província/Provincia:

PIN : PUK: Tel. suport/ tel. soporte **963 866 014** **www.accv.es**

Secció 3 – Dades del operador del Punt de Registre / *Sección 3 – Datos del operador del Punto de Registro*

Nom i cognoms/*Nombre y Apellidos:*

Secció 4 - Data i Firma / Sección 4 – *Fecha y Firma*

Subscric el present contracte de certificació associat a la Política de Certificació de Certificats Reconeguts de Representant d'Entitat amb codi 1.3.6.1.4.1.8149.3.29, emés per la Agencia de Tecnología y Certificación Electrónica. Declare que conec i accepte les normes d'utilització d'este tipus de certificats que es troben exposades en http://www.accv.es. Declare, així mateix, que les dades posades de manifest són certes.

Suscribo el presente contrato de certificación asociado a la Política de Certificación de Certificados Reconocidos de Representante de Entidad con código 1.3.6.1.4.1.8149.3.29*, emitido por la la Agencia de Tecnología y Certificación Electrónica. Declaro conocer y aceptar las normas de utilización de este tipo de certificados que se encuentran expuestas en http://www.accv.es. Declaro, asimismo, que los datos puestos de manifiesto son ciertos.*

Firma del sol.licitant — Firma i segell del Punt de Registre

Firma del solicitante — *Firma y sello del Punto de Registro*

Firmat/*Firmado*: Firmat/*Firmado:*

Exemplar per al sol.licitant - Anvers / *Ejemplar para el solicitante - Anverso*

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.29
Condiciones de utilización de los certificados

1. Los certificados asociados a la Política de Certificación de Certificados Reconocidos de Representante de Entidad, emitidos por la Agencia de Tecnología y Certificación Electrónica son del tipo X.509v3 y se rigen por la Declaración de Prácticas de Certificación de la Agencia de Tecnología y Certificación Electrónica, en tanto que Prestador de Servicios de Certificación, así como por la Política de Certificación referida. Ambos documentos se deben interpretar según la legislación de la Comunidad Europea, el Ordenamiento Jurídico Español y la legislación propia de la Generalitat.
2. Los solicitantes deberán ser personas físicas, en posesión de un NIF, un NIE u otro documento de identificación válido en Derecho, con poder bastante para representar a la Entidad a la que hace referencia el certificado.
3. El solicitante es responsable de la veracidad de los datos aportados en todo momento a lo largo del proceso de solicitud y registro. Será responsable de comunicar cualquier variación de los datos aportados para la obtención del certificado.
4. El titular del certificado es responsable de la custodia de su clave privada y de comunicar a la mayor brevedad posible cualquier pérdida o sustracción de esta clave.
5. El titular del certificado es responsable de limitar el uso del certificado a lo dispuesto en la Política de Certificación asociada, que es un documento público y que se encuentra disponible en http://www.accv.es. En especial, este certificado de Representante de Entidad podrá ser utilizado cuando se admita en las relaciones entre la Entidad y las Administraciones Públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario.
6. La Agencia de Tecnología y Certificación Electrónica no se responsabiliza del contenido de los documentos firmados haciendo uso de los certificados por ella emitidos.
7. La Agencia de Tecnología y Certificación Electrónica es responsable del cumplimiento de las legislaciones Europea, Española y Valenciana, por lo que a Firma Electrónica se refiere. Es, asimismo, responsable del cumplimiento de lo dispuesto en la Declaración de Prácticas de Certificación de la Agencia de Tecnología y Certificación Electrónica y en la Política de Certificación asociada a este tipo de certificados.
8. El periodo de validez de estos certificados es de tres (3) años. Para su renovación deberán seguirse el mismo procedimiento que para la primera solicitud o bien los procedimientos previstos en la Política de Certificación asociada.
9. Los certificados emitidos perderán su eficacia, además de al vencimiento del periodo de validez, cuando se produzca una revocación, cuando se inutilice el soporte del certificado, ante resolución judicial o administrativa que ordene la pérdida de eficacia, por inexactitudes graves en los datos aportados por el solicitante, por extinción o disolución de la personalidad jurídica de la Entidad, por alteración de las condiciones de custodia del certificado. Otras condiciones para la pérdida de eficicacia se recogen en la Declaración de Prácticas de Certificación y en la Política de Certificación asociada a este tipo de certificado.
10. La documentación a aportar por la persona física solicitante del certificado será el Documento Nacional de Identidad, NIE o Pasaporte español, válido y vigente. El solicitante deberá aportar los datos relativos a la constitución y personalidad jurídica y la extensión y facultades de representación del solicitante.
11. En cumplimiento de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se informa al solicitante de la existencia de un fichero automatizado de datos de carácter personal creado bajo la responsabilidad de la Agencia de Tecnología y Certificación Electrónica, denominado \"Usuarios de firma electrónica\". La finalidad de dicho fichero es la de servir a los usos relacionados con los servicios de certificación prestados por la Agencia de Tecnología y Certificación Electrónica. El suscriptor consiente expresamente la utilización de sus datos de carácter personal contenidos en dicho fichero, en la medida en que sea necesario para llevar a cabo las acciones previstas en la Política de Certificación.
12. La Agencia de Tecnología y Certificación Electrónica se compromete a poner los medios a su alcance para evitar la alteración, pérdida o acceso no autorizado a los datos de carácter personal contenidos en el fichero.
13. El solicitante podrá ejercer sus derechos de acceso, rectificación, borrado, portabilidad, restricción de procesamiento y objeción sobre sus datos de carácter personal dirigiendo escrito a la Agencia de Tecnología y Certificación Electrónica, a través de cualquiera de los Registros de Entrada de la Generalitat Valenciana e indicando claramente esta voluntad.
14. Se aconseja al usuario realizar el cambio del PIN inicial que aparece en el presente contrato a través de las herramientas que pone a su disposición la Agencia de Tecnología y Certificación Electrónica.

    Con la firma del presente documento se autoriza a la Agencia de Tecnología y Certificación Electrónica a consultar los datos de identidad que consten en el Ministerio de Interior, evitando que el ciudadano aporte fotocopia de su documento de identidad.

Ejemplar para el solicitante – Reverso

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.29

Secció 1 – Dades del subscriptor / Sección 2 – Datos del suscriptor

Cognoms/*Apellidos*:

Nom/*Nombre*:

DNI/NIF: Tel.:

Adreça de correu electrònic/*Dirección correo electrónico*:

Adreça postal/Dirección postal:

Població/Población: Província/Provincia:

Secció 2 – Dades de l'Entitat / *Sección 1 – Datos de la Entidad*

Raó Social/Razón Social::

CIF de l'Entitat/*CIFde la Entidad*:

Domicili Fiscal/Domicilio Fiscal::

Població/Población: *Província/Provincia:*

Tel. suport/ tel. soporte **963 866 014** **www.accv.es**

Secció 3 – Dades del operador del Punt de Registre / *Sección 3 – Datos del operador del Punto de Registro*

Nom i cognoms/*Nombre y Apellidos:*

Secció 4 - Data i Firma / Sección 4 – *Fecha y Firma*

Subscric el present contracte de certificació associat a la Política de Certificació de Certificats Reconeguts de Representant d'Entitat amb codi 1.3.6.1.4.1.8149.3.29, emés per la Agencia de Tecnología y Certificación Electrónica. Declare que conec i accepte les normes d'utilització d'este tipus de certificats que es troben exposades en http://www.accv.es. Declare, així mateix, que les dades posades de manifest són certes.

Suscribo el presente contrato de certificación asociado a la Política de Certificación de Certificados Reconocidos de Representante de Entidad con código 1.3.6.1.4.1.8149.3.29, emitido por la la Agencia de Tecnología y Certificación Electrónica. Declaro conocer y aceptar las normas de utilización de este tipo de certificados que se encuentran expuestas en http://www.accv.es. Declaro, asimismo, que los datos puestos de manifiesto son ciertos.

Firma del sol.licitant — Firma i segell del Punt de Registre

Firma del solicitante — *Firma y sello del Punto de Registro*

Firmat/*Firmado*: Firmat/*Firmado:*

Nº de petició Exemplar per a la ACCV/ *Ejemplar para la ACCV*

11Anexo II – Formulario de solicitud de revocación de certificado

SOLICITUD DE REVOCACIÓ DE CERTIFICAT ***SOLICITUD DE REVOCACIÓN DE CERTIFICADO***
Data/Fecha:.....
Secció 1 – Dades del subscriptor / *Sección 2 – Datos del suscriptor* Cognoms/*Apellidos*: Nom/*Nombre*: DNI/NIF: Tel.: **Secció 2 – Dades de l'Entitat / Sección 1 – *Datos de la Entidad*** *Raó Social/Razón Social*:: CIF de l'Entitat/*CIFde la Entidad*:
Secció 2 – Identificació del certificat* / *Sección 2* – Identificación del certificado* Certificado personal: Nº de petición del certificado:
Secció 3 - Motiu de la revocació* / Sección 3 – *Motivo de la revocación** * La simple voluntad de revocación del suscriptor o del solicitante del certificado es un motivo válido para la solicitud de la misma.
Secció 4 – Autorització* / *Sección 2* – Autorización* Subscriptor del certificat *Subscriptor del certificado* *Firma* Solicitat al operador del Punt de Registre d'Usuari / Solicitado al operador de Punto de Registro de Usuario: Firma:

Exemplar per a la Agencia de Tecnología y Certificación Electrónica
Ejemplar para la Agencia de Tecnología y Certificación Electrónica

SOLICITUD DE REVOCACIÓ DE CERTIFICAT
SOLICITUD DE REVOCACIÓN DE CERTIFICADO

Data/Fecha:.....

Secció 1 – Dades del subscriptor / *Sección 2 – Datos del suscriptor*

Cognoms/*Apellidos*:

Nom/*Nombre*:

DNI/NIF: Tel.:

Secció 2 – Dades de l'Entitat / Sección 1 – *Datos de la Entidad*

Raó Social/Razón Social::

CIF de l'Entitat*/CIFde la Entidad:*

Secció 2 – Identificació del certificat* / *Sección 2* – Identificación del certificado*
Certificado personal: Nº de petición del certificado:

Secció 3 - Motiu de la revocació* / Sección 3 – *Motivo de la revocación**

* La simple voluntad de revocación del suscriptor o del solicitante del certificado es un motivo válido para la solicitud de la misma.

Secció 4 – Autorització* / *Sección 2* – Autorización*
Subscriptor del certificat
Subscriptor del certificado

Firma

Solicitat al operador del Punt de Registre d'Usuari / Solicitado al operador de Punto de Registro de Usuario:

Firma:

Exemplar per al sol·licitant / Ejemplar para el solicitante