Agencia de Tecnología y Certificación Electrónica

# Política de Certificación de Certificados Cualificados de empleado público con seudónimo en dispositivo seguro

| | |
|---|---|
| **Fecha:** 03/06/2016 | **Versión:** 2.0 |
| **Estado:** APROBADO | **Nº de páginas:** 44 |
| **OID:** 1.3.6.1.4.1.8149.3.21.2.0 | **Clasificación: PÚBLICO** |
| **Archivo:** ACCV-CP-21V2.0.doc | |
| **Preparado por: Agencia de Tecnología y Certificación Electrónica - ACCV** | |

## Tabla de Contenido

# 1 INTRODUCCIÓN

## 1.1 Presentación

El presente documento es la Política de Certificación asociada a los certificados cualificados de empleado público con seudónimo, que contiene las reglas a las que se sujeta la gestión y 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 de empleado público con seudónimo sobre dispositivo seguro, 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 empleado público con seudónimo en dispositivo seguro |
| Calificador de la política | Certificado cualificado de empleado público con seudónimo en dispositivo seguro expedido por la Agencia de Tecnología y Certificación Electrónica IVF (Pl. Napoles y Sicilia, 6. CIF Q9650010C). CPS y CP en http://www.accv.es |
| Versión de la política | 1.0 |
| Estado de la política | APROBADO |
| Referencia de la política / OID (Object Identifier) | 1.3.6.1.4.1.8149.3.21.2.0 |
| Fecha de emisión | 03 de junio de 2016 |
| Fecha de expiración | No aplicable. |
| CPS relacionada | Declaración de Prácticas de Certificación (CPS) de la ACCV. Versión 4.0.<br>OID: 1.3.6.1.4.1.8149.2.4.0<br>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

La CA que puede emitir certificados acordes con esta política es ACCVCA-130 perteneciente a la Agencia de Tecnología y Certificación Electrónica, cuya función es la emisión de certificados de

entidad final para los suscriptores de ACCV. El certificado de ACCVCV-130 es válido desde el día 14 de octubre de 2011 hasta el 1 de enero de 2027

### 1.3.2 Autoridades de Registro

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

### 1.3.3 Usuarios Finales

#### 1.3.3.1 Suscriptores

El grupo de usuarios que pueden solicitar certificados definidos por esta política está compuesto por los empleados públicos que trabajen para cualquier tipo de Administración Pública (europea, estatal, autonómica y local) así como los empleados de sus entes instrumentales, y los empleados de las Corporaciones y Universidades Públicas, que cuenten con los elementos de identificación requeridos (DNI, NIE, etc.) y a las que se les pueda asociar un seudónimo. El colectivo de usuarios formará parte de alguna entidad pública, que se encargará de la gestión de estos usuarios y de la asignación de los citados seudónimos.

El soporte de claves y certificados es tarjeta criptográfica Giesecke & Devrient (G&D) Sm@rtCafé Expert 3.2 y versiones posteriores. En caso de acreditarse otros dispositivos criptográficos serán recogidos en el presente documento, en su punto 6.1.8 Hardware/software de generación de claves

Se limita el derecho de solicitud de certificados definido en la presente Política de Certificación a personas físicas. No se aceptarán solicitudes de certificación realizadas en nombre de personas jurídicas, entidades u organizaciones.

#### 1.3.3.2 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.
- Las actos o tramitaciones que sean propios o concernientes al trabajo asociado al empleado público con seudónimo.

## 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

| | |
|---|---|
| Nombre | *Agencia de Tecnología y Certificación Electrónica IVF* |
| Dirección de email | *accv@accv.es* |
| Dirección | *Plaza Napoles y Sicilia , 6 –46003 Valencia (Spain)* |
| Número de teléfono | *+34 902 482 481* |
| Número de fax | *+34·961 971 771* |

### 1.5.2 Persona de Contacto

| | |
|---|---|
| Nombre | *Agencia de Tecnología y Certificación Electrónica IVF* |
| Dirección de email | *accv@accv.es* |
| Dirección | *Plaza Napoles y Sicilia , 6 –46003 Valencia (Spain)* |
| Número de teléfono | *+34 902 482 481* |
| Número de fax | *+34·961 971 771* |

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

La entidad competente para determinar la adecuación de esta CPS a las diferentes Políticas de Certificación de la ACCV, es la Subdirección de Entidades Financieras y Certificación Electrónica - IVF de conformidad con los Estatutos del Instituto Valenciano de Finanzas (IVF).

## 1.6 Definiciones y Acrónimos

### 1.6.1 Definiciones

No estipulado

### 1.6.2 Acrónimos

No estipulado

# 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

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

## 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 identificación de la Administración o Entidad pública se realizará en el proceso de Alta de la Entidad que será suscrito por una persona física con capacidad de representar a la Administración o Entidad pública.

### 3.2.3 Autenticación de la identidad de un individuo.

La identificación del suscriptor del certificado cualificado de empleado público con seudónimo se realizará mediante su personación ante el Operador del Punto de Registro, acreditándose mediante presentación del Documento Nacional de Identidad (DNI), pasaporte español, el Número de Identificación de Extranjeros (NIE) del solicitante o medios equivalentes aprobados según la legislación vigente.

La determinación de la condición de empleado público es responsabilidad de la Administración o Entidad pública solicitante, la cual deberá comprobar dicha condición de empleado público, bien en su base de datos, si está actualizada, o solicitando el documento por el que el suscriptor ha adquirido esa condición, si no le constare a la propia Administración o Entidad Pública solicitante.

En este tipo de certificados se incluye una dirección de correo electrónico proporcionado por Administración o Entidad Pública solicitante o por el propio suscriptor como elemento necesario para soportar operaciones de firma electrónica y cifrado de correo electrónico, pero la Agencia de

Tecnología y Certificación Electrónica no garantiza que esta dirección de correo esté vinculada con el suscriptor del certificado, por lo que la confianza en que esta dirección sea la del suscriptor del certificado corresponde únicamente a la parte confiante. La Agencia de Tecnología y Certificación Electrónica únicamente garantiza que la dirección de correo que consta en el certificado fue la aportada por la Administración o Entidad pública a la que pertenecía el suscriptor en el momento de la formalización de su solicitud.

## 3.3 Identificación y autenticación de las solicitudes de renovación del par de claves.

### 3.3.1 Identificación y autenticación de las solicitudes de renovación rutinarias.

La identificación y autenticación para la renovación del certificado se puede realizar utilizando las técnicas para la autenticación e identificación inicial (descrita en el punto 3.2.3 *Autenticación de la identidad de un individuo*, de esta Política de Certificación). La primera renovación se podrá realizar a través de la web www.accv.es utilizando los mecanismos y aplicaciones puestas a disposición de los usuarios de este tipo de certificados, identificándose para iniciar el proceso mediante el certificado original que se pretende renovar, siempre que éste no haya vencido ni se haya procedido a su revocación. Existen, por tanto, dos mecanismos alternativos para la renovación:

- Con las aplicaciones puestas a disposición de los usuarios de este tipo de certificados , disponibles en www.accv.es.
- Solicitud de un nuevo certificado por parte de la Administración o Entidad pública a la que pertenezca el suscriptor (ver apartado 3.2.3. *Autenticación de la identidad de un individuo*, de esta Política de Certificación).

Asimismo, y de conformidad con lo establecido en la legislación vigente, la renovación del certificado mediante solicitudes firmadas digitalmente exigirá que haya transcurrido un período de tiempo desde la identificación menor a los cinco años.

### 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 del par de claves

La política de identificación para las solicitudes de revocación acepta los siguientes métodos de identificación:

- Presencial. Es el mismo que para el registro inicial descrito en el punto 3.2.3. *Autenticación de la identidad de un individuo*, de esta Política de Certificación
- Telemática. Mediante la firma electrónica del formulario de revocación (ubicado en http://www.accv.es) por parte de alguna de las personas de contacto dadas de alta para la gestión de certificados de cada Administración o Entidad pública, o realizando la solicitud con la firma electrónica por parte del solicitante del certificado del formulario de revocación ubicado en el Área Personal de Servicios de Certificación (en http://www.accv.es).
- Telefónica. Mediante la respuesta a las preguntas realizadas desde el servicio de soporte telefónico disponible en el número 902482481.

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.

Deberán solicitar la revocación de los certificados las personas de contacto dadas de alta para la gestión de certificados de cada Administración o Entidad pública en cuanto el suscriptor, pierda su condición.

# 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

La solicitud de este tipo de certificados es responsabilidad de la Administración Pública o entidades de carácter público, la cual deberá comprobar la condición de empleado público de los titulares de los certificados mediante consulta a los registros de personal de la organización de su competencia.

El proceso comienza por dar de alta a la Administración, organismo o entidad, a partir de un formulario de alta de entidad, como el que se recoge en el Anexo III de esta Política de Certificación. En ese formulario deben indicarse cuáles son las personas habilitadas para la gestión de certificados con seudónimos para los empleados públicos perteneciente a la entidad en cuestión.

Para llevar a cabo la solicitud de certificados pueden emplearse dos métodos

1- El formulario del Anexo IV y remitirlo a la Agencia de Tecnología y Certificación Electrónica por parte de una de las personas habilitadas para llevar a cabo la gestión de certificados. Este documento de solicitud se deberá enviar preferentemente en formato electrónico y por correo electrónico a la cuenta gestioncerts@accv.es

2- El frontal de Administración del organismo, donde el Administrador del mismo podrá solicitar los certificados necesarios, así como las renovaciones de los ya emitidos y si fuera necesario, las revocaciones. Este frontal puede encontrarse en http://www.accv.es

Asimismo, y de conformidad con lo establecido en el art. 13.4 b) de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica en el caso de la solicitud de certificado mediante medios telemáticos se exigirá que haya transcurrido un período de tiempo desde la identificación presencial menor a los cinco años.

## 4.2 Tramitación de la solicitud de certificados.

Tras recibir la solicitud de certificados por parte de las personas habilitadas al efecto y una vez aceptada la propuesta económica si fuera el caso, se procederá a la generación de los certificados y la preparación de la documentación asociada a éstos. Una vez concluido, se remitirá a la Administración o Entidad pública solicitante, a través de las personas habilitadas para la gestión.

Las personas habilitadas para la gestión de los certificados serán las responsables de la entrega de los certificados a sus suscriptores y de remitir los contratos de certificación a la Agencia de Tecnología y Certificación Electrónica.

## 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, éste puede ser revocado.

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

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

Es tarea de la Autoridad de Registro 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.

## 4.4 Aceptación de certificados

La aceptación de los certificados por parte de los suscriptores se produce en el momento de la firma del contrato de certificación asociado a cada 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 suscriptor y por la persona adscrita al Punto de 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.

## 4.5 Uso del par de claves y del certificado.

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

## 4.6 Renovación de certificados.

Los mecanismos para la renovación se detallan en el punto 3.3 “Identificación y autenticación de las solicitudes de renovación del par de claves”

## 4.7 Renovación de claves

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.

## 4.9 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 suscriptor o del solicitante habilitado por cada entidad 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.

El Administrador del organismo puede solicitar la revocación de los certificados del organismo que administra desde el frontal de gestión disponible en http://www.accv.es

### 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 Circunstancias para la suspensión

Sólo se suspenderá un certificado si así lo dispone una autoridad judicial o administrativa, por el tiempo que la misma establezca.

ACCV no soporta la suspensión de certificados como operación independiente sobre sus certificados.

### 4.9.6 Entidad que puede solicitar la suspensión

La autoridad judicial o administrativa competente.

### 4.9.7 Procedimiento para la solicitud de suspensión

Por Resolución de la autoridad judicial o administrativa competente.

### 4.9.8 Límites del período de suspensión

El límite será el que se establezca en la Resolución de la autoridad judicial o administrativa competente.

### 4.9.9 Frecuencia de emisión de CRLs

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

### 4.9.10 Requisitos de comprobación de CRLs

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

### 4.9.11 Disponibilidad de comprobación on-line de revocación y estado

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

### 4.9.12 Requisitos de comprobación *on-line* de revocación

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

### 4.9.13 Otras formas de divulgación de información de revocación disponibles

Además de la consulta de revocados por medio de Listas de Certificados Revocados (CRL) y por medio del servicio OCSP, es posible comprobar la validez de los certificados por medio de un formulario web que, a partir de una dirección de correo electrónico, devuelve los certificados vinculados a esa dirección y el estado de éstos. Este formulario se encuentra en el sitio web de la Agencia de Tecnología y Certificación Electrónica en la URL http://www.accv.es

### 4.9.14 Requisitos de comprobación para otras formas de divulgación de información de revocación

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

### 4.9.15 Requisitos especiales de renovación de claves comprometidas

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.

## 4.11 Finalización de la suscripción.

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

ACCV informará al suscriptor, mediante correo electrónico firmado digitalmente, en un momento previo anterior a la publicación del certificado en la Lista de Certificados Revocados, acerca de la suspensión o 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.

La ACCV no realiza depósito de las claves asociadas a los certificados de empleado público con seudónimo.

## 4.13 Caducidad de las claves de certificado de CA.

La ACCV evitará generar certificados de empleado publico con seudónimos que caduquen con posterioridad a los certificados de CA. Para ello no se emitirán certificados de empleado público con seudónimo cuyo periodo de validez exceda el del certificado de CA en cuestión y se generarán con el nuevo certificado de CA, con el fin de evitar la notificación a los subscriptores para que procedan a la renovación de su certificado, en el supuesto que el certificado de CA caducara con anterioridad.

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

## 5.1 Controles de Seguridad Física

### 5.1.1 Ubicación 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
No estipulado.

## 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.

### 5.7.1 Alteración de los recursos hardware, software y/o datos
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

### 5.7.2 La clave pública de una entidad se revoca
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

### 5.7.3 La clave de una entidad se compromete
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

### 5.7.4 Instalación de seguridad después de un desastre natural u otro tipo de 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 Agencia de Tecnología y Certificación Electrónica.

### 6.1.1 Generación 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

Las claves de la raíz ACCVRAIZ1 y de la ACCVCA-130 son claves RSA de 4096 bits de longitud.

El tamaño de las claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación es de al menos 2048 bits.

### 6.1.6 Parámetros de generación de la clave pública

Las claves de la raíz ACCVRAIZ1 y de la ACCVCA-130 están creadas con el algoritmo RSA

Se utilizan los parámetros definidos en la suite criptográfica 001 especificada en el documento de ETSI TS 102 176-1 “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signature”. Se define ModLen=2048.

| Signature suite entry name | Signature algorithm | Signature algorithm parameters | Key generation algorithm | Padding method | Cryptographic hash function |
|---|---|---|---|---|---|
| Sha-256-with-rsa | rsa | MinModLen=2048 | rsagen1 | emsa-pkcs1-v1_5 | sha256 |

### 6.1.7 Comprobación de la calidad de los parámetros

Se utilizan los parámetros definidos en la suite criptográfica 001 especificada en el documento de ETSI TS 102 176-1 "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signature". Se define ModLen=2048.

| Signature suite entry name | Signature algorithm | Signature algorithm parameters | Key generation algorithm | Padding method | Cryptographic hash function |
|---|---|---|---|---|---|
| Sha-256-with-rsa | rsa | MinModLen=2048 | rsagen1 | emsa-pkcs1-v1_5 | sha256 |

### 6.1.8 Hardware/software de generación de claves

La generación de las claves se realiza en tarjeta criptográfica, por el chip criptográfico de la misma.

Las tarjetas certificadas para dar soporte a este tipo de certificados son las siguientes:

•Tarjetas G&D:

- Giesecke & Devrient (G&D) SmartCafe Expert 3.2 72K FIPS 140-2 Level 2

### 6.1.9 Fines del uso del par de claves

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 y listas de certificados revocados*".

## 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.

### 6.2.1 Estándares para los módulos criptográficos

Las tarjetas criptográficas empleadas en la emisión de los certificados adscritos a esta Política de Certificación disponen de certificación ITSEC E4 high y soportan los estándares PKCS#11 y CSP.

### 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 firma, autenticación ni cifrado 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 firma, autenticación y cifrado de los suscriptores de los certificados definidos por la presente política, por lo que no es aplicable.

### 6.2.5 Archivo de la clave privada.

No se archivan las claves privadas.

### 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 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.

### 6.2.8 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.

### 6.2.9 Método de destrucción de la clave privada

No estipulado.

## 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.

La clave utilizada para la emisión de los certificados se crea para cada emisión, y por tanto también tienen una validez de tres (3) años.

El certificado de “ACCVCA-130” es válido desde el día 14 de octubre de 2011 hasta el 1 de enero de 2027..

## 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 smartcard que la contiene y que se proporciona al suscriptor del certificado con el mismo.

La generación del PIN de la smartcard 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 estipulado.

## 6.5 Controles 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.

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 Controles de Ingeniería de los Módulos Criptográficos

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

# 7 Perfiles de certificados y listas de certificados revocados

## 7.1 Perfil de Certificado

### 7.1.1 Número de versión

Esta política de certificación especifica el uso de un certificado con tres usos distintos; firma digital, autenticación del suscriptor y cifrado de datos.

### 7.1.2 Extensiones del certificado

Las extensiones utilizadas por los certificados emitidos bajo el amparo de la presente política son:

| **Campo** | **Valor** |
|---|---|
| ***Subject*** | |
| CommonName | Cadena compuesta de la forma:<br>"SEUDONIMO - " + Seudónimo + " - " + Nombre del organismo |
| OrganizationIdentifier<br>(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 |
| Title | Puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad pública o privada |
| PSEUDONYM | Seudónimo |
| OrganizationalUnit | Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado |
| OrganizationalUnit | Cadena fija con el valor<br>"CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO" |
| Organization | Denominación (nombre "oficial") de la Administración, organismo o entidad pública o privada suscriptora del certificado, a la que se encuentra vinculada el empleado |
| Country | Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas (ES) |
| ***Version*** | V3 |
| ***SerialNumber*** | Identificador único del certificado. Menor de 32 caracteres hexadecimales. |
| ***Algoritmo de firma*** | sha256withRSAEncryption |
| ***Issuer (Emisor)*** | |
| CommonName | ACCVCA-130 |
| OrganizationalUnit | PKIACCV |
| Organization | ACCV |
| Country | ES |
| ***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 |
| | Email Protection |
| ***CRL Distribution Point*** | http://www.accv.es/fileadmin/Archivos/certificados/accvca130_der.crl |
| ***SubjectAlternativeName*** | |
| RFC822Name | Correo electrónico del suscriptor. Puede ser genérico de la entidad o relativo al seudónimo. |
| DirectoryName | |
| | Identidad Administrativa (se desarrolla en el punto 7.1.5) |
| ***Certificate Policy Extensions*** | |
| Policy OID | 2.16.724.1.3.5.4.2 |
| Policy Notice | Certificado de empleado público con seudónimo de nivel medio |
| | |
| 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;<br>Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2) |
| | |
| Policy OID | 1.3.6.1.4.1.8149.3.6.21.2.0 |
| Policy CPS Location | http://www.accv.es/legislacion_c.htm* |
| Policy Notice | Certificado Cualificado de empleado público con seudónimo en dispositivo seguro expedido por la Agencia de Tecnología y Certificación Electrónica (Pl. Cánovas del Castillo, 1. CIF Q4601156E). CPS y CP en http://www.accv.es) |
| ***Authority Information Access*** | |
| *Access Method* | Id-ad-ocsp |
| *Access Location* | http://ocsp.accv.es |
| *Access Method* | Id-ad-calssuers |
| *Access Location* | http://www.accv.es/gestcert/ACCVCA130SHA2.cacert.crt |
| ***Fingerprint issuer*** | 28 97 f9 b6 52 9c 6a af b4 3c 32 ff c6 25 e1 f6 49 40 1c 2c<br>00 55 b7 7f 43 2b 54 24 54 06 06 8c c8 f7 78 05 c3 25 dc f5 |
| ***Algoritmo de hash*** | SHA-256 |
| ***KeyUsage (críticos)*** | |
| | Digital Signature<br>Content Commintment<br>Key Encipherment |

| QcStatement | Campos QC (Qualified Certificate) | |
|---|---|---|
| QcCompliance | | El certificado es cualificado |
| QcType | eSign | Tipo particular de certificado cualificado |
| QcRetentionPeriod | 15y | Periodo de retención de la información material |
| QcPDS | http://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-V1.0-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:

- a) SHA1withRSA (1.2.840.113549.1.1.5)
- b) SHA256withRSA (1.2.840.113549.1.1.11)

### 7.1.4 Formatos 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.

El campo cn del subject name se cumplimenta obligatoriamente en mayúsculas, prescindiendo de acentos y sustituyendo la letra “Ñ” por la “N” y la letra “Ç” por la “C”. Esta característica se da únicamente en el atributo CommonName.

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 Identidad Administrativa

A efectos de garantizar la interoperabilidad entre las distintas AAPP se crea en el campo SubjectAlternativeName dentro del objeto DirectoryName la siguiente estructura de datos de Identidad Administrativa.

| Campo | Contenido | Observaciones |
|---|---|---|
| Tipo de Certificado | Indica la naturaleza del certificado | Tipo= CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (de nivel medio)<br>OID.2.16.724.1.3.5.4.2.1 |
| Nombre de la entidad suscriptora | La entidad propietaria de dicho certificado | Entidad Suscriptora = ie: ACCV<br>OID.2.16.724.1.3.5.4.2.2 |
| NIF entidad suscriptora | Número de identificación de la entidad | NIF entidad suscriptora ie: S-2833002 |

| | | |
|---|---|---|
| | | OID.2.16.724.1.3.5.4.2.3 |
| Correo electrónico | Correo electrónico del responsable del certificado | Correo electrónico de la persona responsable del certificado ie: jseudonimo@unknown.esOID.2.16.724.1.3.5.4.2.9 |
| Unidad organizativa | Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado | Unidad = ie: AGENCIA DE TECNOLOGÍA Y CERTIFICACION ELECTRONICA<br>OID.2.16.724.1.3.5.4.2.10 |
| Puesto o cargo | Puesto desempeñado por el suscriptor del certificado dentro de la administración | Puesto = ie: ANALISTA PROGRAMADOR<br>OID.2.16.724.1.3.5.4.2.11 |
| Seudónimo | Seudónimo | Seudonimo= p. ej: NIP1111<br>O.I.D 2.16.724.1.3.5.4.2.12 |

Se han utilizado los OIDs asociados a los campos sugeridos por el Ministerio de Administraciones Públicas para garantizar la interoperabilidad.

### 7.1.6 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.

### 7.1.7 Identificador de objeto (OID) de la Política de Certificación

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

1.3.6.1.4.1.8149.3.21.2.0

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.

**2.16.724.1.3.5.4.2** **Certificado de empleado público con seudónimo de nivel medio**

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**

### 7.1.8 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.

### 7.1.9 Sintaxis y semántica de los cualificadores de política

No estipulado

### 7.1.10 Tratamiento semántico para la extensión critica “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

### 7.2.1 Número de versión

El formato de las CRLs utilizadas en la presente política es el especificado en la versión 2 (X509 v2).

### 7.2.2 CRL y extensiones

La presente Política de Certificación soporta y utiliza CRLs conformes al estándar X.509.

## 7.3 7.3 Listas de Certificados Revocados

### 7.3.1 7.3.1 Límite Temporal de los certificados en las CRLs

Los números de serie de los certificados revocados se mantienen siempre en la CRL.

# 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

El acceso a los certificados emitidos bajo esta política, dada su naturaleza pública, es libre y gratuito y por tanto no hay ninguna tarifa de aplicación sobre el mismo.

### 9.1.3 Tarifas de acceso a la información de estado o revocación

El acceso a la información de estado o revocación de los certificados es libre y gratuita y por tanto no se aplicará ninguna tarifa.

### 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

No se prevén reintegros de las cantidades entregadas para el pago de este tipo de certificados.

## 9.2 Capacidad financiera

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

Tal y como se especifica en la Declaración de Prácticas de Certificación (CPS), la ACCV dispone de garantía de cobertura suficiente de responsabilidad civil a través de aval bancario por importe de tres Millones de Euros (3.000.000 €) que cubre el riesgo de la responsabilidad por los daños y perjuicios que pudiera ocasionar el uso de los certificados expedidos por esta Agencia, cumpliendo así con la obligación establecida en el artículo 20.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

### 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.

No obstante no existen límites económicos asociados a las transacciones que se realicen con este tipo de certificados por parte de los suscriptores.

### 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.

## 9.9 Plazo y finalización.

### 9.9.1 Plazo.

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

### 9.9.2 Finalización.

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

### 9.9.3 Supervivencia.

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

## 9.10 Notificaciones.

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

Todos los correos que la ACCV envíe a los suscriptores de los certificados emitidos bajo esta Política de Certificación, en el ejercicio de la prestación del servicio de certificación, serán firmados digitalmente para garantizar su autenticidad e integridad.

## 9.11 Modificaciones.

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

### 9.11.1 Procedimientos de especificación de cambios

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

### 9.11.2 Procedimientos de publicación y notificación.

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

### 9.11.3 Procedimientos de aprobación de la Declaración de Prácticas de Certificación

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

## 9.12 Resolución de conflictos.

### 9.12.1 Resolución extrajudicial de conflictos.

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

### 9.12.2 Jurisdicción competente.

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

## 9.13 Legislación aplicable

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

## 9.14 Conformidad con la Ley aplicable.

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

## 9.15 Cláusulas diversas.

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

# 10 Anexo I

## CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.21

**Secció 1 – Dades del subscriptor / *Sección 1 – Datos del suscriptor***
Cognoms/*Apellidos*:
Nom/*Nombre*:
DNI/NIF: Tel.:
Seudónimo / Número de Identificación:
Càrrec/Puesto o cargo:
Unitat Organitzativa-Departament/Unidad Organizativa-Departamento:
Administració-Organització/Administración-Organización:
CIF de la Organització/CIF de la Organización:

Adreça de correu electrònic/*Dirección correo electrónico*:

Adreça postal/Dirección postal:

Població/Población: Província/Provincia:

PIN : PUK: Tel. suport/ tel. soporte **902 482 481** **www.accv.es**

**Secció 2 – Dades del operador del Punt de Registre / *Sección 2 – Datos del operador del Punto de Registro de Usuario***
Nom i cognoms/*Nombre y Apellidos*:

**Secció 3 - Data i Firma / Sección 3 – *Fecha y Firma***
Subscric el present contracte de certificació associat a la Política de Certificació de Certificats qualificats d'empleat públic amb Seudonim amb codi 1.3.6.1.4.1.8149.3.21, 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 Cualificados de empleado público con Seudónimo con código 1.3.6.1.4.1.8149.3.21, emitido por 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 subscriptor
*Firma del suscriptor*

Firma i segell del Punt de Registre
*Firma y sello del Punto de Registro*

Firmat/*Firmado*:

Firmat/*Firmado:*

Exemplar per al subscriptor - Anvers / *Ejemplar para el suscriptor - Anverso*

## CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.21
## Condiciones de utilización de los certificados

1.Los certificados asociados a la Política de Certificación para Certificados Cualificados de empleado público con Seudónimo, emitidos por la ACCV son del tipo X.509v3 y se rigen por la Declaración de Prácticas de Certificación de la ACCV, 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 suscriptores de los certificados deberán ser personas físicas, en posesión de un NIF, un NIE u otro documento de identificación válido en Derecho, y deben estar empleados en una Administración Pública, Ente Instrumental de la Administración o Entidad Corporativa pública.

3.El solicitante de los certificados, especialmente habilitado para la gestión de éstos por parte de una Administración o Entidad pública determinada, 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 suscriptor 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 suscriptor 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.

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 ACCV 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 y por fallecimiento del suscriptor del certificado. Otras condiciones para la pérdida de eficacia se recogen en la Declaración de Prácticas de Certificación y en la Política de Certificación asociada a este tipo de certificados.

10.La documentación a aportar para la identificación de los solicitantes será el Documento Nacional de Identidad, NIE o Pasaporte válido y vigente.

11.. El cumplimiento de la ley 15/1.999, de 13 de diciembre, de Protección de Datos de Carácter Personal, 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. La finalidad de dicho fichero es la 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 o cancelación 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 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.

15.La Agencia de Tecnología y Certificación Electrónica ha constituido un aval bancario por un importe de tres millones de euros (3.000.000,00 €) para afrontar el riesgo por la responsabilidad por los daños y perjuicios que pudiera ocasionar el uso de los certificados expedidos y los servicios de certificación digital.

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 1.3.6.1.4.1.8149.3.21

**Secció 1 – Dades del subscriptor / *Sección 1 – Datos del suscriptor***
Cognoms/*Apellidos*:
Nom/*Nombre*:
DNI/NIF: Tel.:
Seudónimo / Número de Identificación:
Càrrec/Puesto o cargo:
Unitat Organitzativa-Departament/Unidad Organizativa-Departamento:
Administració-Organització/Administración-Organización:
CIF de la Organització/CIF de la Organización:
Adreça de correu electrònic/*Dirección correo electrónico*:

Adreça postal/Dirección postal:

Població/Población: Província/Provincia:

**Secció 2 – Dades del operador del Punt de Registre / *Sección 2 – Datos del operador del Punto de Registro de Usuario***
Nom i cognoms/*Nombre y Apellidos*:

**Secció 3 - Data i Firma / Sección 3 – *Fecha y Firma***
Subscric el present contracte de certificació associat a la Política de Certificació de Certificats qualificats d'empleat públic amb Seudonim amb codi 1.3.6.1.4.1.8149.3.21, 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 Cualificados de empleado público con Seudónimo con código 1.3.6.1.4.1.8149.3.21, emitido por 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 subscriptor
*Firma del suscriptor*

Firma i segell del Punt de Registre
*Firma y sello del Punto de Registro*

Firmat/*Firmado*:

Firmat/*Firmado:*

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

# 11 Anexo II – Formulario de solicitud de revocación de certificado

**SOLICITUD DE REVOCACIÓ DE CERTIFICAT**
***SOLICITUD DE REVOCACIÓN DE CERTIFICADO***

V3.0

Fecha:.....

**Secció 1 – Dades del subscriptor del certificat / *Sección 1 – Datos del subscriptor del certificado***
Cognoms/*Apellidos*:
Nom/*Nombre*:
DNI/NIF:
Seudónimo / Número de Identificación:
Administració-Organització/Administración-Organización:
CIF de la Organització/CIF de la Organización:

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

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

* La simple voluntad de revocación del suscriptor 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 l'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*

V3.0

Fecha:.....

**Secció 1 – Dades del subscriptor del certificat / *Sección 1 – Datos del subscriptor del certificado***

Cognoms/*Apellidos*:
Nom/*Nombre*:
DNI/NIF:
Seudónimo / Número de Identificación:
Administració-Organització/Administración-Organización:
CIF de la Organització/CIF de la Organización:

**Secció 2 – Identificació del certificat* / *Sección 2* – Identificación del certificado***

Certificat personal/ Certificado personal:

Nº de petició del certificat/ Nº de petición del certificado:

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

* La simple voluntad de revocación del suscriptor 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*

# 12 Anexo III – Formulario de solicitud de alta de entidad

Agencia de Tecnología y Certificación Electrónica

## ALTA ORGANITZACIÓ / *ALTA ORGANIZACIÓN*

### A DADES DE LA ORGANITZACIÓ / *DATOS DE LA ORGANIZACIÓN*

| NOM DE L'ORGANISME / *NOMBRE DEL ORGANISMO* | | | CIF |
|---|---|---|---|
| NOM DEL DEPARTAMENT / *NOMBRE DEL DEPARTAMENTO* | | | |
| ADREÇA FISCAL / *DOMICILIO FISCAL* | | | CP |
| LOCALITAT / *LOCALIDAD* | PROVINCIA / *PROVINCIA* | TELÈFON / *TELEFONO* | FAX |
| ADREÇA ELECTRÒNICA / *CORREO ELECTRÓNICO* | | | |

### B DADES DEL PERSONAL RESPONSABLE / *DATOS DEL PERSONAL RESPONSABLE*

Persones responsables per a la petició dels certificats reconeguts de Pseudònim. Estes persones s'encarregaran de la sol·licitud d'alta i revocació dels certificats reconeguts de Pseudónim. A més, estes persones es comprometen a informar els usuaris de les seues obligacions i responsabilitats.

/ Personas responsables para la petición de los certificados reconocidos de Seudónimo. Estas personas se encargaran de la solicitud de alta y revocación de los certificados reconocidos de Seudónimo. Además, estas personas se comprometen a informar a los usuarios de sus obligaciones y responsabilidades.

| NOM / *NOMBRE* | COGNOMS / *APELLIDOS* | NIF / NIE | ADREÇA ELECTRÒNICA / *CORREO ELECTRÓNICO* | CÀRREC / CARGO |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

### C MOTIU DE LA PETICIÓ / *MOTIVO DE LA PETICIÓN*

☐ Creació inicial / *Creación inicial.*

☐ Modificació de dades / *Modificación de datos.*

_____, ____ d _____ de _____

Firma del declarant / *Firma del declarante*

Firma del responsable de l'ACCV / *Firma del responsable de la ACCV*

Firma: _____ Firma: _____

**EXEMPLAR PER A L'ORGANISME / EJEMPLAR PARA EL ORGANISMO**

# 13 Anexo IV – Formulario de solicitud de certificados

Agencia de Tecnología y Certificación Electrónica

**SOL·LICITUD DE CERTIFICATS / SOLICITUD DE CERTIFICADOS**

D'acord amb la Política de Certificació de Certificats Reconeguts de Pseudònim, es requereixen les següents dades per a la correcta emissió de certificats.
*De acuerdo con la Política de Certificación de Certificados Reconocidos de Seudónimo, se requieren los siguientes datos para la correcta emisión de certificados.*

**DADES COMUNES / DATOS COMUNES**
NOM DE L'ORGANISME / NOMBRE DEL ORGANISMO:
CIF:
Domicilio:
Localidad:

**DADES DEL PERSONAL / DATOS DEL PERSONAL** (los campos con * son opcionales)
NIF/NIE Cognom1/Apellido1 Cognom2/Apellido2 Nom/Nombre Adreça electrònica/Correo electrónico Càrrec/Cargo* Unitat/Unidad* Pseudònim/Seudónimo*