



Agencia de Tecnología y Certificación Electrónica

Política de Certificación de Certificados Cualificados de sede electrónica administrativa en soporte software

Fecha: 01/09/2020	Versión: 4.0.6
Estado: APROBADO	Nº de páginas: 45
OID: 1.3.6.1.4.1.8149.3.15.4.0	Clasificación: PÚBLICO
Archivo: ACCV-CP-15V4.0.6-ESP-2020.odt	
Preparado por: Agencia de Tecnología y Certificación Electrónica - ACCV	



Versión	Autor	Gecha	Observaciones
4.0.1	ACCV	27/06/2018	Sin cambios
4.0.2	ACCV	16/07/2019	CAB/Forum modificación
4.0.3	ACCV	16/07/2019	Extensión OCSP
4.0.4	ACCV	16/01/2020	RFC3647 cumplimiento
4.0.5	ACCV	09/03/2020	RFC3647 cumplimiento
4.0.6	ACCV	01/09/2020	Validez Certificado



Tabla de Contenido

1. INTRODUCCIÓN.....	9
1.1. PRESENTACIÓN.....	9
1.2. IDENTIFICACIÓN.....	9
1.3. COMUNIDAD DE USUARIOS Y ÁMBITO DE APLICACIÓN.....	10
1.3.1. Autoridades de Certificación.....	10
1.3.2. Autoridades de Registro.....	10
1.3.3. Suscriptores.....	10
1.3.4. Partes confiantes.....	10
1.3.5. Otros participantes.....	10
1.4. USO DE LOS CERTIFICADOS.....	10
1.4.1. Usos Permitidos.....	10
1.4.2. Usos prohibidos.....	10
1.5. POLÍTICA DE ADMINISTRACIÓN DE LA ACCV.....	11
1.5.1. Especificación de la Organización Administradora.....	11
1.5.2. Competencia para determinar la adecuación de la CPS a la Políticas.....	11
1.5.3. Procedimiento de aprobación.....	11
1.6. DEFINICIONES Y ACRÓNIMOS.....	11
1.6.1. Definiciones.....	11
1.6.2. Acrónimos.....	11
2. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS.....	12
2.1. REPOSITORIO DE CERTIFICADOS.....	12
2.2. PUBLICACIÓN.....	12
2.3. FRECUENCIA DE ACTUALIZACIONES.....	12
2.4. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS.....	12
3. IDENTIFICACIÓN Y AUTENTICACIÓN.....	13
3.1. REGISTRO DE NOMBRES.....	13
3.1.1. Tipos de nombres.....	13
3.1.2. Significado de los nombres.....	13
3.1.3. Interpretación de formatos de nombres.....	13
3.1.4. Unicidad de los nombres.....	13
3.1.5. Resolución de conflictos relativos a nombres.....	13
3.1.6. Reconocimiento, autenticación y función de las marcas registradas.....	13
3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD.....	13
3.2.1. Métodos de prueba de posesión de la clave privada.....	13
3.2.2. Autenticación de la identidad de una organización.....	13
3.2.3. Autenticación de la identidad de un individuo.....	15
3.2.4. Información no verificada de los suscriptores.....	15
3.2.5. Validación de la representación.....	15
3.2.6. Criterios para la interoperación.....	15
3.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DEL PAR DE CLAVES.....	15
3.3.1. Identificación y autenticación de las solicitudes de renovación rutinarias.....	15
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. Procedimiento de alta 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 rechazo de la solicitud.....	18



4.2.3. Plazo para resolver la solicitud.....	18
4.3. EMISIÓN DE CERTIFICADOS.....	18
4.3.1. Acciones de la CA durante el proceso de emisión.....	18
4.3.2. Notificación de la emisión al suscriptor.....	19
4.4. ACEPTACIÓN DE CERTIFICADOS.....	19
4.4.1. Conducta que constituye aceptación del certificado.....	19
4.4.2. Publicación del certificado por la CA.....	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.....	20
4.6.1. Circunstancia para la renovación del certificado.....	20
4.6.2. Quién puede solicitar renovación.....	20
4.6.3. Procesamiento de solicitudes de renovación de certificados.....	20
4.6.4. Notificación de nueva emisión de certificado al suscriptor.....	20
4.6.5. Conducta que constituye la aceptación de un certificado de renovación.....	20
4.6.6. Publicación del certificado de renovación por la CA.....	20
4.6.7. Notificación de 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.....	21
4.7.7. Notificación de emisión de certificado por la CA a otras entidades.....	21
4.8. MODIFICACIÓN DE CERTIFICADOS.....	21
4.8.1. Circunstancia para la modificación del certificado.....	21
4.8.2. Quién puede solicitar la modificación del certificado.....	21
4.8.3. Procesamiento de solicitudes de modificación de certificados.....	21
4.8.4. Notificación de nueva emisión de certificado al suscriptor.....	21
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.....	22
4.9.3.2. Telefónico.....	22
4.9.4. Periodo de gracia de la solicitud de revocación.....	22
4.9.5. Tiempo dentro del cual CA debe procesar la solicitud de revocación.....	22
4.9.6. Requisitos de comprobación de CRLs.....	22
4.9.7. Frecuencia de emisión de CRLs.....	22
4.9.8. Máxima latencia de CRL.....	22
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 periodo de suspensión.....	23
4.10. SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS.....	23
4.10.1. Características operacionales.....	23
4.10.2. Disponibilidad del servicio.....	23
4.10.3. Características opcionales.....	23
4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN.....	23
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, DE GESTIÓN Y DE OPERACIONES.....	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.....	24
5.2.3. Identificación y autenticación para cada papel.....	24
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.....	25
5.3.10. Finalización de los contratos.....	25
5.4. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD.....	25
5.4.1. Tipos de eventos registrados.....	25
5.4.2. Frecuencia de procesado de logs.....	26
5.4.3. Periodo de retención para los logs de auditoría.....	26
5.4.4. Protección de los logs de auditoría.....	26
5.4.5. Procedimientos de backup de los logs 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.....	26
5.5.1. Tipo de informaciones y eventos registrados.....	26
5.5.2. Periodo de retención para el archivo.....	26
5.5.3. Protección del archivo.....	26
5.5.4. Procedimientos de backup del archivo.....	26
5.5.5. Requerimientos para el sellado de tiempo de los registros.....	26
5.5.6. Sistema de recogida de información de auditoría (interno vs externo).....	26
5.5.7. Procedimientos para obtener y verificar información archivada.....	26
5.6. CAMBIO DE CLAVE.....	27
5.7. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O DE DESASTRE.....	27
5.7.1. Alteración de los recursos hardware, software y/o datos.....	27
5.7.2. La clave pública de una entidad se revoca.....	27
5.7.3. La clave de una entidad se compromete.....	27
5.7.4. Instalación de seguridad después de un desastre natural u otro tipo de desastre.....	27
5.8. CESE DE UNA CA.....	27
6. CONTROLES DE SEGURIDAD TÉCNICA.....	28
6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES.....	28
6.1.1. Generación del par de claves.....	28
6.1.2. Entrega de la clave privada a la entidad.....	28
6.1.3. Entrega de la clave pública al emisor del certificado.....	28



6.1.4. Entrega de la clave pública de la CA a los usuarios.....	28
6.1.5. Tamaño de las claves.....	28
6.1.6. Parámetros de generación de la clave pública.....	28
6.1.7. Propósitos de uso de claves.....	28
6.2. PROTECCIÓN DE LA CLAVE PRIVADA.....	29
6.2.1. Estándares para los módulos criptográficos.....	29
6.2.2. Control multipersona de la clave privada.....	29
6.2.3. Custodia de la clave privada.....	29
6.2.4. Copia de seguridad de la clave privada.....	29
6.2.5. Archivo de la clave privada.....	29
6.2.6. Introducción de la clave privada en el módulo criptográfico.....	29
6.2.7. Almacenamiento de clave privada en el módulo criptográfico.....	29
6.2.8. Método de activación de la clave privada.....	29
6.2.9. Método de desactivación de la clave privada.....	30
6.2.10. Método de destrucción de la clave privada.....	30
6.2.11. Calificación del módulo criptográfico.....	30
6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES.....	30
6.3.1. Archivo de la clave pública.....	30
6.3.2. Periodo de uso para las claves públicas y privadas.....	30
6.4. DATOS DE ACTIVACIÓN.....	30
6.4.1. Generación y activación de los datos de activación.....	30
6.4.2. Protección de los datos de activación.....	30
6.4.3. Otros aspectos de los datos de activación.....	30
6.5. CONTROLES DE SEGURIDAD INFORMÁTICA.....	30
6.5.1. Requerimientos técnicos de seguridad informática específicos.....	30
6.5.2. Valoración de la seguridad informática.....	31
6.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA.....	31
6.6.1. Controles de desarrollo del sistema.....	31
6.6.2. Controles de gestión de la seguridad.....	31
6.6.3. Evaluación de la seguridad del ciclo de vida.....	31
6.7. CONTROLES DE SEGURIDAD DE LA RED.....	31
6.8. TIMESTAMPING.....	31
7. PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS.....	32
7.1. PERFIL DE CERTIFICADO.....	32
7.1.1. Número de versión.....	32
7.1.2. Extensiones del certificado.....	32
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”.....	36
7.1.8. Sintaxis y semántica de los cualificadores de política.....	36
7.1.9. Tratamiento semántico para la extensión “Certificate Policy”.....	36
7.1.10. Lista de Signed Certificate Timestamp (SCT).....	36
7.2. PERFIL DE CRL.....	36
7.2.1. Número de versión.....	36
7.2.2. CRL y extensiones.....	36
7.3. PERFIL DE OCSP.....	37
7.3.1. Número de versión.....	37
7.3.2. Extensiones.....	37
8. AUDITORÍA DE CONFORMIDAD.....	38
8.1. FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD PARA CADA ENTIDAD.....	38
8.2. IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR.....	38
8.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA.....	38
8.4. TÓPICOS CUBIERTOS POR EL CONTROL DE CONFORMIDAD.....	38
8.5. ACCIONES A TOMAR COMO RESULTADO DE UNA DEFICIENCIA.....	38
8.6. COMUNICACIÓN DE RESULTADOS.....	38



8.7. AUTO AUDITORIAS.....	38
9. REQUISITOS COMERCIALES Y LEGALES.....	39
9.1. TARIFAS.....	39
9.1.1. Tarifas de emisión de certificado o renovación.....	39
9.1.2. Tarifas de acceso a los certificados.....	39
9.1.3. Tarifas de acceso a la información de estado o revocación.....	39
9.1.4. Tarifas de otros servicios como información de políticas.....	39
9.1.5. Política de reintegros.....	39
9.2. CAPACIDAD FINANCIERA.....	39
9.2.1. Indemnización a los terceros que confían en los certificados emitidos por la ACCV.....	39
9.2.2. Relaciones fiduciarias.....	39
9.2.3. Procesos administrativos.....	39
9.3. POLÍTICA DE CONFIDENCIALIDAD.....	39
9.3.1. Información confidencial.....	39
9.3.2. Información no confidencial.....	39
9.3.3. Divulgación de información de revocación /suspensión de certificados.....	40
9.4. PROTECCIÓN DE DATOS PERSONALES.....	40
9.4.1. Plan de Protección de Datos Personales.....	40
9.4.2. Información considerada privada.....	40
9.4.3. Información no considerada privada.....	40
9.4.4. Responsabilidades.....	40
9.4.5. Prestación del consentimiento en el uso de los datos personales.....	40
9.4.6. Comunicación de la información a autoridades administrativas y/o judiciales.....	40
9.4.7. Otros supuestos de divulgación de la información.....	40
9.5. DERECHOS DE PROPIEDAD INTELECTUAL.....	40
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. Obligaciones de los terceros confiantes en los certificados emitidos por la ACCV.....	41
9.6.5. Obligaciones del repositorio.....	41
9.7. RENUNCIAS DE GARANTÍAS.....	41
9.8. LIMITACIONES DE RESPONSABILIDAD.....	41
9.8.1. Garantías y limitaciones de garantías.....	41
9.8.2. Deslinde de responsabilidades.....	41
9.8.3. Limitaciones de pérdidas.....	41
9.9. INDEMNIZACIONES.....	41
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.....	42
9.12.1. Procedimientos de especificación de cambios.....	42
9.12.2. Procedimientos de publicación y notificación.....	42
9.12.3. Procedimientos de aprobación de la Declaración de Prácticas de Certificación.....	42
9.13. RESOLUCIÓN DE CONFLICTOS.....	42
9.13.1. Resolución extrajudicial de conflictos.....	42
9.13.2. Jurisdicción competente.....	42
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.....	43
9.16.4. Cumplimiento (honorarios de abogados y exención de derechos).....	43
9.16.5. Fuerza mayor.....	43
9.17. OTRAS CUESTIONES.....	43



10. ANEXO I.....44

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0.6
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 8

1.INTRODUCCIÓN

1.1.Presentación

El presente documento es la Política de Certificación asociada a los certificados cualificados de sede electrónica administrativa en soporte software, que contiene las reglas a las que se sujeta la gestión y el uso de los certificados definidos en esta política. Se describen los papeles, responsabilidades y relaciones entre el usuario final y la Agencia de Tecnología y Certificación Electrónica y las reglas de solicitud, adquisición gestión y uso de los certificados. Este documento matiza y complementa a la *Declaración de Prácticas de Certificación (CPS)* de la Agencia de Tecnología y Certificación Electrónica.

La Política de Certificación referida en este documento se utilizará para la emisión de certificados cualificados de sede electrónica en soporte software.

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

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

1.2.Identificación

Nombre de la política	Política de Certificación de Certificados Cualificados de sede electrónica administrativa en soporte software
Calificador de la política	Certificado cualificado de sede electrónica administrativa expedido por la ACCV (Plz Nápoles y Sicilia, 6. Valencia CP 46003, ESPAÑA. CIF A40573396)
Versión de la política	4.0.6
Estado de la política	APROBADO
Referencia de la política / OID (Object Identifier)	1.3.6.1.4.1.8149.3.15.4.0
Fecha de emisión	01/09/2020
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 de usuarios y ámbito de aplicación

1.3.1.Autoridades de Certificación

La CA que puede emitir certificados acordes con esta política es 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 ACCVCA-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 grupo de usuarios que pueden solicitar certificados definidos por esta política está limitado exclusivamente al compuesto por el conjunto 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.

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

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

- a. Los usuarios de clientes de aplicaciones en el ámbito de la verificación de la identidad de la sede electrónica a la que se conectan y del cifrado del canal de los datos transmitidos entre ellos.
- b. Las aplicaciones y servicios con capacidades de soporte SSL y/o TLS, en el ámbito de verificación de la identidad de las sedes electrónica a las que se conectan, y del cifrado del canal de los datos transmitidos entre ellos.

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 dotar a las sedes electrónicas de capacidades SSL/TLS. Asimismo, pueden utilizarse como mecanismo de identificación de estas sedes de forma inequívoca ante servicios y aplicaciones informáticas.

1.4.2.Usos prohibidos

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

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 10



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. 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.

1.5.3. 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

Bastionado: es el proceso mediante el cual se implementa una política de seguridad específica sobre una instalación de un sistema operativo. El bastionado de un equipo intenta reducir el nivel de exposición de un equipo y, por tanto, los riesgos y vulnerabilidades asociados a éste.

1.6.2. Acrónimos

SSL: Secure Sockets Layer

TLS: Transport Security Layer

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 11



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

Ademas de lo especificado en la Declaración de Prácticas de Certificación (CPS), ACCV mantiene sitios web de test que permiten a los integradores y desarrolladores de aplicaciones probar sus desarrollos con certificados de usuario de la presente política.

VALIDO

<https://activo.accv.es/test/hola.html>

REVOCADO

<https://revocado.accv.es:442/test/hola.html>

CADUCADO

<https://caducado.accv.es:444/test/hola.html>

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-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 12



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.

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 sede electrónica.

El solicitante debe suministrar la documentación necesaria que incluye:

La información relativa a la organización, como la inclusión en el Registro Mercantil o equivalente, razón social, dirección, provincia, país, códigos de operación, etc..

La capacidad de representación de la entidad que posee los dominios correspondientes a la solicitud.

Las pruebas de posesión de los dominios

Toda la documentación y pruebas se suministrara de manera electrónica, utilizando para ello los procedimientos y aplicaciones establecidos por la ACCV.

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 13



ACCV validará la información, incluyendo el país del solicitante, utilizando la información disponible en:

- Registros Públicos disponibles (Registro Comercial o equivalente)
- Registros de personal
- Agencias de protección de datos
- Servicios de verificación y consulta de datos de identidad

reclamando al solicitante las explicaciones o subsanaciones que fueran necesarias.

Todas las Agencias y registros usados son oficiales y de confianza reconocida, proporcionando evidencia de todas las búsquedas realizadas.

ACCV conserva esta información para propósitos de auditoria, y permite la reutilización de la información durante 13 meses desde la última consulta validada.

Verificación de dominios

ACCV verificará que los dominios de la solicitud y sus direcciones asociadas pertenecen al solicitante usando para ello la información disponible en registros personales y de dominio, requiriendo al solicitante las explicaciones o documentos adicionales que se consideren necesarios. ACCV no emitirá en ningún caso certificados a direcciones ip o dominios internos. En el caso de gTLD, solo se aceptarán solicitudes con nombre gTLD aprobados, y solo a solicitantes que puedan probar el control del gTLD tal y como aparecen en ICANN/IANA.

Específicamente:

- Comprobando que el solicitante, cuya identidad ha sido verificada sin duda, es uno de los propietarios del dominio. Para esta validación se deben utilizar uno de los siguientes métodos:

Contactando por correo, enviando un número aleatorio único a la dirección de correo que aparece en la información de registro del dominio, La respuesta, que no debe demorarse más de 30 días, debe contener el mismo número aleatorio del correo inicial.

Contactando por correo, enviando un número aleatorio único a una o más direcciones creadas usando 'admin', 'administrator', 'webmaster', 'hostmaster', o 'postmaster' como parte local, seguido por el carácter arroba ("@") y a continuación el dominio a verificar. Se enviará un número aleatorio único en el correo que se debe utilizar en la respuesta. Este mecanismo solo es válido por 30 días desde el envío del correo inicial.

Confirmando la presencia de un valor único aleatorio como dato de un fichero de texto enlazado en el directorio "/.well-known/pki-validation" del nombre de dominio solicitado, accesible desde la CA utilizando HTTP/HTTPS en un puerto autorizado. Una vez el valor del número aleatorio único es comunicado al solicitante solo será válido por 30 días.

Confirmando la presencia de un valor único aleatorio como dato de un registro DNS de tipo CNAME, TXT o CAA. Este registro puede ser para 1)El dominio de la solicitud o 2)el dominio de la solicitud con una etiqueta inicial que empiece con un guion bajo. Una vez el valor del número aleatorio único es comunicado al solicitante solo será válido por 30 días.

- ACCV comprobará los registros CAA antes de la emisión del certificado, actuando como se define en el estándar RFC 6844 y en los documentos del CAB/Forum si el registro está presente. El identificador asociado con ACCV para los registros CAA issue y issuewild es "accv.es".

- Además de las consultas WHOIS se deben efectuar tests de conexión con el dominio solicitado y test de las respuestas DNS usando protocolos seguros.

- Si es un certificado con un carácter wildcard (*), la aplicación para hacer las solicitudes (NPSC) solo permite que el comodín aparezca en una posición válida (nunca se permite un comodín en la primera posición a la izquierda de un sufijo público genérico o de país).

Si se detecta cualquier irregularidad ACCV informará al solicitante y la emisión se suspenderá hasta su corrección. Si esta corrección no ocurre en el plazo máximo de un mes la solicitud será denegada.

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 14



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 sede electrónica.

El solicitante deberá presentar además la documentación necesaria que determine la capacidad de representar a la entidad propietaria de la sede electrónica y la posesión del dominio al que hace referencia. Esta presentación se realizará de manera telemática utilizando los medios que la ACCV ponga a disposición de los usuarios (3.2.2).

ACCV validará la información, incluyendo el país del solicitante, utilizando la información disponible en:

Registros Públicos disponibles (Registro Comercial o equivalente)

Registros de personal

Agencias de protección de datos

Servicios de verificación y consulta de datos de identidad

reclamando al solicitante las explicaciones o subsanaciones que fueran necesarias.

Todas las Agencias y registros usados son oficiales y de confianza reconocida, proporcionando evidencia de todas las búsquedas realizadas.

ACCV conserva esta información para propósitos de auditoria, y permite la reutilización de la información durante 13 meses desde la última consulta validada.

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). ACCV puede reutilizar la información almacenada de validaciones anteriores si no han pasado más de 13 meses desde la última verificación de los datos. Existe, por tanto, un mecanismo para la renovación:

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

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	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, y es posible reutilizar la información en posesión de la ACCV si no han pasado más de 13 meses desde la última verificación de datos.

ACCV puede implementar otros mecanismos electrónicos que garanticen de manera fiable e inequívoca la identidad del solicitante y la autenticidad de la solicitud debido a posibles dificultades técnicas, detallando siempre cada paso del proceso y almacenando todas las evidencias.

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.

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

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	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

4.1.1.Legitimación de la solicitud

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

La solicitud de este tipo de certificados es responsabilidad de la Administración Pública o entidades de carácter público. Una solicitud de certificado puede ser realizada por el suscriptor del certificado o por un representante autorizado de dicho suscriptor.

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://npsc.accv.es:8450/npsc>. Si se solicita por primera vez el certificado de sede asociado a una Administración Pública 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), en formato pdf firmado electrónicamente. Si el acceso se ha efectuado con certificado de Empleado Público o de Representante se utilizarán los datos de Organización, Unidad Organizativa y Cargo de dicho certificado.

ACCV comprobará los datos de la solicitud y acreditará al solicitante para la solicitud de certificados de sede electrónica, 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.

ACCV conserva la información de la solicitud y todos los datos asociados a la misma durante al menos 15 años, incluyendo su aprobación o rechazo y las razones de la misma.

El usuario deberá marcar la opción software en servidor bastionado en la solicitud de certificado.

4.2.Tramitación de la solicitud de certificados.

4.2.1.Ejecución de las funciones de identificación y autenticación

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*. Una vez identificado se procederá a proporcionar por los canales establecidos toda la documentación necesaria para este tipo de certificados que no estuviera en posesión de la ACCV o no estuviera en vigor.

- Documentación asociada al organismo

- Documentación asociada a las credenciales personales para la solicitud y gestión en nombre de dicho organismo.

La Autoridad de registro comprueba la documentación y valida los datos utilizando registros accesibles al público para dicha verificación (3.2.2). Una vez comprobados todos los datos, ACCV acreditará al solicitante para la solicitud de certificados de sede electrónica administrativa, 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.

Además de validar las credenciales personales y de la entidad, ACCV verifica en los registros autorizados la posesión del dominio o dominios asociados a la solicitud, de forma que no haya dudas

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 17



en la existencia de esta posesión tal y como se ha detallado en los apartados 3.2.2 y 3.2.3 de esta política. ACCV proporciona registros de esas búsquedas garantizando que pueden reproducirse en cada paso. Para todas estas validaciones se utilizan las direcciones de correo y telefonéo proporcionados en el proceso de registro, siendo necesario una conexión directa entre estos datos y los dominios incluidos en la solicitud.

Como parte de este proceso, ACCV comprueba que la solicitud de certificado no incluye dominios que puedan ser usados para phishing u otros usos fraudulentos, utilizando listas y mecanismos de uso público y de confianza.

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 firmado digitalmente 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 firmado a la dirección que figura en la solicitud. La solicitud se cancelará y no podrá reutilizarse, aunque es posible reutilizar la documentación suministrada que haya sido verificada por un periodo no superior a 13 meses.

Este proceso es llevado a cabo por un miembro de ACCV diferente al que ha llevado a cabo la validación de los datos. La diferenciación de roles se consigue usando las capacidades incluidas en la aplicación de gestión y registro.

ACCV utilizará esta información para decidir sobre nuevas solicitudes.

4.2.3. Plazo para resolver la solicitud

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

4.3. Emisión de certificados

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

4.3.1. Acciones de la CA durante el proceso de emisión

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 aceptación debe acceder a NPSC de nuevo, identificándose con certificado personal cualificado para generar y descargar el certificado.

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. En este punto se hace de nuevo la comprobación del registro CAA.
- CA realiza una verificación de la firma de la RA y confirma el formato del CSR.

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 18



- 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.

El responsable del certificado de sede electrónica puede solicitar a ACCV que añada a otros usuarios con capacidad para realizar los trámites asociados al ciclo de vida del certificado 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.

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.

ACCV llevara acabo revisiones frecuentes sobre una muestra de los certificados de sede emitidos para garantizar la exactitud de los datos. Si en el curso de esas revisiones se confirman cambios en los datos que pueden involucrar perdidas de posesión de los dominios, ACCV revocara los certificados afectados. En caso de inexactitud de la información contenida en el certificado se llevara a cabo el mismo proceso. ACCV mantendrá prueba documental de todas las revisiones y acciones.

4.3.2. Notificación de la emisión al suscriptor

ACCV notifica al suscriptor sobre la emisión del certificado, a través de un correo electrónico firmado 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 sello, con el conocimiento de las normas de uso y con la veracidad de los datos presentados. El formulario del Contrato de Certificación se recoge en el Anexo I de esta Política de Certificación.

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

4.4.2. Publicación del certificado por la CA

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

4.4.3. Notificación de la emisión a terceros

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

4.5. Uso del par de claves y del certificado.

4.5.1. Uso del certificado y la clave privada del suscriptor

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

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

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

Clf.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 19



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.

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.

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 20



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.

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.

Clf.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 21



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 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.

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

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.

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 22



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 sede, mediante correo electrónico firmado digitalmente, en un momento previo anterior a la publicación del certificado en la Lista de Certificados Revocados, acerca de la suspensión o revocación de 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 esta soportado.

Clf.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 23



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-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 24



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.

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 25



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-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 26



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.Alteración de los recursos hardware, software y/o datos

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

5.7.2.La clave pública de una entidad se revoca

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

5.7.3.La clave de una entidad se compromete

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

5.7.4.Instalación de seguridad después de un desastre natural u otro tipo de desastre

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

5.8.Cese de una CA

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

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 27

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

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" (6 - Signature schemes). Se define ModLen=2048.

El esquema de relleno (padding) utilizado es emsa-pkcs1-v2.1 (RFC 3447 sección 9.2)

Signature suite entry name	Signature algorithm	Signature algorithm parameters	Key generation algorithm	Padding method	Cryptographic hash function
sha256-with-rsa	RSA-PKCSv1_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.

Se recomienda utilizar sistemas para almacenar las claves privadas que cumplan una serie de requisitos de seguridad físicos y lógicos. ACCV puede solicitar a su discreción que el suscriptor describa los mecanismos utilizados para bastionar dichos sistemas.

ACCV aconseja utilizar las guías del Centro Criptológico Nacional (Serie STIC del CCN) para asegurar la seguridad de los sistemas de información y comunicaciones involucrados.

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.

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 29



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 12 meses como máximo.

La clave utilizada para la emisión de los certificados se crea para cada emisión, y por tanto también tienen una validez de 12 meses 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

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.

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 30



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. TimeStamping

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

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 31



7. Perfiles de certificados y listas de certificados revocados

7.1. Perfil de Certificado

7.1.1. Número de versión

ACCV utiliza certificados X.509 versión 3 (X.509 v3).

Esta política de certificación especifica el uso de un certificado con dos usos distintos; firma digital, y cifrado de clave.

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 suscriptora del certificado, a la que se encuentra vinculada la sede.
CommonName	Denominación de nombre de dominio (DNS) donde residirá el certificado.
OrganizationIdentifier (2.5.4.97)	NIF de la entidad, tal como figura en los registros oficiales. Codificado Según la Norma Europea ETSI EN 319 412-1
OrganizationalUnit	El nombre descriptivo de la sede.
OrganizationalUnit	Cadena fija con el valor SEDE ELECTRONICA
Organization	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada la sede
Jurisdiction Country	ES
Business Category	Government Entity
Locality	Ciudad
State	Provincia
Country	ES Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas.
Version	V3
SerialNumber	Identificador único del certificado. Menor de 32 caracteres hexadecimales.
Algoritmo de firma	sha256withRSAEncryption
Issuer (Emisor)	
CommonName	ACCVCA-120
OrganizationalUnit	PKIGVA
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 sede
Extended Key Usage		
	Server Authentication	
	Client Authentication	
CRL Distribution Point		
	distributionPoint	http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl
SubjectAlternativeName		
	dnsName	Nombre Dominio DNS de la Sede
	dnsName	Nombre Dominio DNS de la Sede
	dnsName	Nombre Dominio DNS de la Sede
Certificate Policy Extensions		
Policy OID	{itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovc(7)}	
	0.4.0.2042.1.7	
Policy OID	{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)}	
	2.23.140.1.2.2	
Policy OID	2.16.724.1.3.5.5.2	
Policy OID	QCP-w Certificado cualificado de sitio web acorde al Reglamento UE 910/2014	
	itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web (4)	
	0.4.0.194112.1.4	
Policy OID	1.3.6.1.4.1.8149.3.15.4.0	
Policy CPS Location	http://www.accv.es/legislacion_c.htm *	
Policy Notice	Certificado cualificado de sede electrónica administrativa expedido por la ACCV (Plz Nápoles y Sicilia, 6. Valencia CP 46003, ESPAÑA. CIF A40573396)	
Authority Information Access	<i>Access Method</i>	ld-ad-ocsp
	<i>Access Location</i>	http://ocsp.accv.es
	<i>Access Method</i>	ld-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 Key Encipherment	
SCT List 1.3.6.1.4.1.11129.2.4.2	Signed Certificate Timestamp List	
QcStatement	Campos QC (Qualified Certificate)	
QcCompliance		El certificado es cualificado
QcType	web	Tipo particular de certificado cualificado
QcRetentionPeriod	15y	Periodo de retención de la información material
QcPDS	https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-V1.0-EN.pdf	Ubicación de PKI Disclosure Statement
CA/Browser Forum Organization Identifier Field	cabfOrganizationIdentifier (OID: 2.23.140.3.1) {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-extensions(3) cabf-organization-identifier(1) }	
	registrationSchemeIdentifier	3 character Registration Scheme identifier (VAT)
	registrationCountry	2 character ISO 3166 country code (ES)
	registrationStateOrProvince	State or Province (optional)
	registrationReference	Registration Reference allocated in accordance with the identified Registration Scheme (CIF)

En todos los casos se cumplirán las especificaciones y límites establecidas en el estándar RFC-5280

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)

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.

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

Clf.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 34



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.

El campo subjectAlternativeName contiene al menos una entrada. Cada entrada en el campo subjectAlternativeName debe ser del tipo dNSName conteniendo el nombre completo cualificado de un sistema.

Subject:

commonName (obligatorio). Debe ser igual a uno de las entradas DNSName del subjectAlternativeName

serialNumber (obligatorio). NIF de la entidad, definido en [Real Decreto 1065/2007, de 27 de Julio](#).

OrganizationIdentifier (obligatorio) Identificador de la entidad, siguiendo el formato definido en el estándar europeo ETSI EN 319 412-1

OrganizationalUnit (obligatorio) cadena fija "SEDE ELECTRONICA"

jurisdictionCountry (obligatorio) Código de país ISO 3166-1

BusinessCategory (obligatorio) cadena fija "Government Entity"

Organization (obligatorio) Designación (nombre oficial) de la Administración, organismo o entidad en nombre de la cual actúa el suscriptor del certificado y propietario del dominio.

locality (obligatorio) Ciudad

state (obligatorio) Estado o provincia

country (obligatorio) Código de país ISO 3166-1

7.1.5. Restricciones de los nombres

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

No hay restricciones definidas para los certificados emitidos bajo la presente política.

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:

1.3.6.1.4.1.8149.3.15.4.0

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

2.16.724.1.3.5.5.2 Certificado de sede electrónica de nivel medio/sustancial

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

0.4.0.194112.1.4 Política de certificación para certificados cualificados EU emitidos a sitios web

En este caso se añade un OID para identificar el tipo de entidad que se representa según las guías del CAB/Forum

2.23.140.1.2.2 Certificates issued in accordance with the CA/Browser Forum's Baseline Requirements - Organization identity asserted

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 35

En este caso se añade un OID para identificar el tipo de entidad que se representa según el estándar ETSI EN 319 411-1

0.4.0.2042.1.7

Organizational Validation Certificate Policy (OVCP)

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. lado

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.

7.1.10. Lista de Signed Certificate Timestamp (SCT)

Respuestas de logs cualificados conocidos que complan con la política de Transparencia de Certificados de Chrome.

Extensión OID: 1.3.6.1.4.1.11129.2.4.2

RFC 6962 (Certificate Transparency): <https://tools.ietf.org/html/rfc6962>

El mínimo número de respuestas viene determinado por el ciclo de vida de los certificados:

Lifetime of Certificate Number of SCTs from distinct logs

< 15 months	2
>= 15, <= 27 months	3
> 27, <= 39 months	4
> 39 months	5

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-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 36



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-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 37



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.

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 38



9.Requisitos comerciales y legales

9.1.Tarifas

9.1.1.Tarifas de emisión de certificado o renovación

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

9.1.2.Tarifas de acceso a los certificados

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

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

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

9.1.4.Tarifas de otros servicios como información de políticas

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

9.1.5.Política de reintegros

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

9.2.Capacidad financiera

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

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

9.2.2.Relaciones fiduciarias

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

9.2.3.Procesos administrativos

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

9.3.Política de Confidencialidad

9.3.1.Información confidencial.

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

9.3.2.Información no confidencial

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

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 39



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

9.4.Protección de datos personales

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

9.4.1.Plan de Protección de Datos Personales.

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

9.4.2.Información considerada privada.

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

9.4.3.Información no considerada privada.

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

9.4.4.Responsabilidades.

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

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

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

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

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

9.4.7.Otros supuestos de divulgación de la información.

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

9.5.Derechos de propiedad Intelectual

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

9.6.Obligaciones y Responsabilidad Civil

9.6.1.Obligaciones de la Entidad de Certificación

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

9.6.2.Obligaciones de la Autoridad de Registro

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

9.6.3.Obligaciones de los suscriptores

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

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 40



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

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

9.6.5.Obligaciones del repositorio

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

9.7.Renuncias de garantías

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

9.8.Limitaciones de responsabilidad

9.8.1.Garantías y limitaciones de garantías

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

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

9.8.2.Deslinde de responsabilidades

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

9.8.3.Limitaciones de pérdidas

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

9.9.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.

Clf.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 41



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.

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. Procedimientos de aprobación de la Declaración de Prácticas de Certificación

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

9.13. Resolución de conflictos.

9.13.1. Resolución extrajudicial de conflictos.

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

9.13.2. Jurisdicción competente.

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

9.14. Legislación aplicable

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

9.15. Conformidad con la Ley aplicable.

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

9.16. Cláusulas diversas.

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.

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 42



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.

9.17. Otras cuestiones

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

Cif.: PÚBLICO	Ref.: ACCV-CP-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 43



10.Anexo I

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.15

Sección 1 – Datos del solicitante

Apellidos:

Nombre:

NIF:

Tel.:

Puesto o cargo:

Administración-Organización:

CIF de la Organización:

Dirección correo electrónico:

Dirección postal:

Sección 2 – Datos de la sede electrónica

Nombre cualificado:

Alias (si el certificado no se emite al nombre cualificado):

Nombre descriptivo de la sede electrónica:

Dirección de correo de contacto:

Sección 3 – Fecha y Firma

Suscribo el presente contrato de certificación asociado a la Política de Certificación de Certificados Cualificados de Sede Electrónica Administrativa en soporte software con código 1.3.6.1.4.1.8149.3.15, 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:



CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.15

Condiciones de utilización de los certificados

1. Los certificados asociados a la Política de Certificación para Certificados Cualificados de Sede Electrónica Administrativa en soporte software, emitidos por la ACCV son del tipo X.509v3 y se rigen por la Declaración de Prácticas de Certificación de la ACCV, en tanto que Prestador de Servicios de Certificación, así como por la Política de Certificación referida. Ambos documentos se deben interpretar según la legislación de la Comunidad Europea, el Ordenamiento Jurídico Español y la legislación propia de la Generalitat.
 2. 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 contenido de los documentos firmados haciendo uso de los certificados por ella emitidos.
 7. La Agencia de Tecnología y Certificación Electrónica, es responsable del cumplimiento de las legislaciones Europea, Española y Valenciana, por lo que a Firma Electrónica se refiere. Es, asimismo, responsable del cumplimiento de lo dispuesto en la Declaración de Prácticas de Certificación de la ACCV y en la Política de Certificación asociada a este tipo de certificados.
 8. El periodo de validez de estos certificados es de 12 meses 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 documentación a aportar para la identificación de la persona física solicitante del certificado será su certificado cualificado personal frente a la autoridad de registro. El solicitante deberá aportar los datos relativos a su relación con la Administración Pública, Ente Instrumental de la Administración o Entidad Corporativa de Derecho Público.
 11. El cumplimiento de la ley 15/1.999, de 13 de diciembre, de Protección de Datos de Carácter Personal y la Regulación (EU) 2016(679) del Parlamento y Consejo Europeos del 27 de abril, se informa al solicitante de la existencia de un fichero automatizado de datos de carácter personal creado bajo la responsabilidad de la Agencia de Tecnología y Certificación Electrónica. La finalidad de dicho fichero es la servir a los usos relacionados con los servicios de certificación prestados por la 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, cancelación, portabilidad, restricción de proceso y objeción sobre sus datos de carácter personal dirigiendo escrito a la Agencia de Tecnología y Certificación Electrónica, a través de cualquiera de los Registros de Entrada de la Generalitat 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-15V4.0.6-ESP-2020.odt	Versión: 4.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pág. 45