



Agencia de Tecnología y Certificación Electrónica

Política de Certificación de Certificados para Firma de Código

Fecha: 29 de septiembre de 2.019	Versión: 3.0.4
Estado: APROBADO	Nº de páginas: 44
OID: 1.3.6.1.4.1.8149.3.4.3.0	Clasificación: PUBLICO
Archivo: ACCV-CP-04V3.0.4-ES-2019.odt	
Preparado por: Agencia de Tecnología y Certificación Electrónica	

Tabla de Contenido

1. INTRODUCCIÓN.....	10
1.1. PRESENTACIÓN.....	10
1.2. IDENTIFICACIÓN.....	10
1.3. COMUNIDAD Y ÁMBITO DE APLICACIÓN.....	11
1.3.1. Autoridades de Certificación.....	11
1.3.2. Autoridades de Registro.....	11
1.3.3. Suscriptores.....	11
1.3.4. Partes confiantes.....	11
1.3.5. Otros participantes.....	11
1.4. USO DE LOS CERTIFICADOS.....	12
1.4.1. Usos permitidos.....	12
1.4.2. Usos prohibidos.....	12
1.5. POLÍTICA DE ADMINISTRACIÓN.....	12
1.5.1. Especificación de la Organización Administradora.....	12
1.5.2. Persona de Contacto.....	12
1.5.3. Competencia para determinar la adecuación de la CPS a la Políticas.....	12
1.5.4. Procedimiento de aprobación.....	12
1.6. DEFINICIONES Y ACRÓNIMOS.....	12
1.6.1. Definiciones.....	12
1.6.2. Acrónimos.....	12
2. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS.....	13
2.1. REPOSITORIO DE CERTIFICADOS.....	13
2.2. PUBLICACIÓN.....	13
2.3. FRECUENCIA DE ACTUALIZACIONES.....	13
2.4. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS.....	13
3. IDENTIFICACIÓN Y AUTENTIFICACIÓN.....	14
3.1. REGISTRO DE NOMBRES.....	14
3.1.1. Tipos de nombres.....	14
3.1.2. Significado de los nombres.....	14
3.1.3. Interpretación de formatos de nombres.....	14
3.1.4. Unicidad de los nombres.....	14
3.1.5. Procedimientos de resolución de disputas de nombres.....	14
3.1.6. Reconocimiento, autenticación y función de las marcas registradas.....	14
3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD.....	14
3.2.1. Métodos de prueba de posesión de la clave privada.....	14
3.2.2. Autenticación de la identidad de una organización.....	14

3.2.3. Autenticación de la identidad de un individuo.....	14
3.2.4. Información del suscriptor no verificada.....	15
3.2.5. Validación de la representación.....	15
3.2.6. Criterio para la Interoperación.....	15
3.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DEL PAR DE CLAVES.....	16
3.3.1. Identificación y autenticación de las solicitudes de renovación rutinarias.....	16
3.3.2. Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida.....	16
3.4. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DEL PAR DE CLAVES.....	16
4. EL CICLO DE VIDA DE LOS CERTIFICADOS.....	17
4.1. SOLICITUD DE CERTIFICADOS.....	17
4.1.1. Legitimación de la solicitud.....	17
4.1.2. Proceso de solicitud y responsabilidades.....	17
4.2. TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADOS.....	17
4.2.1. Ejecución de las funciones de identificación y autenticación.....	17
4.2.2. Aprobación o denegación de la solicitud de certificado.....	17
4.2.3. Plazo para resolver la solicitud.....	18
4.3. EMISIÓN DE CERTIFICADOS.....	18
4.3.1. Acciones de la CA durante la emisión del certificado.....	18
4.3.2. Notificación de la emisión al suscriptor.....	18
4.4. ACEPTACIÓN DE CERTIFICADOS.....	18
4.4.1. Conducta que constituye aceptación del certificado.....	18
4.4.2. Publicación del certificado por la CA.....	19
4.4.3. Notificación de la emisión a terceros.....	19
4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO.....	19
4.5.1. Uso del certificado y la clave privada del suscriptor.....	19
4.5.2. Uso de la clave pública y del certificado por la parte que confía.....	19
4.6. RENOVACIÓN DE CERTIFICADOS.....	19
4.6.1. Circunstancia para la renovación del certificado.....	19
4.6.2. Quién puede solicitar renovación.....	19
4.6.3. Procesamiento de solicitudes de renovación de certificados.....	19
4.6.4. Notificación de nueva emisión de certificado al suscriptor.....	19
4.6.5. Conducta que constituye la aceptación de un certificado de renovación.....	19
4.6.6. Publicación del certificado de renovación por la CA.....	19
4.6.7. Notificación de emisión de certificado por la CA a otras entidades.....	20
4.7. RENOVACIÓN DE CLAVES.....	20
4.7.1. Circunstancia para la renovación de claves (re-key) certificado.....	20
4.7.2. Quién puede solicitar la certificación de una nueva clave pública.....	20
4.7.3. Procesamiento de solicitudes de cambio de claves del certificado.....	20

4.7.4. Notificación de nueva emisión de certificado al suscriptor.....	20
4.7.5. Conducta que constituye la aceptación de un certificado con nuevas claves (re-keyed).....	20
4.7.6. Publicación del certificado con renovación de claves (re-keyed) por la CA.....	20
4.7.7. Notificación de emisión de certificado por la CA a otras entidades.....	20
4.8. MODIFICACIÓN DE CERTIFICADOS.....	20
4.8.1. Circunstancia para la modificación del certificado.....	20
4.8.2. Quién puede solicitar la modificación del certificado.....	20
4.8.3. Procesamiento de solicitudes de modificación de certificados.....	20
4.8.4. Notificación de nueva emisión de certificado al suscriptor.....	20
4.8.5. Conducta que constituye la aceptación de un certificado modificado.....	21
4.8.6. Publicación del certificado modificado por la CA.....	21
4.8.7. Notificación de emisión de certificado por la CA a otras entidades.....	21
4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.....	21
4.9.1. Circunstancias para la revocación.....	21
4.9.2. Entidad que puede solicitar la revocación.....	21
4.9.3. Procedimiento de solicitud de revocación.....	21
4.9.3.1. Telemático.....	21
4.9.3.2. Telefónico.....	21
4.9.4. Periodo de gracia de la solicitud de revocación.....	21
4.9.5. Tiempo dentro del cual CA debe procesar la solicitud de revocación.....	21
4.9.6. Requisitos de comprobación de CRLs.....	21
4.9.7. Frecuencia de emisión de CRLs.....	21
4.9.8. Máxima latencia de CRL.....	21
4.9.9. Disponibilidad de comprobación on-line de la revocación.....	22
4.9.10. Requisitos de la comprobación on-line de la revocación.....	22
4.9.11. Otras formas de divulgación de información de revocación disponibles.....	22
4.9.12. Requisitos especiales de revocación por compromiso de las claves.....	22
4.9.13. Circunstancias para la suspensión.....	22
4.9.14. Entidad que puede solicitar la suspensión.....	22
4.9.15. Procedimiento para la solicitud de suspensión.....	22
4.9.16. Límites del período de suspensión.....	22
4.10. SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS.....	22
4.10.1. Características operacionales.....	22
4.10.2. Disponibilidad del servicio.....	22
4.10.3. Características opcionales.....	22
4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN.....	22
4.12. DEPÓSITO Y RECUPERACIÓN DE CLAVES.....	23
4.12.1. Política y prácticas clave de custodia y recuperación.....	23
4.12.2. Política y prácticas de encapsulado y recuperación de claves de sesión.....	23
5. CONTROLES DE SEGURIDAD FÍSICA, PROCEDURAL Y DE PERSONAL.....	24

5.1. CONTROLES DE SEGURIDAD FÍSICA.....	24
5.1.1. Ubicación y construcción.....	24
5.1.2. Acceso físico.....	24
5.1.3. Alimentación eléctrica y aire acondicionado.....	24
5.1.4. Exposición al agua.....	24
5.1.5. Protección y prevención de incendios.....	24
5.1.6. Sistema de almacenamiento.....	24
5.1.7. Eliminación de residuos.....	24
5.1.8. Backup remoto.....	24
5.2. CONTROLES DE PROCEDIMIENTOS.....	24
5.2.1. Papeles de confianza.....	24
5.2.2. Número de personas requeridas por tarea.....	25
5.2.3. Identificación y autenticación para cada rol.....	25
5.2.4. Roles que requieren separación de tareas.....	25
5.3. CONTROLES DE SEGURIDAD DE PERSONAL.....	25
5.3.1. Requerimientos de antecedentes, calificación, experiencia, y acreditación.....	25
5.3.2. Procedimientos de comprobación de antecedentes.....	25
5.3.3. Requerimientos de formación.....	25
5.3.4. Requerimientos y frecuencia de actualización de la formación.....	25
5.3.5. Frecuencia y secuencia de rotación de tareas.....	25
5.3.6. Sanciones por acciones no autorizadas.....	25
5.3.7. Requerimientos de contratación de personal.....	25
5.3.8. Documentación proporcionada al personal.....	25
5.3.9. Controles periódicos de cumplimiento.....	26
5.3.10. Finalización de los contratos.....	26
5.4. PROCEDIMIENTOS DE REGISTRO DE EVENTOS.....	26
5.4.1. Tipos de eventos registrados.....	26
5.4.2. Frecuencia de procesamiento de los registros de auditoría.....	26
5.4.3. Periodo de retención para los registros de auditoría.....	26
5.4.4. Protección de los registros de auditoría.....	26
5.4.5. Procedimientos de respaldo de los registros de auditoría.....	26
5.4.6. Sistema de recogida de información de auditoría (interno vs externo).....	26
5.4.7. Notificación al sujeto causa del evento.....	26
5.4.8. Análisis de vulnerabilidades.....	26
5.5. ARCHIVO DE INFORMACIONES Y REGISTROS.....	27
5.5.1. Tipo de informaciones y eventos registrados.....	27
5.5.2. Periodo de retención para el archivo.....	27
5.5.3. Protección del archivo.....	27
5.5.4. Procedimientos de respaldo del archivo.....	27
5.5.5. Requerimientos para el sellado de tiempo de los registros.....	27

5.5.6. Sistema de recogida de información de auditoría (interno vs externo).....	27
5.5.7. Procedimientos para obtener y verificar información archivada.....	27
5.6. CAMBIO DE CLAVE.....	27
5.7. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O DE DESASTRE.....	27
5.7.1. Procedimientos de gestión de incidencias y compromisos.....	27
5.7.2. Corrupción de recursos, aplicaciones o datos.....	27
5.7.3. Compromiso de la clave privada de la entidad.....	28
5.7.4. Continuidad del negocio después de un desastre.....	28
5.8. CESE DE UNA CA.....	28
6. CONTROLES DE SEGURIDAD TECNICA.....	29
6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES.....	29
6.1.1. Generación del par de claves.....	29
6.1.2. Entrega de la clave privada a la entidad.....	29
6.1.3. Entrega de la clave pública al emisor del certificado.....	29
6.1.4. Entrega de la clave pública de la CA a los usuarios.....	29
6.1.5. Tamaño de las claves.....	29
6.1.6. Parámetros de generación de la clave pública.....	29
6.1.7. Propósitos de uso de claves.....	30
6.2. PROTECCIÓN DE LA CLAVE PRIVADA.....	30
6.2.1. Estándares para los módulos criptográficos.....	30
6.2.2. Control multipersona de la clave privada.....	30
6.2.3. Custodia de la clave privada.....	30
6.2.4. Copia de seguridad de la clave privada.....	30
6.2.5. Archivo de la clave privada.....	30
6.2.6. Introducción de la clave privada en el módulo criptográfico.....	30
6.2.7. Almacenamiento de clave privada en el módulo criptográfico.....	30
6.2.8. Método de activación de la clave privada.....	31
6.2.9. Método de desactivación de la clave privada.....	31
6.2.10. Método de destrucción de la clave privada.....	31
6.2.11. Calificación del módulo criptográfico.....	31
6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES.....	31
6.3.1. Archivo de la clave pública.....	31
6.3.2. Periodo de uso para las claves públicas y privadas.....	31
6.4. DATOS DE ACTIVACIÓN.....	31
6.4.1. Generación y activación de los datos de activación.....	31
6.4.2. Protección de los datos de activación.....	31
6.4.3. Otros aspectos de los datos de activación.....	31
6.5. CONTROLES DE SEGURIDAD INFORMÁTICA.....	32
6.5.1. Requerimientos técnicos de seguridad informática específicos.....	32

6.5.2. Valoración de la seguridad informática.....	32
6.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA.....	32
6.6.1. Controles de desarrollo del sistema.....	32
6.6.2. Controles de gestión de la seguridad.....	32
6.6.3. Evaluación de la seguridad del ciclo de vida.....	32
6.7. CONTROLES DE SEGURIDAD DE LA RED.....	32
6.8. FUENTES DE TIEMPO.....	32
7. PERFILES DE CERTIFICADO, CRL Y OCSP.....	33
7.1. PERFIL DE CERTIFICADO.....	33
7.1.1. Número de versión.....	33
7.1.2. Extensiones del certificado.....	33
7.1.3. Identificadores de objeto (OID) de los algoritmos.....	34
7.1.4. Formatos de nombres.....	34
7.1.5. Restricciones de los nombres.....	35
7.1.6. Identificador de objeto (OID) de la Política de Certificación.....	35
7.1.7. Uso de la extensión “Policy Constraints”.....	35
7.1.8. Sintaxis y semántica de los cualificadores de política.....	35
7.1.9. Tratamiento semántico para la extensión “Certificate Policy”.....	35
7.2. PERFIL DE CRL.....	35
7.2.1. Número de versión.....	35
7.2.2. CRL y extensiones.....	36
7.3. PERFIL DE OCSP.....	36
7.3.1. Número de versión.....	36
7.3.2. Extensiones.....	36
8. AUDITORÍA DE CONFORMIDAD.....	37
8.1. FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD PARA CADA ENTIDAD.....	37
8.2. IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR.....	37
8.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA.....	37
8.4. TÓPICOS CUBIERTOS POR EL CONTROL DE CONFORMIDAD.....	37
8.5. ACCIONES A TOMAR COMO RESULTADO DE UNA DEFICIENCIA.....	37
8.6. COMUNICACIÓN DE RESULTADOS.....	37
8.7. AUTO AUDITORIAS.....	37
9. REQUISITOS COMERCIALES Y LEGALES.....	38
9.1. TARIFAS.....	38
9.1.1. Tarifas de emisión de certificado o renovación.....	38
9.1.2. Tarifas de acceso a los certificados.....	38
9.1.3. Tarifas de acceso a la información de estado o revocación.....	38
9.1.4. Tarifas de otros servicios como información de políticas.....	38

9.1.5. Política de reintegros.....	38
9.2. CAPACIDAD FINANCIERA.....	38
9.2.1. Cobertura del Seguro.....	38
9.2.2. Otros activos.....	38
9.2.3. Seguro o cobertura de garantía para entidades finales.....	38
9.3. POLÍTICA DE CONFIDENCIALIDAD.....	38
9.3.1. Información confidencial.....	38
9.3.2. Información no confidencial.....	39
9.3.3. Divulgación de información de revocación /suspensión de certificados.....	39
9.4. PROTECCIÓN DE DATOS PERSONALES.....	39
9.4.1. Plan de privacidad.....	39
9.4.2. Información considerada privada.....	39
9.4.3. Información no considerada privada.....	39
9.4.4. Responsabilidad de proteger la información privada.....	39
9.4.5. Prestación del consentimiento en el uso de los datos personales.....	39
9.4.6. Comunicación de la información a autoridades administrativas y/o judiciales.....	39
9.4.7. Otros supuestos de divulgación de la información.....	39
9.5. DERECHOS DE PROPIEDAD INTELECTUAL.....	39
9.6. OBLIGACIONES Y RESPONSABILIDAD CIVIL.....	40
9.6.1. Obligaciones de la Entidad de Certificación.....	40
9.6.2. Obligaciones de la Autoridad de Registro.....	40
9.6.3. Obligaciones de los suscriptores.....	40
9.6.4. Obligación y responsabilidad de terceras partes.....	40
9.6.5. Obligación y responsabilidad de otros participantes.....	40
9.7. RENUNCIAS DE GARANTÍAS.....	40
9.8. LIMITACIONES DE RESPONSABILIDAD.....	40
9.8.1. Garantías y limitaciones de garantías.....	40
9.8.2. Deslinde de responsabilidades.....	40
9.8.3. Limitaciones de pérdidas.....	40
9.9. INDEMNIZACIONES.....	40
9.10. PLAZO Y FINALIZACIÓN.....	41
9.10.1. Plazo.....	41
9.10.2. Finalización.....	41
9.10.3. Supervivencia.....	41
9.11. NOTIFICACIONES.....	41
9.12. MODIFICACIONES.....	41
9.12.1. Procedimientos de especificación de cambios.....	41
9.12.2. Procedimientos de publicación y notificación.....	41
9.12.3. Circunstancias en las que se debe cambiar el OID.....	41
9.13. RESOLUCIÓN DE CONFLICTOS.....	41

9.13.1. Resolución extrajudicial de conflictos.....	41
9.13.2. Jurisdicción competente.....	41
9.14. LEGISLACIÓN APLICABLE.....	42
9.15. CONFORMIDAD CON LA LEY APLICABLE.....	42
9.16. CLÁUSULAS DIVERSAS.....	42
9.16.1. Acuerdo completo.....	42
9.16.2. Asignación.....	42
9.16.3. Separabilidad.....	42
9.16.4. Cumplimiento (honorarios de abogados y exención de derechos).....	42
9.16.5. Fuerza mayor.....	42
ANEXO I.....	43

1. INTRODUCCIÓN

1.1. Presentación

El presente documento es la Política de Certificación asociada a los certificados para firma de código, 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 para firma de código.

La presente Política 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.

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.

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 para Firma de Código
Calificador de la política	Certificado para firma de Código expedido por la ACCV (Plaza Nápoles y Sicilia, 6. Valencia CP 46003, ESPAÑA. CIF A40573396)
Versión de la política	3.0.4
Estado de la política	APROBADO
Referencia de la política / OID (Object Identifier)	1.3.6.1.4.1.8149.3.4.3.0
Fecha de emisión	27 de septiembre de 2019
Fecha de expiración	No aplicable.
CPS relacionada	Declaración de Prácticas de Certificación (CPS) de la ACCV. Versión 4.0 OID: 1.3.6.1.4.1.8149.2.4.0

	Disponible en http://www.accv.es/pdf-politicas
Localización	Esta Política de certificación se puede encontrar en: http://www.accv.es/legislacion_c.htm

1.3. Comunidad y Ámbito de aplicación

1.3.1. Autoridades de Certificación

La CA que puede emitir certificados acordes con esta política es la "ACCVCA-120" 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-120 es válido desde el día 13 de octubre de 2011 hasta el 1 de enero de 2027.

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 suscriptor es el sujeto del certificado de firma de código. El grupo de usuarios que pueden solicitar certificados definidos por esta política está formado por los responsables de entidades públicas o privadas, en situación de representar a la entidad solicitante (suscriptor). En el caso de entidades públicas, las solicitudes pueden llevarlas a cabo Jefes de Área o puestos organizativos equivalentes en cualquier tipo de Administración Pública (europea, estatal, autonómica y local), siendo éstos los responsables últimos de su uso dentro de los distintos proyectos o sistemas de información.

En el caso de entidades privadas, podrán solicitar los certificados aquellas personas con capacidad de representar la entidad o que hayan sido autorizadas para la gestión de este tipo de certificados.

Se limita el derecho de solicitud de certificados definido en la presente Política de Certificación a personas físicas con capacidad de representación o delegación de la entidad o persona jurídica suscriptora del certificado. No se aceptarán solicitudes de certificación realizadas directamente por personas jurídicas, entidades u organizaciones.

1.3.4. Partes confiantes

La confianza en los certificados para firma de código emitidos bajo esta Política esta limitada a la verificación de la identidad del código ejecutado por parte de cualquier persona física o sistema informático.

1.3.5. Otros participantes

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

Cif.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 11

1.4. Uso de los certificados

1.4.1. Usos permitidos

Los certificados emitidos por la ACCV bajo esta Política de Certificación pueden utilizarse para firmar aplicaciones o partes de ellas, asignándoles así identidad.

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

1.5.1. Especificación de la Organización Administradora

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

1.5.2. Persona de Contacto

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

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

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

1.5.4. 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.

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.

Cif.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 13

3. IDENTIFICACIÓN Y AUTENTIFICACIÓN

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

El certificado para firma de código se emitirá con el nombre legal completo del organismo o empresa al que este adscrito el responsable que solicita el certificado. No se aceptarán nombres parciales.

CN = NOMBRE LEGAL COMPLETO DEL ORGANISMO O EMPRESA

3.1.5. Procedimientos de resolución de disputas de 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 se realizará mediante el uso de su certificado personal cualificado para la firma de la solicitud del certificado para firma de código.

El solicitante deberá presentar además la documentación necesaria que determine la capacidad de representar a la Administración Pública o la entidad privada a nombre de la cual, en última instancia,

Cif.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 14

se va a emitir el certificado. Esta presentación se realizará de manera telemática utilizando los medios que la Agencia de Tecnología y Certificación Electrónica ponga a disposición de los usuarios (acceso en <https://npsc.accv.es:8450/npsc>)

La Agencia de Tecnología y Certificación Electrónica comprobará los datos presentados:

La veracidad de los datos del solicitante

La capacidad de representación del solicitante

La veracidad de los datos de la empresa u organismo

utilizando para ello la información disponible de

Agencias de Protección de Datos

Registros de Administraciones Públicas

Registros Comerciales y Mercantiles

Servicios oficiales de consulta y verificación de identidad

Registros de personal

requiriendo al solicitante o a la Administración o Empresa representada las aclaraciones o documentos adicionales que considere necesarios.

ACCV conserva esta información a efectos de auditoria y la mantiene vigente durante 13 meses, permitiendo reutilizarla durante ese periodo.

3.2.4. Información del subscritor no verificada

Toda la información suministrada es verificada.

3.2.5. Validación de la representación

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

3.2.6. Criterio para la Interoperación

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

3.3. Identificación y autenticación de las solicitudes de renovación 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 utilizando formularios web firmados en el Área de Gestión de Certificados No Personales, disponible en <https://npsc.accv.es:8450/npsc>. ACCV puede reutilizar la información almacenada si no han pasado mas de 13 meses desde sus aportación y comprobación.

Cif.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 15

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. ACCV puede reutilizar la información almacenada si no han pasado más de 13 meses desde su aportación y comprobación.

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 902482481.

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.

Cif.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 16

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

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

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. Proceso de solicitud 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 utilizará los datos del certificado como punto de partida para realizar las funciones de autenticación e identificación.

ACCV verifica los datos de la solicitud y en caso necesario (si no hubiera autorización previa) acredita al solicitante para la solicitud de certificados asociados al organismo o empresa durante 13 meses sin necesidad de aportar documentación adicional. En caso de utilizar certificados de representante o de Empleado Público, no hay límite temporal mientras el certificado este en vigor.

Además, durante el procedimiento de identificación se realiza un chequeo contra una Base de Datos de productores, publicadores y distribuidores de código sospechoso.

ACCV proporciona registros de esas búsquedas y verificaciones, posibilitando que puedan reproducirse paso a paso. Para estas verificaciones ACCV utiliza las direcciones de correo y teléfonos que se suministración en el proceso de registro.

4.2.2. Aprobación o denegación de la solicitud de certificado

En caso de aprobación, la Autoridad de Registro lo notificará al solicitante mediante el envío de un correo electrónico firmado a la dirección que figure en la solicitud.

En caso de denegación, la Autoridad de Registro lo notificará al solicitante mediante el envío de un correo electrónico firmado a la dirección que figure en la solicitud. La solicitud se cancelara y no podrá

Clf.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 17

reutilizarse, aunque es posible reutilizar la documentación suministrada que haya sido verificado por un periodo no superior a 13 meses.

ACCV usará esta información para decidir sobre nuevas solicitudes.

4.2.3. Plazo para resolver la solicitud

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

4.3. Emisión de certificados

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

4.3.1. Acciones de la CA durante la emisión del certificado

La emisión del certificado tendrá lugar una vez que la Autoridad de Registro 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 el solicitante recibe el correo de aprobación, deberá entrar en el Área de gestión de certificados no personales (NPSC) ubicada en <https://npsc.accv.es:8450/npsc> para generar y descargar el certificado.

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

La Agencia de Tecnología y Certificación Electrónica puede efectuar esta autorización de oficio en los casos en los que el responsable del certificado para firma de código pierda la capacidad necesaria para gestionarlo y no haya otras personas autorizadas.

ACCV llevará a cabo revisiones frecuentes sobre muestreos aleatorios de los certificados de firma de código para garantizar la exactitud de los datos y el mantenimiento de la vigencia de los mismos. Si en el curso de esos muestreos se confirma que los datos no son exactos o ya no son de aplicación, la ACCV revocará los certificados involucrados. En el caso de recibir esta información de terceros, se realizarán las comprobaciones oportunas y se obrará de igual manera. ACCV mantendrá pruebas documentales de todas las revisiones y acciones.

4.3.2. Notificación de la emisión al suscriptor

ACCV notificará al suscriptor de la emisión del certificado utilizando un correo electrónico firmado a la dirección 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.

Cif.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 18

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 para firma de código, 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 suscriptor debe aceptar el contrato antes de la emisión del certificado.

4.4.2. Publicación del certificado por la CA

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

4.4.3. Notificación de la emisión a terceros

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

4.5. Uso del par de claves y del certificado.

4.5.1. Uso del certificado y la clave privada del suscriptor

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

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

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

4.6. Renovación de certificados.

La renovación del certificado debe ser realizada usando los mismos procedimientos y métodos de identificación que en 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.

Clf.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 19

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.

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.

Cif.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 20

4.8.5. Conducta que constituye la aceptación de un certificado modificado
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.6. Publicación del certificado modificado por la CA
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.7. Notificación de emisión de certificado por la CA a otras entidades
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9. Revocación y suspensión de certificados.

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

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

4.9.3. Procedimiento de solicitud de revocación
La Agencia de Tecnología y Certificación Electrónica acepta solicitudes de revocación por los siguientes procedimientos.

4.9.3.1. Telemático

Accediendo al Área de Gestión de certificados no personales (NPSC) ubicada en <https://npsc.ac-cv.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 902482481.

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.

Clf.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 21

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.

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 subscriptor del certificado de firma de código, mediante correo electrónico firmado digitalmente, en un momento previo anterior a la publicación del certificado en la Lista de Certificados

Cif.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 22

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.

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

La recuperación de las claves de sesión no está soportado.

Cif.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 23

5. CONTROLES DE SEGURIDAD FÍSICA, PROCEDURAL Y DE PERSONAL

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.

Cif.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 24

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 rol

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

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.

Clf.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 25

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 registro de eventos

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 los registros de auditoría

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

5.4.3. Periodo de retención para los registros de auditoría

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

5.4.4. Protección de los registros de auditoría

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

5.4.5. Procedimientos de respaldo de los registros 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 respaldo del archivo.

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

5.5.5. Requerimientos para el sellado de tiempo de los registros.

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

5.5.6. Sistema de recogida de información de auditoría (interno vs externo).

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

5.5.7. Procedimientos para obtener y verificar información archivada

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

5.6. Cambio de Clave

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

5.7. Recuperación en caso de compromiso de una clave o de desastre

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

5.7.1. 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.

Clf.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 27

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.

6. CONTROLES DE SEGURIDAD TECNICA

6.1. Generación e Instalación del par de claves

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

6.1.1. 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

Las claves de la raíz ACCVRAIZ1 y de la ACCVCA-120 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-120 están creadas con el algoritmo RSA

Se utilizan los parámetros definidos en la suite criptográfica sha256-with-rsa especificada en el documento de ETSI TS 119 312 "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites". 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-PK-CSv1_5	MinModLen=2048	rsagen1	emsa-pkcs1-v1_5	sha-256

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.

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

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

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.

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

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.

Clf.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 30

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.

6.2.11. Calificación del módulo criptográfico

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

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.

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

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

Cif.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 31

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.

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. Fuentes de tiempo

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

7. PERFILES DE CERTIFICADO, CRL Y OCSP

7.1. Perfil de Certificado

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

7.1.1. Número de versión

Además de lo establecido en la Declaración de Prácticas de Certificación (CPS) de la ACCV, esta política de certificación especifica la emisión de un certificado con el uso de firma digital.

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 entidad, tal como figura en los registros oficiales. Codificado según la Norma Europea ETSI EN 319 412-1
commonName	Denominación legal del nombre del organismo, empresa o servicio al que se emite el certificado tal y como figura en los registros oficiales.
organizationName	Denominación legal del nombre del organismo, empresa o servicio al que se emite el certificado, igual que en el CommonName. Pueden incluirse nombres alternativos o abreviaturas de uso común mientras no se distorsione o confunda el valor original del nombre del organismo.
localityName	Localidad, Ciudad, Municipio
stateOrProvinceName	Provincia, Estado
countryName	ES (código ISO 3166-1)
Postal Code	Código postal
Street	Dirección (calle o plaza)
Version	V3
SerialNumber	Identificador único del certificado. Menor de 32 caracteres hexadecimales.
Algoritmo de firma	sha256withRSAEncryption
Issuer (Emisor)	
CommonName	ACCVCA-120
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 certificado de firma de código	
Extended Key Usage		
	codeSigning	
CRL Distribution Point		
	http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl	
SubjectAlternativeName		
Permanent Identifier 1.3.6.1.5.5.7.8.3	30 0b 0c 09 53 34 36 31 31 30 30 31 41	
Certificate Policy Extensions		
Policy OID	1.3.6.1.4.1.8149.3.4.3.0	
Policy CPS Location	http://www.accv.es/legislacion_c.htm *	
Policy Notice	Certificado para firma de código expedido por la ACCV (Plaza Nápoles y Sicilia, 6. Valencia CP 46003, ESPAÑA. CIF A40573396)	
Authority Information Access	<i>Access Method</i>	Id-ad-ocsp
	<i>Access Location</i>	http://ocsp.accv.es
	<i>Access Method</i>	Id-ad-calssuers
	<i>Access Location</i>	http://www.accv.es/gestcert/ACCVCA120SHA2.cacert.crt
Fingerprint issuer	48 72 a4 c3 df 17 4c ef 34 d7 7f e6 a3 b4 e7 be 7d f2 d2 5d	
Algoritmo de hash	SHA-256	
KeyUsage (críticos)		
	Digital Signature	

7.1.3. Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

SHA1withRSAEncryption (1.2.840.113549.1.1.5)

SHA256withRSA (1.2.840.113549.1.1.11)

7.1.4. Formatos de nombres

Los certificados emitidos bajo la presente Política de Certificación contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

- Subject name: cn=*Denominación del nombre del organismo, empresa o servicio al que se emite el certificado*, ou=Código, o=ACCV, c=ES

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.

- Issuer name: cn=ACCVCA-120, ou=PKIACCV, o=ACCV, c=ES

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:

1.3.6.1.4.1.8149.3.4.3.0

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-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 35

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-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 36

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 auditorías

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. 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.

Cif.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 38

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 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. 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. 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.

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. Indemnizaciones

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

Clf.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 40

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.

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.

9.12. Modificaciones.

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

9.12.1. Procedimientos de especificación de cambios

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

9.12.2. Procedimientos de publicación y notificación.

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

9.12.3. 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.

Clf.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 41

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.

Anexo I**CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.4****Sección 1 – Datos del solicitante**

Apellidos:

Nombre: DNI/NIF:

Organismo / Servicio:

Organización:

Dirección correo electrónico:

Dirección postal: Tel.:

Sección 2 – Datos del Servicio

Nombre completo:

Razón Social:

Sección 4 – Fecha y Firma

Solicito el Certificado asociado a la Política de Certificación con código 1.3.6.1.4.1.8149.3.4, para Firma de Código, 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 expuestos en <http://www.accv.es>. Declaro, asimismo, que los datos expuestos son verdaderos.

En a de de 2.0....

Firma del solicitante

Fdo.:

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.4.3.0**Condiciones de utilización de los certificados**

1. Los certificados asociados a la la Política de Certificación para Certificados de Firma de Código, emitidos por la ACCV son del tipo X.509v3 y se rigen por la Declaración de Prácticas 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. 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 código firmado 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 como máximo. 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 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 indicando claramente esta voluntad.
14. 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.

Clf.: PÚBLICO	Ref.: ACCV-CP-04V3.0.4-ES-2019.odt	Versión: 3.0.4
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.4.3.0	Pág. 44