



Agencia de Tecnología y Certificación Electrónica

Política de Certificación de Certificados de Aplicación

Fecha: 12/10/2023	Versión: 5.0.1
Estado: APROBADO	Nº de páginas: 39
OID: 1.3.6.1.4.1.8149.3.5.5.0	Clasificación: PÚBLICO
Archivo: ACCV-CP-05V5.0.1-ES-2023.odt	
Preparado por: Agencia de Tecnología y Certificación Electrónica	

Documento provisional. Los procesos aquí descritos no serán de aplicación hasta la obtención de la acreditación por parte del Organismo de Supervisión

Cambios

Versión	Autor	Fecha	Observaciones
4.0.1	ACCV	03/05/2018	Cambios de adaptación RFC3647
4.0.2	ACCV	10/03/2020	Cambios de adaptación RFC3647
4.0.3	ACCV	20/03/2021	Policy Notice
4.0.4	ACCV	31/08/2023	Se elimina el ECU SMIME
5.0.1	ACCV	12/10/2023	Nueva jerarquía

Tabla de Contenido

1 INTRODUCCIÓN.....	8
1.1 PRESENTACIÓN.....	8
1.2 IDENTIFICACIÓN.....	8
1.3 COMUNIDAD DE USUARIOS Y ÁMBITO DE APLICACIÓN.....	8
1.3.1 Autoridades de Certificación.....	8
1.3.2 Autoridades de Registro.....	9
1.3.3 Suscriptores.....	9
1.3.4 Partes confiantes.....	9
1.3.5 Otros participantes.....	9
1.4 USO DE LOS CERTIFICADOS.....	9
1.4.1 Usos Permitidos.....	9
1.4.2 Usos prohibidos.....	9
1.5 POLÍTICA DE ADMINISTRACIÓN DE LA ACCV.....	9
1.5.1 Especificación de la Organización Administradora.....	9
1.5.2 Persona de Contacto.....	9
1.5.3 Competencia para determinar la adecuación de la CPS a la Políticas.....	10
1.5.4 Procedimiento de aprobación.....	10
1.6 DEFINICIONES Y ACRÓNIMOS.....	10
1.6.1 Definiciones.....	10
1.6.2 Acrónimos.....	10
2 PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS.....	11
2.1 REPOSITORIO DE CERTIFICADOS.....	11
2.2 PUBLICACIÓN.....	11
2.3 FRECUENCIA DE ACTUALIZACIONES.....	11
2.4 CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS.....	11
3 IDENTIFICACIÓN Y AUTENTICACIÓN.....	12
3.1 REGISTRO DE NOMBRES.....	12
3.1.1 Tipos de nombres.....	12
3.1.2 Significado de los nombres.....	12
3.1.3 Interpretación de formatos de nombres.....	12
3.1.4 Unicidad de los nombres.....	12
3.1.5 Resolución de conflictos relativos a nombres.....	12
3.1.6 Reconocimiento, autenticación y función de las marcas registradas.....	12
3.2 VALIDACIÓN INICIAL DE LA IDENTIDAD.....	12
3.2.1 Métodos de prueba de posesión de la clave privada.....	12
3.2.2 Autenticación de la identidad de una organización.....	12
3.2.3 Autenticación de la identidad de un individuo.....	12
3.2.4 Información no verificada de los suscriptores.....	13
3.2.5 Validación de la representación.....	13
3.2.6 Criterios para la interoperación.....	13
3.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DEL PAR DE CLAVES.....	13
3.3.1 Identificación y autenticación de las solicitudes de renovación rutinarias.....	13
3.3.2 Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida.....	13
3.4 IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DEL PAR DE CLAVES.....	13
4 EL CICLO DE VIDA DE LOS CERTIFICADOS.....	14
4.1 SOLICITUD DE CERTIFICADOS.....	14
4.1.1 Legitimación de la solicitud.....	14
4.1.2 Procedimiento de alta y responsabilidades.....	14
4.2 TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADOS.....	14
4.2.1 Ejecución de las funciones de identificación y autenticación.....	14



4.2.2	Aprobación o rechazo de la solicitud.....	14
4.2.3	Plazo para resolver la solicitud.....	14
4.3	EMISIÓN DE CERTIFICADOS.....	15
4.3.1	Acciones de la CA durante el proceso de emisión.....	15
4.3.2	Notificación de la emisión al suscriptor.....	15
4.4	ACEPTACIÓN DE CERTIFICADOS.....	15
4.4.1	Conducta que constituye aceptación del certificado.....	15
4.4.2	Publicación del certificado por la CA.....	15
4.4.3	Notificación de la emisión a terceros.....	16
4.5	USO DEL PAR DE CLAVES Y DEL CERTIFICADO.....	16
4.5.1	Uso del certificado y la clave privada del suscriptor.....	16
4.5.2	Uso de la clave pública y del certificado por la parte que confía.....	16
4.6	RENOVACIÓN DE CERTIFICADOS.....	16
4.6.1	Circunstancia para la renovación del certificado.....	16
4.6.2	Quién puede solicitar renovación.....	16
4.6.3	Procesamiento de solicitudes de renovación de certificados.....	16
4.6.4	Notificación de nueva emisión de certificado al suscriptor.....	16
4.6.5	Conducta que constituye la aceptación de un certificado de renovación.....	16
4.6.6	Publicación del certificado de renovación por la CA.....	16
4.6.7	Notificación de emisión de certificado por la CA a otras entidades.....	16
4.7	RENOVACIÓN DE CLAVES.....	16
4.7.1	Circunstancia para la renovación de claves (re-key) certificado.....	16
4.7.2	Quién puede solicitar la certificación de una nueva clave pública.....	17
4.7.3	Procesamiento de solicitudes de cambio de claves del certificado.....	17
4.7.4	Notificación de nueva emisión de certificado al suscriptor.....	17
4.7.5	Conducta que constituye la aceptación de un certificado con nuevas claves (re-keyed).....	17
4.7.6	Publicación del certificado con renovación de claves (re-keyed) por la CA.....	17
4.7.7	Notificación de emisión de certificado por la CA a otras entidades.....	17
4.8	MODIFICACIÓN DE CERTIFICADOS.....	17
4.8.1	Circunstancia para la modificación del certificado.....	17
4.8.2	Quién puede solicitar la modificación del certificado.....	17
4.8.3	Procesamiento de solicitudes de modificación de certificados.....	17
4.8.4	Notificación de nueva emisión de certificado al suscriptor.....	17
4.8.5	Conducta que constituye la aceptación de un certificado modificado.....	17
4.8.6	Publicación del certificado modificado por la CA.....	17
4.8.7	Notificación de emisión de certificado por la CA a otras entidades.....	17
4.9	REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.....	18
4.9.1	Circunstancias para la revocación.....	18
4.9.2	Entidad que puede solicitar la revocación.....	18
4.9.3	Procedimiento de solicitud de revocación.....	18
4.9.3.1	Telemático.....	18
4.9.3.2	Telefónico.....	18
4.9.4	Periodo de gracia de la solicitud de revocación.....	18
4.9.5	Tiempo dentro del cual CA debe procesar la solicitud de revocación.....	18
4.9.6	Requisitos de comprobación de CRLs.....	18
4.9.7	Frecuencia de emisión de CRLs.....	18
4.9.8	Máxima latencia de CRL.....	18
4.9.9	Disponibilidad de comprobación on-line de la revocación.....	18
4.9.10	Requisitos de la comprobación on-line de la revocación.....	18
4.9.11	Otras formas de divulgación de información de revocación disponibles.....	18
4.9.12	Requisitos especiales de revocación por compromiso de las claves.....	19
4.9.13	Circunstancias para la suspensión.....	19
4.9.14	Entidad que puede solicitar la suspensión.....	19
4.9.15	Procedimiento para la solicitud de suspensión.....	19
4.9.16	Límites del periodo de suspensión.....	19
4.10	SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS.....	19
4.10.1	Características operacionales.....	19
4.10.2	Disponibilidad del servicio.....	19
4.10.3	Características opcionales.....	19
4.11	FINALIZACIÓN DE LA SUSCRIPCIÓN.....	19

4.12	DEPÓSITO Y RECUPERACIÓN DE CLAVES.....	19
4.12.1	<i>Política y prácticas clave de custodia y recuperación.....</i>	19
4.12.2	<i>Política y prácticas de encapsulado y recuperación de claves de sesión.....</i>	20
5	CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES.....	21
5.1	CONTROLES DE SEGURIDAD FÍSICA.....	21
5.1.1	<i>Ubicación y construcción.....</i>	21
5.1.2	<i>Acceso físico.....</i>	21
5.1.3	<i>Alimentación eléctrica y aire acondicionado.....</i>	21
5.1.4	<i>Exposición al agua.....</i>	21
5.1.5	<i>Protección y prevención de incendios.....</i>	21
5.1.6	<i>Sistema de almacenamiento.....</i>	21
5.1.7	<i>Eliminación de residuos.....</i>	21
5.1.8	<i>Backup remoto.....</i>	21
5.2	CONTROLES DE PROCEDIMIENTOS.....	21
5.2.1	<i>Papeles de confianza.....</i>	21
5.2.2	<i>Número de personas requeridas por tarea.....</i>	21
5.2.3	<i>Identificación y autenticación para cada papel.....</i>	21
5.2.4	<i>Roles que requieren separación de tareas.....</i>	22
5.3	CONTROLES DE SEGURIDAD DE PERSONAL.....	22
5.3.1	<i>Requerimientos de antecedentes, calificación, experiencia, y acreditación.....</i>	22
5.3.2	<i>Procedimientos de comprobación de antecedentes.....</i>	22
5.3.3	<i>Requerimientos de formación.....</i>	22
5.3.4	<i>Requerimientos y frecuencia de actualización de la formación.....</i>	22
5.3.5	<i>Frecuencia y secuencia de rotación de tareas.....</i>	22
5.3.6	<i>Sanciones por acciones no autorizadas.....</i>	22
5.3.7	<i>Requerimientos de contratación de personal.....</i>	22
5.3.8	<i>Documentación proporcionada al personal.....</i>	22
5.3.9	<i>Controles periódicos de cumplimiento.....</i>	22
5.3.10	<i>Finalización de los contratos.....</i>	22
5.4	PROCEDIMIENTOS DE CONTROL DE SEGURIDAD.....	22
5.4.1	<i>Tipos de eventos registrados.....</i>	22
5.4.2	<i>Frecuencia de procesado de logs.....</i>	23
5.4.3	<i>Periodo de retención para los logs de auditoría.....</i>	23
5.4.4	<i>Protección de los logs de auditoría.....</i>	23
5.4.5	<i>Procedimientos de backup de los logs de auditoría.....</i>	23
5.4.6	<i>Sistema de recogida de información de auditoría (interno vs externo).....</i>	23
5.4.7	<i>Notificación al sujeto causa del evento.....</i>	23
5.4.8	<i>Análisis de vulnerabilidades.....</i>	23
5.5	ARCHIVO DE INFORMACIONES Y REGISTROS.....	23
5.5.1	<i>Tipo de informaciones y eventos registrados.....</i>	23
5.5.2	<i>Periodo de retención para el archivo.....</i>	23
5.5.3	<i>Protección del archivo.....</i>	23
5.5.4	<i>Procedimientos de backup del archivo.....</i>	23
5.5.5	<i>Requerimientos para el sellado de tiempo de los registros.....</i>	23
5.5.6	<i>Sistema de recogida de información de auditoría (interno vs externo).....</i>	23
5.5.7	<i>Procedimientos para obtener y verificar información archivada.....</i>	23
5.6	CAMBIO DE CLAVE.....	24
5.7	RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O DE DESASTRE.....	24
5.7.1	<i>Procedimientos de gestión de incidencias y compromisos.....</i>	24
5.7.2	<i>Corrupción de recursos, aplicaciones o datos.....</i>	24
5.7.3	<i>Compromiso de la clave privada de la entidad.....</i>	24
5.7.4	<i>Continuidad del negocio después de un desastre.....</i>	24
5.8	CESE DE UNA CA.....	24
6	CONTROLES DE SEGURIDAD TÉCNICA.....	25
6.1	GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES.....	25
6.1.1	<i>Generación del par de claves.....</i>	25
6.1.2	<i>Entrega de la clave privada a la entidad.....</i>	25

6.1.3	Entrega de la clave pública al emisor del certificado.....	25
6.1.4	Entrega de la clave pública de la CA a los usuarios.....	25
6.1.5	Tamaño de las claves.....	25
6.1.6	Parámetros de generación de la clave pública.....	25
6.1.7	Propósitos de uso de claves.....	25
6.2	PROTECCIÓN DE LA CLAVE PRIVADA.....	26
6.2.1	Estándares para los módulos criptográficos.....	26
6.2.2	Control multipersona de la clave privada.....	26
6.2.3	Custodia de la clave privada.....	26
6.2.4	Copia de seguridad de la clave privada.....	26
6.2.5	Archivo de la clave privada.....	26
6.2.6	Introducción de la clave privada en el módulo criptográfico.....	26
6.2.7	Almacenamiento de clave privada en el módulo criptográfico.....	26
6.2.8	Método de activación de la clave privada.....	26
6.2.9	Método de desactivación de la clave privada.....	26
6.2.10	Método de destrucción de la clave privada.....	26
6.2.11	Calificación del módulo criptográfico.....	27
6.3	OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES.....	27
6.3.1	Archivo de la clave pública.....	27
6.3.2	Periodo de uso para las claves públicas y privadas.....	27
6.4	DATOS DE ACTIVACIÓN.....	27
6.4.1	Generación y activación de los datos de activación.....	27
6.4.2	Protección de los datos de activación.....	27
6.4.3	Otros aspectos de los datos de activación.....	27
6.5	CONTROLES DE SEGURIDAD INFORMÁTICA.....	27
6.5.1	Requerimientos técnicos de seguridad informática específicos.....	27
6.5.2	Valoración de la seguridad informática.....	27
6.6	CONTROLES DE SEGURIDAD DEL CICLO DE VIDA.....	27
6.6.1	Controles de desarrollo del sistema.....	27
6.6.2	Controles de gestión de la seguridad.....	27
6.6.3	Evaluación de la seguridad del ciclo de vida.....	28
6.7	CONTROLES DE SEGURIDAD DE LA RED.....	28
6.8	TIMESTAMPING.....	28
7	PERFILES DE CERTIFICADOS, CRL Y OCSP.....	29
7.1	PERFIL DE CERTIFICADO.....	29
7.1.1	Número de versión.....	29
7.1.2	Extensiones del certificado.....	29
7.1.3	Identificadores de objeto (OID) de los algoritmos.....	30
7.1.4	Formatos de nombres.....	30
7.1.5	Restricciones de los nombres.....	31
7.1.6	Identificador de objeto (OID) de la Política de Certificación.....	31
7.1.7	Uso de la extensión “Policy Constraints”.....	31
7.1.8	Sintaxis y semántica de los cualificadores de política.....	31
7.1.9	Tratamiento semántico para la extensión “Certificate Policy”.....	31
7.2	PERFIL DE CRL.....	31
7.2.1	Número de versión.....	31
7.2.2	CRL y extensiones.....	31
7.3	PERFIL DE OCSP.....	31
7.3.1	Número de versión.....	31
7.3.2	Extensiones.....	31
8	AUDITORÍA DE CONFORMIDAD.....	32
8.1	FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD PARA CADA ENTIDAD.....	32
8.2	IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR.....	32
8.3	RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA.....	32
8.4	TÓPICOS CUBIERTOS POR EL CONTROL DE CONFORMIDAD.....	32
8.5	ACCIONES A TOMAR COMO RESULTADO DE UNA DEFICIENCIA.....	32
8.6	COMUNICACIÓN DE RESULTADOS.....	32

8.7 AUTO AUDITORIAS.....	32
9 REQUISITOS COMERCIALES Y LEGALES.....	33
9.1 TARIFAS.....	33
9.1.1 Tarifas de emisión de certificado o renovación.....	33
9.1.2 Tarifas de acceso a los certificados.....	33
9.1.3 Tarifas de acceso a la información de estado o revocación.....	33
9.1.4 Tarifas de otros servicios como información de políticas.....	33
9.1.5 Política de reintegros.....	33
9.2 CAPACIDAD FINANCIERA.....	33
9.2.1 Cobertura del Seguro.....	33
9.2.2 Otros activos.....	33
9.2.3 Seguro o cobertura de garantía para entidades finales.....	33
9.3 POLÍTICA DE CONFIDENCIALIDAD.....	33
9.3.1 Información confidencial.....	33
9.3.2 Información no confidencial.....	33
9.3.3 Divulgación de información de revocación /suspensión de certificados.....	34
9.4 PROTECCIÓN DE DATOS PERSONALES.....	34
9.4.1 Plan de privacidad.....	34
9.4.2 Información considerada privada.....	34
9.4.3 Información no considerada privada.....	34
9.4.4 Responsabilidad de proteger la información privada.....	34
9.4.5 Aviso y consentimiento para usar información privada.....	34
9.4.6 Comunicación de la información a autoridades administrativas y/o judiciales.....	34
9.4.7 Otros supuestos de divulgación de la información.....	34
9.5 DERECHOS DE PROPIEDAD INTELECTUAL.....	34
9.6 OBLIGACIONES Y RESPONSABILIDAD CIVIL.....	34
9.6.1 Obligaciones de la Entidad de Certificación.....	34
9.6.2 Obligaciones de la Autoridad de Registro.....	34
9.6.3 Obligaciones de los suscriptores.....	34
9.6.4 Obligación y responsabilidad de terceras partes.....	35
9.6.5 Obligación y responsabilidad de otros participantes.....	35
9.7 RENUNCIAS DE GARANTÍAS.....	35
9.8 LIMITACIONES DE RESPONSABILIDAD.....	35
9.8.1 Garantías y limitaciones de garantías.....	35
9.8.2 Deslinde de responsabilidades.....	35
9.8.3 Limitaciones de pérdidas.....	35
9.9 INDEMNIZACIONES.....	35
9.10 PLAZO Y FINALIZACIÓN.....	35
9.10.1 Plazo.....	35
9.10.2 Finalización.....	35
9.10.3 Supervivencia.....	35
9.11 NOTIFICACIONES.....	35
9.12 MODIFICACIONES.....	35
9.12.1 Procedimientos de especificación de cambios.....	35
9.12.2 Procedimientos de publicación y notificación.....	36
9.12.3 Circunstancias en las que se debe cambiar el OID.....	36
9.13 RESOLUCIÓN DE CONFLICTOS.....	36
9.13.1 Resolución extrajudicial de conflictos.....	36
9.13.2 Jurisdicción competente.....	36
9.14 LEGISLACIÓN APLICABLE.....	36
9.15 CONFORMIDAD CON LA LEY APLICABLE.....	36
9.16 CLÁUSULAS DIVERSAS.....	36
9.16.1 Acuerdo completo.....	36
9.16.2 Asignación.....	36
9.16.3 Separabilidad.....	36
9.16.4 Cumplimiento (honorarios de abogados y exención de derechos).....	36
9.16.5 Fuerza mayor.....	36
10 ANEXO I.....	37

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 7

1 INTRODUCCIÓN

1.1 Presentación

El presente documento es la Política de Certificación asociada a los certificados de Aplicación, 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 de Aplicación.

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 de Aplicación
Calificador de la política	Certificado de Aplicación expedido por la ACCV (Pol. Ademuz, s/n. Burjassot, CP 46100, ESPAÑA. CIF A40573396)
Versión de la política	5.0.1
Estado de la política	APROBADO
Referencia de la política / OID (Object Identifier)	1.3.6.1.4.1.8149.3.5.5.0
Fecha de emisión	12 de octubre de 2023
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/pdf-politicas

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 ACCVCA-120, ACCV RSA1 COMPONENTES y ACCV ECC1 COMPONENTES pertenecientes a la Agencia de Tecnología y Certificación Electrónica, cuya función es la emisión de certificados de entidad final para los

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 8

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.

El certificado de ACCVCA-120 es válido desde el día 13 de octubre de 2011 hasta el 1 de enero de 2027.

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

1.3.2 Autoridades de Registro

La Autoridad de Registro que gestiona este tipo de certificados es la Agencia de Tecnología y Certificación Electrónica.

1.3.3 Suscriptores

El grupo de usuarios que pueden solicitar certificados definidos por esta política engloba a los responsables de aplicaciones informáticas o de sistemas de información, tanto de entidades públicas como privadas.

El soporte de claves y certificados es software, debiendo garantizar por parte del suscriptor que la ubicación de la clave privada es un sistema bastionado o que reúna condiciones de seguridad suficientes para proteger la clave privada que alberga.

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 por personas jurídicas, entidades u organizaciones.

1.3.4 Partes confiantes

Todos las entidades usuarios de los certificados de la Agencia de Tecnología y Certificación electrónica podrán confiar en este tipo de certificados, ajustándose a esta Política y a otras limitaciones que se establecieran en los certificados.

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 identificación y autenticación de aplicaciones informáticas, para la firma electrónica de documentación por parte de éstas o para el cifrado de documentación.

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.

Clf.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 9

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.

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

1.6 Definiciones y Acrónimos

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

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

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 10

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.

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 11

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.

El derecho de solicitud de certificados definido en la presente Política de Certificación se encuentra limitado a personas físicas. No se aceptarán solicitudes de certificación realizadas en nombre de personas jurídicas, entidades u organizaciones. Por tanto, no se considera necesaria la identificación de ninguna organización.

3.2.3 Autenticación de la identidad de un individuo.

La autenticación de la identidad del solicitante de un certificado se realizará mediante el uso de su certificado cualificado personal para la firma de la solicitud del certificado de Aplicación.

El solicitante deberá presentar además la documentación necesaria que determine los datos y características de la entidad en nombre de la cual se solicita. Esta presentación se realizará de manera telemática utilizando los medios y aplicaciones que a tal efecto la ACCV ponga a disposición de los usuarios.

ACCV comprobará todos los datos (incluyendo el país del solicitante) utilizando para ello la información disponible de registros de personal y de dominio, requiriendo al solicitante o a la entidad representada las aclaraciones o documentos adicionales que considere necesarios. ACCV guardará esta información a efectos de auditoría, permitiendo su reutilización durante un plazo no superior a 13 meses desde la última comprobación.

Clf.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 12

3.2.4 Información no verificada de los suscriptores

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

3.2.5 Validación de la representación

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

3.2.6 Criterios 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 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). Existe, por tanto, un mecanismo para la renovación:

- Formularios web en el Área de Gestión de Certificados No Personales, disponible en <https://npsc.accv.es:8450/npsc>.

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:

- Telemática. Mediante la firma electrónica de la solicitud de revocación (ubicada en el Área de Gestión de Certificados No Personales <https://npsc.accv.es:8450/npsc>) por parte del solicitante del certificado o del responsable del mismo en la fecha de la solicitud de revocación.
- Telefónico: Mediante llamada telefónica al número de soporte telefónico de la Agencia de Tecnología y Certificación Electrónica 963 866 014.

La Agencia de Tecnología y Certificación Electrónica 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 asociada al certificado emitido al amparo de esta Política de Certificación, o cualquier otro hecho que recomendará emprender dicha acción.

Clf.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 13

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 proceso comienza por acceder al Área de gestión de certificados no personales (NPSC) ubicada en <https://npvc.accv.es:8450/npvc>. Si se solicita por primera vez un certificado el usuario debe adjuntar el documento que lo acredita como capacitado para efectuar esa solicitud (documento de toma de posesión en el puesto o diario oficial donde se recoge el nombramiento correspondiente, poderes notariales e inscripción en los registros correspondientes), en formato pdf firmado electrónicamente. Si el acceso se ha efectuado con un certificado que acredita la capacidad necesaria para gestionar los certificados de aplicación, se utilizarán los datos de Organización, Unidad Organizativa y Cargo de dicho certificado.

4.2 Tramitación de la solicitud de certificados.

4.2.1 Ejecución de las funciones de identificación y autenticación

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 revisión de la solicitud.

ACCV comprobará los datos de la solicitud y acreditará al solicitante para la solicitud de certificados de Aplicación, durante 13 meses a partir de la aprobación sin necesidad de aportar documentación adicional. En el caso de identificación con certificado de empleado público no existe limitación temporal mientras el certificado esté en vigor.

La autenticación de la identidad del solicitante se hará mediante la identificación con la Autoridad de Registro correspondiente (en este caso NPSC), utilizando los mecanismos descritos en la sección 3.2.3 *Autenticación de la identidad de un individuo*. La Autoridad de registro comprueba la documentación y valida los datos utilizando registros accesibles al público para dicha verificación.

4.2.2 Aprobación o rechazo de la solicitud

En caso de aceptación, la Autoridad de Registro notificará al solicitante por medio de un correo electrónico a la dirección de correo que figura en el perfil del usuario en la aplicación NPSC.

El solicitante debe acceder a NPSC con su certificado personal cualificado. Si el solicitante está en condiciones técnicas y administrativas de llevar a cabo esta generación, la correspondiente opción le aparecerá habilitada en la aplicación.

En caso de denegación, la Autoridad de Registro lo notificará al solicitante mediante el envío de un correo electrónico a la dirección que figure en la solicitud. La solicitud se cancelará y no podrá reutilizarse, aunque es posible reutilizar la documentación suministrada que haya sido verificado por un periodo no superior a 13 meses.

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.

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 14

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.

El responsable del certificado de Aplicación puede solicitar a la ACCV que añada a otros usuarios con capacidad para realizar los trámites asociados al ciclo de vida del certificado de Aplicación que tiene asociado. La Autoridad de Registro comprobará la solicitud de credenciales y comunicará mediante correo electrónico al solicitante la autorización o denegación de los permisos.

ACCV puede efectuar esta autorización de oficio en los casos en los que el responsable del certificado pierda la capacidad necesaria para gestionarlo y no haya otras personas autorizadas.

4.3.1 Acciones de la CA durante el proceso de emisión

La emisión del certificado se produce una vez la RA a llevado a cabo las verificaciones necesarias para validar la solicitud de certificado. El mecanismo que determina la naturaleza y forma de esas validaciones es esta Política de Certificación.

En la solicitudes realizadas con un certificado personal cualificado los pasos son los siguientes:

- El solicitante se identifica con su certificado personal cualificado correspondiente en NPSC
- Accede a la parte de solicitudes aceptadas y busca las disponibles.
- Pulsa el enlace asociado a la acción de Generar.
- RA pregunta al solicitante el mecanismo de generación del par de claves y la petición de certificado de entre las opciones permitidas y con los parámetros definidos en esta política..
- RA envía la petición de certificado firmada (CSR) a la CA.
- CA realiza una verificación de la firma de la RA y confirma el formato del CSR.
- CA firma el CSR y lo envía de vuelta a la RA.
- RA comunica el certificado al solicitante.

Todos estos procesos se realizan en la plataforma de generación proporcionada por la ACCV.

4.3.2 Notificación de la emisión al suscriptor

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 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 solicitante, y cuyo fin es vincular a la persona que solicita el certificado de Aplicación, 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.

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 15

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 Circunstancia para la renovación de claves (re-key) certificado

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

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 16

4.7.2 Quién puede solicitar la certificación de una nueva clave pública

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

4.7.3 Procesamiento de solicitudes de cambio de claves del certificado

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

4.7.4 Notificación de nueva emisión de certificado al suscriptor

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

4.7.5 Conducta que constituye la aceptación de un certificado con nuevas claves (re-keyed)

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

4.7.6 Publicación del certificado con renovación de claves (re-keyed) por la CA

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

4.7.7 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.

4.8 Modificación de certificados.

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

4.8.1 Circunstancia 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.

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 17

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 Telemático

Accediendo al Área de Gestión de certificados no personales (NPSC) ubicada en <https://npsc.accv.es:8450/npsc> el usuario puede revocar los certificados que ha solicitado o de los que tiene permiso para ello.

4.9.3.2 Telefónico

Mediante llamada telefónica al número de soporte telefónico de la Agencia de Tecnología y Certificación Electrónica 963 866 014.

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 CA debe 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.

4.9.10 Requisitos de la comprobación on-line de la revocación

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

4.9.11 Otras formas de divulgación de información de revocación disponibles

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

Clf.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 18

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

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.

4.9.14 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.

4.10.1 Características 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 responsable del certificado de Aplicación, mediante correo electrónico, en un momento previo anterior a la publicación del certificado en la Lista de Certificados Revocados, acerca de la suspensión o revocación de los certificados en los cuales aparezca como suscriptor o responsable, 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.

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 19



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

La recuperación de las claves de sesión no esta soportado.

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 20

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.

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 21

5.2.4 Roles que requieren separación de tareas

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.

Clf.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 22

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.

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 23

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.

5.7.1 Procedimientos de gestión de incidencias y compromisos

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

5.7.2 Corrupción de recursos, aplicaciones o datos

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

5.7.3 Compromiso de la clave privada de la entidad

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

5.7.4 Continuidad 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.

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 24

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 software por el suscriptor del certificado.

6.1.2 Entrega de la clave privada a la entidad

La clave privada se genera por el suscriptor, por tanto, no procede hacerle entrega de la misma.

6.1.3 Entrega de la clave pública al emisor del certificado

La clave pública a ser certificada es generada por el suscriptor 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 suscriptor.

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 ECC P-256.

6.1.6 Parámetros de generación de la clave pública

Se utilizan los parámetros definidos en el documento ETSI TS 119 312 "Electronic Signatures and Infrastructures (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

6.1.7 Propósitos 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.

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 25

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

Los certificados emitidos en virtud de esta política se basan en software, por lo que las normas y controles de los módulos criptográficos dependen del sistema operativo del suscriptor.

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.

El par de claves se genera en software. No hay dispositivos criptográficos.

6.2.7 Almacenamiento de clave privada en el módulo criptográfico.

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

6.2.8 Método de activación de la clave privada.

La clave privada es generada por el solicitante y nunca está en posesión de la Agencia de Tecnología y Certificación Electrónica.

6.2.9 Método de desactivación de la clave privada

La clave privada es generada por el solicitante y nunca está en posesión de la Agencia de Tecnología y Certificación Electrónica.

6.2.10 Método de destrucción de la clave privada

La clave privada es generada por el solicitante y nunca está en posesión de la Agencia de Tecnología y Certificación Electrónica. Se podrá destruir mediante el borrado de esta siguiendo las instrucciones de la aplicación que la alberga.

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 26

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 como máximo.

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 como máximo.

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

El certificado de ACCVCA-120 es válido desde el día 13 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

La clave privada es generada por el solicitante y nunca está en posesión de la Agencia de Tecnología y Certificación Electrónica.

6.4.2 Protección de los datos de activación

El responsable 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 Requerimientos técnicos de seguridad informática específicos

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

6.5.2 Valoración de la 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.

6.6.1 Controles de desarrollo del sistema

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

Clf.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 27

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 Evaluación de la 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 TimeStamping

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

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 28

7 Perfiles de certificados, CRL y OCSP

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	
SerialNumber	NIF de la Administración, organismo o entidad de derecho público o privado suscriptor del certificado.
CommonName	Nombre descriptivo del sistema automático junto con el nombre descriptivo del organismo o empresa solicitante, separados por espacios y un guion. Asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades. Ejemplo: APLICACIÓN - ORGANISMO
OrganizationalUnit	Cadena fija con el valor APLICACIONES
Organization	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptor del certificado y propietaria del dominio.
Locality	Ciudad
State	Provincia
Country	Cadena fija con el valor ES
Version	V3
SerialNumber	Identificador único del certificado. Menor de 32 caracteres hexadecimales.
Algoritmo de firma	ACCVCA120 sha256withRSAEncryption ACCV_RSA1_COMPONENTES sha256withRSAEncryption ACCV_ECC1_COMPONENTES 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 certificado de sello
Extended Key Usage	
	Client Authentication
	Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)
CRL Distribution Point	ACCVCA-120: http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl ACCV_RSA1_COMPONENTES: http://www.accv.es/gestcert/accv_rsa1_componentes.crl

ACCV_ECC1_COMPONENTES: http://www.accv.es/gestcert/accv_ecc1_componentes.crl		
SubjectAlternativeName		
	DirectoryName (opcional incluir custodio)	Cadena con nombre y apellidos del custodio separados por Nombre Apellido1 Apellido2
Certificate Policy Extensions		
Policy OID	1.3.6.1.4.1.8149.3.5.5.0	
Policy CPS Location	http://www.accv.es/legislacion_c.htm *	
Policy Notice	Certificado de Aplicación 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	ACCVCA-120: http://www.accv.es/gestcert/ACCVCA120SHA2_cacert.crl ACCV RSA1 COMPONENTES: http://www.accv.es/gestcert/accv_rsa1_componentes.crl ACCV ECC1 COMPONENTES: http://www.accv.es/gestcert/accv_ecc1_componentes.crl
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 Commitment Key encipherment Data encipherment	ECC: Digital Signature Non-repudiation Key agreement

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)

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 30

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.

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

- cn=ACCVCA-120, ou=PKIACCV o=ACCV, c=ES
- cn=ACCV RSA1 COMPONENTES,2.5.4.97=VATES-A40573396,o=ISTEC,I=BURJASSOT,s=VALENCIA,c=ES
- cn=ACCV ECC1 COMPONENTES,2.5.4.97=VATES-A40573396,o=ISTEC,I=BURJASSOT,s=VALENCIA,c=ES

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.

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

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

1.3.6.1.4.1.8149.3.5.5.0

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 CertificatePolicy puede incluir dos campos Cualificadores de Política, ambos opcionales:

CPS Pointer: Contiene la URL donde se publica la Política.

User Notice: Contiene un texto descriptivo.

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

7.2.1 Número de versión

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

7.2.2 CRL y extensiones

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

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 31

7.3 Perfil de OCSP

7.3.1 Número de versión

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

7.3.2 Extensiones

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

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 32

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.

8.7 Auto auditorias

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

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 33

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 Cobertura del Seguro

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

9.2.2 Otros activos

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

9.2.3 Seguro o cobertura de garantía para entidades finales

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.

Clf.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 34

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 privacidad

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 Responsabilidad de proteger la información privada

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

9.4.5 Aviso y consentimiento para usar información privada

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.

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 35

9.6.4 Obligación y responsabilidad de terceras partes

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

9.6.5 Obligación y responsabilidad de otros participantes

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.

9.9 Indemnizaciones

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.

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 36

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 Circunstancias en las que se debe cambiar el OID

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.

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

9.16.1 Acuerdo completo

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

9.16.2 Asignación

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

9.16.3 Separabilidad

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

9.16.4 Cumplimiento (honorarios de abogados y exención de derechos)

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

9.16.5 Fuerza mayor

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

Clf.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 37

10 Anexo I

CONTRATO DE CERTIFICACIÓN - CÓDIGO 1.3.6.1.4.1.8149.3.5

Sección 1 – Datos del solicitante

Apellidos:

Nombre:

NIF:

Tel.:

Puesto o cargo:

Entidad - Organización:

CIF de la Entidad - Organización:

Dirección correo electrónico:

Dirección postal:

Sección 2 – Datos de la Aplicación

Nombre descriptivo de la aplicación o sistema automatizado:

Dirección de correo de contacto:

Sección 3 – Fecha y Firma

Suscribo el presente contrato de certificación asociado a la Política de Certificación de Certificados de Aplicación con código 1.3.6.1.4.1.8149.3.5, 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 solicitante

Firmat/*Firmado*:

Cif.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 38

CONTRATO DE CERTIFICACIÓN - CÓDIGO 1.3.6.1.4.1.8149.3.5

Condiciones de utilización de los certificados

1. Los certificados asociados a la Política de Certificación de certificados de aplicación, 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 Valenciana.

2. El solicitante de los certificados debe ser una persona física, en posesión de un certificado cualificado, y deben estar empleados en una Administración Pública, Ente Instrumental de la Administración o Entidad Corporativa.

3. El solicitante de los certificados, especialmente habilitado para la gestión de éstos por parte de una Administración o Entidad 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 funcionamiento de los servidores informáticos que hacen uso de los certificados 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 como máximo. Para su renovación deberá 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 identificación de los solicitantes se hará en base a su certificado cualificado personal.

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 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 Valenciana e indicando claramente esta voluntad.

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.

Clf.: PÚBLICO	Ref.: ACCV-CP-05V5.0.1-ES-2023.odt	Versión: 5.0.1
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.5.5.0	Pág. 39