Agencia de Tecnología y Certificación Electrónica

Declaración de Prácticas y Políticas de Certificación de certificados de autenticación de sitios web

Fecha: 03/06/2025	**Versión:** 4.0.17
Estado: APROBADO	**Nº de páginas:** 115
OID: 1.3.6.1.4.1.8149.2.4.0	**Clasificación: PUBLICO**
Archivo: ACCV-CPS-CP-V4.0.17-ES-2025.docx	

Cambios

Versión	Autor	Fecha	Observaciones
4.0.1	ACCV	20/05/2017	Sin cambios
4.0.2	ACCV	03/09/2018	Modificación CAB/Forum
4.0.3	ACCV	03/02/2019	Extensión OCSP
4.0.4	ACCV	19/07/2019	Correcciones RFC364. Modificaciones en el tratamiento del correo
4.0.5	ACCV	29/07/2019	Modificación en el numero de serie
4.0.6	ACCV	15/01/2020	Correcciones menores RFC3647. .
4.0.7	ACCV	24/02/2020	Cambios menores en la Ley. Correcciones RFC3647
4.0.8	ACCV	20/03/2021	Cambio en la dirección de la sede. Pruebas del compromiso de clave
4.0.9	ACCV	20/04/2022	Revisión y corrección
4.0.10	ACCV	02/12/2022	Se incluye la video identificación
4.0.11	ACCV	16/03/2023	Revisión y cambios menores
4.0.12	ACCV	10/09/2023	Adaptación a la política 2.0.0 del CAB/Forum
4.0.13	ACCV	02/04/2024	Revisión
4.0.14	ACCV	10/06/2024	Nueva jerarquía TLS y revisión
4.0.15	ACCV	13/01/2025	Eliminación nueva jerarquía
4.0.16	ACCV	12/02/2025	Nueva jerarquía TLS y revisión
4.0.17	ACCV	03/06/2025	Unificación CPS y CP

Tabla de Contenido

1. INTRODUCCIÓN 13

1.1. PRESENTACIÓN 13

1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN 13

1.3. COMUNIDAD DE USUARIOS Y ÁMBITO DE APLICACIÓN 14

1.3.1. Autoridades de Certificación 14

1.3.1.1. Autoridades de Certificación Raíz 14

1.3.1.1.1. ACCVRAIZ1 14

1.3.1.1.2. ACCV ROOT ECC TLS 2024 15

1.3.1.1.3. ACCV ROOT RSA TLS 2024 15

1.3.1.2. Autoridades de Certificación Subordinadas 15

1.3.2. Autoridades de Registro 17

1.3.3. Suscriptores 18

1.3.4. Partes confiantes 18

1.3.5. Otros participantes 18

1.3.5.1. Solicitantes 18

1.4. USO DE LOS CERTIFICADOS 18

1.4.1. Usos permitidos 18

1.4.2. Usos prohibidos 19

1.5. POLÍTICA DE ADMINISTRACIÓN DE ACCV 19

1.5.1. Especificación de la Organización Administradora 19

1.5.2. Persona de Contacto 19

1.5.2.1. Dirección de comunicación de problemas 19

1.5.3. Competencia para determinar la adecuación de la DPC 19

1.5.4. Procedimiento de aprobación de la DPC 19

1.6. DEFINICIONES Y ACRÓNIMOS 20

1.6.1. Definiciones 20

1.6.2. Acrónimos 23

2. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS 24

2.1. REPOSITORIO DE CERTIFICADOS 24

2.2. PUBLICACIÓN 25

2.3. FRECUENCIA DE ACTUALIZACIONES 26

2.4. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS 26

3. IDENTIFICACIÓN Y AUTENTICACIÓN 27

3.1. REGISTRO DE NOMBRES 27

3.1.1. Tipos de nombres 27

3.1.2. Significado de los nombres 27

3.1.3. Anonimización o seudoanonimización de los suscriptores 27

3.1.4. Interpretación de formatos de nombres 27
3.1.5. Unicidad de los nombres 27
3.1.6. Reconocimiento, autenticación y función de las marcas registradas 27
3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD 28
3.2.1. Métodos de prueba de posesión de la clave privada 28
3.2.2. Autenticación de la identidad de una organización 28
3.2.3. Autenticación de la identidad de un individuo 31
3.2.4. Información no verificada 31
3.2.5. Validación de la autoridad 31
3.2.6. Criterio para la interoperación 32
3.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DE LA CLAVE 32
3.3.1. Identificación y autenticación de las solicitudes de renovación rutinarias 32
3.3.2. Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida 32
3.4. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DE LA CLAVE 32

4. EL CICLO DE VIDA DE LOS CERTIFICADOS 33

4.1. SOLICITUD DE CERTIFICADOS 33
4.1.1. Quien puede enviar una solicitud de certificado 33
4.1.2. Proceso de registro y responsabilidades 33
4.2. TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADOS 33
4.2.1. Realización de las funciones de identificación y autenticación 33
4.2.2. Aprobación o rechazo de la solicitud del certificado 34
4.2.3. Tiempo en procesar la solicitud 34
4.3. EMISIÓN DE CERTIFICADOS 34
4.3.1. Acciones de la Autoridad de Certificación durante la emisión 34
4.3.2. Notificación al suscriptor 35
4.4. ACEPTACIÓN DE CERTIFICADOS 35
4.4.1. Proceso de aceptación 35
4.4.2. Publicación del certificado por la Autoridad de Certificación 35
4.4.3. Notificación de la emisión a otras entidades 35
4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO 35
4.5.1. Clave privada del suscriptor y uso del certificado 35
4.5.2. Uso del certificado y la clave pública por terceros que confían 36
4.6. RENOVACIÓN DE CERTIFICADOS 36
4.6.1. Circunstancias para la renovación del certificado 36
4.6.2. Quién puede solicitar la renovación del certificado 36
4.6.3. Tramitación de solicitudes de renovación de certificados 36
4.6.4. Notificación de la emisión de un nuevo certificado al suscriptor 36
4.6.5. Conducta que constituye la aceptación de la renovación del certificado 36

4.6.6. Publicación del certificado de renovación por parte de la Autoridad de Certificación....36
4.6.7. Notificación de la renovación del certificado a otras entidades....37
4.7. RENOVACIÓN DE CLAVES....37
4.7.1. Circunstancias para la renovación con regeneración de claves....37
4.7.2. Quién puede solicitar la renovación con regeneración de claves....37
4.7.3. Procesamiento de solicitudes de renovación con regeneración de claves....37
4.7.4. Notificación de la renovación con regeneración de claves....37
4.7.5. Conducta que constituye la aceptación de la renovación con regeneración de claves....37
4.7.6. Publicación del certificado renovado....37
4.7.7. Notificación de la renovación con regeneración de claves a otras entidades....37
4.8. MODIFICACIÓN DE CERTIFICADOS....37
4.8.1. Circunstancias para la modificación del certificado....37
4.8.2. Quién puede solicitar la modificación del certificado....38
4.8.3. Procesamiento de solicitudes de modificación del certificado....38
4.8.4. Notificación de la modificación del certificado....38
4.8.5. Conducta que constituye la aceptación de la modificación del certificado....38
4.8.6. Publicación del certificado modificado....38
4.8.7. Notificación de la modificación del certificado a otras entidades....38
4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS....38
4.9.1. Circunstancias para la revocación....38
4.9.1.1. Razones para revocar un certificado de usuario....38
4.9.1.2. Razones para revocar un certificado de AC subordinada (intermedia)....39
4.9.2. Entidad que puede solicitar la revocación....40
4.9.3. Procedimiento de solicitud de revocación....40
4.9.3.1. Telemático interactivo....40
4.9.3.2. Telemático ACME....40
4.9.3.3. Telefónico....40
4.9.4. Periodo de gracia de la solicitud de revocación....40
4.9.5. Plazo de tiempo para procesar la solicitud de revocación....40
4.9.6. Obligación de verificar las revocaciones por las partes que confían....40
4.9.7. Frecuencia de emisión de CRLs....41
4.9.8. Latencia máxima para la publicación de CRLs....41
4.9.9. Disponibilidad del sistema de verificación online del estado de los certificados....41
4.9.10. Requisitos de comprobación en línea de la revocación....41
4.9.11. Otras formas de aviso de revocación disponibles....42
4.9.12. Requisitos especiales de revocación de claves comprometidas....42
4.9.13. Circunstancias para la suspensión....42
4.9.14. Entidad que puede solicitar la suspensión....42
4.9.15. Procedimiento para la solicitud de suspensión....42
4.9.16. Límites del período de suspensión....42

4.10. SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS....42
4.10.1. Características operativas....43
4.10.2. Disponibilidad del servicio....43
4.10.3. Características opcionales....43
4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN....43
4.12. DEPÓSITO Y RECUPERACIÓN DE CLAVES....43
4.12.1. Prácticas y políticas de custodia y recuperación de claves....43
4.12.2. Prácticas y políticas de protección y recuperación de la clave de sesión....43
4.13. CADUCIDAD DE LAS CLAVES DE CERTIFICADO DE CA....44

5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES....45

5.1. CONTROLES DE SEGURIDAD FÍSICA....45
5.1.1. Ubicación y construcción....45
5.1.2. Acceso físico....45
5.1.3. Alimentación eléctrica y aire acondicionado....45
5.1.4. Exposición al agua....45
5.1.5. Protección y prevención de incendios....45
5.1.6. Sistema de almacenamiento....45
5.1.7. Eliminación de residuos....45
5.1.8. Backup remoto....46
5.2. CONTROLES DE PROCEDIMIENTOS....46
5.2.1. Papeles de confianza....46
5.2.1.1. Gerencia....46
5.2.1.2. Administrador de Sistemas....46
5.2.1.3. Administrador de PRUs....47
5.2.1.4. Administrador de Seguridad....47
5.2.1.5. Operador de la Autoridad de Certificación....48
5.2.1.6. Operador de Punto de Registro de Usuario....48
5.2.1.7. Responsable de formación, soporte y comunicación....48
5.2.1.8. Responsable de Seguridad....48
5.2.1.9. Auditor....49
5.2.1.10. Jurista....49
5.2.1.11. Responsable de Documentación....49
5.2.1.12. Asistencia al Desarrollo de Aplicaciones y Soporte al Despliegue....50
5.2.1.13. Coordinador de Autoridad de Certificación....50
5.2.2. Número de personas requeridas por tarea....50
5.2.3. Identificación y autenticación para cada papel....51
5.2.4. Papeles que requieren separación de tareas....51
5.3. CONTROLES DE SEGURIDAD DE PERSONAL....51
5.3.1. Requerimientos de antecedentes, calificación, experiencia, y acreditación....51
5.3.2. Procedimientos de comprobación de antecedentes....51

5.3.3. Requerimientos de formación 51
5.3.4. Requerimientos y frecuencia de actualización de la formación 52
5.3.5. Frecuencia y secuencia de rotación de tareas 52
5.3.6. Sanciones por acciones no autorizadas 52
5.3.7. Requisitos de contratación de terceros 52
5.3.8. Documentación proporcionada al personal 52
5.3.9. Controles periódicos de cumplimiento 53
5.3.10. Finalización de los contratos 53
5.3.10.1. Acceso a ubicaciones de la organización 53
5.3.10.2. Acceso a los Sistemas de Información 53
5.3.10.3. Acceso a la documentación 53
5.3.10.4. Información al resto de la organización 53
5.3.10.5. Información a proveedores y entidades colaboradoras 54
5.3.10.6. Devolución de material 54
5.3.10.7. Suspensión como Operador de PRU 54
5.4. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD 54
5.4.1. Tipos de eventos registrados 54
5.4.2. Frecuencia de procesado de logs 55
5.4.3. Periodo de retención para los logs de auditoría 55
5.4.4. Protección de los logs de auditoría 55
5.4.5. Procedimientos de backup de los logs de auditoría 55
5.4.6. Sistema de recogida de información de auditoría (interno vs externo) 55
5.4.7. Notificación al sujeto causa del evento 55
5.4.8. Análisis de vulnerabilidades 55
5.5. ARCHIVO DE INFORMACIONES Y REGISTROS 56
5.5.1. Tipo de informaciones y eventos registrados 56
5.5.2. Periodo de retención para el archivo 56
5.5.3. Protección del archivo 56
5.5.4. Procedimientos de backup del archivo 56
5.5.5. Requerimientos para el sellado de tiempo de los registros 56
5.5.6. Sistema de recogida de información de auditoría (interno vs externo) 56
5.5.7. Procedimientos para obtener y verificar información archivada 57
5.6. CAMBIO DE CLAVE 57
5.7. PLAN DE RECUPERACIÓN DE DESASTRES 57
5.7.1. Procedimientos de gestión de incidentes y vulnerabilidades 57
5.7.2. Alteración de los recursos hardware, softwarey/o datos 57
5.7.3. Procedimiento de actuación ante la vulnerabilidad de la clave privada de una entidad de ACCV 57
5.7.4. Continuidad de negocio después de un desastre 58
5.8. CESE DE UNA CA 58
6. CONTROLES DE SEGURIDAD TÉCNICA 60

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES....60
6.1.1. Generación del par de claves....60
6.1.1.1. Generación de pares de claves de CA....60
6.1.1.2. Generación de pares de claves RA....60
6.1.1.3. Generación de pares de claves de suscriptores....60
6.1.1.3.1. Certificados Cualificados de Autenticación de Sitios Web....60
6.1.1.3.2. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro....60
6.1.1.3.3. Certificados Cualificados de sede electrónica administrativa en soporte software....61
6.1.1.3.4. Certificados de Autenticación de Servidor....61
6.1.2. Entrega de la clave privada a la entidad....61
6.1.3. Entrega de la clave publica al emisor del certificado....61
6.1.4. Entrega de la clave pública de la CA a las partes confiantes....61
6.1.5. Tamaño de las claves....61
6.1.6. Parámetros de generación de la clave pública y verificación de la calidad....61
6.1.7. Usos admitidos de la clave (campo KeyUsagede X.509v3)....62
6.1.8. Hardware/software de generación de claves....62
6.1.8.1. Claves de CA....62
6.1.8.2. Certificados Cualificados de Autenticación de Sitios Web....63
6.1.8.3. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro....63
6.1.8.4. Certificados Cualificados de sede electrónica administrativa en soporte software....63
6.1.8.5. Certificados de Autenticación de Servidor....63
6.2. PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE LOS MÓDULOS CRIPTOGRÁFICOS....63
6.2.1. Estándares para los módulos criptográficos....63
6.2.1.1. Claves de CA....63
6.2.1.2. Certificados Cualificados de Autenticación de Sitios Web....63
6.2.1.3. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro....63
6.2.1.4. Certificados Cualificados de sede electrónica administrativa en soporte software....64
6.2.1.5. Certificados de Autenticación de Servidor....64
6.2.2. Control multi-persona de la clave privada....64
6.2.3. Custodia de la clave privada....64
6.2.4. Copia de seguridad de la clave privada....64
6.2.5. Archivo de la clave privada....64
6.2.6. Introducción de la clave privada en el módulo criptográfico....65
6.2.6.1. Claves de CA....65
6.2.6.2. Certificados Cualificados de Autenticación de Sitios Web....65
6.2.6.3. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro....65
6.2.6.4. Certificados Cualificados de sede electrónica administrativa en soporte software....65
6.2.6.5. Certificados de Autenticación de Servidor....65
6.2.7. Almacenamiento de la clave privada en el módulo criptográfico....65
6.2.7.1. Claves de CA....65
6.2.7.2. Certificados Cualificados de Autenticación de Sitios Web....65
6.2.7.3. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro....65

6.2.7.4. Certificados Cualificados de sede electrónica administrativa en soporte software....65
6.2.7.5. Certificados de Autenticación de Servidor....65
6.2.8. Método de activación de la clave privada....66
6.2.8.1. Claves de CA....66
6.2.8.2. Certificados Cualificados de Autenticación de Sitios Web....66
6.2.8.3. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro....66
6.2.8.4. Certificados Cualificados de sede electrónica administrativa en soporte software....66
6.2.8.5. Certificados de Autenticación de Servidor....66
6.2.9. Método de desactivación de la clave privada....66
6.2.9.1. Claves de CA....66
6.2.9.2. Certificados Cualificados de Autenticación de Sitios Web....66
6.2.9.3. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro....66
6.2.9.4. Certificados Cualificados de sede electrónica administrativa en soporte software....66
6.2.9.5. Certificados de Autenticación de Servidor....66
6.2.10. Método de destrucción de la clave privada....66
6.2.10.1. Hardware criptográfico....67
6.2.10.2. Tarjetas criptográficas....67
6.2.10.3. Certificados Cualificados de Autenticación de Sitios Web....67
6.2.10.4. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro....67
6.2.10.5. Certificados Cualificados de sede electrónica administrativa en soporte software....67
6.2.10.6. Certificados de Autenticación de Servidor....67
6.2.11. Clasificación de los módulos criptográficos....67
6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES....67
6.3.1. Archivo de la clave pública....67
6.3.2. Periodos de operación del certificado y periodos de uso del par de claves....67
6.4. DATOS DE ACTIVACIÓN....68
6.4.1. Generación e instalación de datos de activación....68
6.4.1.1. Autoridades de Certificación....68
6.4.1.2. Certificados Cualificados de Autenticación de Sitios Web....68
6.4.1.3. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro....68
6.4.1.4. Certificados Cualificados de sede electrónica administrativa en soporte software....68
6.4.1.5. Certificados de Autenticación de Servidor....68
6.4.2. Protección de los datos de activación....68
6.4.2.1. Autoridades de Certificación....68
6.4.2.2. Certificados Cualificados de Autenticación de Sitios Web....68
6.4.2.3. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro....69
6.4.2.4. Certificados Cualificados de sede electrónica administrativa en soporte software....69
6.4.2.5. Certificados de Autenticación de Servidor....69
6.4.3. Otros aspectos de los datos de activación....69
6.5. CONTROLES DE SEGURIDAD INFORMÁTICA....69
6.5.1. Requisitos técnicos específicos de seguridad informática....69
6.5.2. Evaluación del nivel de seguridad informática....69

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA 70
6.6.1. Controles de desarrollo de sistemas *70*
6.6.2. Controles de gestión de la seguridad *70*
6.6.3. Controles de seguridad del ciclo de vida *71*
6.7. CONTROLES DE SEGURIDAD DE LA RED 71
6.8. SELLO DE TIEMPO 71
7. PERFILES DE CERTIFICADOS, CRL Y OCSP 72
7.1. PERFIL DE CERTIFICADO 72
7.1.1. Número de versión *72*
7.1.2. Extensiones del certificado; aplicación de la RFC 5280 ..... *72*
7.1.2.1. Root CA 72
7.1.2.2. CA Subordinada 73
7.1.2.3. Certificados de suscriptor 74
7.1.2.3.1. Certificados Cualificados de Autenticación de Sitios Web 74
7.1.2.3.2. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro 76
7.1.2.3.3. Certificados Cualificados de sede electrónica administrativa en soporte software 78
7.1.2.3.4. Certificados de Autenticación de Servidor 80
7.1.3. Identificadores de objeto (OID) de los algoritmos *82*
7.1.3.1. SubjectPublicKeyInfo 82
7.1.3.1.1. RSA 82
7.1.3.1.2. ECDSA 83
7.1.3.2. Identificador del algoritmo de firma 83
7.1.3.2.1. RSA 83
7.1.3.2.2. ECDSA 84
7.1.4. Formatos de nombres *84*
7.1.4.1. Codificación de nombres 86
7.1.5. Restricciones de los nombres *86*
7.1.6. Identificador de objeto (OID) de la Política de Certificación *86*
7.1.6.1. Certificados Cualificados de Autenticación de Sitios Web 86
7.1.6.2. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro 87
7.1.6.3. Certificados Cualificados de sede electrónica administrativa en soporte software 87
7.1.6.4. Certificados de Autenticación de Servidor 88
7.1.7. Uso de la extensión "Policy Constraints" *88*
7.1.8. Sintaxis y semántica de los cualificadores de política *88*
7.1.9. Tratamiento semántico para la extensión critica "Certificate Policy" *88*
7.1.10. Signed Certificate Timestamp (SCT) List *88*
7.2. PERFIL DE CRL 89
7.2.1. Número de versión *89*
7.2.2. CRL y extensiones *89*
7.3. PERFIL OCSP 90
7.3.1. Número de versión *90*

7.3.2. Extensiones del OCSP *90*

8. AUDITORÍA DE CONFORMIDAD **91**

8.1. FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD PARA CADA ENTIDAD 91

8.2. IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR 91

8.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA 91

8.4. TÓPICOS CUBIERTOS POR EL CONTROL DE CONFORMIDAD 92

8.5. ACCIONES A TOMAR COMO RESULTADO DE UNA DEFICIENCIA 92

8.6. COMUNICACIÓN DE RESULTADOS 92

8.7. AUTOEVALUACIÓN 93

9. REQUISITOS COMERCIALES Y LEGALES **94**

9.1. TARIFAS 94

9.1.1. Tarifas de emisión de certificado o renovación *94*

9.1.2. Tarifas de acceso a los certificados *94*

9.1.3. Tarifas de acceso a la información de estado o revocación *94*

9.1.4. Tarifas de otros servicios como información de políticas *94*

9.1.5. Política de reintegros *94*

9.2. RESPONSABILIDADES FINANCIERAS 94

9.2.1. Seguro de responsabilidad civil *94*

9.2.2. Otros activos *94*

9.2.3. Seguros y garantías para entidades finales *94*

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN 95

9.3.1. Alcance de la Información confidencial *95*

9.3.2. Información no confidencial *95*

9.3.3. Responsabilidad para proteger la información confidencial *95*

9.4. PROTECCIÓN DE DATOS PERSONALES 96

9.4.1. Plan de Protección de Datos Personales *96*

9.4.2. Información considerada privada *97*

9.4.3. Información no considerada privada *97*

9.4.4. Responsabilidades *98*

9.4.5. Prestación del consentimiento en el uso de los datos personales *98*

9.4.6. Comunicación de la información a autoridades administrativas y/o judiciales *98*

9.4.7. Otros supuestos de divulgación de la información *98*

9.5. DERECHOS DE PROPIEDAD INTELECTUAL 98

9.6. OBLIGACIONES Y GARANTÍAS 98

9.6.1. Obligaciones y garantías de la Autoridad de Certificación *98*

9.6.2. Obligaciones de la Autoridad de Registro *100*

9.6.3. Obligaciones de los suscriptores *101*

9.6.4. Obligaciones de los terceros confiantes en los certificados emitidos por ACCV *102*

9.6.5. Obligaciones de otros participantes *102*
9.7. RENUNCIAS DE GARANTÍAS 102
9.8. LIMITACIONES DE RESPONSABILIDAD 103
9.9. INDEMNIZACIONES 103
9.10. PLAZO Y FINALIZACIÓN 104
9.10.1. Plazo *104*
9.10.2. Finalización *104*
9.10.3. Supervivencia *104*
9.11. NOTIFICACIONES INDIVIDUALES Y COMUNICACIÓN CON LOS PARTICIPANTES 104
9.12. MODIFICACIONES 104
9.12.1. Procedimiento para las modificaciones *104*
9.12.2. Procedimientos de publicación y notificación *105*
9.12.3. Circunstancias en las que el OID debe ser cambiado *105*
9.13. RESOLUCIÓN DE CONFLICTOS 105
9.14. LEGISLACIÓN APLICABLE 105
9.15. CONFORMIDAD CON LA LEY APLICABLE 106
9.16. CLÁUSULAS DIVERSAS 106
9.16.1. Acuerdo integro *106*
9.16.2. Asignación *106*
9.16.3. Severabilidad *106*
9.16.4. Cumplimiento (honorarios de los abogados y renuncia a los derechos) *107*
9.16.5. Fuerza Mayor *107*
9.17. OTRAS ESTIPULACIONES 107

10. ANEXO I 108

10.1. CERTIFICADOS CUALIFICADOS DE AUTENTICACIÓN DE SITIOS WEB 108
10.2. CERTIFICADOS CUALIFICADOS DE SEDE ELECTRÓNICA ADMINISTRATIVA EN DISPOSITIVO SEGURO 110
10.3. CERTIFICADOS CUALIFICADOS DE SEDE ELECTRÓNICA ADMINISTRATIVA EN SOPORTE SOFTWARE 112
10.4. CERTIFICADOS DE AUTENTICACIÓN DE SERVIDOR 114

1. INTRODUCCIÓN

1.1. Presentación

El presente documento contiene la *Declaración de Prácticas y Políticas de Certificación (DPC)* de la Agencia de Tecnología y Certificación Electrónica en la emisión de certificados de autenticación de sitios web.

La Agencia de Tecnología y Certificación Electrónica (ACCV) forma parte de Infraestructures i Serveis de Telecomunicacions i Certificació, SAU (ISTEC), entidad de derecho público con personalidad jurídica propia y plena capacidad para el cumplimiento de sus fines, que se rige por sus Estatutos.

De acuerdo con lo anterior, en cumplimiento con la legislación vigente y alineados con el Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE y su modificación en el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.° 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital, la presente Declaración de Prácticas y Políticas de Certificación (DPC) detalla las normas y condiciones generales de los servicios de certificación que presta la Agencia de Tecnología y Certificación Electrónica, en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados, las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su caso, la existencia de procedimientos de coordinación con los registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros, siempre en el ámbito de certificados de autenticación de sitios web.

Así pues, la presente Declaración de Prácticas de Certificación constituye el compendio de normas aplicables a la actividad certificadora de la Agencia de Tecnología y Certificación Electrónica (ACCV) en tanto que Prestador de Servicios de Confianza Cualificado en la emisión de certificados de autenticación de sitios web.

Asimismo cabe indicar que la presente Declaración de Prácticas y Políticas 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.

Finalmente, indicar que 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://wwww.cabforum.org/. En el caso de cualquier incompatibilidad entre este documento y los requisitos del CAB Forum, dichos requisitos prevalecerán.

ACCV NO emitirá certificados oficiales firmados por Autoridades de Certificación que no hayan pasado las auditorias y certificaciones necesarias en cada caso.

1.2. Nombre del documento e identificación

Nombre del documento	Declaración de Prácticas y Políticas de Certificación de certificados de autenticación de sitios web
Versión del documento	4.0.17
Estado del documento	APROBADO
Referencia de la DPC/ OID (Object Identifier)	1.3.6.1.4.1.8149.2.4.0
Fecha de emisión	03/06/2025

Fecha de expiración	No aplicable.
Localización	Esta DPC se puede encontrar en http://www.accv.es/pdf-politicas

El Certificado de autenticación de sitios web es un tipo de certificado utilizado para confirmar la identidad del sitio web al que se conectan los usuarios, utilizando técnicas de criptografía de clave pública y mediante el uso de protocolos bien establecidos que proporcionan cifrado de datos y autenticación entre aplicaciones y servidores (TLS/SSL).

Bajo esta DPC se emiten los siguientes tipos de certificados:

Nombre	OID propietario
Certificados Cualificados de Autenticación de Sitios Web	1.3.6.1.4.1.8149.3.3.5.0
Certificados Cualificados de sede electrónica administrativa en dispositivo seguro	1.3.6.1.4.1.8149.3.14.6.0
Certificados Cualificados de sede electrónica administrativa en soporte software	1.3.6.1.4.1.8149.3.15.6.0
Certificados de Autenticación de Servidor	1.3.6.1.4.1.8149.3.36.2.0

Todos los certificados emitidos bajo esta DPC son OV (Organization Validated), esto quiere decir que se siguen como mínimo los requisitos de emisión y gestión OVCP descritos en

https://cabforum.org/working-groups/server/baseline-requirements/documents/

1.3. Comunidad de usuarios y ámbito de aplicación

1.3.1. Autoridades de Certificación

En la presente Declaración de Prácticas de Certificación, se utilizará el acrónimo “ACCV” para designar en su conjunto a las Autoridades de Certificación que integran la Agencia de Tecnología y Certificación Electrónica.

Las Autoridades de Certificación que componen ACCV se estructuran en varias jerarquías de certificación, compuestas por varias autoridades de certificación raíz y subordinadas.

Las jerarquías bajo el ámbito de aplicación de esta CPS está formada por las siguientes autoridades de certificación

1.3.1.1. Autoridades de Certificación Raíz

Autoridad de Certificación de primer nivel. Su función es la de establecer la raíz del nuevo modelo de confianza de la Infraestructura de Clave Pública o PKI. Esta CA no emite certificados para entidades finales. Esta Autoridad de Certificación de primer nivel se auto-firma, emitiendo un certificado cuyo firmante es la propia Autoridad de Certificación, y que contiene la clave pública (o datos de verificación de firma) firmada con los datos de creación de firma (clave privada).

1.3.1.1.1. ACCVRAIZ1

- C=ES,O=ACCV,OU=PKIACCV,CN=ACCVRAIZ1

- Huella (HASH) SHA1:

- **93057A8815C64FCE882FFA9116522878BC536417**

- Huella (HASH) SHA256:

- **9A6EC012E1A7DA9DBE34194D478AD7C0DB1822FB071DF12981496ED104384113**

Válido desde el 5 de mayo de 2011 al 31 de diciembre de 2030.

Tipo de clave: RSA 4096 bits – SHA1

1.3.1.1.2. ACCV ROOT ECC TLS 2024

- CN=ACCV ROOT ECC TLS 2024,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJAS-SOT,ST=VALENCIA,C=ES

- Huella (HASH) SHA1:

- **2E529E361D817B33E1FE095E91A4EB969458B3F4**

- Huella (HASH) SHA256:

- **79CD55455296ADFB55CDF0DBE9176985A0B503C544276C5A9305F2EC9B66693A**

Válido desde el 27 de febrero de 2024 al 26 de enero de 2049.

Tipo de clave: ECDSA P384 SHA384

1.3.1.1.3. ACCV ROOT RSA TLS 2024

- CN=ACCV ROOT RSA TLS 2024,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJAS-SOT,ST=VALENCIA,C=ES

- Huella (HASH) SHA1:

- **970ABA25EC3D78649B305BA75F8C914C275D8654**

- Huella (HASH) SHA256:

- **B40BFA8880A02F93025643C6DBBD39DF194A2854D076E167A2BD8467CF9E2C34**

Válido desde el 27 de febrero de 2024 al 26 de enero de 2049.

Tipo de clave: RSA 4096 SHA512

1.3.1.2. Autoridades de Certificación Subordinadas

- Raíz **ACCVRAIZ1**

- “ACCVCA-110"

Valido desde el día 7 de mayo de 2015 hasta el 1 de enero de 2027.

SHA256 Fingerprint:

E9327A347CBE1CB94CDC9AA54CB31B6E43D68968D17D09CE326A091BFC2F0B11

SHA1 Fingerprint:

677CDF63B95E9EAEAE696F44506718FE0D2F6E41

Tipo de clave: RSA 4096 bits – SHA256

- “ACCVCA-120".

Válido desde el día 27 de enero de 2015 hasta el 01 de enero de 2027.

SHA256 Fingerprint:

2DE620F2D1200AA90B16C3CCF670FD7ED14379AB06FA8B031CFEF8DA051EA5A2

SHA1 Fingerprint:

4872A4C3DF174CEF34D77FE6A3B4E7BE7DF2D25D

Tipo de clave: RSA 4096 bits – SHA256

- "ACCVCA-130"

Válido desde el día 15 de enero de 2015 hasta el 01 de enero de 2027.

SHA256 Fingerprint:

572BF899FD774362DC19219625ECC157BB55434EA5166D5758DC4B4F890D6653

SHA1 Fingerprint:

0055B77F432B54245406068CC8F77805C325DCF5

Tipo de clave: RSA 4096 bits – SHA256

- Raíz **ACCV ROOT ECC TLS 2024**

- "ACCV ECC1 TLS"

Válido desde el día 27 de febrero de 2024 hasta el 23 de febrero de 2039.

SHA256 Fingerprint:

93C087AB9331B74C0FCCCE11BC61FB9FA6D432077D8F1018194FA4CCA664D781

SHA1 Fingerprint:

4F35E0547A8E74D9D3EC1B260F0F9AD4809246E3

Tipo de clave: ECDSA P384 SHA384

- Raíz **ACCV ROOT RSA TLS 2024**

- "ACCV RSA1 TLS"

Válido desde el día 27 de febrero de 2024 hasta el 23 de febrero de 2039.

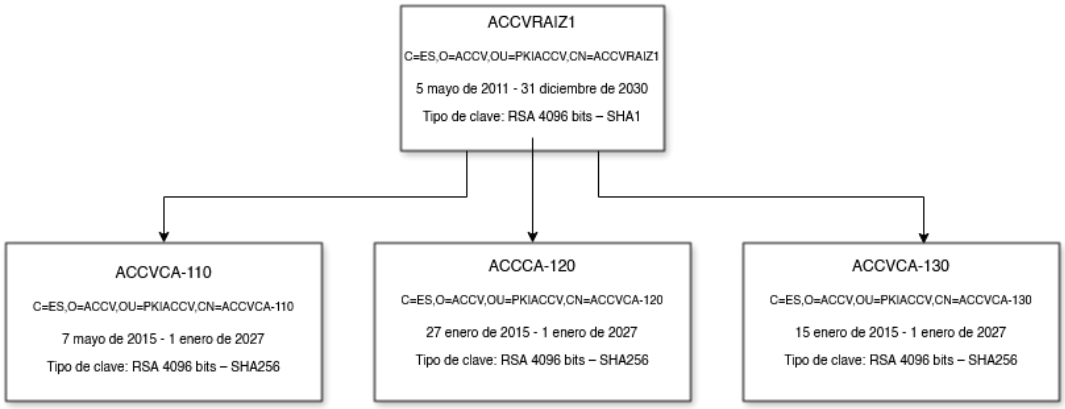
SHA256 Fingerprint:

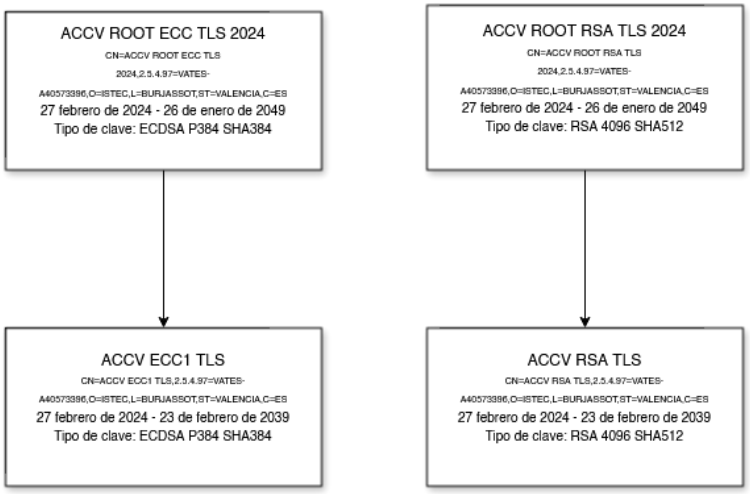
346440CF7674A529305545563322FCFB38F5A4B3F1E7E852DFF8A4B7A5EF72D1

SHA1 Fingerprint:

D9698B1190136DAE3C3B0164329D050AB84D416D

Tipo de clave: RSA 4096 SHA512





1.3.2. Autoridades de Registro

La única Autoridad de Registro para los certificados de autenticación de sitios web es la ACCV, y realiza la identificación y verificación del solicitante y comprobación de todos los datos incluidos en el certificado, haciendo especial hincapié en las verificaciones necesarias para comprobar la posesión del dominio o dominios por parte del solicitante del certificado. A tal efecto, la Autoridad de Registro se encargará de garantizar que la solicitud del certificado contiene información veraz y completa, y que la misma se ajusta a los requisitos exigidos en la correspondiente Política.

Las funciones básicas de la Autoridad de Registro se extienden a:

- Comprobar la identidad y cualesquiera circunstancias personales de los solicitantes de certificados relevantes para el fin propio de éstos.
- Informar con carácter previo a la emisión del certificado a la persona que lo solicite, de las condiciones precisas para la utilización del certificado y de sus limitaciones de uso.
- Verificar que la información contenida en el certificado es exacta y que incluye toda la información prescrita para un certificado del tipo en cuestión.
- Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.

- Verificar por los métodos establecidos y aceptados para este tipo de certificados la posesión del dominio o dominios por parte del solicitante

1.3.3. Suscriptores

El grupo de usuarios que pueden solicitar certificados definidos por esta política está formado por los responsables de entidades públicas o privadas, en situación de representar a la entidad solicitante.

En el caso de entidades públicas, las solicitudes pueden llevarlas a cabo Jefes de Servicio 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. Éstos (o en quién ellos deleguen de forma explicita) son los únicos suscriptores autorizados para solicitar certificados de sede electrónica.

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

Se limita el derecho de solicitud de certificados definido en la presente Política de Certificación a personas físicas. No se aceptarán solicitudes de certificación realizadas por personas jurídicas, entidades u organizaciones sin una persona física identificada como solicitante.

1.3.4. Partes confiantes

Se limita el derecho a confiar en los certificados emitidos conforme a las presentes prácticas y políticas a:

1. Los usuarios de clientes de aplicaciones en el ámbito de la verificación de la identidad de los sitios web a los que se conectan y del cifrado del canal de los datos transmitidos entre ellos.
2. Las aplicaciones y servicios con capacidades de soporte SSL y/o TLS, en el ámbito de verificación de la identidad de los sitios web a los que se conectan, y del cifrado del canal de los datos transmitidos entre ellos

1.3.5. Otros participantes

1.3.5.1. Solicitantes

Un Solicitante es la persona física que, en nombre propio o como representante de un tercero, y previa identificación, solicita la emisión de un Certificado.
En el caso de Solicitantes de Certificados cuyo Suscriptor sea una persona jurídica, dicha persona física sólo podrá ser un representante legal o voluntario o un administrador con facultades suficientes a estos efectos de la persona jurídica que será el suscriptor del certificado.

1.4. Uso de los certificados

Las Políticas de Certificación correspondientes a cada tipo de certificado emitido por ACCV constituyen los documentos en los que se determinan los usos y limitaciones de cada certificado. En esta DPC se establecen los usos y limitaciones para los certificados emitidos para autenticación de sitios web.

1.4.1. Usos permitidos

Los certificados emitidos por la Agencia de Tecnología y Certificación Electrónica bajo esta DPC pueden utilizarse para dotar a los sitios web de capacidades SSL/TLS. Asimismo y mientras los usos lo permitan, pueden utilizarse como mecanismo de identificación de estos sitios de forma inequívoca ante servicios y aplicaciones informáticas.

Los Certificados de sede electrónica son un subconjunto de los Certificados de autenticación de sitios web, que se expiden como sistemas de identificación de una Sede electrónica que garantiza la comunicación segura con la misma, en los términos definidos en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y en la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia

1.4.2. Usos prohibidos

Los Certificados emitidos por ACCV para autenticación de sitios web se utilizarán únicamente conforme a la función y finalidad que tengan establecida en la presente Declaración de Prácticas y Políticas de Certificación, y con arreglo a la normativa vigente.

1.5. Política de Administración de ACCV

1.5.1. Especificación de la Organización Administradora

Nombre	*Agencia de Tecnología y Certificación Electrónica*
Dirección de email	*accv@accv.es*
Dirección	*Pol. Ademuz, s/n.- 46100 Burjassot (España)*
Número de teléfono	*+34 963 866 014*

1.5.2. Persona de Contacto

Nombre	*Agencia de Tecnología y Certificación Electrónica*
Dirección de email	*accv@accv.es*
Dirección	*Pol. Ademuz, s/n. - 46100 Burjassot (España)*
Número de teléfono	*+34 963 866 014*

1.5.2.1. Dirección de comunicación de problemas

El usuario puede proporcionar información relativa a claves comprometidas o certificados incorrectos utilizando el formulario https://www.accv.es/contacta/
En el formulario el usuario puede pegar el certificado o las claves en formato PEM, incluyendo las lineas BEGIN y END.
Puede utilizar tambien directamente la dirección para el envio de problemas detectados problem_reporting@accv.es (el formulario envia una copia a esa dirección).
En el caso de certificados ACME puede utilizarse para la revocación el mecanismo habilitado siguiendo el protocolo

https://npsc.accv.es:8450/npsc/acme/revoke-cert

1.5.3. Competencia para determinar la adecuación de la DPC

La entidad competente para determinar la adecuación de esta DPC, es Infraestructures i Serveis de Telecomunicacions i Certificació, SA (ISTEC) de conformidad con sus estatutos.

1.5.4. Procedimiento de aprobación de la DPC

ISTEC aprueba la DPC y sus posibles modificaciones. Las modificaciones se realizan mediante la actualización de toda la DPC o la publicación de un apéndice. ISTEC determina si una modificación de esta DPC requiere una notificación o un cambio de OID.

ISTEC revisará sus políticas y prácticas de certificación y actualizará anualmente la presente Declaración de Prácticas y Políticas de Certificación para mantenerla acorde a la última versión de los requisitos definidos en "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", publicados en https://www.cabforum.org/, incrementando el número de versión y agregando una entrada de registro de cambios con fecha, incluso si no se realizaron otros cambios en el documento.

1.6. Definiciones y Acrónimos

1.6.1. Definiciones

A los efectos de determinar el alcance de los conceptos que son utilizados en la presente Declaración de Prácticas de Certificación deberá entenderse:

- Autoridad de Certificación: es aquella persona física o jurídica que, de conformidad con la legislación sobre firma electrónica expide certificados electrónicos, pudiendo prestar además otros servicios en relación con la firma electrónica. A efectos de la presente Declaración de Prácticas de Certificación, son Autoridad de Certificación todas aquellas que en la misma se definan como tales.
- Autoridad de Registro: persona física o jurídica que ACCV designa para realizar la comprobación de la identidad de los solicitantes y suscriptores de certificados, y en su caso de la vigencia de facultades de representantes y subsistencia de la personalidad jurídica o de la representación voluntaria. En ACCV reciben también el nombre de Puntos de Registro del Usuario o PRU.
- 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.
- Cadena de certificación: lista de certificados que contiene al menos un certificado y el certificado raíz de ACCV.
- Certificado: documento electrónico firmado electrónicamente por un Prestador de Servicios de Certificación que vincula al suscriptor unos datos de verificación de firma y confirma su identidad. En la presente Declaración de Prácticas de Certificación, cuando se haga referencia a certificado se entenderá realizada a un Certificado emitidos por ACCV.
- Certificado raíz: Certificado cuyo suscriptor es ACCV y pertenece a la jerarquía de ACCV como Prestador de Servicios de Certificación, y que contiene los datos de verificación de firma de dicha Autoridad firmado con los datos de creación de firma de la misma como Prestador de Servicios de Certificación.
- Certificado cualificado: Certificado expedido por un Prestador de Servicios de Confianza que cumple los requisitos establecidos en el Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten. Para ser considerado como certificado cualificado debe aparecer en la lista de confianza (TSL) mencionada en el artículo 22, apartado 1 de dicho Reglamento.
- Certificado de autenticación de sitios web: Es un Certificado que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el Certificado.
- Certificado OV: Certificado de autenticación de sitios web expedido según la política de validación de Organización (OVCP), garantizando al usuario que el titular del sitio web al que accede coincide con la Organización identificada por el Certificado OV.
- Certificado de sede electrónica: Certificado de autenticación de sitios web que identifica a una Sede electrónica, garantizando la comunicación segura con la misma en los términos definidos en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Clave: secuencia de símbolos.
- Datos de creación de Firma (Clave Privada): son datos únicos, como códigos o claves criptográficas privadas, que el suscriptor utiliza para crear la Firma electrónica.
- Datos de verificación de Firma (Clave Pública): son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la Firma electrónica.
- Declaración de Prácticas de Certificación: declaración de ACCV puesta a disposición del público por vía electrónica y de forma gratuita realizada en calidad de Prestador de Servicios de Certificación en cumplimiento de lo dispuesto por la Ley.

- Dispositivo seguro de creación de Firma: instrumento que sirve para aplicar los datos de creación de firma cumpliendo con los requisitos establecidos en el Reglamento (EU) No 910/2014 (Anexo II Requisitos de los Dispositivos Cualificados de Creación de la Firma Electrónica).
- Directorio de Certificados: repositorio de información que sigue el estándar X.500 del ITU-T.
- Documento electrónico: información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado, y susceptible de identificación y tratamiento diferenciado
- Registro de Actividades: documento exigido por Reglamento (UE) 2016/679 cuyo objetivo es establecer las medidas de seguridad implantadas, a los efectos de este documento, por ACCV como Prestador de Servicios de Certificación, para la protección de los datos de carácter personal contenidos en los Ficheros de la actividad de certificación que contienen datos personales (en adelante los Ficheros).
- Encargado del Tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable de los ficheros.
- Firma electrónica cualificada: es aquella firma electrónica avanzada basada en un certificado cualificado y generada mediante un dispositivo cualificado de creación de firma.
- Firma electrónica avanzada: es aquella firma electrónica que permite establecer la identidad personal del suscriptor respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al suscriptor, como a los datos a que se refiere, y por haber sido creada por medios que mantiene bajo su exclusivo control.
- Firma electrónica: es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación personal.
- Función hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la Función hash.
- Hash o Huella digital: resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.
- Infraestructura de Claves Públicas (PKI, public key infrastucture): infraestructura que soporta la emisión y gestión de claves y certificados para los servicios de autenticación, cifrado, integridad, o no repudio.
- Listas de Revocación de Certificados o Listas de Certificados Revocados: lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados).
- Módulo Criptográfico Hardware de Seguridad: módulo hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.
- Número de serie de Certificado: valor entero y único que está asociado inequívocamente con un certificado expedido por una CA.
- OCSP (Online Certificate Status Protocol): protocolo informático que permite la comprobación del estado de un certificado en el momento en que éste es utilizado.
- OCSP Responder: servidor informático que responde, siguiendo el protocolo OCSP, a las peticiones OCSP con el estado del certificado por el que se consulta.
- OID (Object Identifier): valor de naturaleza jerárquica y comprensivo de una secuencia de componentes variables, aunque siempre constituidos por enteros no negativos separados por un punto, que pueden ser asignados a objetos registrados y que tienen la propiedad de ser únicos entre el resto de OID.
- Petición OCSP: petición de consulta de estado de un certificado a OCSP Responder siguiendo el protocolo OCSP.

- PIN: (Personal Identification Number) número específico sólo conocido por la persona que tiene que acceder a un recurso que se encuentra protegido por este mecanismo.
- Prestador de Servicios de Certificación: es aquella persona física o jurídica que, de conformidad con la legislación sobre firma electrónica expide certificados electrónicos, pudiendo prestar además otros servicios en relación con la firma electrónica. En la presente Declaración de Prácticas de Certificación se corresponderá con las Autoridades de Certificación pertenecientes a la jerarquía de ACCV.
- Política de Certificación: documento que completa la Declaración de Prácticas de Certificación, estableciendo las condiciones de uso y los procedimientos seguidos por ACCV para emitir Certificados.
- PKCS#10 (Certification Request Syntax Standard): estándar desarrollado por RSA Labs, y aceptado internacionalmente como estándar, que define la sintaxis de una petición de certificado.
- Precertificado: Estructura de datos firmada que puede enviarse a un log de Certificate Tramsparency, tal como se define en el RFC 6962
- PUK: (Personal Unblocking Key) número o clave específica sólo conocido por la persona que tiene que acceder a un recurso que se utiliza para desbloquear el acceso a dicho recurso.
- Registro AAC (CAA records): Registro de recursos DNS (Sistema de Nombres de Dominio) de Autorización de Autoridad de Certificación (AAC). Permite a un titular de nombre de dominio DNS especificar las Autoridades de Certificación (AC) autorizadas para emitir certificados para ese dominio. La publicación de los registros de recursos de AAC permite a un titular de nombres de dominio implementar controles adicionales para reducir el riesgo de que se produzca una emisión no autorizada
- Responsable del Fichero (o del Tratamiento del Fichero): persona que decide sobre la finalidad, contenido y uso del tratamiento de los Ficheros.
- Responsable de Seguridad: encargado de coordinar y controlar las medidas que impone el documento de seguridad en cuanto a los ficheros.
- Sede electrónica: Dirección electrónica, disponible para los ciudadanos a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública, o bien a uno o varios organismos públicos o entidades de Derecho Público en el ejercicio de sus competencias.
- SHA Secure Hash Algorithm (algoritmo seguro de resumen –hash-). familia de funciones hash de cifrado publicadas por el Instituto Nacional de Estándares y Tecnología (NIST). La primera versión del algoritmo fue creada en 1993 con el nombre de SHA, aunque en la actualidad se la conoce como SHA-0 para evitar confusiones con las versiones posteriores. La segunda versión del sistema, publicada con el nombre de SHA-1, fue publicada dos años más tarde. Posteriormente se han publicado SHA-2 en 2001 (formada por diversas funciones: SHA-224, SHA-256, SHA-384, y SHA-512) y la más reciente, SHA-3, que fue seleccionada en una competición de funciones hash celebrada por el NIST en 2012.). El algoritmo consiste en tomar mensajes de menos de 264 bits y generar un resumen de longitud fija. La probabilidad de encontrar dos mensajes distintos que produzcan un mismo resumen es prácticamente nula. Por este motivo se usa para asegurar la Integridad de los documentos durante el proceso de Firma electrónica.
- Sellado de Tiempo: constatación de la fecha y hora en un documento electrónico mediante procedimientos criptográficos indelebles, basándose en las especificaciones Request For Comments: 3161 – “Internet X.509 Public Key Infrastructure Time–Stamp Protocol (TSP)”, que logra datar el documento de forma objetiva.
- Solicitante: persona física que solicita la emisión de un certificado.
- Suscriptor (o Subject): el titular o firmante del certificado. La persona cuya identidad personal queda vinculada a los datos firmados electrónicamente, a través de una clave pública certificada por el Prestador de Servicios de Certificación. El concepto de suscriptor, será referido en los certificados y en las aplicaciones informáticas relacionadas con su emisión como Subject, por estrictas razones de estandarización internacional.

- Tarjeta criptográfica: tarjeta utilizada por el suscriptor para almacenar claves privadas de firma y descifrado, para generar firmas electrónicas y descifrar mensajes de datos. Tiene la consideración de dispositivo seguro de creación de firma de acuerdo con la Ley de firma electrónica y permite la generación de firma electrónica reconocida.
- Terceras partes confiantes o partes confiantes: aquellas personas que depositan su confianza en un certificado de ACCV, comprobando la validez y vigencia del certificado según lo descrito en esta Declaración de Prácticas de Certificación y en las Políticas de Certificación asociadas a cada tipo de certificado.
- X.500: estándar desarrollado por la UIT que define las recomendaciones del directorio. Se corresponde con el estándar ISO/IEC 9594-1: 1993. Da lugar a la serie de recomendaciones siguientes: X.501, X.509, X.511, X.518, X.519, X.520, X.521 y X.525.
- X.509: estándar desarrollado por la UIT, que define el formato electrónico básico para certificados electrónicos.

1.6.2. Acrónimos

ACCV	Agencia de Tecnología y Certificación Electrónica
CA	Certification Authority
CN	Common Name
CP	Certificate Policy
DPC	Certification Practice Statement
CRL	Certificate Revocation List
DGTIC GVA	Dirección General de Tecnologías de la Información y las Comunicaciones Generalitat Valenciana
FIPS	Federal Information Processing Standard
IETF	Internet Engineering Task Force
IVF	Insitut Valencià de Finances
ISTEC	Infraestructures i Serveis de Telecomunicacions i Certificació
OID	Object identifier
OCSP	On-line Certificate Status Protocol
OPRU	Operador de Punto de Registro
OV	Organization Validated
PKI	Public Key Infrastructure
PKIGVA	PKI de la Agencia de Tecnología y Certificación Electrónica
PRU	Punto de Registro de Usuario
RA	Registration Authority
RFC	Request For Comment
SSL	Secure Sockets Layer
Sub CA	Subordinate Certification Authority
TLS	Transport Security Layer

2. Publicación de información y repositorio de certificados

2.1. Repositorio de certificados

El servicio de repositorio de certificados estará disponible durante las 24 horas del día, los 7 días de la semana, y en caso de interrupción por causa de fuerza mayor, el servicio se restablecerá en el menor tiempo posible.

El repositorio de ACCV está compuesto por:

Servidor OCSP acorde RFC-6960 accesible en: http://ocsp.accv.es

URL de acceso a los certificados con alta disponibilidad

ACCVRAIZ1: https://www.accv.es/fileadmin/Archivos/certificados/ACCVRAIZ1.crt

ACCVCA-110: https://www.accv.es/fileadmin/Archivos/certificados/ACCVCA110SHA2.cacert.crt

ACCVCA-120: https://www.accv.es/fileadmin/Archivos/certificados/ACCVCA120.crt

ACCVCA-130: https://www.accv.es/fileadmin/Archivos/certificados/ACCVCA130SHA2.cacert.crt

ACCV ROOT RSA TLS 2024: http://www.accv.es/gestcert/accv_root_rsa_tls_2024.crt

ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crt

ACCV ROOT ECC TLS 2024: http://www.accv.es/gestcert/accv_root_ecc_tls_2024.crt

ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crt

URL de acceso a las CRLs con alta disponibilidad

ACCVRAIZ1: http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl

ACCVCA-110: http://www.accv.es/fileadmin/Archivos/certificados/accvca110_der.crl

ACCVCA-120: http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl

ACCVCA-130: http://www.accv.es/fileadmin/Archivos/certificados/accvca130_der.crl

ACCV ROOT RSA TLS 2024: http://www.accv.es/gestcert/accv_root_rsa_tls_2024.crl

ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crl

ACCV ROOT ECC TLS 2024: http://www.accv.es/gestcert/accv_root_ecc_tls_2024.crl

ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crl

El repositorio de ACCV no contiene ninguna información de naturaleza confidencial y no se utiliza ningún otro repositorio operado por ninguna otra organización.

ACCV se ajusta a la versión actual de los "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", publicados en https://www.cabforum.org/. En caso de que haya alguna incoherencia entre esta política de certificación y los requisitos del CAB Forum, éstos tendrán prioridad sobre el presente documento.

Entre la condiciones establecidas se encuentra la obligatoriedad de revocar los certificados si se detecta que la emisión u operación no cumple con lo definido en la normativa. **Esta revocación se debe hacer en un plazo máximo de entre uno (1) y cinco (5) días naturales (dependiendo del tipo de incumplimiento) y no es posible aplazamiento de ningún tipo. Si no es posible cumplir esta condición no se deben utilizar nunca certificados emitidos bajo esta normativa.**

2.2. Publicación

Es obligación de las CAs pertenecientes a la jerarquía de confianza de ACCV publicar la información relativa a sus prácticas, sus certificados y el estado actualizado de dichos certificados.

La presente DPC es pública y se encuentra disponible en el sitio web de ACCV http://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-CPS-CP-V4.0.17-ES-2025.pdf, en formato PDF.

Las Políticas de Certificación de ACCV son públicas y se encuentran disponibles en el sitio de web de ACCV http://www.accv.es/pdf-politicas, en formato PDF.

El certificado de la CA de ACCV es público y se encuentra disponible en el repositorio de ACCV, en formato X.509 v3. También se encuentra en la http://www.accv.es.

Los certificados emitidos por ACCV son públicos y se encuentran disponibles en el repositorio de ACCV, en formato X.509 v3.

La lista de certificados revocados por ACCV es pública y se encuentra disponible, en formato CRL v2, en el repositorio de ACCV.

ACCV proporciona páginas web de prueba que permiten a los proveedores de software de aplicación probar su software con certificados de suscriptor que se encadenan a cada certificado raíz de confianza pública.

- ACCVCA-120
  - VALID
    - https://activo.accv.es/test/hola.html
  - REVOKED
    - https://revocado.accv.es:442/test/hola.html
  - EXPIRED
    - https://caducado.accv.es:444/test/hola.html
- ACCV RSA1 TLS
  - VALID
    - https://activonjrsa.accv.es/test/hola.html
  - REVOKED
    - https://revocadonjrsa.accv.es:442/test/hola.html
  - EXPIRED
    - https://caducadonjrsa.accv.es:444/test/hola.html

- ACCV ECC1 TLS
  - VALID
    - https://activonjecc.accv.es/test/hola.html
  - REVOKED
    - https://revocadonjecc.accv.es:442/test/hola.html
  - EXPIRED
    - https://caducadonjecc.accv.es:444/test/hola.html

En el ámbito del proyecto Certificate Transparency,en el caso de certificados TLS (como los emitidos bajo la presente política), los precertificados se publicarán en el servicio CT Log de los proveedores de servidores de registro cualificados para cumplir con los requisitos del proyecto.

2.3. Frecuencia de actualizaciones

La DPC y las Políticas de Certificación se publicarán cada vez que sean modificadas, llevando a cabo una revisión anual de las mismas para verificar el cumplimiento y la adaptación de las nuevas directivas y normativa técnica. Se indicara esta revisión cambiando el numero menor de versión.

Los certificados emitidos por la CA se publicarán de forma inmediatamente posterior a su emisión.

La CA añadirá los certificados revocados a la CRL pertinente dentro del periodo de tiempo estipulado en el punto 4.4.9 *Frecuencia de emisión de CRLs*.

2.4. Controles de acceso al repositorio de certificados.

El acceso a lectura de la información del repositorio de ACCV y de su sitio web es libre y gratuito.

Sólo ACCV está autorizada a modificar, sustituir o eliminar información de su repositorio y sitio web. En este sentido, ACCV utiliza los medios de control adecuados a fin de restringir la capacidad de escritura o modificación de estos elementos.

3. Identificación y Autenticación

3.1. Registro de nombres

3.1.1. Tipos de nombres

Todos los suscriptores de certificados requieren un *nombre distintivo* (distinguished name) conforme con el estándar X.500.

3.1.2. Significado de los nombres

En todos los casos los nombres distintivos deben tener sentido. Esta DPC y la Política de Certificación aplicable al tipo de certificado describe los atributos utilizados para los nombres distintivos en los puntos en 7.1.2 y 7.1.4. Los nombres en los certificados identifican al sujeto y al emisor respectivamente.

3.1.3. Anonimización o seudoanonimización de los suscriptores

ACCV no emite certificados con seudónimo para la autenticación de servidores.

3.1.4. Interpretación de formatos de nombres

Las reglas utilizadas por ACCV para interpretar los nombres distintivos de los certificados que emite son las contenidas en la ISO/IEC 9594 (X.500) Distinguished Name (DN) y RFC-2253.

3.1.5. Unicidad de los nombres

Los nombres distintivos deben identificar al suscriptor y no inducirán a ambigüedad.

ACCV no impone la unicidad de los nombres distintivos. Como diferencia, los números de serie asignados que se incluyen en los certificados son únicos. ACCV genera números de serie de 64 bits como mínimo. Estos números son el resultado de un CSPRNG. Se verifica que los números de serie nunca se reutilizan.

En el caso de certificados de identificación web el CN puede no estar u opcionalmente puede ir uno de los nombres incluidos en la extensión Subject Alternative Name. La segunda opción esta desaconsejada.

3.1.6. Reconocimiento, autenticación y función de las marcas registradas.

La inclusión en un certificado de un nombre no implica la existencia de ningún derecho sobre el mismo y lo es sin perjuicio del mejor derecho que pudieren ostentar terceros.

ACCV no actúa como árbitro o mediador, ni resuelve ninguna disputa relativa a la titularidad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales, etc.

ACCV se reserva el derecho de rehusar una solicitud de certificado por causa de conflicto sobre el nombre.

La Oficina Española de Patentes y Marcas del Ministerio de Industria, Comercio y Turismo ha concedido las siguientes marcas, propiedad de ISTEC.

- "Autoritat de Certificació de la Comunitat Valenciana", marca mixta nº 2.591.232, concedida el 15 de septiembre de 2004, publicada en el Boletín Oficial de la Propiedad Industrial de 16 de octubre de 2004.

Autoritat de Certificació de la Comunitat Valenciana

- "ACCV", marca nº 2.591.037, concedida el 19 de mayo de 2005, publicada en el Boletín Oficial de la Propiedad Industrial de 16 de junio de 2005.
- "Agencia de Tecnología y Certificación Electrónica", marca nº 2.943.180, solicitada a la Propiedad Industrial Oficial española el 13 de agosto de 2010.

ACCV prohíbe deliberadamente el uso de un nombre cuyo derecho de uso no sea propiedad del suscriptor. Sin embargo, no está obligada a buscar pruebas de la propiedad de la marca antes de emitir los certificados.

3.2. Validación Inicial de la Identidad

3.2.1. Métodos de prueba de posesión de la clave privada.

En el caso que el par de claves sea generado por la entidad final (subscriptor) de forma externa a las herramientas y aplicaciones proporcionadas por ACCV, esté deberá probar la posesión de la clave privada correspondiente a la clave pública que solicita que se certifique mediante el envío de la solicitud de certificación firmada por la clave privada asociada a la clave pública suministrada.

3.2.2. Autenticación de la identidad de una organización.

ACCV no asume compromisos en la emisión de certificados respecto al uso de una marca registrada o nombre comercial, no permitiendo deliberadamente el uso de un nombre cuyo derecho de uso no sea propiedad del Suscriptor. En caso de disputa, ACCV puede rechazar la solicitud o revocar cualquier certificado sin responsabilidad alguna. ACCV utilizará las herramientas indicadas en este punto para realizar las búsquedas correspondientes y confirmar los derechos de uso.

ACCV utiliza los mecanismos establecidos por la normativa técnica vigente, concretamente el Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, relativo al establecimiento de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de los métodos de identificación electrónica, según lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) número 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

El derecho de solicitud de certificados definido en la presente DPC se encuentra limitado a suscriptores identificados como personas físicas. No se aceptarán solicitudes de certificación realizadas por suscriptores identificados como personas jurídicas, entidades u organizaciones.

La autentificación de la identidad del solicitante se realiza mediante el uso de su certificado personal cualificado, firmando con el la solicitud del certificado de autenticación de sitios web al identificarse en la aplicación que para esta función pone a disposición de los usuarios la ACCV (NPSC https://npsc.accv.es:8450/npsc)

El solicitante debe presentar la documentación necesaria que determine

Los datos relativos a la entidad como la inclusión en el registro mercantil correspondiente, domicilio, localidad, estado o provincia, país, códigos de funcionamiento, etc.

Las capacidades de representación necesarias de la entidad propietaria del referido dominio.

La posesión del dominio

Esta presentación se realizará de forma digital utilizando las fuentes y aplicaciones que ACCV pone a disposición de los usuarios para ello.

ACCV comprobará los datos suministrados (incluyendo el país del solicitante) utilizando para ello la información disponible en:

Boletines oficiales

https://boe.es/diario_boe/

https://dogv.gva.es/va/inici/

Agencias de Protección de Datos

https://sedeagpd.gob.es/sede-electronica-web/

Registros de Administraciones Públicas

https://face.gob.es/es/directorio/administraciones

https://sede.administracion.gob.es/

https://www.pap.hacienda.gob.es/invente2/pagMenuPrincipalV2.aspx

Registros mercantiles

https://sede.registradores.org/site/

Oficinas de Patentes y Marcas

https://www.oepm.es/en/index.html

Servicios de Verificación y Consulta de Identidad

https://administracionelectronica.gob.es/ctt/SVD

reclamando al solicitante las subsanaciones o documentos adicionales que pudiera considerar necesarios.

Todos los organismos y registros utilizados son oficiales y de alta fiabilidad, proporcionando pruebas rastreables de todas las búsquedas.

La ACCV conserva esta información a efectos de auditoría, permitiendo su reutilización durante un periodo no superior a 13 meses desde su última comprobación.

Verificación de dominio

ACCV verificará que el dominio de los certificados y sus direcciones asociadas pertenecen a los datos del solicitante utilizando para ello la información disponible de los registros personales y de dominios, exigiendo al solicitante las explicaciones o documentos adicionales que pudiera considerar necesarios e incluyendo en el proceso mecanismos de comprobación técnicamente fiables y aprobados por la industria.

ACCV conserva la información de comprobación dominio con fines de auditoría pero no la reutiliza, verificando el dominio para cada solicitud de forma independiente. La ACCV no emitirá certificados para direcciones IP o nombres de dominio privados, y las entradas en el dNSName deben estar en la "sintaxis de nombre preferida", como se especifica en el RFC 5280, y por lo tanto no deben contener caracteres de subrayado ("_"). En el caso de los gTLD, sólo se emitirán certificados con nombres de gTLD aprobados, y sólo se emitirán a los suscriptores que tengan el control del gTLD, tal y como aparece en ICANN/IANA.

En concreto:

- Comprobación de que el solicitante, cuya identidad ha sido verificada sin lugar a dudas, es uno de los propietarios del dominio. Para esta comprobación, la ACCV debe utilizar uno o varios de los siguientes métodos:

  Contactar por correo, enviando un número aleatorio único en el correo a una o más direcciones creadas usando 'admin', 'administrator', 'webmaster', 'hostmaster', o 'postmaster' como parte local, seguido del signo de arroba ("@"), seguido de un nombre de dominio a autorizar, incluyendo un valor aleatorio en el correo electrónico, y recibiendo una respuesta de confirmación utilizando el mismo valor aleatorio del correo inicial. ACCV debe esperar la respuesta un tiempo no superior a 30 días y debe confirmar que la respuesta incluye el mismo número aleatorio.

  (CAB/Forum BR 3.2.2.4.4 Correo electrónico construido al contacto del dominio)

  Confirmar la presencia de un valor aleatorio incluido en el contenido de un archivo bajo el directorio "/.well-known/pki-validation" en el nombre de dominio a autorizar. Esta URL debe ser accesible por la CA a través de HTTP/HTTPS sobre un Puerto Autorizado. Una vez co-

municado el valor al solicitante, sólo será válido durante 30 días. En la URL no aparece en ningún caso el contenido del fichero y solo se considera como valor correcto de respuesta HTTP 200 (no se permiten re direcciones). Para realizar la verificación del valor aleatorio en la conexión HTTP/HTTPS se utilizaran múltiples perspectivas de red (al menos dos). Este método NO esta permitido para validar nombres de dominio comodín.

(CAB/Forum BR 3.2.2.4.18 Cambio acordado en el sitio web v2)

Confirmación del control del solicitante sobre un FQDN mediante la validación del control del dominio del FQDN utilizando el método ACME HTTP Challenge definido en la sección 8.3 de la RFC 8555.

ACCV DEBE recibir una respuesta HTTP satisfactoria de la solicitud (lo que significa que se debe recibir un código de estado HTTP 2xx).

El token (tal y como se define en RFC 8555, Sección 8.3) una vez comunicado el valor al solicitante, sólo será válido durante 30 días. En la URL no aparece en ningún caso el contenido del fichero y solo se considera como valor correcto de respuesta HTTP 200 (no se permiten re direcciones). Para realizar la verificación del valor aleatorio en la conexión HTTP/HTTPS se utilizaran múltiples perspectivas de red (al menos dos). Este método NO esta permitido para validar nombres de dominio comodín.

Los datos necesarios para establecer la comunicación utilizando ACME con la ACCV se pueden obtener de la cuenta asociada al organismo en la aplicación NPSC proporcionada por la ACCV.

Para llevar a cabo la generación y renovación automática de certificados es imprescindible que todos los documentos del suscriptor y del organismo estén validados y vigentes. Para ello se envían recordatorios a los usuarios registrados con certificados ACME indicando que los documentos o credenciales están próximos a caducar. Estos avisos empiezan 30 días antes de la caducidad y se repiten de forma diaria.

(CAB/Forum BR 3.2.2.4.19 Cambio acordado en el sitio web - ACME)

Confirmar la presencia de un valor aleatorio en un registro DNS CNAME, TXT o CAA para 1) un Nombre de Dominio de Autorización; o 2) un Nombre de Dominio de Autorización que tenga como prefijo una etiqueta que comience con un carácter de subrayado. Una vez comunicado el valor al solicitante, sólo será válido durante 30 días. Para realizar la verificación se utilizaran múltiples perspectivas de red (al menos dos).

(CAB/Forum BR 3.2.2.4.7 Cambio de DNS)

ACCV comprobará la existencia de registros CAA justo antes de emitir el certificado, actuando como se define en el RFC 8659 y en los documentos del CAB/Forum si el registro está presente. Para realizar la verificación del registro CAA se utilizaran múltiples perspectivas de red (al menos dos).

El identificador asociado a ACCV como registros CAA *issue* e *issuewild* es "accv.es".

Se realizarán pruebas de conexión con el dominio dado y pruebas de respuesta de DNS mediante protocolo seguro (por ejemplo, HTTPS).

Si se trata de un certificado con carácter comodín (*), la aplicación para realizar la petición (NPSC) sólo permite colocar el carácter en una posición válida (nunca se permite en una primera posición a la izquierda de una etiqueta "controlada por el registro" o sufijo público). Los certificados de sede no pueden llevar el carácter comodín (*).

Ante cualquier irregularidad el solicitante del certificado será notificado por la ACCV y se suspenderá su emisión hasta su corrección. Si dicha corrección no se produce en un mes, la solicitud será denegada.

3.2.3. Autenticación de la identidad de un individuo.

ACCV utiliza los mecanismos establecidos por la normativa técnica vigente, concretamente el Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, relativo al establecimiento de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de los métodos de identificación electrónica, según lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) número 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Véase la Política correspondiente.

La autentificación de la identidad del solicitante de un certificado se realizará mediante el uso de su certificado cualificado personal admitido para la firma de la solicitud del certificado cualificado de sitio web.

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

ACCV comprobará los datos suministrados (incluyendo el país del solicitante) utilizando para ello la información disponible en:

Boletines oficiales

https://boe.es/diario_boe/

https://dogv.gva.es/va/inici/

Agencias de Protección de Datos

https://sedeagpd.gob.es/sede-electronica-web/

Registros de Administraciones Públicas

https://face.gob.es/es/directorio/administraciones

https://sede.administracion.gob.es/

https://www.pap.hacienda.gob.es/invente2/pagMenuPrincipalV2.aspx

Registros mercantiles

https://sede.registradores.org/site/

Oficinas de Patentes y Marcas

https://www.oepm.es/en/index.html

Servicios de Verificación y Consulta de Identidad

https://administracionelectronica.gob.es/ctt/SVD

reclamando al solicitante las subsanaciones o documentos adicionales que pudiera considerar necesarios.

Todos los organismos y registros utilizados son oficiales y de alta fiabilidad, proporcionando pruebas rastreables de todas las búsquedas.

La ACCV conserva esta información a efectos de auditoría, permitiendo su reutilización durante un periodo no superior a 13 meses desde su última comprobación.

3.2.4. Información no verificada

Toda la información proporcionada es verificada.

3.2.5. Validación de la autoridad

La autoridad de los solicitantes de certificados para pedirlos en nombre de alguien se verifica durante la validación de la identidad del solicitante. Como establece la ley, es necesario un poder específico para esta operación.

3.2.6. Criterio para la interoperación

ACCV ni interopera ni tiene certificados cruzados con otras Autoridades de Certificación.

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

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

La identificación y autenticación para la renovación del certificado se puede realizar utilizando las técnicas para la autenticación e identificación inicial (descrita en los puntos 3.2.2 *Autenticación de la identidad de una organización* y 3.2.3 *Autenticación de la identidad de un individuo,* de esta DPC). ACCV puede reutilizar la información almacenada en comprobaciones previas si no han pasado mas de 13 meses desde la ultima verificación de los datos, exceptuando la información de comprobación de dominio, que no se reutiliza, y las claves asociadas, que se deben suministrar de nuevo. Existe, por tanto, mecanismos para la renovación:

- Formularios web en el Área de Gestión de Certificados No Personales, disponible en https://npsc.accv.es:8450/npsc.
- Automatización vía ACME (con la documentación correspondiente vigente)

Para mas información véase apartado 4.6 del presente documento.

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, pudiendo reutilizar la información en posesión de la ACCV si no han pasado mas de 13 meses desde la ultima verificación de los datos, exceptuando la información de comprobación de dominio que no se reutiliza, y las claves asociadas, que se deben suministrar de nuevo.

ACCV, por cuestiones técnicas y detallando todos los pasos, puede emplear algún método electrónico que garantice de manera fiable e inequívoca la identidad del solicitante y la autenticidad de la solicitud.

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

La política de identificación para las solicitudes de revocación podrá ser la misma que para el registro inicial. La política de autenticación aceptará solicitudes de revocación firmadas digitalmente por el subscriptor del certificado.

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

- Mediante formulario de revocación (ubicado en el Área de Gestión de Certificados No Personales https://npsc.accv.es:8450/npsc) accediendo por parte del solicitante del certificado o del responsable del mismo en la fecha de la solicitud de revocación mediante certificado cualificado personal.
- Utilizando el mecanismo de revocación de ACME

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

Para mas información véase apartado 4.9 del presente documento.

4. El ciclo de vida de los certificados

4.1. Solicitud de certificados

4.1.1. Quien puede enviar una solicitud de certificado

Este tipo de solicitud de certificados es responsabilidad de entidades privadas o públicas. Una solicitud de certificado puede ser presentada por el sujeto del certificado o por un representante autorizado del mismo, y que hayan acreditado tener el control sobre el nombre del dominio a incluir en el Certificado. En el caso de certificados de sede solo pueden solicitarlo entidades públicas.

4.1.2. Proceso de registro 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 autenticación de sitio web asociado a una entidad el usuario debe adjuntar el documento que lo acredita como capacitado para efectuar esa solicitud (documento de toma de posesión en el puesto o diario oficial donde se recoge el nombramiento correspondiente, poderes notariales e inscripción en los registros correspondientes), en formato pdf firmado electrónicamente. Si el acceso se ha efectuado con un certificado que acredita la capacidad necesaria para gestionar los certificados de autenticación de sitio web, se utilizaran 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 autenticación de sitio web, durante 13 meses a partir de la aprobación sin necesidad de aportar documentación adicional, exceptuando la información de comprobación de dominio que no se reutiliza. En el caso de identificación con certificado de empleado público no existe limitación temporal mientras el certificado esté en vigor.

Ademas de comprobar las credenciales asociados a la entidad, ACCV comprobará en los registros autorizados la posesión del dominio o dominios que aparecen en la solicitud de certificado, de forma que no exista duda de dicha posesión. ACCV dejará constancia de estas búsquedas y comprobaciones de forma que puedan reproducirse en todos los pasos. Para esta comprobación ACCV utilizara los datos suministrados en el proceso de alta, siendo necesaria una vinculación directa entre estos datos y los dominios incluidos en la solicitud.

Para la verificación del dominio y si el tipo del certificado lo permite pueden utilizarse los servicios ACME proporcionados por la ACCV, automatizando el proceso de registro y generación si la documentación de validación de organismo es valida y esta vigente. Para registrar una cuenta ACME previamente hay que hacer el alta de usuario y de la organización. A partir del registro se pueden obtener los datos necesarios para la solicitud.

4.2. Tramitación de la solicitud de certificados.

El identificador asociado con ACCV como registros CAA issue y issuewild es “accv.es”.

4.2.1. Realización de las funciones de identificación y autenticación

El solicitante se identifica con un certificado personal cualificado en el Área de Gestión de Certificados No Personales (NPSC) ubicada en https://npsc.accv.es:8450/npsc, utilizando los datos del certificado para realizar las funciones de identificación y autenticación. En caso de utilizar ACME la solicitud se completa de forma automatizada mediante los mecanismos de comunicación descritos en el protocolo ya que la identificación se realiza con los datos suministrados al activar la cuenta ACME.

Una vez recibida la solicitud de certificado en formato electrónico a través de la plataforma por parte de las personas autorizadas y una vez aceptada la proposición económica, la ACCV procede a la revisión de la solicitud. En el caso de utilizar ACME solo se aceptara la solicitud si la documentación requerida esta vigente y es válida.

La ACCV comprueba los datos de la solicitud y acredita al solicitante de la solicitud de certificado de autenticación de sitios web, durante 13 meses desde la aprobación sin necesidad de presentar ninguna

documentación adicional. En el caso de identificarse con certificado de empleado público o representante no existe límite temporal mientras el certificado esté vigente.

Además de comprobar las credenciales asociadas a la entidad, la ACCV verifica en los registros autorizados la posesión del dominio o dominios que aparecen en la solicitud del certificado, para que no haya dudas sobre la existencia de esta posesión, tal y como se detalla en los apartados 3.2.2 y 3.2.3 de esta política. ACCV proporciona registros de estas búsquedas y comprobaciones para que puedan ser reproducidas en cada paso. Para esta comprobación ACCV utiliza los datos que se presentaron en el proceso de registro, siendo necesaria una conexión directa entre estos datos y los dominios que se incluyen en la solicitud.

En este proceso, ACCV comprueba que las solicitudes de certificados no incluyen dominios que puedan ser utilizados para phishing u otros usos fraudulentos, utilizando los mecanismos y listas disponibles.

4.2.2. Aprobación o rechazo de la solicitud del certificado

En caso de aceptación, la Autoridad de Registro notificará al solicitante a través de un correo electrónico firmado digitalmente a la dirección de correo electrónico que figura en la solicitud. En el caso de utilizar los servicios ACME la solicitud se aprueba de forma automatizada si se cumplen los requisitos de dominio y las credenciales del organismo y suscriptor están vigentes y válidas.

En caso de rechazo, la Autoridad de Registro notificará al solicitante mediante un correo electrónico firmado digitalmente a la dirección de correo electrónico que figura en la solicitud. La solicitud queda anulada y no puede ser reutilizada, aunque es posible reutilizar la documentación aportada marcada como correcta durante un periodo no superior a 13 meses.

Este proceso lo lleva a cabo un miembro de la ACCV diferente al responsable de realizar la verificación de los datos. La diferenciación de funciones se realiza utilizando las capacidades establecidas en la aplicación de gestión. En el caso de servicios ACME todos los procesos se llevan a cabo de forma automatizada.

ACCV utilizará esta información para decidir sobre nuevas solicitudes.

4.2.3. Tiempo en procesar la solicitud

El tiempo máximo para tramitar las solicitudes de certificado es de cinco (5) días hábiles. Este tiempo contabiliza el procesado por parte de la ACCV y no incluye el tiempo utilizado por el usuario para aportar la información y documentación necesarias.

4.3. Emisión de certificados

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

4.3.1. Acciones de la Autoridad de Certificación durante la emisión

La emisión del certificado tiene lugar una vez que la Autoridad de Registro ha realizado las comprobaciones necesarias para validar la solicitud. El mecanismo que determina la naturaleza y forma de realizar estas comprobaciones es esta DPC.

Cuando el solicitante recibe el correo electrónico de aprobación, debe entrar de nuevo en NPSC, identificándose con un certificado personal cualificado para generar y descargar el certificado. Esto no es de aplicación si se utiliza ACME, donde la solicitud, comprobación de documentación y posesión de dominio, y generación se hace en un solo paso.

La organización responsable del certificado de autenticación de los sitios web puede solicitar a la ACCV que añada otros usuarios con capacidad para realizar las transacciones que están asociadas al ciclo de vida de los certificados. La Autoridad de Registro comprobará la solicitud de credencial y notificará al solicitante la autorización o denegación del permiso, a través de un correo electrónico firmado.

ACCV podrá realizar esta autorización de oficio en el caso de que el responsable de la organización pierda su capacidad de gestión y no exista otra persona autorizada.

Cuando la AC de ACCV emite un certificado de acuerdo con una solicitud de certificación válida, enviará una copia del certificado a la Autoridad de Registro que emitió la solicitud y otra al repositorio de ACCV.

ACCV revisa que los certificados se ajustan a los perfiles aceptados utilizando distintos validadores que se ejecutan antes de la firma de las solicitudes por la CA (se firman por una claves genéricas no reconocidas). Concretamente se utilizan:

- zlint

- pkilint

Si alguno de esos validadores devuelve un error la emisión se detiene y se avisa al solicitante y a los operadores de la CA.

ACCV realizará revisiones frecuentes de las muestras de los certificados de autentificación de sitios web para garantizar la exactitud de los datos y el formato de los certificados mediante los validadores utilizados en la emisión. Si en el transcurso de estos muestreos se confirma un cambio de datos que pueda implicar la pérdida de la posesión del dominio, la ACCV revocará los certificados implicados. En caso de inexactitud de los datos que figuran en el certificado o de su inaplicabilidad se seguirá el mismo proceso. ACCV dejará constancia documental de todas estas revisiones y actuaciones.

En el caso de certificados emitidos por una CA raíz se requiere que una persona autorizada por la ACCV intervenga de forma manual para que dicha CA raíz realice una operación de firma de certificados.

4.3.2. Notificación al suscriptor

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

4.4. Aceptación de certificados

4.4.1. Proceso de aceptación

La aceptación de los certificados por parte de los firmantes 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 usuario debe aceptar el contrato antes de la emisión del certificado.

4.4.2. Publicación del certificado por la Autoridad de Certificación

Una vez que el certificado ha sido aceptado por el suscriptor y generado, el certificado se publicará en el repositorio de ACCV y se pondrá a disposición de los usuarios autorizados.

4.4.3. Notificación de la emisión a otras entidades

Antes de la expedición de Certificados de autenticación de sitios web se envía un pre-certificado a los registros del servicio Certificate Transparency (CT LOG) siguiendo los requisitos establecidos en las políticas de aplicación. El numero de operadores a los que se envía el pre-certificado y el formato de las extensiones se indica en 7.1.10.

No hay mas notificaciones.

4.5. Uso del par de claves y del certificado.

4.5.1. Clave privada del suscriptor y uso del certificado

ACCV no genera ni almacena las Claves Privadas asociadas a los Certificados de autenticación de sitios web. La custodia y el control de las claves privadas corresponde al suscriptor o a sus Representantes que hayan acreditado tener el control sobre el nombre del dominio a incluir en el Certificado.

El alcance de uso previsto para una clave privada se especificará a través de extensiones de certificado, incluido el uso de clave y las extensiones de uso de clave extendido, en el certificado asociado.

Los certificados pueden emplearse para identificar al servidor a cuyo dominio esta emitido el certificado de manera segura, y para establecer canales seguros de comunicación (incluyendo cifrado) utilizando los mecanismos disponibles en cada caso.

En el caso de certificados de sede se utilizan para identificar una sede electrónica de un organismo público.

4.5.2. Uso del certificado y la clave pública por terceros que confían

La partes que confían se comprometen a:

- Los usos de los certificados se corresponden con el ámbito de aplicación.

- Se cumplen las disposiciones de la DPC

- Comprobar el estado del certificado y verificar el estado de la cadena jerárquica antes de establecer la confianza.

- No comprometer o utilizar los servicios ofrecidos de forma maliciosa.

- Informar de cualquier anomalía o problema detectado utilizando los canales adecuados.

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.

ACCV no renueva Certificados manteniendo la Clave pública del mismo, sino que, en todo caso, la renovación de Certificados se realiza aportando siempre Claves.

4.6.1. Circunstancias para la renovación del certificado

El periodo de renovación de los certificados comienza 30 días antes de la fecha de caducidad del certificado, cuando el suscriptor recibe un correo electrónico en el que se le notifican los pasos a seguir para proceder a la renovación del certificado. En el caso de utilizar ACME el proceso de renovación se puede iniciar de forma automática si se ha configurado esta opción y los documentos necesarios para la validación de la organización están vigentes y son válidos.

4.6.2. Quién puede solicitar la renovación del certificado

Cualquier suscriptor puede solicitar la renovación de su certificado. Para ello deben cumplirse los mismos requisitos que en la solicitud inicial.

4.6.3. Tramitación de solicitudes de renovación de certificados

Se seguirá el mismo proceso que el descrito para la emisión inicial.

4.6.4. Notificación de la emisión de un nuevo certificado al suscriptor

Es responsabilidad de la Autoridad de Registro notificar al suscriptor la emisión del certificado y entregarle una copia, o en su defecto, informarle de cómo puede obtener una copia.

Se seguirá el mismo proceso que el descrito para la emisión inicial.

4.6.5. Conducta que constituye la aceptación de la renovación del certificado

Se seguirá el mismo proceso que el descrito para la emisión inicial.

4.6.6. Publicación del certificado de renovación por parte de la Autoridad de Certificación

Se seguirá el mismo proceso que el descrito para la emisión inicial.

4.6.7. Notificación de la renovación del certificado a otras entidades

Se seguirá el mismo proceso que el descrito para la emisión inicial.

4.7. Renovación de claves

La renovación de claves implica necesariamente la renovación de certificado y no se pueden llevar a cabo como procesos separados.

4.7.1. Circunstancias para la renovación con regeneración de claves

La renovación de claves implica necesariamente la renovación de certificado y no se pueden llevar a cabo como procesos separados.

4.7.2. Quién puede solicitar la renovación con regeneración de claves

La renovación de claves implica necesariamente la renovación de certificado y no se pueden llevar a cabo como procesos separados.

ACCV puede regenerar las claves de los certificados de las CA, de acuerdo con el documento de la ceremonia de generación correspondiente. ACCV puede regenerar las claves de los certificados de los servicios OCSP y TSA de acuerdo con el correspondiente procedimiento interno.

4.7.3. Procesamiento de solicitudes de renovación con regeneración de claves

La renovación de claves implica necesariamente la renovación de certificado y no se pueden llevar a cabo como procesos separados.

4.7.4. Notificación de la renovación con regeneración de claves

La renovación de claves implica necesariamente la renovación de certificado y no se pueden llevar a cabo como procesos separados.

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

La renovación de claves implica necesariamente la renovación de certificado y no se pueden llevar a cabo como procesos separados.

4.7.6. Publicación del certificado renovado

La renovación de claves implica necesariamente la renovación de certificado y no se pueden llevar a cabo como procesos separados.

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

La renovación de claves implica necesariamente la renovación de certificado y no se pueden llevar a cabo como procesos separados.

4.8. Modificación de certificados.

No se permite la modificación de los campos del certificado. Cuando sea necesario modificar alguna información del certificado, ACCV revocará el certificado y emitirá uno nuevo siguiendo los procesos establecidos.

4.8.1. Circunstancias para la modificación del certificado

No se permite la modificación de los campos del certificado. Cuando sea necesario modificar alguna información del certificado, ACCV revocará el certificado y emitirá uno nuevo siguiendo los procesos establecidos.

4.8.2. Quién puede solicitar la modificación del certificado

No se permite la modificación de los campos del certificado. Cuando sea necesario modificar alguna información del certificado, ACCV revocará el certificado y emitirá uno nuevo siguiendo los procesos establecidos.

4.8.3. Procesamiento de solicitudes de modificación del certificado

No se permite la modificación de los campos del certificado. Cuando sea necesario modificar alguna información del certificado, ACCV revocará el certificado y emitirá uno nuevo siguiendo los procesos establecidos.

4.8.4. Notificación de la modificación del certificado

No se permite la modificación de los campos del certificado. Cuando sea necesario modificar alguna información del certificado, ACCV revocará el certificado y emitirá uno nuevo siguiendo los procesos establecidos.

4.8.5. Conducta que constituye la aceptación de la modificación del certificado

No se permite la modificación de los campos del certificado. Cuando sea necesario modificar alguna información del certificado, ACCV revocará el certificado y emitirá uno nuevo siguiendo los procesos establecidos.

4.8.6. Publicación del certificado modificado

No se permite la modificación de los campos del certificado. Cuando sea necesario modificar alguna información del certificado, ACCV revocará el certificado y emitirá uno nuevo siguiendo los procesos establecidos.

4.8.7. Notificación de la modificación del certificado a otras entidades

No se permite la modificación de los campos del certificado. Cuando sea necesario modificar alguna información del certificado, ACCV revocará el certificado y emitirá uno nuevo siguiendo los procesos establecidos.

4.9. Revocación y suspensión de certificados.

4.9.1. Circunstancias para la revocación

4.9.1.1. Razones para revocar un certificado de usuario

Un certificado se revoca en un periodo no superior a 24 horas cuando:

- Se recibe por parte del suscriptor una petición valida de revocación
- Se recibe por parte de una tercera parte autorizada una petición valida de revocación, por ejemplo mediante una orden judicial
- El subscriptor del certificado o sus claves o las claves de sus certificados se han comprometido por:
  - El robo, pérdida, revelación, modificación, u otro compromiso o sospecha de compromiso de la clave privada del usuario.
  - El mal uso deliberado de claves y certificados, o la falta de observación de los requerimientos operacionales del acuerdo de suscripción, la CP asociada o de la presente DPC.
- El par de claves generado por el suscriptor se revela como “débil”.

- El certificado de una RA o CA superior en la jerarquía de confianza del certificado es revocado.
- ACCV tiene conocimiento de un método demostrado o comprobado que expone la clave privada del Suscriptor a un compromiso o si hay pruebas claras de que el método específico utilizado para generar la Clave Privada era defectuoso.

Un certificado debe revocarse en un periodo no superior a los cinco días, siendo recomendable revocar en un periodo no superior a las 24 horas cuando:

- No se ha cumplido un prerrequisito necesario para la emisión del certificado.
- Se sabe que un factor fundamental del certificado es falso o se cree razonablemente que puede serlo.
- Ha ocurrido un error introduciendo o procesando los datos.
- La información contenida en un certificado se vuelve inexacta, por ejemplo, cuando el propietario de un certificado cambia su nombre.
- ACCV tiene conocimiento de cualquier circunstancia que indique que el uso de un nombre de dominio en el certificado ya no está legalmente permitido (por ejemplo, si un tribunal o una instancia similar ha revocado el derecho del propietario del nombre de dominio a utilizarlo, si se ha rescindido un acuerdo de licencia o de servicios pertinente entre el propietario del nombre de dominio y el solicitante del certificado, o si el propietario del nombre de dominio no lo ha renovado).
- ACCV tiene conocimiento de que se ha utilizado un Certificado Wildcard para autenticar un nombre de dominio subordinado de forma fraudulenta.
- El Certificado no se ha emitido de conformidad con las políticas establecidas en este documento.

4.9.1.2. Razones para revocar un certificado de AC subordinada (intermedia)

Un certificado de CA intermedia (subordinada) se revoca cuando:

- ACCV obtiene pruebas de que la clave privada de la AC subordinada correspondiente a la clave pública del certificado se ha visto comprometida.
- ACCV obtiene pruebas de que se ha utilizado de forma indebida.
- ACCV tiene conocimiento de que el certificado no se ha emitido de acuerdo con esta DPC, con la Política de Certificación o la Declaración de Prácticas de Certificación aplicables, o de que la AC subordinada no las ha cumplido.
- ACCV determina que cualquier información que aparece en el Certificado es inexacta o engañosa.
- ACCV deja de operar por cualquier razón y no ha hecho arreglos para que otra CA pro porcione soporte de revocación para el Certificado.
- El derecho de ACCV a emitir certificados en virtud de estos requisitos expira, se revoca o se extingue, a menos que la AC emisora haya tomado medidas para seguir manteniendo el repositorio CRL/OCSP.
- La revocación es requerida por la Política de Certificados de ACCV y/o la Declaración de Prácticas de Certificación.
- El contenido técnico o el formato del certificado presenta un riesgo inaceptable para los proveedores de software de aplicación o las partes que confían en él.

La revocación debe realizarse en un plazo no superior a 7 días desde que ACCV es consciente del cumplimiento de estas condiciones.

4.9.2. Entidad que puede solicitar la revocación

La revocación de un certificado se puede instar tanto por el suscriptor del mismo como por parte de ACCV, así como por cualquier persona que conozca fehacientemente que los datos asociados al certificado se convierten en inexactos o incorrectos o que se ha incurrido en alguno de los supuestos establecidos para la revocación.

Los suscriptores de certificados pueden solicitar su revocación por cualquier causa y deben solicitarla bajo las condiciones especificadas en el siguiente apartado.

4.9.3. Procedimiento de solicitud de revocación

ACCV acepta solicitudes de revocación de certificados de autenticación de sitios web por los siguientes procedimientos

4.9.3.1. Telemático interactivo

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.

Puede revocarse tambien a traves del formulario de contacto en https://www.accv.es/# donde el usuario debe pegar la clave privada en formato PEM, incluyendo las líneas BEGIN y END.

4.9.3.2. Telemático ACME

Utilizando el servicio de automatización mediante ACME, desde la cuenta para la que se emitio el certificado.

https://npsc.accv.es:8450/npsc/acme/revoke-cert

4.9.3.3. Telefónico

Utilizando el teléfono de contacto en horario 24x7 963 866 014.

Los suscriptores, las partes confiantes, los proveedores de software de aplicación y otras terceras partes pueden informar sobre sospechas de compromiso de claves privadas, uso indebido de certificados u otros tipos de fraude, compromiso, uso indebido, conducta inapropiada o cualquier otro asunto relacionado con los certificados en la URL https://www.accv.es/contacto/. En dicha URL se encuentran el correo electrónico de soporte y los teléfonos de contacto.

4.9.4. Periodo de gracia de la solicitud de revocación

En el caso de que no se defina un Periodo de Gracia en el Acuerdo de Suscripción, los suscriptores están obligados a solicitar la revocación dentro de las 24 horas siguientes a la detección de cualquier problema que invalide el uso del certificado (la pérdida o el compromiso de la Clave Privada, etc.).

4.9.5. Plazo de tiempo para procesar la solicitud de revocación

ACCV tratará las solicitudes de revocación de conformidad con las secciones 4.9.1.1 y 4.9.5 de las BR/TLS, garantizando siempre que en las 24 horas posteriores a la recepción de un CPR se ha realizado un estudio preliminar y un informe inicial. ACCV informará al suscriptor y a la entidad ha comunicado el problema.

4.9.6. Obligación de verificar las revocaciones por las partes que confían

Las terceras partes que confían y aceptan el uso de los Certificados emitidos por ACCV están obligadas a verificar el estado de los certificados (revocación y caducidad) en toda la cadena de certificación y en cada uso de los mismos contra la CRL pertinente publicada o utilizando el servidor OCSP.
ACCV pone a disposición de sus usuarios varios servicios de comprobación de revocación para los

certificados que emite (CRL, OCSP, otros..). Las partes que confían deben utilizar al menos OCSP (preferentemente) o CRL.

4.9.7. Frecuencia de emisión de CRLs

ACCV publicará una nueva CRL de entidad final en su repositorio a intervalos máximos de 5 horas, aunque no se hayan producido modificaciones en la CRL (cambios en el estado de los certificados) durante el periodo mencionado. El campo nextUpdate tiene un valor máximo de 4 días.

ACCV publicará una nueva CRL raíz en su repositorio con una periodicidad máxima de 6 meses, aunque no se hayan producido modificaciones en la CRL. En caso de revocación de un autoridad de certificación intermedia, la CRL se publicará en un plazo no superior a doce horas.

El OCSP se actualiza de manera previa a la CRL. La información mas reciente será la que proporcione el OCSP.

La CRL no contiene los certificados caducados. Para consultar sobre el estado de un certificado caducado la información válida será la que proporcione el OCSP.

4.9.8. Latencia máxima para la publicación de CRLs

El tiempo máximo entre la generación de las CRLs y su publicación en el repositorio es de 30 minutos.

4.9.9. Disponibilidad del sistema de verificación online del estado de los certificados

ACCV proporciona un servidor OCSP para la verificación del estado de los certificados en línea en: ocsp.accv.es:80 conforme a RFC 6960 y RFC 5019.

Las respuestas OCSP están firmadas por un servidor OCSP cuyo certificado está firmado por la CA que emitió el certificado que estamos comprobando, y que tiene los usos de clave específicos para ello.

ACCV mantiene la información del estado del certificado de forma indefinida, garantizando esta información durante al menos 15 años.

4.9.10. Requisitos de comprobación en línea de la revocación

El servidor OCSP es de libre acceso y no hay requisitos para su uso, salvo los derivados del uso del protocolo OCSP según las disposiciones del RFC 6960.

OCSP admite llamadas al servicio mediante el método GET (además del método POST).

Para el estado de los certificados de suscriptor:

- ACCV actualiza la información proporcionada a través de OCSP en un periodo no superior a 3 horas.

- Las respuestas OCSP de este servicio tienen un tiempo de caducidad máximo de 3 días.

- Debe haber disponible una respuesta OCSP autorizada (es decir, el servicio OCSP NO DEBE responder con el estado «desconocido») en un plazo no superior a 15 minutos a partir de la primera publicación o puesta a disposición del certificado.

Para el estado de los certificados de CA subordinada:

- ACCV actualiza la información proporcionada vía OCSP en un periodo no superior a 6 meses y dentro de las 12 horas siguientes a la revocación de un certificado de CA intermedia.

El servicio OCSP de la ACCV proporciona respuestas definitivas sobre números de serie de certificados «reservados», como si hubiera un certificado correspondiente que coincidiera con el precertificado, tal y como se indica en el RFC 6962. Un número de serie de certificado dentro de una solicitud OCSP esta en una de las tres opciones siguientes:

- 1 . «asignado» si la CA emisora ha emitido un certificado con ese número de serie
- 2 «reservado» si un Precertificado [RFC6962] con ese número de serie ha sido emitido por la CA emisora
- 3 «no utilizado» si no se cumple ninguna de las condiciones anteriores.

Si el servidor OCSP recibe una solicitud de estado de un certificado que no ha sido emitido(«no utilizado»), entonces responde con un estado "revocado", con la razón certificateHold(6) y revocationTime 1 de enero de 1970. ACCV supervisa la respuesta a este tipo de solicitudes como parte de sus procedimientos de respuesta de seguridad.

ACCV también proporciona servicios web para consultar el estado de validez de los certificados emitidos.

4.9.11. Otras formas de aviso de revocación disponibles

No definidas

4.9.12. Requisitos especiales de revocación de claves comprometidas

No habrá variación en las cláusulas anteriores en el caso de que la revocación se deba al compromiso de la clave privada.

El usuario puede proporcionar la clave privada comprometida utilizando el formulario de soporte que se indica en la siguiente URL: https://www.accv.es/ayuda/certificates-revocation/how-revoke-certificate/

En el formulario deberá pegar dicha clave en formato PEM, incluyendo las líneas BEGIN y END.

4.9.13. Circunstancias para la suspensión

La suspensión conlleva la invalidez del certificado durante todo el tiempo que esté suspendido.

ACCV no permite la suspensión de los certificados.

4.9.14. Entidad que puede solicitar la suspensión

ACCV no permite la suspensión de los certificados.

4.9.15. Procedimiento para la solicitud de suspensión

ACCV no permite la suspensión de los certificados.

4.9.16. Límites del período de suspensión

ACCV no permite la suspensión de los certificados.

4.10. Servicios de comprobación de estado de certificados.

La información relativa a la verificación del estado de revocación de los Certificados electrónicos expedidos por la ACCV puede ser consultada mediante CRLs y/o el Servicio de información y consulta del estado de los Certificados mediante el protocolo OCSP, y son accesibles a través de los siguientes medios indicados en nuestra pagina web:

https://www.accv.es/servicios/validacion/

CRL:

CRL ACCVRAIZ1 https://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl

CRL ACCVCA110 https://www.accv.es/fileadmin/Archivos/certificados/accvca110_der.crl

CRL ACCVCA120 https://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl

CRL ACCVCA130 https://www.accv.es/fileadmin/Archivos/certificados/accvca130_der.crl

CRL ACCV ROOT RSA TLS 2024 http://www.accv.es/gestcert/accv_root_rsa_tls_2024.crl

CRL ACCV RSA1 TLS http://www.accv.es/gestcert/accv_rsa1_tls.crl

CRL ACCV ROOT ECC TLS 2024 http://www.accv.es/gestcert/accv_root_ecc_tls_2024.crl

CRL ACCV ECC1 TLS http://www.accv.es/gestcert/accv_ecc1_tls.crl

OCSP (toda la jerarquía): http://ocsp.accv.es

4.10.1. Características operativas

Los certificados revocados permanecen en la CRL hasta que alcanzan su fecha de caducidad.

Una vez alcanzada ésta, se eliminan de la lista de certificados revocados.

OCSP establece un límite de 180 meses, lo que permite comprobar el estado del certificado más allá de la fecha de caducidad.

El Servicio de información y consulta del estado de los Certificados mediante protocolo OCSP soporta el método GET para recuperar la información de validación de los certificados emitidos, de acuerdo con los requisitos de la RFC6960 y aquellos establecidos por la entidad CA/Browser Forum (que pueden consultarse en la dirección https://cabforum.org/baseline-requirements-documents/). Las respuestas OCSP tienen un intervalo de validez de 3 días y la información se actualiza constantemente accediendo directamente a la base de datos. El servidor OCSP no responderá "good"a la consulta sobre el estado de un certificado que no ha sido emitido.

4.10.2. Disponibilidad del servicio

Los sistemas CRL y los sistemas de consulta del estado de los certificados en línea (OCSP) estarán disponibles las 24 horas del día y los 7 días de la semana.

El tiempo de respuesta del OCSP se debe mantener inferior a 1s y el tiempo de descarga de CRL se debe mantener inferior a 10s.

4.10.3. Características opcionales

No hay restricciones de acceso o de consulta para el OCSP y la CRL.

4.11. Finalización de la suscripción.

La suscripción finaliza con:

Ceso de operación de ACCV

la expiración o revocación del certificado sin una renovación.

ACCV informará al responsable del certificado de autenticación de sitio web, mediante correo electrónico, en un momento previo anterior a la publicación del certificado en la Lista de Certificados Revocados, acerca de la suspensión o revocación de los certificados en los cuales aparezca como suscriptor o responsable, especificando los motivos, la fecha y la hora en que su certificado quedará sin efecto, y comunicándole que no debe continuar utilizándolo.

4.12. Depósito y recuperación de claves.

4.12.1. Prácticas y políticas de custodia y recuperación de claves

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

4.12.2. Prácticas y políticas de protección y recuperación de la clave de sesión

La recuperación de las claves de sesión no esta soportado.

4.13. Caducidad de las claves de certificado de CA.

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

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

5.1. Controles de Seguridad Física

5.1.1. Ubicación y construcción

Los sistemas de información de ACCV se ubican en Centros de Proceso de Datos con unos niveles de protección y solidez de la construcción adecuado y con vigilancia durante las 24 horas al día, los 7 días a la semana. Las barreras físicas se utilizan para segregar las zonas seguras dentro de los CPD y se construyen de manera que se extiendan desde el suelo real hasta el techo real para evitar la entrada no autorizada.

5.1.2. Acceso físico

Los Centros de Proceso de Datos de ACCV disponen de diversos perímetros de seguridad, con diferentes requerimientos de seguridad y autorizaciones. Entre los equipos que protegen los perímetros de seguridad se encuentran sistemas de control de acceso físico por combinación, sistemas de videovigilancia y de grabación, de detección de intrusiones entre otros.

Para acceder a las áreas más protegidas se requiere dualidad en el acceso y la estancia.

5.1.3. Alimentación eléctrica y aire acondicionado

Las instalaciones disponen de sistemas de alimentación ininterrumpida con una potencia suficiente para mantener autónomamente la red eléctrica durante los períodos de apagado controlado del sistema y para proteger a los equipos frente a fluctuaciones eléctricas que los pudieran dañar.

El apagado de los equipos sólo se producirá en caso de fallo de los sistemas de generación autónoma de alimentación.

El sistema de acondicionamiento ambiental está compuesto por varios equipos independientes con capacidad para mantener niveles de temperatura y humedad dentro de los márgenes de operación óptimos de los sistemas.

5.1.4. Exposición al agua

Los Centros de Proceso de Datos de ACCV disponen de detectores de inundación y sistemas de alarma apropiados al entorno.

5.1.5. Protección y prevención de incendios

Los Centros de Proceso de Datos de ACCV disponen de sistemas automatizados para la detección y extinción de incendios.

5.1.6. Sistema de almacenamiento

Los soportes de información sensible se almacenan de forma segura en armarios ignífugos y cajas fuertes, según el tipo de soporte y la clasificación de la información en ellos contenida.

Estos armarios se encuentran en diversas dependencias para eliminar riesgos asociados a una única ubicación.

El acceso a estos soportes está restringido a personal autorizado.

5.1.7. Eliminación de residuos

La eliminación de soportes magnéticos, ópticos e información en papel se realiza de forma segura siguiendo procedimientos establecidos para este fin, adoptando procesos de desmagnetización, de esterilización, de destrucción o triturado en función del tipo soporte a tratar.

5.1.8. Backup remoto

Diariamente se realizan copias de bakup remotas cifradas, siendo almacenadas en dependencias próximas al Centro de Proceso de Datos de respaldo, donde las operaciones de ACCV continuarían en caso de incidente grave o caída del Centro de Proceso de Datos principal.

5.2. Controles de procedimientos

Los sistemas de información y los servicios de ACCV se operan de forma segura, siguiendo procedimientos preestablecidos.

Por razones de seguridad, la información relativa a los controles de procedimiento se considera materia confidencial y solo se explican de forma resumida.

5.2.1. Papeles de confianza

Los roles identificados para el control y la gestión de los servicios son:

a. Gerencia
b. Administrador de Sistemas
c. Administrador de Puntos de Registro de Usuario (PRU)
d. Administrador de Seguridad
e. Operador de Autoridad de Certificación
f. Operador de PRU
g. Responsable de formación, soporte y comunicación
h. Responsable de Seguridad
i. Auditor
j. Jurista
k. Responsable de Documentación
l. Asistencia al Desarrollo de Aplicaciones y Soporte al Despliegue
m. Coordinador de Autoridad de Certificación

5.2.1.1. Gerencia

Al frente de la plantilla de ACCV y bajo el control del Consejo de Administración de ISTEC, es la persona responsable de la gestión económica y financiera y el control técnico y administrativo de las actividades de ACCV.

Se corresponde con el cargo de Gerente de la entidad Infraestructures i Serveis de Telecomunicacions i Certificació, SAU (ISTEC).

5.2.1.2. Administrador de Sistemas

Es el encargado de la instalación y configuración de sistemas operativos, de productos software, del mantenimiento y actualización de los productos y programas instalados.

Se le encomienda el establecimiento y documentación de los procedimientos de monitorización de los sistemas y de los servicios que se prestan, así como del control de las tareas realizadas por los Operadores de Autoridad de Certificación.

Debe velar por la prestación de servicios con el adecuado nivel de calidad y fiabilidad, en función del grado de criticidad de éstos.

Son responsables de la correcta ejecución de la Política de Copias, y en particular, de mantener la información suficiente que permita restaurar eficientemente cualquiera de los sistemas. Junto con el perfil de Operador de Autoridad de Certificación y, excepcionalmente, de Administrador de PRU, se encargará de llevar a cabo las copias de backup locales.

Debe mantener el inventario de servidores y equipamiento que compone el núcleo de la plataforma de certificación de ACCV.

No debe tener acceso a aspectos relacionados con la seguridad de los sistemas, de la red, etc. (altas/bajas de usuarios, gestión de reglas de firewall, gestión y mantenimiento de los sistemas de detección de intrusiones, etc.).

Debe colaborar con los Auditores en todo aquello que les sea requerido.

5.2.1.3. Administrador de PRUs.

Este perfil es similar al de Administrador de Sistemas pero dedicado a las tareas relacionadas con la instalación, mantenimiento y control de los sistemas que componen los Puntos de Registro de Usuario.

Se encarga de las tareas administrativas relacionadas con las autorizaciones de Operadores de PRU, acuerdos de confidencialidad, etc.

Debe mantener el inventario de PRUs y equipamiento que se dedica a las operaciones de los PRUs.

Excepcionalmente podrá colaborar con el Administrador de Sistemas y Operador de Autoridad de Certificación para llevar a cabo los bakups locales de los sistemas de la PKI.

De igual manera que los Administradores de Sistemas, no debe tener acceso a aspectos relacionados con la seguridad de los sistemas, de la red, etc. (altas/bajas de usuarios, gestión de reglas de firewall, gestión y mantenimiento de los sistemas de detección de intrusiones, etc.).

Debe colaborar con los Auditores en todo aquello que les sea requerido.

5.2.1.4. Administrador de Seguridad.

Debe cumplir y hacer cumplir las políticas de seguridad de ACCV, y debe encargarse de cualquier aspecto relativo a la seguridad de ACCV, desde seguridad física hasta la seguridad de las aplicaciones, pasando por seguridad de la red.

Será el encargado de gestionar los sistemas de protección perimetral y en concreto de la configuración y gestión de las reglas de los firewalls, de acuerdo con la política de seguridad y las pautas marcadas por el Responsable de Seguridad

Debe encargarse de la instalación, configuración y gestión de los sistemas de detección de intrusiones (IDS) y de las herramientas asociadas a éstos.

Tratará de resolver o hacer que se resuelvan las incidencias de seguridad producidas, de hacer que se eliminen vulnerabilidades detectadas, etc. dejando siempre registro de las incidencias y de las acciones realizadas.

Se encargará de mantener actualizados los documentos relacionados con los dispositivos de seguridad y, en general, con sus tareas.

Informará al Responsable de Seguridad de las incoherencias entre la Política de Seguridad, la Declaración de Prácticas de Certificación, etc. con la realidad práctica.

Controlará que los sistemas de seguridad física de los CPDs se operan y se mantienen correctamente por parte de las empresas que proporcionan los servicios de collocation.

De manera coordinada con el Responsable de Seguridad, debe encargarse de explicar los mecanismos de seguridad al personal que deba conocerlos, de concienciar a todo el personal de ACCV y de hacer cumplir las normas y políticas de seguridad. Debe colaborar con los Auditores en todo aquello que les sea requerido.

5.2.1.5. Operador de la Autoridad de Certificación

Dará asistencia a los Administradores de Sistemas y Administradores de PRU en aquellos aspectos técnicos o administrativos que no requieran acceso al CPD.

Deberá prestar asistencia al Responsable de formación, soporte y comunicación en aquellas tareas que les indique.

Deberá prestar la colaboración requerida por los Administradores de PRU, tanto para funciones de inventario, ayuda a la instalación de sistemas componentes de los PRUs, preparación de documentación, colaboración en la formación y soporte de operadores de PRU, etc.

Prestará colaboración al Responsable de Documentación para el control de documentos existentes, control de archivo de documentación (en papel) y revisión de certificados y contratos.

Colaborará con el Responsable de Seguridad en tareas administrativas, de inventario y, en general, aquellas tareas técnicas o administrativas.

Junto con el perfil de Administrador de Sistemas y, excepcionalmente, de Administrador de PRU, se encargará de llevar a cabo las copias de backup locales. Esta será la única tarea que el Operador de Autoridad de Certificación desarrolle en el interior del CPD.

Debe colaborar con los Auditores en todo aquello que les sea requerido.

5.2.1.6. Operador de Punto de Registro de Usuario

Se encarga de las funciones relacionadas con la identificación de solicitantes de certificados, la tramitación de certificados digitales, la revocación de éstos y el desbloqueo de tarjetas criptográficas, todo ello haciendo uso en exclusiva de las herramientas y aplicaciones que les proporcionen los Administradores de PRU, y siguiendo estrictamente los procedimientos aprobados.

Debe colaborar con los Auditores en todo aquello que les sea requerido.

5.2.1.7. Responsable de formación, soporte y comunicación

Se encarga del mantenimiento de contenidos de la web de la Agencia de Tecnología y Certificación Electrónica.

Se le encomiendan las labores de comunicación y actualización de la web de ACCV.

Se encarga de definir el plan de formación para usuarios finales, para agentes de Call Center y para personal implicado directamente en la operación y administración de la plataforma de certificación de ACCV. Asimismo, colaborará con el Administrador de PRU en la preparación de la formación a Operadores de PRU.

El Responsable de formación, soporte y comunicación será el responsable de la preparación de los contenidos de los cursos impartidos sobre la plataforma corporativa de e-learning.

Debe revisar mensualmente los ficheros de incidencias y respuestas de Call Center, y revisar los argumentarios de los agentes de Call Center.

Debe coordinar la actuación del personal de microinformática y facilitar las herramientas y material necesario para que desarrollen correctamente su labor.

El Responsable de formación, soporte y comunicación podrá contar con la colaboración de los Operadores de Autoridad de Certificación, para aquellas tareas que estime oportuno.

5.2.1.8. Responsable de Seguridad

Debe cumplir y hacer cumplir las políticas de seguridad de ACCV, y debe encargarse de cualquier aspecto relativo a la seguridad de ACCV: física, de las aplicaciones, de la red, etc.

Será el encargado de gestionar los sistemas de protección perimetral y en concreto de la gestión de las reglas de los firewalls.

Debe encargarse de la instalación, configuración y gestión de los sistemas de detección de intrusiones (IDS) y de las herramientas asociadas a éstos.

Es el responsable de resolver o hacer que se resuelvan las incidencias de seguridad producidas, de eliminar vulnerabilidades detectadas, etc.

Es el responsable de la gestión y control de los sistemas de seguridad física del CPD, de los sistemas de control de acceso, de los sistemas de acondicionamiento ambiental y de alimentación eléctrica.

Debe encargarse de explicar los mecanismos de seguridad al personal que deba conocerlos, de concienciar a todo el personal de ACCV y de hacer cumplir las normas y políticas de seguridad.

Debe establecer los calendarios para la ejecución de análisis de vulnerabilidades, ensayos y pruebas de los planes de continuidad del servicio y auditorías de los sistemas de información.

Debe colaborar con los Auditores en todo aquello que les sea requerido.

5.2.1.9. Auditor

Responde a un perfil de auditor es interno, sin perjuicio del personal responsable de las auditorías externas.

El Auditor debe encargarse de:

- Constatar la existencia de toda la documentación requerida y enumerada
- Comprobar la coherencia de la documentación con los procedimientos, activos inventariados, etc.
- Comprobar el seguimiento de incidencias y eventos
- Comprobar la protección de los sistemas (explotación de vulnerabilidades, logs de acceso, usuarios, etc.).
- Comprobar alarmas y elementos de seguridad física
- Comprobar adecuación a normativa y legislación
- Comprobar conocimiento de los procedimientos por parte del personal implicado

En definitiva, debe comprobar todos los aspectos recogidos en la política de seguridad, políticas de copias, prácticas de certificación, políticas de certificación, etc. tanto en el núcleo de sistemas de ACCV y personal de ACCV, como en los PRUs.

5.2.1.10. Jurista

Se encargará de los aspectos legales de la prestación de servicios de certificación y de la formalización de la prestación de estos servicios a otras entidades, con las que hubiera que establecer convenio de certificación.

Se le encomienda la tramitación de la aprobación y publicación de Políticas de Certificación, las modificaciones del documento de Declaración de Prácticas de Certificación y, en general, de cualquier normativa pública que afecte a la plataforma de certificación y los servicios de la Autoridad de Certificación.

Velará por el cumplimiento de la legislación de firma electrónica vigente en cada momento, analizando las Políticas de Certificación y Declaración de Prácticas de Certificación existentes y las que sean objeto de aprobación, e informando de las incoherencias o de los problemas que detectara.

Debe colaborar con los Auditores en todo aquello que les sea requerido.

5.2.1.11. Responsable de Documentación

Se encargará de mantener el repositorio de documentación electrónica de ACCV y los archivos de documentación en papel.

Controlará que se lleven a cabo la actualización de documentos cuando se requiera y por parte de quien el Responsable de Documentación designe, incluso superando lo especificado en los documentos a actualizar o mantener.

Se encargará de mantener actualizado el fichero de índice de documentos y estará habilitado para almacenar, borrar o modificar documentos en el repositorio de documentación de ACCV.

Podrá contar con la colaboración de los Operadores de Autoridad de Certificación para llevar a cabo tareas de control o inventario documental.

Deberá garantizar que todo certificado emitido tiene asociado un contrato de certificación en papel.

Debe colaborar con los Auditores en todo aquello que les sea requerido.

5.2.1.12. Asistencia al Desarrollo de Aplicaciones y Soporte al Despliegue

Se encargará de mantener el contacto con equipos de desarrollo de aplicaciones informáticas de organismos y entidades usuarios de los servicios de ACCV, a fin de facilitar el soporte y asistencia precisos para el desarrollo y despliegue de aplicaciones y servicios telemáticos, que utilicen la certificación digital y la firma electrónica.

Se encargará de redirigir al personal adecuado las consultas técnicas informáticas o jurídicas que no pueda solventar.

Deberá recabar información suficiente (plantilla de información de proyectos) para estar en situación de proporcionar un nivel óptimo de asistencia y consejo.

Deberá orientar sobre las posibilidades, técnicas y herramientas de desarrollo, teniendo en cuenta los sistemas de información corporativos, política de seguridad, legislación aplicable, etc.

El Responsable de Soporte al Despliegue deberá orientar sobre la normativa técnica y administrativa existente, sobre el deber de creación de PRUs por parte de los organismos y entidades que ofrezcan servicios telemáticos, la manera de funcionar de éstos, etc. Deberá colaborar con las consellerias o entidades con las que se hubiera establecido el convenio de certificación para analizar mecanismos de distribución de certificados, creación de PRUs, etc.

Debe colaborar con los Auditores en todo aquello que les sea requerido.

5.2.1.13. Coordinador de Autoridad de Certificación

Se encargará del seguimiento y control en el desarrollo de las funciones atribuidas a cada perfil de los descritos anteriormente, y de la distribución de nuevas tareas entre los perfiles.

Se encargará de servir de medio de comunicación entre el personal adscrito a cada uno de los perfiles y la dirección de la Autoridad de Certificación. De la misma forma, se encargará de servir de enlace con otros departamentos de la Generalitat Valenciana.

Se encargará de plantear decisiones estratégicas a la dirección de la Autoridad de Certificación y de aprobar decisiones tácticas.

Orientará al personal de ACCV sobre la formación a adquirir, cursos de reciclaje, etc. y facilitará el desarrollo de esos cursos y planes de formación.

Debe colaborar con los Auditores en todo aquello que les sea requerido.

5.2.2. Número de personas requeridas por tarea

Se requieren dos personas para la activación de claves de los dispositivos criptográficos hardware de generación y almacenamiento de claves. La modificación de los parámetros de configuración del hardware criptográfico implica la autenticación por parte de dos personas autorizadas y con privilegios suficientes.

5.2.3. Identificación y autenticación para cada papel

Todos los usuarios autorizados de ACCV se identifican mediante certificados digitales emitidos por la propia ACCV y se autentifican por medio de smart-cards criptograficas y/o dispositivos biométricos.

La autenticación se complementa con las correspondientes autorizaciones para acceder a determinados activos de información o sistemas de ACCV.

5.2.4. Papeles que requieren separación de tareas

Ninguna identidad está autorizada a asumir tanto un rol de Administrador de Sistemas como de Administrador/Responsable de Seguridad;

Ninguna identidad está autorizada a asumir tanto un rol de Administrador de Sistemas como de Auditor;

Ninguna identidad está autorizada a asumir a la vez la función de Administrador/Responsable de Seguridad y la de Auditor;

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

La Agencia de Tecnología y Certificación Electrónica requiere que todo el personal que desarrolla tareas en sus instalaciones tenga la suficiente cualificación y experiencia en entornos de prestación de servicios de certificación.

Todo el personal debe cumplir los requerimientos de seguridad de la organización y deben poseer:

- Conocimientos y formación sobre entornos de certificación digital.
- Formación básica sobre seguridad en sistemas de información.
- Formación específica para su puesto.
- Título académico o experiencia en la industria equivalente

Antes de empezar a desarrollar cualquier tarea o labor para la ACCV se comprobará con registros oficiales su identidad y cuestiones relativas a su confianza.

5.3.2. Procedimientos de comprobación de antecedentes

Mediante comprobación de Curriculum Vitae del personal.

5.3.3. Requerimientos de formación

El personal de la Agencia de Tecnología y Certificación Electrónica está sujeto a un plan de formación específico para el desarrollo de su función dentro de la organización.

Dicho plan de formación incluye los siguientes aspectos:

1. Formación en los aspectos legales básicos relativos a la prestación de servicios de certificación.
2. Formación en seguridad de los sistemas de información.
3. Servicios proporcionados por la Agencia de Tecnología y Certificación Electrónica.
4. Conceptos básicos sobre PKI.
5. Declaración de Prácticas de Certificación y las Políticas de Certificación pertinentes.
6. Gestión de incidencias.

ACCV mantiene registros de dicha formación y se asegura de que el personal al que se encomiendan tareas de Especialista en Validación mantiene un nivel de conocimientos que le permite realizar dichas tareas satisfactoriamente.

ACCV documenta que cada Especialista en Validación posee las habilidades requeridas por una tarea antes de permitir que realice dicha tarea.

ACCV exige que todos los Especialistas en Validación superen un examen proporcionado por la CA sobre los requisitos de verificación de la información descritos en los “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”.

5.3.4. Requerimientos y frecuencia de actualización de la formación

Ante cambios tecnológicos del entorno, introducción de nuevas herramientas o modificación de procedimientos operativos, se llevará a cabo la formación adecuada para el personal afectado.

Ante cambios en la Declaración de Prácticas de Certificación, Políticas de Certificación u otros documentos relevantes, se llevarán a cabo sesiones formativas.

5.3.5. Frecuencia y secuencia de rotación de tareas

No se ha definido ningún plan de rotación en la asignación de sus tareas para el personal de la Agencia de Tecnología y Certificación Electrónica.

5.3.6. Sanciones por acciones no autorizadas

En el caso de comisión de una acción no autorizada con respecto a la operación de la Autoridad de Certificación se tomarán medidas disciplinarias. Se considerarán acciones no autorizadas las que contravengan la Declaración de Prácticas de Certificación o las Políticas de Certificación pertinentes tanto de forma negligente como malintencionada.

Si se produce alguna infracción, ACCV suspenderá el acceso de las personas involucradas a todos los sistemas de información de ACCV de forma inmediata al conocimiento del hecho.

Adicionalmente, en función de la gravedad de las infracciones, se aplicarán las sanciones previstas en la Ley de la Función Pública, convenio colectivo de la empresa, o el Estatuto de los Trabajadores según corresponda a la situación laboral del infractor.

5.3.7. Requisitos de contratación de terceros

El personal externo que interviene en la emisión de certificados recibe la formación técnica y jurídica necesaria para realizar sus tareas con la debida diligencia (al menos la formación detallada en el apartado Requerimientos de formación).

Todo el personal está sujeto a una obligación de secreto en virtud de la firma del acuerdo de confidencialidad al comenzar a trabajar para ACCV. En este acuerdo, también se comprometen a desempeñar sus funciones de acuerdo con esta Declaración de Prácticas de Certificación, la Política de Seguridad de la Información de ACCV y los procedimientos aprobados de ACCV.

5.3.8. Documentación proporcionada al personal

Al personal que se incorpora a ACCV se le proporciona acceso a la siguiente documentación:

- Declaración de Prácticas de Certificación
- Políticas de certificación
- Política de privacidad
- Política de Seguridad de la Información
- Organigrama y funciones del personal

Se facilitará acceso a la documentación relativa a normas y planes de seguridad, procedimientos de emergencia y toda aquella documentación técnica necesaria para llevar a cabo sus funciones.

5.3.9. Controles periódicos de cumplimiento

El control de que el personal posee los conocimientos necesarios se lleva a cabo al finalizar las sesiones formativas y discrecionalmente, por parte del profesorado encargado de impartir estos cursos y, en última instancia, por parte del responsable de formación, soporte y comunicación.

El control de la existencia de la documentación que los empleados deben conocer y firmar, se lleva a cabo anualmente por parte del Responsable de Documentación.

Anualmente, el Responsable de Seguridad llevará a cabo una revisión de la adecuación de las autorizaciones otorgadas a los efectivos privilegios concedidos a los empleados.

5.3.10. Finalización de los contratos

En caso de finalización de la relación laboral del personal que desarrolla sus funciones en ACCV, el Responsable de Seguridad procederá a llevar a cabo las acciones o comprobaciones que se detallan en los puntos siguientes, bien directamente o dando instrucciones para ello al personal adecuado.

5.3.10.1. Acceso a ubicaciones de la organización

Se deberá suprimir los privilegios de acceso del individuo a las instalaciones de la organización cuyo acceso sea restringido. Esto supone, al menos, la eliminación de la autorización de acceso a las siguientes ubicaciones

- Supresión privilegio acceso al CPD principal
- Supresión privilegio acceso al CPD secundario
- Supresión privilegio acceso a salas de informática e instalaciones y dependencias de Polígono Ademuz S/N en Burjassot (Valencia).

5.3.10.2. Acceso a los Sistemas de Información

Se deberán suprimir los privilegios de acceso del individuo a los Sistemas de Información de la organización, con especial atención a los privilegios de administración y a los de acceso remoto.

- Supresión de usuario en servidores
- Supresión de usuario en Repositorio Documental de ACCV (RD-ACCV)
- Supresión de usuario en Sistema de Control de Incidencias
- Cambio contraseñas conocidas
  - Root / Administrador servidores
  - FW
  - Electrónica de red (switches, balanceadores, routers,…)
  - IDS

5.3.10.3. Acceso a la documentación

Supresión de acceso a toda información, a excepción de la considerada PÚBLICA.

Eliminación del acceso a la Zona Segura de Desarrolladores en la web de ACCV.

5.3.10.4. Información al resto de la organización

Se deberá informar al resto de la organización claramente de la marcha de individuo y de su pérdida de privilegios. De este modo se pretende minimizar la posibilidad de ataques de “ingeniería social” por parte del mismo

5.3.10.5. Información a proveedores y entidades colaboradoras

Así mismo se deberá de informar a los proveedores y entidades colaboradoras de ACCV de la marcha de individuo y de que ya no representa a ACCV.

5.3.10.6. Devolución de material

Se deberá verificar la devolución del material proporcionado por ACCV. Por ejemplo:

- PC y monitor / portátil
- Llaves mobiliario oficinas
- Teléfono móvil
- etc

5.3.10.7. Suspensión como Operador de PRU

Se deberá revisar la necesidad del colaborador de mantener su capacidad de operar como Operador de PRU tras abandonar la organización. Si no existiera esta necesidad se deberán revocar su permiso de acceso al sistema ARCA

5.4. Procedimientos de Control de Seguridad

5.4.1. Tipos de eventos registrados

ACCV registra todos los eventos relacionados con:

- Intentos exitosos o fracasados de cambiar los parámetros de seguridad del sistema operativo.
- Arranque y parada de aplicaciones.
- Intentos exitosos o fracasados de inicio y fin de sesión.
- Intentos exitosos o fracasados de crear, modificar o borrar cuentas del sistema.
- Intentos exitosos o fracasados de crear, modificar o borrar usuarios del sistema autorizados.
- Intentos exitosos o fracasados de solicitar, generar, firmar, emitir o revocar claves y certificados.
- Intentos exitosos o fracasados de generar, firmar o emitir una CRL.
- Intentos exitosos o fracasados de crear, modificar o borrar información de los titulares de certificados.
- Intentos exitosos o fracasados de acceso a las instalaciones por parte de personal autorizado o no.
- Backup, archivo y restauración.
- Cambios en la configuración del sistema.
- Actualizaciones de software y hardware.
- Mantenimiento del sistema.
- Cambios de personal
- Intentos de inicio de sesión exitosos y fallidos en enrutadores y firewalls
- Registro de todas las acciones administrativas realizadas en enrutadores y firewalls, incluidos cambios de configuración, actualizaciones de firmware y modificaciones del control de acceso.

- Registro de todos los cambios realizados en las reglas del firewall, incluidas las adiciones, modificaciones y eliminaciones.
- Registro de todos los eventos y errores del sistema, incluidos fallos de hardware, fallos de software y reinicios del sistema.

Todos estos registros se centralizan en varios puntos:

- El sistema de gestión de incidencias (gestión de cambio, seguimiento de certificados no personales, etc...)
- El sistema de log centralizado (centraliza vía syslog los eventos de los sistemas core)
- El registro de Directorio Activo para la LAN de la organización

5.4.2. Frecuencia de procesado de logs

Se establecen dos niveles de auditorías de control de los eventos registros con una frecuencia semanal y mensual respectivamente.

5.4.3. Periodo de retención para los logs de auditoría

ACCV retendrá todos los registros de auditoría relevantes generados por el sistema por un periodo mínimo desde la fecha de su creación de dos (2) años para los pertenecientes a auditorías diarias, cinco (5) años para las mensuales y quince (15) años para los de auditorías anuales

5.4.4. Protección de los logs de auditoría

Se adaptarán medidas para garantizar la disponibilidad y conservación de los logs de auditoria de los sistemas asociados a las CAs y las RAs.

5.4.5. Procedimientos de backup de los logs de auditoría

Se generan copias incrementales locales y remotas diariamente, de acuerdo con la Política de Copias de Seguridad de ACCV.

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

El sistema de recolección de auditorías de los sistemas de información de ACCV es una combinación de procesos automáticos y manuales ejecutados por los sistemas operativos, las aplicaciones de ACCV, y por el personal que las opera.

5.4.7. Notificación al sujeto causa del evento

No está previsto que se notifique al sujeto que da lugar al registro.

5.4.8. Análisis de vulnerabilidades

Se establece la realización de, al menos, un análisis semestral de vulnerabilidades y de seguridad perimetral.

Es responsabilidad de los coordinadores de los equipos de análisis el informar a ACCV, a través del Responsable de Seguridad, de cualquier problema que impida la realización de las auditorias, o la entrega de la documentación resultante. Es responsabilidad de ACCV informar a los equipos auditores de la suspensión de los análisis.

Los análisis de seguridad implican el inicio de las tareas precisas para corregir las vulnerabilidades detectadas y la emisión de un contra-informe por parte de ACCV.

5.5. Archivo de informaciones y registros

5.5.1. Tipo de informaciones y eventos registrados

Las informaciones y eventos registrados son:

- Los registros de auditoría especificados en el punto 5.4 de esta Declaración de Prácticas de Certificación.
- Los soportes de backup de los servidores que componen la infraestructura de ACCV.
- Documentación relativa al ciclo de vida de los certificados, entre la que se encuentra:
    - Contrato de certificación
    - Copia de la documentación de identificación aportada por el solicitante del certificado
    - Ubicación del Punto de Registro de Usuario -PRU- donde se emitió el certificado
    - Identidad del operador del PRU donde se emitió el certificado
    - Fecha de la última identificación cara a cara del suscriptor
- Acuerdos de confidencialidad
- Convenios suscritos por ACCV
- Autorizaciones de acceso a los Sistemas de Información (autorización de operador de Punto de Registro de Usuario, entre otras).

5.5.2. Periodo de retención para el archivo.

Toda la información y documentación relativa al ciclo de vida de los certificados emitidos por ACCV se conserva durante un periodo de 15 años.

5.5.3. Protección del archivo.

El acceso al archivo se encuentra restringido a personal autorizado.

Asimismo los eventos relativos a los certificados emitidos por ACCV se encuentra protegida criptográficamente para garantizar la detección de manipulaciones en su contenido.

5.5.4. Procedimientos de backup del archivo.

Se realizan dos copias diarias de los ficheros que componen los archivos a retener.

Una copia se realiza en local y se almacena en una caja fuerte ignífuga dentro del Centro de Proceso de Datos principal de ACCV.

La segunda copia de los datos se realiza de forma cifrada y remota y se almacena en el Centro de Proceso de Datos de continuidad o respaldo sito en un edificio distinto al del CDP principal de ACCV.

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

Los sistemas de ACCV realizan el registro del instante de tiempo en los que se realizan. El tiempo de los sistemas proviene de una fuente fiable de hora. Todos los sistemas de ACCV sincronizan su instante de tiempo con esta fuente.

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

El sistema de recogida de información es interno a la entidad ACCV.

5.5.7. Procedimientos para obtener y verificar información archivada

Sólo el personal autorizado tiene acceso a los archivos físicos de soportes y archivos informáticos, para llevar a cabo verificaciones de integridad u otras.

De forma automática se realizan comprobaciones de la integridad de los archivos electrónicos (backups), en tiempo de su generación y se crea una incidencia en el caso de errores o comportamientos imprevistos.

5.6. Cambio de Clave

La clave privada de firma de ACCV se cambia periódicamente. ACCV dejará de emitir certificados asociados y procederá a firmar o emitir nuevos certificados de la Autoridad de Certificación correspondiente antes de que finalice el periodo de validez, de acuerdo con lo establecido en el apartado 6.3.2. La clave anterior seguirá firmando y publicando CRLs hasta el final de su vida útil. El cambio de clave o la emisión de un nuevo certificado para la firma de los certificados de suscriptor se realizará de forma que el impacto sobre los suscriptores y las partes de confianza sea mínimo. Todas las entidades afectadas serán notificadas antes de un cambio de clave previsto.

5.7. Plan de recuperación de desastres

5.7.1. Procedimientos de gestión de incidentes y vulnerabilidades

El Plan de Respuesta a Incidentes y el Plan de Recuperación de Catástrofes describen todas las acciones llevadas a cabo y los recursos materiales y humanos para resolver un incidente concreto.
Estos documentos detallan las acciones para:

Notificar a los usuarios, evaluar el incidente, activar las salvaguardas

En este punto si procede se notificara a los distintos actores del ecosistema WebPKI utilizando las herramientas disponibles y de uso comun (Bugzilla, listas de distribucín,etc..) tal y como se haya estipulado en las distintas políticas de reconocimiento.

Recuperar los servicios afectados para ofrecer niveles adecuados

Restablecer las operaciones y procesos regulares a los niveles normales

En caso de indisponibilidad de las instalaciones de la Autoridad de Certificación por un periodo superior a seis horas, se activará el Plan de Respuesta a Incidentes de ACCV y un Plan de Recuperación de Desastres.
El Plan de Recuperación de Desastres garantiza que los servicios identificados como críticos por su requisito de disponibilidad estarán disponibles en el CPD de Continuidad en menos de 12 horas tras la activación del Plan.
ACCV probará, revisará y actualizará anualmente estos procedimientos.

5.7.2. Alteración de los recursos hardware, softwarey/o datos

Si el hardware, el software y/o los recursos de datos son alterados o se sospecha que han sido alterados, se suspenderá el funcionamiento de los servicios de ACCV hasta que se restablezca un entorno seguro con la incorporación de nuevos componentes de eficacia acreditada. Paralelamente, se realizará una auditoría para identificar la causa de la alteración y asegurar la no repetición de la misma.

En el caso de que los certificados emitidos se vean afectados, se notificará a los suscriptores del certificado y se procederá a su recertificación.

Todas estas acciones están incluidas en el plan de respuesta a incidentes.

5.7.3. Procedimiento de actuación ante la vulnerabilidad de la clave privada de una entidad de ACCV

En caso de compromiso de la clave de una entidad, ésta será inmediatamente revocada y se notificará al resto de entidades que forman parte de ACCV sean o no dependientes de la entidad afectada. Se generará y publicará la correspondiente CRL, se suspenderán las operaciones de la entidad y se

iniciará el proceso de generación, certificación y puesta en marcha de una nueva entidad con el mismo nombre que la retirada y con un nuevo par de claves.

En el caso de que la entidad afectada sea una AC, el certificado revocado de la entidad permanecerá accesible en el repositorio de ACCV a efectos de seguir permitiendo la verificación de los certificados emitidos durante el periodo de funcionamiento de la entidad.

Las entidades que componen ACCV y que dependen de la entidad renovada serán informadas del hecho y se les ordenará que soliciten su recertificación debido a que la entidad ha sido renovada.

Los certificados firmados por las entidades dependientes de la entidad comprometida durante el periodo comprendido entre el compromiso de la clave y la revocación del certificado correspondiente, serán a su vez revocados, y sus suscriptores informados y recertificados.

5.7.4. Continuidad de negocio después de un desastre

En caso de producirse una catástrofe natural que afecte a las instalaciones del Centro de Proceso de Datos principal de ACCV y, por tanto, a los servicios que se prestan desde esta ubicación, se activará el Plan de Continuidad del Servicio, garantizando que los servicios identificados como críticos por su exigencia de disponibilidad, estarán disponibles en el CPD de Continuidad en menos de 12 horas desde la activación del Plan, y el resto de servicios esenciales estarán disponibles en plazos razonables y adecuados a su nivel de necesidad y criticidad.

5.8. Cese de una CA

Las causas que pueden producir el cese de la actividad de ACCV son:

- Compromiso de la clave privada de la CA
- Decisión política por parte de la Gerencia de ISTEC SA

En caso de cese de su actividad como Prestador de Servicios de Confianza, ACCV realizará, con una antelación mínima de dos (2) meses, las siguientes acciones:

- Informar debidamente sobre sus intenciones de terminar su actividad a todos los suscriptores de sus certificados, así como a las terceras partes con las que haya firmado un contrato/convenio o que puedan verse afectadas.
- Finalizar cualquier contrato/convenio que permita actuar en su nombre en el procedimiento de emi sión de certificados.
- Con el consentimiento de los suscriptores, transferir a otro Prestador de Servicios de Confianza Cualificado aquellos certificados que sigan siendo válidos en la fecha efectiva de cese de actividad. a otro Prestador de Servicios de Confianza que los asuma. De no aceptarse o no ser posible esta transferencia se extinguirá la vigencia de los certificados revocándolos.
- Comunicar al Ministerio que en ese momento tenga las competencias en la materia el cese de su actividad y el destino que va a dar a los certificados, así como cualquier otra circunstancia relevante relacionada con el cese de actividad.

- Remitir al Ministerio competente en la materia toda la información relativa a los certificados revocados para que éste se haga cargo de su custodia a los efectos pertinentes.

6. Controles de seguridad técnica

6.1. Generación e Instalación del Par de Claves

6.1.1. Generación del par de claves

6.1.1.1. Generación de pares de claves de CA

Siguiendo este procedimiento, la ACCV elaborará y seguirá un Guión de Generación de Claves, hará que un Auditor Cualificado sea testigo del proceso de generación del Par de Claves de la CA y que un Auditor Cualificado emita un informe opinando que la CA siguió su ceremonia de llaves durante su proceso de generación de Claves y Certificados y los controles utilizados para asegurar la integridad y confidencialidad del Par de Claves.

Este procedimiento describe lo siguiente:

- roles que participan en la ceremonia;
- funciones a realizar por cada rol y en qué fases;
- responsabilidades durante y después de la ceremonia; y
- requisitos de las pruebas que se recogerán de la ceremonia.

El procedimiento de emisión, firma y distribución de nuevo Certificado CA, especificando que antes de la caducidad del Certificado se genera uno nuevo, evitando así posibles interrupciones en las operaciones de cualquier entidad que pueda confiar en el Certificado.

Por razones de seguridad y calidad, las Claves que la ACCV necesita para desarrollar sus actividades como Prestador de Servicios de Confianza serán generadas por la propia Entidad dentro de sus propias infraestructuras, en un entorno físicamente seguro y por al menos dos personas autorizadas.

Los pares de claves de todos los componentes internos de ACCV se generan en módulos de hardware de criptografía con certificación FIPS 140-1 Nivel 4. En el caso de los componentes de tipo CA, existe una documentación auditada de la ceremonia de creación, que incluye los pasos seguidos, el personal implicado y la distribución de los mecanismos de activación. Todos estos pasos se llevan a cabo y se registran en presencia de un auditor cualificado y en un entorno seguro.

Los algoritmos clave y las longitudes empleadas se basan en estándares ampliamente reconocidos por el propósito para el que se generan.

Los componentes técnicos necesarios para crear Claves están diseñados para que una Clave solo se genere una vez y para que una Clave Privada no se pueda calcular utilizando su Clave Pública.

6.1.1.2. Generación de pares de claves RA

No estipulado

6.1.1.3. Generación de pares de claves de suscriptores

6.1.1.3.1. Certificados Cualificados de Autenticación de Sitios Web

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.

6.1.1.3.2. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro

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

6.1.1.3.3. Certificados Cualificados de sede electrónica administrativa en soporte software

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.

6.1.1.3.4. Certificados de Autenticación de Servidor

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 subscriptor, por tanto, no procede hacerle entrega de la misma.

6.1.3. Entrega de la clave publica al emisor del certificado

La clave pública a ser certificada es generada por el suscriptor en el dispositivo correspondiente al tipo de certificado 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.

Si se detecta que la clave pública de la solicitud no cumple los requisitos (clave débil, compromiso etc...) será rechazada.

6.1.4. Entrega de la clave pública de la CA a las partes confiantes

Las claves públicas de todas las CA pertenecientes a la jerarquía de confianza de ACCV se pueden descargar del sitio web http://www.accv.es.

6.1.5. Tamaño de las claves

Las claves de la raíz ACCVRAIZ1 y las autoridades de certificación que se encuentran en la misma nueva jerarquía son claves RSA de 4096 bits de longitud.

Las claves de la raíz ACCV ROOT RSA TLS 2024 y las autoridades de certificación que se encuentran en la misma jerarquía son claves RSA de 4096 bits de longitud.

Las claves de la raíz ACCV ROOT ECC TLS 2024 y las autoridades de certificación que se encuentran en la misma jerarquía son claves ECC de 384 bits de longitud.

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

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

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

Las claves para ACCVRAIZ1 y las CA de la misma jerarquía se crean con el algoritmo RSA.

Las claves para ACCV ROOT RSA TLS 2024 y las CA de la misma jerarquía se crean con el algoritmo RSA.

Las claves para ACCV ROOT ECC TLS 2024 y las CA de la misma jerarquía se crean con el algoritmo ECC.

Para los certificados de entidad final se utilizan los parámetros definidos en el documento ETSI TS 119 312 “Electronic Signatures and Infraestructures (ESI); Cryptographic Suites”.

Los parámetros utilizados son los siguientes:

Signature Suite	Hash Function	Padding Method	Signature algorithm
sha256-with-rsa	sha256	emsa-pkcs1-v1.5	rsa
sha2-with-ecdsa	SHA-256, SHA-384 or SHA-512		ecdsa

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

6.1.7. Usos admitidos de la clave (campo KeyUsagede X.509v3)

Todos los certificados de suscriptores emitidos por ACCV contienen las extensiones KEY USAGE y EXTENDED KEY

USAGE definidas por la norma X.509 v3 para la definición y limitación de dichos fines.

Las claves privadas correspondientes a los certificados raíz no se utilizan para firmar certificados, salvo en los siguientes casos

Certificados autofirmados para representar a la propia CA Raíz

Certificados para SubCAs, y, si se da el caso, Certificados Cruzados.

Certificados para fines de infraestructura (certificados de función administrativa, certificados de dispositivo operativo de la CA interna)

Certificados para la verificación de la respuesta OCSP

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 certificados, CRL y OCSP"*.

6.1.8. Hardware/software de generación de claves

6.1.8.1. Claves de CA

Las claves para las entidades de la PKI se generan en dispositivos HSM criptográficos con certificación FIPS 140-1 Nivel 4

Los dispositivos utilizados son:

- Thales Nshield 500e F2, con certificación EAL-4+ y FIPS 140-2 Level3
- AEP Keyper Enterprise Model 9720, con certificación FIPS-140-2 Level4
- Thales Luna PCIe HSM A700 con certificación FIPS 140-2 Level3
- Thales Luna Network HSM A790 con certificación FIPS 140-2 Level3

6.1.8.2. Certificados Cualificados de Autenticación de Sitios Web

La generación de las claves se realiza en software por el suscriptor del certificado.

6.1.8.3. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro

La generación de las claves se realiza en HSM.

Los requisitos mínimos para estos dispositivos son los especificados por el Ministerio correspondiente que tenga las competencias, y acorde a la normativa técnica europea.

6.1.8.4. Certificados Cualificados de sede electrónica administrativa en soporte software

La generación de las claves se realiza en software por el suscriptor del certificado.

6.1.8.5. Certificados de Autenticación de Servidor

La generación de las claves se realiza en software por el suscriptor del certificado.

6.2. Protección de la Clave Privada y controles de los módulos criptográficos

La ACCV protegerá su(s) Clave(s) Privada(s) de acuerdo con lo dispuesto en esta DPC y en cumplimiento de los Requisitos Baseline de CA/Browser Forum

6.2.1. Estándares para los módulos criptográficos

6.2.1.1. Claves de CA

Es obligatorio que los módulos utilizados para la creación de claves que utilizan todas las CAs integradas en las jerarquías de confianza cumplan con una certificación de seguridad adecuada a su funcionalidad y a la seguridad que requiere.

Un módulo de seguridad hardware (HSM) es un dispositivo de seguridad que genera y protege claves criptográficas. Por lo tanto, estos productos deben cumplir, como mínimo, con los criterios del nivel 3 de FIPS 140-2, o del EAL 4+ de Common Criteria para el perfil de protección correspondiente. ACCV dispone de procedimientos y políticas para comprobar que un HSM no ha sido manipulado durante su transporte y almacenamiento

Los dispositivos criptográficos con certificados cualificados de firma electrónica, aptos como dispositivos cualificados de creación de firma (DSCF), cumplen los requisitos del nivel de seguridad CC EAL4+, aunque también son aceptables las certificaciones que cumplan un mínimo de criterios de seguridad ITSEC E3, FIPS 140-2 Nivel 2 o equivalente. La norma europea de referencia para los dispositivos utilizados es la Decisión de Ejecución (UE) 2016/650 de la Comisión, de 25 de abril de 2016.

6.2.1.2. Certificados Cualificados de Autenticación de Sitios Web

Los módulos criptográficos se encuentran en software en el equipo del usuario suscriptor.

6.2.1.3. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro

Los dispositivos HSM empleados en la emisión de estos certificados deben disponer de certificación ITSEC E5 high, FIPS 140-2 nivel 3 o equivalente y soportan los estándares PKCS#11 y CSP.

También se aceptan los HSM certificados por la agencia acreditada para ello a nivel nacional (OC-CCN https://oc.ccn.cni.es/index.php/es/).

La generación de claves se realiza en los HSM.

Los requisitos mínimos para estos dispositivos son los especificados por el Organismo correspondiente que tenga las competencias, y según la normativa técnica europea.

Estos HSMs deben tener la acreditación como Dispositivo Seguro de Creación de Firma / Dispositivo Seguro de Creción de Sellos según la normativa eIDAS (QsigCD/QsealCD).

6.2.1.4. Certificados Cualificados de sede electrónica administrativa en soporte software

Los módulos criptográficos se encuentran en software en el equipo del usuario suscriptor.

6.2.1.5. Certificados de Autenticación de Servidor

Los módulos criptográficos se encuentran en software en el equipo del usuario suscriptor.

6.2.2. Control multi-persona de la clave privada

Las claves privadas utilizadas por las autoridades de certificación que componen ambas jerarquías se encuentran bajo control multipersonal. Todas ellas se encuentran divididas en varios fragmentos y es necesario un mínimo de dos de esos fragmentos para poder volver a recomponer la clave.

No es aplicable en el caso de claves privadas de entidad final.

6.2.3. Custodia de la clave privada

No se custodian claves privadas de firma de los suscriptores. Las de encriptación pueden custodiarse de acuerdo con lo dispuesto por la Política de Certificación aplicable.

Las claves privadas de las Autoridades de Certificación y Autoridades de Registro que componen ACCV se encuentran alojadas en dispositivos de hardware criptográfico con certificación FIPS 140-2 de nivel 3.

El resto de claves privadas de entidades componentes de ACCV se encuentran contenidas en smart cards criptográficas en poder de los administradores de cada entidad.

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

6.2.4. Copia de seguridad de la clave privada

No existen copias de seguridad de las claves privadas de las entidades de ACCV, sino que existe un procedimiento de activación de las claves del módulo criptográfico de reserva de la AC (raíz o subordinada) que puede aplicarse en caso de contingencia.

Todas las claves privadas de las entidades de ACCV están bajo el control exclusivo de ACCV.

No se custodian ni se realizan copias de seguridad de las claves privadas de los suscriptores de los certificados definidos por la presente política.

6.2.5. Archivo de la clave privada.

Las copias de seguridad de las claves privadas caducadas de las entidades de ACCV se guardan de forma encriptada en una caja de seguridad a prueba de incendios, a la que sólo puede acceder el personal autorizado con al menos doble acceso.

Todas las claves privadas de las entidades de ACCV están bajo el control exclusivo de ACCV.

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

6.2.6. Introducción de la clave privada en el módulo criptográfico

6.2.6.1. Claves de CA

Las claves privadas de las entidades de ACCV se crean en el módulo criptográfico en el momento de la creación de cada una de las entidades de ACCV que hacen uso de dichos módulos, cumpliendo los requerimientos definidos en la sección 6.2.1

6.2.6.2. Certificados Cualificados de Autenticación de Sitios Web

No aplicable en el ámbito de la presente Política.

6.2.6.3. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro

La generación de las claves vinculadas al certificado se realiza en el HSM y nunca la abandonan.

6.2.6.4. Certificados Cualificados de sede electrónica administrativa en soporte software

No aplicable en el ámbito de la presente Política.

6.2.6.5. Certificados de Autenticación de Servidor

No aplicable en el ámbito de la presente Política.

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

6.2.7.1. Claves de CA

Las claves privadas se crean en el módulo criptográfico en el momento de la creación de cada una de las entidades de ACCV que hacen uso de dichos módulos, cumpliendo los requerimientos definidos en la sección 6.2.1

6.2.7.2. Certificados Cualificados de Autenticación de Sitios Web

No aplicable en el ámbito de la presente Política.

6.2.7.3. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro

La clave privada es generada por el solicitante y nunca está en posesión de la Agencia de Tecnología y Certificación Electrónica. El almacenamiento de la clave privada dependerá de los mecanismos del HSM elegido para generar y almacenar las claves.

6.2.7.4. Certificados Cualificados de sede electrónica administrativa en soporte software

No aplicable en el ámbito de la presente Política.

6.2.7.5. Certificados de Autenticación de Servidor

No aplicable en el ámbito de la presente Política.

6.2.8. Método de activación de la clave privada.

6.2.8.1. Claves de CA

Las claves privadas de las autoridades de certificación que componen ambas jerarquías se activan mediante la inicialización del software de CA y la activación del hardware criptográfico que contiene las claves.

6.2.8.2. Certificados Cualificados de Autenticación de Sitios Web

La clave privada es generada por el solicitante y nunca está en posesión de la ACCV.

6.2.8.3. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro

La clave privada es generada por el solicitante y nunca está en posesión de la Agencia de Tecnología y Certificación Electrónica. La activación dependerá de los mecanismos del HSM elegido para generar y almacenar las claves.

6.2.8.4. Certificados Cualificados de sede electrónica administrativa en soporte software

La clave privada es generada por el solicitante y nunca está en posesión de la ACCV.

6.2.8.5. Certificados de Autenticación de Servidor

La clave privada es generada por el solicitante y nunca está en posesión de la ACCV.

6.2.9. Método de desactivación de la clave privada

6.2.9.1. Claves de CA

Un Administrador puede proceder a la desactivación de la clave de las Autoridades de Certificación de ACCV mediante la detención del software de CA.

6.2.9.2. Certificados Cualificados de Autenticación de Sitios Web

La clave privada es generada por el solicitante y nunca está en posesión de la ACCV.

6.2.9.3. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro

La clave privada es generada por el solicitante y nunca está en posesión de la Agencia de Tecnología y Certificación Electrónica. La desactivación dependerá de los mecanismos del HSM elegido para generar y almacenar las claves.

6.2.9.4. Certificados Cualificados de sede electrónica administrativa en soporte software

La clave privada es generada por el solicitante y nunca está en posesión de la ACCV.

6.2.9.5. Certificados de Autenticación de Servidor

La clave privada es generada por el solicitante y nunca está en posesión de la ACCV.

6.2.10. Método de destrucción de la clave privada

La destrucción de un token puede realizarse por los siguientes motivos:

- Cese del uso de las claves contenidas

- Deterioro tal que no permita un uso eficiente del token, pero no evite totalmente su uso.
- Recuperación de un Token perdido o sustraído.

La destrucción siempre debe ser precedida por una revocación del certificado asociado al token, si éste estuviese todavía vigente.

6.2.10.1. Hardware criptográfico

No se contempla la destrucción de HSM, debido a su alto coste. En su lugar se procederá a las tareas de Inicialización del mismo. Durante el paso del estado "operacional" al de "inicialización" se produce el borrado seguro de las claves en él contenidas.

6.2.10.2. Tarjetas criptográficas

La destrucción del Token puede realizarse cuando la información impresa en la misma pierda validez y deba emitirse una nueva tarjeta.

La tarea a realizar consiste en una **Destrucción Segura** del Token a nivel físico.

6.2.10.3. Certificados Cualificados de Autenticación de Sitios Web

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

6.2.10.4. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro

La clave privada es generada por el solicitante y nunca está en posesión de la Agencia de Tecnología y Certificación Electrónica. La destrucción dependerá de los mecanismos del HSM elegido para generar y almacenar las claves.

6.2.10.5. Certificados Cualificados de sede electrónica administrativa en soporte software

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

6.2.10.6. Certificados de Autenticación de Servidor

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

6.2.11. Clasificación de los módulos criptográficos

Ver la sección 6.2.1 de este documento.

6.3. Otros Aspectos de la Gestión del par de Claves.

6.3.1. Archivo de la clave pública

ACCV mantiene un archivo de todos los certificados emitidos por un periodo de quince (15) años.

6.3.2. Periodos de operación del certificado y periodos de uso del par de claves

El certificado de la CA raíz ACCVRAIZ1 tiene vigencia hasta el 31/12/2030 y las CAs pertenecientes a su jerarquía tienen una vigencia de 4 años menos que la raíz.

El certificado de la CA raíz ACCV ROOT RSA TLS 2024 tiene vigencia hasta el sábado, 26 de enero de 2049 y las CAs pertenecientes a su jerarquía tienen una vigencia hasta el 23 de febrero de 2039.

El certificado de la CA raíz ACCV ROOT ECC TLS 2024 tiene vigencia hasta el sábado, 26 de enero de 2049 y las CAs pertenecientes a su jerarquía tienen una vigencia hasta el 23 de febrero de 2039

Las Autoridades de Registro y el resto de entidades de ACCV tienen una vigencia máxima de tres (3) años.

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. Esa es la fecha máxima de validez que se admite en la solicitud de los certificados emitidos en virtud de esta política.

El certificado de ACCVCA-120 es válido desde el día 27 de enero de 2015 hasta el 1 de enero de 2027.

El certificado de ACCV RSA1 TLS es válido desde el día 27 de febrero de 2024 hasta el 23 de febrero de 2039.

El certificado de ACCV ECC1 TLS es válido desde el día 27 de febrero de 2024 hasta el 23 de febrero de 2039.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

6.4.1.1. Autoridades de Certificación

Los datos de activación de las Autoridades de Certificación de ACCV se generan y almacenan en dispositivos seguros en posesión de personal autorizado.

6.4.1.2. Certificados Cualificados de Autenticación de Sitios Web

La clave privada es generada por el solicitante y nunca está en posesión de la ACCV.

6.4.1.3. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro

La clave privada es generada por el solicitante y nunca está en posesión de la Agencia de Tecnología y Certificación Electrónica. Los datos de activación dependerán de los mecanismos del HSM elegido para generar y almacenar las claves.

6.4.1.4. Certificados Cualificados de sede electrónica administrativa en soporte software

La clave privada es generada por el solicitante y nunca está en posesión de la ACCV.

6.4.1.5. Certificados de Autenticación de Servidor

La clave privada es generada por el solicitante y nunca está en posesión de la ACCV.

6.4.2. Protección de los datos de activación

Solo el personal autorizado conoce los PINs y contraseñas para acceder a los datos de activación.

6.4.2.1. Autoridades de Certificación

Solo el personal autorizado conoce los PINs y contraseñas para acceder a los datos de activación.

6.4.2.2. Certificados Cualificados de Autenticación de Sitios Web

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

6.4.2.3. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro

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

6.4.2.4. Certificados Cualificados de sede electrónica administrativa en soporte software

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

6.4.2.5. Certificados de Autenticación de Servidor

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

6.4.3. Otros aspectos de los datos de activación

No hay otros aspectos a considerar.

6.5. Controles de Seguridad Informática

6.5.1. Requisitos técnicos específicos de seguridad informática

ACCV implanta un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma **ISO-27001** y establece controles y procedimientos para su correcto cumplimiento.

- Controles operativos
- Procedimientos de usuario documentados
- Procedimientos de borrado seguro de los soportes de almacenamiento y extraíbles, así como de los equipos obsoletos
- Planes de contingencia y continuidad
- Antivirus y antimalware
- Política estricta sobre qué tipos de software pueden instalar los usuarios
- Intercambio de datos de seguridad
- Transmisión con CA y RA
- Transmisión con bases de datos de CA y RA
- Datos del usuario
- Control de acceso
- Autenticación basada en doble factor para los operadores de CA y RA
- Utilización del principio de mínimo privilegio
- Identificaciones de usuario únicas y nominales
- Auditorías periódicas de los privilegios aplicados
- Procedimientos estrictos de aprovisionamiento
- Guías de aplicación de contraseñas y tokens de seguridad

ACCV dispone de una política de seguridad y de procedimientos para garantizar la seguridad.

6.5.2. Evaluación del nivel de seguridad informática

ACCV implanta un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma **ISO-27001** y establece controles y procedimientos para su correcto cumplimiento.

Durante la evaluación continua del SGSI, se realizan análisis de impacto y de riesgo que valoran la seguridad informática.

6.6. Controles Técnicos del Ciclo de Vida.

6.6.1. Controles de desarrollo de sistemas

ACCV implanta un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma **ISO-27001** y establece controles y procedimientos para su correcto cumplimiento.

Existen varios procedimientos y directrices de ACCV asociados al control del desarrollo:

- Política de desarrollo y pruebas
- Directrices de mejores prácticas de desarrollo de ACCV
- Procedimiento de control de cambios
- Gestión de la capacidad
- Plan de Continuidad de Negocio

Todos estos procedimientos tienen su correspondiente soporte documental en el gestor documental de ACCV.

Las características del sistema de desarrollo de ACCV:

- Proceso de integración continua
- Herramientas de análisis y detección de anomalías en el código
- Estricta separación entre la plataforma de desarrollo y pruebas y la plataforma de trabajo
- Los datos de prueba y los reales son independientes.
- Las pruebas y el desarrollo nunca trabajan con datos reales

El proceso de producción se lleva a cabo tras un exhaustivo proceso de aprobación, siguiendo el procedimiento de control de cambios, garantizando siempre el roll-back.

6.6.2. Controles de gestión de la seguridad

ACCV implanta un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma **ISO-27001** y establece controles y procedimientos para su correcto cumplimiento.

Existen varios procedimientos y directrices de ACCV relacionados con el control de la seguridad:

- Funciones y controles de seguridad del personal

- Inventario de activos

- Procedimiento para el uso seguro de dispositivos y soportes

- Plan de continuidad de negocio

- Procedimiento de control de cambios

- Procedimiento de gestión de incidentes

- Procedimiento de gestión de vulnerabilidades

Todos estos procedimientos tienen su correspondiente soporte documental en el gestor documental de ACCV.

Los suscriptores del certificado pueden ponerse en contacto con ACCV para comunicar cualquier incidencia utilizando los canales especificados en:

https://www.accv.es/contacto/

y lo indicado en el punto 1.5.2.

ACCV mantiene un registro detallado de todas las incidencias, así como de las soluciones implementadas en su resolución, tal y como se especifica en el SGSI.

6.6.3. Controles de seguridad del ciclo de vida

ACCV realiza periódicamente pruebas de seguridad y vulnerabilidad en las diferentes fases del ciclo de vida del software (SDL).

- Modelado de amenazas para evitar errores en la fase de diseño

- Herramientas de revisión automática de código para detectar errores, vulnerabilidades y defectos de código (Sonarqube)

- Escaneo de vulnerabilidades y pruebas de penetración.

6.7. Controles de Seguridad de la Red

ACCV protege el acceso físico a los dispositivos de gestión de la red y cuenta con una arquitectura que distribuye el tráfico en función de sus características de seguridad, creando secciones de red claramente definidas. Estas secciones están divididas por una zonificación de varios niveles, utilizando múltiples cortafuegos redundantes. La información confidencial que se transfiere a través de redes inseguras se encripta mediante protocolos SSL.

6.8. Sello de Tiempo

ACCV dispone de una Autoridad de Sellado de Tiempo (TSA) cualificada.

Las normas y procedimientos que regulan la TSA pueden encontrarse en su respectiva política en https://www.accv.es/quienes-somos/practicas-y-politicas-de-certificacion/politicas-de-certificacion/.

La URL de acceso anónimo está en:

http://tss.accv.es:8318/tsa

7. Perfiles de Certificados, CRL y OCSP

7.1. Perfil de Certificado

ACCV genera números de serie con 127 bits de entropía. La aplicación principal fuerza este comportamiento. Implementa un generador de números de serie singleton usando SecureRandom. Este generador genera números de serie aleatorios de 16 octecs (128 bits).

7.1.1. Número de versión

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

X.509 es un estándar desarrollado por la Unión Internacional de Telecomunicaciones (organización internacional de las Naciones Unidas para coordinación de servicios de redes de telecomunicaciones entre Gobiernos y empresas) para las Infraestructuras de Clave Pública y los Certificados digitales.

7.1.2. Extensiones del certificado; aplicación de la RFC 5280

Las extensiones de certificado, su criticidad y los identificadores de objeto de algoritmo criptográfico se aprovisionan de acuerdo con los estándares IETF RFC 5280 y cumplen con los CAB Forum Baseline Requirements.

7.1.2.1. Root CA

Las extensiones utilizadas de forma genérica en los certificados de Root CA son:

- Key Usage. Marcado como crítico en todos los casos
  - KeyCertSign CRLSign
- Basic Constraint
  - Presente y marcado como crítico
  - Campo CA TRUE
- Políticas de certificación
  - ACCVRAIZ1: Presente y marcado como no crítico
  - ACCV ROOT RSA TLS 2024: No presente
  - ACCV ROOT ECC TLS 2024: No presente
- Nombre alternativo del sujeto.
  - ACCVRAIZ1: Presente y marcado como no crítico
  - ACCV ROOT RSA TLS 2024: No presente
  - ACCV ROOT ECC TLS 2024: No presente
- Punto de distribución de CRL.
  - ACCVRAIZ1: Presente y marcado como no crítico
  - ACCV ROOT RSA TLS 2024: No presente
  - ACCV ROOT ECC TLS 2024: No presente
- extKeyUsage
  - No están presentes
- authorityInformationAccess
  - ACCVRAIZ1: Presente y marcado como no crítico
  - ACCV ROOT RSA TLS 2024: No presente

- ACCV ROOT ECC TLS 2024: No presente
- nameConstraints
  - No está presente

7.1.2.2. CA Subordinada

Las extensiones utilizadas de forma genérica en los certificados de SubCA son:

- Key Usage. Marcado como crítico en todos los casos
  - KeyCertSign CRLSign
- Basic Constraint
  - Presente y marcado como crítico
  - Campo CA TRUE
- Políticas de certificación
  - Presente y marcado como no crítico
- Nombre alternativo del sujeto.
  - ACCVCA-110: Presente y marcado como no crítico
  - ACCVCA-120: Presente y marcado como no crítico
  - ACCVCA-130: Presente y marcado como no crítico
  - ACCV RSA1 TLS: No presente
  - ACCV ECC1 TLS: No presente
- Punto de distribución de CRL.
  - ACCVCA-110: Presente y marcado como no crítico
  - ACCVCA-120: Presente y marcado como no crítico
  - ACCVCA-130: Presente y marcado como no crítico
  - ACCV RSA1 TLS: Presente y marcado como no crítico
  - ACCV ECC1 TLS: Presente y marcado como no crítico
- extKeyUsage
  - ACCVCA-110: No están presentes
  - ACCVCA-120: No están presentes
  - ACCVCA-130: No están presentes
  - ACCV RSA1 TLS: Client autentication, Server autentication
  - ACCV ECC1 TLS: Client autentication, Server autentication
- authorityInformationAccess
  - Presente y marcado como no crítico
- nameConstraints
  - No está presente

7.1.2.3. Certificados de suscriptor

7.1.2.3.1. Certificados Cualificados de Autenticación de Sitios Web

Campo	Valor
Subject	
SerialNumber	NIF de la Administración, organismo o entidad de derecho público o privado suscriptora del certificado, a la que se encuentra vinculado el sitio web.
CommonName	Denominación de nombre de dominio (DNS) donde residirá el certificado. Si aparece debe coincidir con un DNSName del SAN. (OPCIONAL no recomendado)
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
Organization	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado y propietaria del dominio.
Locality	Ciudad
State	Provincia
Country	ES (code ISO 3166-1)
Version	V3
SerialNumber	Identificador único del certificado. Menor de 32 caracteres hexadecimales.
Algoritmo de firma	ACCVCA-120 sha256withRSAEncryption ACCV RSA1 TLS sha256withRSAEncryption ACCV ECC1 TLS ecdsa-with-SHA384
Issuer (Emisor)	DN de la CA que emite el certificado (ver punto 7.1.4)
Válido desde	Fecha de Emisión
Válido hasta	Fecha de Caducidad
Clave Pública	Octet String conteniendo la clave pública del certificado
Extended Key Usage	Server Authentication Client Authentication
CRL Distribution Point	ACCVCA-120: http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crl ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crl
SubjectAlternativeName	
	dnsName: Nombre Dominio DNS 1 (si se incluye commonName debe tener el mismo valor)
Opcional	dnsName: Nombre Dominio DNS 2
Opcional	dnsName: Nombre Dominio DNS 3
Opcional	dnsName: Nombre Dominio DNS 4
Opcional	dnsName: Nombre Dominio DNS 5
Opcional	dnsName: Nombre Dominio DNS 6
Certificate Policy Extensions	
Policy OID	{itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp(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	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) qncp-web (5)
Policy OID	1.3.6.1.4.1.8149.3.3.5.0
Policy CPS Location	http://www.accv.es/CERT-CUALIFICADO-WEB_ACCV-ISTEC_CIF-A40573396_SPAIN
Authority Information Access	
Access Method	Id-ad-ocsp
Access Location	http://ocsp.accv.es
Access Method	Id-ad-calssuers
Access Location	ACCVCA-120: http://www.accv.es/gestcert/ACCVCA120SHA2.cacert.crt ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crt ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crt
Fingerprint issuer	Fingerprint del certificado de la CA que emite el certificado (ver CPS)
Algoritmo de hash	RSA: SHA-256 ECC: SHA-384
KeyUsage (críticos)	RSA: Digital Signature, Key Encipherment ECC: Digital Signature
SCT List 1.3.6.1.4.1.11129.2.4.2	Signed Certificate Timestamp List Respuestas SCT de Logs cualificados. Al menos tres respuestas diferentes.
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-V1.1-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 carácter Identificador del esquema de registro (VAT)*
	registrationCountry *2 carácter ISO 3166 código de país (ES)*
	registrationStateOrProvince *Provincia (opcional)*
	registrationReference Referencia de registro asignada de acuerdo con el esquema de registro identificado (CIF)

7.1.2.3.2. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro

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. Si aparece debe coincidir con un DNSName del SAN. (OPCIONAL no recomendado)
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
Organization	Denominación (nombre “oficial”) de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada la sede
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	ACCVCA-120 sha256withRSAEncryption ACCV RSA1 TLS sha256withRSAEncryption ACCV ECC1 TLS ecdsa-with-SHA384
Issuer (Emisor)	DN de la CA que emite el certificado (ver punto 7.1.4)
Válido desde	Fecha de Emisión
Válido hasta	Fecha de Caducidad
Clave Pública	Octet String conteniendo la clave pública del certificado de sede
Extended Key Usage	Server Authentication Client Authentication
CRL Distribution Point	ACCVCA-120: http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crl ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crl
SubjectAlternativeName	
	DnsName: Nombre Dominio DNS de la Sede (si se incluye commonName debe tener el mismo valor)
Opcional	DnsName: Nombre Dominio DNS de la Sede
Opcional	DnsName: Nombre Dominio DNS de la Sede
Opcional	DnsName: Nombre Dominio DNS de la Sede
Opcional	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) ovcp(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	2.16.724.1.3.5.5.1
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) qncp-web (5)
Policy OID	1.3.6.1.4.1.8149.3.14.6.0
Policy CPS Location	http://www.accv.es/CERT-CUALIFICADO-WEB_ACCV-ISTEC_CIF-A40573396_SPAIN
Authority Information Access	
Access Method	Id-ad-ocsp
Access Location	http://ocsp.accv.es
Access Method	Id-ad-calssuers
Access Location	ACCVCA-120: http://www.accv.es/gestcert/ACCVCA120SHA2.cacert.crt ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crt ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crt
Fingerprint issuer	Fingerprint del certificado de la CA que emite el certificado (ver CPS)
Algoritmo de hash	RSA: SHA-256 ECC: SHA-384
KeyUsage (críticos)	RSA: Digital Signature, Key Encipherment ECC: Digital Signature
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-V1.1-EN.pdf *Ubicación de PKI Disclosure Statement*
QcSCD	Dispositivo seguro de creación de firma (SSCD)
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)*

7.1.2.3.3. Certificados Cualificados de sede electrónica administrativa en soporte software

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. Si aparece debe coincidir con un DNSName del SAN. (OPCIONAL no recomendado)
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
Organization	Denominación (nombre “oficial”) de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada la sede
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	ACCVCA-120 sha256withRSAEncryption ACCV RSA1 TLS sha256withRSAEncryption ACCV ECC1 TLS ecdsa-with-SHA384
Issuer (Emisor)	DN de la CA que emite el certificado (ver punto 7.1.4)
Válido desde	Fecha de Emisión
Válido hasta	Fecha de Caducidad
Clave Pública	Octet String conteniendo la clave pública del certificado de sede
Extended Key Usage	
	Server Authentication Client Authentication
CRL Distribution Point	
	ACCVCA-120: http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crl ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crl
SubjectAlternativeName	
	DnsName: Nombre Dominio DNS de la Sede (si se incluye commonName debe tener el mismo valor)
Opcional	DnsName: Nombre Dominio DNS de la Sede

Opcional	DnsName: Nombre Dominio DNS de la Sede
Opcional	DnsName: Nombre Dominio DNS de la Sede
Opcional	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) ovcp(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) qncp-web (5) 0.4.0.194112.1.5
Policy OID	1.3.6.1.4.1.8149.3.15.6.0
Policy CPS Location	http://www.accv.es/CERT-CUALIFICADO-WEB_ACCV-ISTEC_CIF-A40573396_SPAIN
Authority Information Access	
Access Method	Id-ad-ocsp
Access Location	http://ocsp.accv.es
Access Method	Id-ad-calssuers
Access Location	ACCVCA-120: http://www.accv.es/gestcert/ACCVCA120SHA2.cacert.crt ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crt ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crt
Fingerprint issuer	Fingerprint del certificado de la CA que emite el certificado (ver CPS)
Algoritmo de hash	RSA: SHA-256 ECC: SHA-384
KeyUsage (críticos)	
	RSA: Digital Signature, Key Encipherment ECC: Digital Signature
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-V1.1-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)*

7.1.2.3.4. Certificados de Autenticación de Servidor

Campo	**Valor**
Subject	
SerialNumber	NIF de la Administración, organismo o entidad de derecho público o privado suscriptora del certificado, a la que se encuentra vinculado el sitio web.
CommonName	Denominación de nombre de dominio (DNS) donde residirá el certificado. Si aparece debe coincidir con un DNSName del SAN. (OPCIONAL no recomendado)
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
Organization	Denominación (nombre “oficial”) de la Administración, organismo o entidad de derecho público suscriptora del certificado y propietaria del dominio.
Locality	Ciudad
State	Provincia
Country	ES (code ISO 3166-1)
Version	V3
SerialNumber	Identificador único del certificado. Menor de 32 caracteres hexadecimales.
Algoritmo de firma	ACCVCA-120 sha256withRSAEncryption ACCV RSA1 TLS sha256withRSAEncryption ACCV ECC1 TLS ecdsa-with-SHA384
Issuer (Emisor)	DN de la CA que emite el certificado (ver punto 7.1.4)
Válido desde	Fecha de Emisión
Válido hasta	Fecha de Caducidad
Clave Pública	Octet String conteniendo la clave pública del certificado

Extended Key Usage	
	Server Authentication Client Authentication
CRL Distribution Point	ACCVCA-120: http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl
	ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crl
	ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crl
SubjectAlternativeName	
	dnsName: Nombre Dominio DNS (si se incluye commonName debe tener el mismo valor)
Opcional	dnsName: Nombre Dominio DNS 2
Opcional	dnsName: Nombre Dominio DNS 3
Opcional	dnsName: Nombre Dominio DNS 4
Opcional	dnsName: Nombre Dominio DNS 5
Certificate Policy Extensions	
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	1.3.6.1.4.1.8149.3.36.2.0
Policy CPS Location	http://www.accv.es/CERT-CUALIFICADO-WEB_ACCV-ISTEC_CIF-A40573396_SPAIN
Authority Information Access	
Access Method	Id-ad-ocsp
Access Location	http://ocsp.accv.es
Access Method	Id-ad-calssuers
Access Location	ACCVCA-120: http://www.accv.es/gestcert/ACCVCA120SHA2.cacert.crt ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crt ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crt
Fingerprint issuer	Fingerprint del certificado de la CA que emite el certificado (ver CPS)
Algoritmo de hash	RSA: SHA-256 ECC: SHA-384
KeyUsage (críticos)	
	RSA: Digital Signature, Key Encipherment ECC: Digital Signature
SCT List1.3.6.1.4.1.11129.2.4.2	Signed Certificate Timestamp List *Respuestas SCT de Logs cualificados. Al menos tres respuestas diferentes.*
CA/Browser Forum Organization	cabfOrganizationIdentifier (OID: 2.23.140.3.1)

Identifier Field	{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-extensions(3) cabf-organization-identifier(1) }
	registrationSchemeIdentifier *3 carácter Identificador del esquema de registro (VAT)*
	registrationCountry *2 carácter ISO 3166 código de país (ES)*
	registrationStateOrProvince *Provincia (opcional)*
	registrationReference *Referencia de registro asignada de acuerdo con el esquema de registro identificado (CIF)*

En todos los casos se cumplirán las especificaciones y límites establecidos en el RFC-5280.

En el caso de los precertificados (solo aplicable a certificados publicados en los logs de Certificate Transparency) el perfil es estrucuralmente identico al certificado final, con la excepción de una extensión especial marcada como crítica con el OID

1.3.6.1.4.1.11129.2.4.3

Esta extensión asegura que el precertificado no se acepta como un certificado final por parte del cinete tal y como se indica en el RFC 5280. La existencia de un precertificado firmado puede tratarse como evidencia de que el correspondiente certificado tambien existe. La firma representa un compromiso vinculante por parte de la CA de que puede emitir dicho Certificado.

7.1.3. Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

- sha1withRSAEncryption (1.2.840.113549.1.1.5)
- sha256withRSAEncryption (1.2.840.113549.1.1.11)
- sha384WithRSAEncryption(1.2.840.113549.1.1.12)
- sha512withRSAEncryption (1.2.840.113549.1.1.13)
- rsaEncryption (1.2.840.113549.1.1.1)
- ECC P-256 secp256r1 (OID: 1.2.840.10045.3.1.7).
- ECC P-384 secp384r1 (OID: 1.3.132.0.34).
- ECC P-521 secp521r1 (OID: 1.3.132.0.35).
- ecdsa-with-SHA256 (1.2.840.10045.4.3.2)
- ecdsa-with-SHA384 (1.2.840.10045.4.3.3)

A partir del 16 de enero de 2015, ACCV no emite certificados de suscriptor que utilicen el algoritmo SHA-1 con una fecha de caducidad superior al 1 de enero de 2017.

7.1.3.1. SubjectPublicKeyInfo

Los siguientes requisitos se aplican al campo subjectPublicKeyInfo de un certificado o Precertificado. No se permiten otras codificaciones.

7.1.3.1.1. RSA

ACCV indica una clave RSA utilizando el identificador de algoritmo rsaEncryption (OID: 1.2.840.113549.1.1.1). Los parámetros estan presentes, y son un NULL explícito.

El AlgorithmIdentifier para claves RSA es idéntico byte a byte con los siguientes bytes codificados hexadecimalmente: **300d06092a864886f70d0101010500**

7.1.3.1.2. ECDSA

ACCV indica la clave ECDSA utilizando el identificador de algoritmo id-ecPublicKey (OID: 1.2.840.10045.2.1). Para los parámetros se utiliza la codificación namedCurve.

Para claves P-256, el namedCurve DEBE ser secp256r1 (OID: 1.2.840.10045.3.1.7).
Para claves P-384, el namedCurve DEBE ser secp384r1 (OID: 1.3.132.0.34).
Para claves P-521, el namedCurve DEBE ser secp521r1 (OID: 1.3.132.0.35).

Cuando se codifica, el AlgorithmIdentifier para claves ECDSA es idéntico byte a byte con los siguientes bytes codificados hexadecimalmente:

Para claves P-256, **301306072a8648ce3d020106082a8648ce3d030107**.
Para claves P-384, **301006072a8648ce3d020106052b81040022**.
Para llaves P-521, **301006072a8648ce3d020106052b81040023**.

7.1.3.2. Identificador del algoritmo de firma

Todos los objetos firmados por ACCV cumplen estos requisitos sobre el uso del tipo AlgorithmIdentifier o AlgorithmIdentifier-derived en el contexto de las firmas.

En particular, se aplica a todos los objetos y campos siguientes:

- El campo signatureAlgorithm de un certificado o precertificado.
- El campo signatureAlgorithm de un TBSCertificate (por ejemplo, el utilizado por un certificado o precertificado).
- El campo signatureAlgorithm de un CertificateList.
- El campo signature de un TBSCertList
- El campo signatureAlgorithm de un BasicOCSPResponse.

No se permiten otras codificaciones para estos campos.

7.1.3.2.1. RSA

ACCV utiliza uno de los siguientes algoritmos y codificaciones de firma. Cuando esté codificado, el AlgorithmIdentifier DEBERÁ ser idéntico byte a byte con los bytes codificados hexadecimalmente especificados.

RSASSA-PKCS1-v1_5 con SHA-256:

Codificación: **300d06092a864886f70d01010b0500**.

RSASSA-PKCS1-v1_5 con SHA-384:

Codificación: **300d06092a864886f70d01010c0500**.

RSASSA-PKCS1-v1_5 con SHA-512:

Codificación: **300d06092a864886f70d01010d0500**.

RSASSA-PSS con SHA-256, MGF-1 con SHA-256 y una longitud de sal de 32 bytes:

Codificación:

304106092a864886f70d01010a3034a00f300d060960864801650304020 10500a11c301a06092a864886f70d010108300d060960864801650304020 10500a203020120

RSASSA-PSS con SHA-384, MGF-1 con SHA-384 y una longitud de sal de 48 bytes:

Codificación:

304106092a864886f70d01010a3034a00f300d060960864801650304020 20500a11c301a06092a864886f70d010108300d060960864801650304020 20500a203020130

RSASSA-PSS con SHA-512, MGF-1 con SHA-512 y una longitud de sal de 64 bytes:

Codificación:

304106092a864886f70d01010a3034a00f300d060960864801650304020 30500a11c301a06092a864886f70d010108300d060960864801650304020 30500a203020140

7.1.3.2.2. ECDSA

ACCV utiliza el algoritmo de firma y la codificación adecuados en función de la clave de firma utilizada.

Si la clave de firma es P-256, la firma DEBE utilizar ECDSA con SHA-256. Cuando se codifique, el AlgorithmIdentifier DEBERÁ ser idéntico byte a byte con los siguientes bytes codificados hexadecimalmente: **300a06082a8648ce3d040302**.

Si la clave de firma es P-384, la firma DEBE utilizar ECDSA con SHA-384. Cuando se codifica, el AlgorithmIdentifier DEBE ser idéntico byte a byte con los siguientes bytes codificados hexadecimalmente: **300a06082a8648ce3d040303**.

Si la clave de firma es P-521, la firma DEBE utilizar ECDSA con SHA-512. Cuando se codifica, el AlgorithmIdentifier DEBE ser idéntico byte a byte con los siguientes bytes codificados hexadecimalmente: **300a06082a8648ce3d040304**.

7.1.4. Formatos de nombres

Los nombres del sujeto y del emisor para todas las posibles cadenas de certificación son idénticos byte a byte.

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.

En el caso de ACCVRAIZ1 RootCA o SubCAs

Nombre del emisor: cn=ACCVRAIZ1, ou=PKIACCV o=ACCV, c=ES

- Asunto:
  - commonName (obligatorio). Debe coincidir con el nombre de la entidad ACCV
  - OrganizationalUnit (obligatorio) cadena fija "PKIACCV"
  - Organization (obligatorio) cadena fija "ACCV"

- País (obligatorio) Código de país ISO 3166-1

En el caso de ACCV ROOT RSA TLS 2024 RootCA y sus SubCAs

Nombre del emisor: CN=ACCV ROOT RSA TLS 2024, organizationIdentifier=VATES-A40573396, O=ISTEC, L=BURJASSOT, ST=VALENCIA, C=ES

- Asunto:
  - commonName (obligatorio). Debe coincidir con el nombre de la entidad ACCV
  - organizationIdentifier (obligatorio) cadena fija **VATES-A40573396**
  - Organization (obligatorio) cadena fija **ISTEC**
  - Locality (obligatorio): cadena fija **BURJASSOT**
  - State (obligatorio): cadena fija **VALENCIA**
  - País (obligatorio) código de país ISO 3166-1 **ES**

En el caso de ACCV ROOT ECC TLS 2024 RootCA y sus SubCAs

Nombre del emisor: CN=ACCV ROOT ECC TLS 2024, organizationIdentifier=VATES-A40573396, O=ISTEC, L=BURJASSOT, ST=VALENCIA, C=ES

- Asunto:
  - commonName (obligatorio). Debe coincidir con el nombre de la entidad ACCV
  - organizationIdentifier (obligatorio) cadena fija **VATES-A40573396**
  - Organization (obligatorio) cadena fija **ISTEC**
  - Locality (obligatorio): cadena fija **BURJASSOT**
  - State (obligatorio): cadena fija **VALENCIA**
  - País (obligatorio) código de país ISO 3166-1 **ES**

Los Issuer names admitidos para certificados de entidad final emitidos bajo esta DPC son:

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

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

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

Todos los campos del certificado de entidad final 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 (SAN) contiene al menos una entrada. Cada entrada en el campo SAN debe ser del tipo dNSName conteniendo el nombre completo cualificado de un sistema.

Subject:

commonName (opcional). Si se incluye debe coincidir con uno de los campos DNSName del SAN

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

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

locality (obligatorio) Ciudad

state (obligatorio) Estado o provincia

country (obligatorio) Código de país ISO 3166-1

7.1.4.1. Codificación de nombres

Reglas aplicadas al codificar un Nombre:

- Cada Nombre contiene una RDNSequence.
- Cada RelativeDistinguishedName contiene exactamente un AttributeTypeAndValue.
- Cada RelativeDistinguishedName, si está presente, se codifica dentro de RDNSequence en el orden en que aparece en la Sección 7.1.2. de la Política de Certificación.
- Cada Nombre no contiene más de una instancia de un AttributeTypeAndValue dado en todos los RelativeDistinguishedNames.

7.1.5. Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a distinguished names (DN) X.500, diferenciables por suscriptor y no ambiguos.

No hay restricciones de nombre definidas en los certificados SubCA.

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

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

ACCV tiene definida una política de asignación de OID's dentro de su arco privado de numeración. El OID de todas la Políticas de Certificación de ACCV comienzan con el prefijo 1.3.6.1.4.1.8149.3

En el caso de la CA raíz y las Cas intermedias la política es *anyPolicy* (2.5.29.32.0)

7.1.6.1. Certificados Cualificados de Autenticación de Sitios Web

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

1.3.6.1.4.1.8149.3.3.5.0

En este caso se añade un OID para identificar el tipo de entidad que se representa según la normativa ETSI EN 319 411-2

0.4.0.194112.1.5	**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 siguiendo las guias del CAB/Forum

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

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

0.4.0.2042.1.7 Organizational Validation Certificate Policy (OVCP)

7.1.6.2. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro

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

1.3.6.1.4.1.8149.3.14.6.0

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.

2.16.724.1.3.5.5.1 Certificado de sede electrónica de nivel alto

En este caso se añade un OID para identificar el tipo de entidad que se representa según la normativa ETSI EN 319 411-2

0.4.0.194112.1.5 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 guiás del CAB/Forum

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

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)

7.1.6.3. Certificados Cualificados de sede electrónica administrativa en soporte software

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

1.3.6.1.4.1.8149.3.15.6.0

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 EN 319 411-2

0.4.0.194112.1.5 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 guiás del CAB/Forum

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

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)**

7.1.6.4. Certificados de Autenticación de Servidor

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

1.3.6.1.4.1.8149.3.36.2.0

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

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

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 "Certificate Policy" puede incluir un campo de Calificación de Políticas (opcional):

- CPS Pointer: contiene la URL donde se publican las Políticas de Certificación

7.1.9. Tratamiento semántico para la extensión critica “Certificate Policy”

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

7.1.10. Signed Certificate Timestamp (SCT) List

Respuestas de registros calificados bien conocidos, que actualmente cumplen con la política de transparencia de certificados de Chrome.

Extension OID: 1.3.6.1.4.1.11129.2.4.2

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

Para los certificados con un valor notBefore mayor o igual al 21 de abril de 2021 (2021-04-21T00:00:00Z), el número de SCT incrustados se basa en la vida útil del certificado:

Certificate lifetime	**# of SCTs from separate logs**	**Maximum # of SCTs per log operator which count towards the SCT requirement**
180 days or less	2	1
181 to 398 days	3	2

Para los certificados con un valor notBefore inferior al 21 de abril de 2021 (2021-04-21T00:00:00Z), el número de SCT incrustados se basa en la vida útil del certificado:

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

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

El número de serie de los certificados revocados permanece en la CRL hasta su caducidad.

7.2.2. CRL y extensiones

Esta Declaración de Prácticas de Certificación soporta y utiliza CRLs que cumplen con el estándar X.509 y soportan los siguientes campos:

Version: Establecido como v2

Signature Algorithm: Identificador del algoritmo utilizado para firmar la CRL

Hash Algorithm: Identificador del algoritmo utilizado para el hash de la CRL

Issuer: El nombre distinguido de la CA emisora

This update: Hora de emisión de la CRL

Next Update: Hora de la próxima actualización de la CRL

CRL Number: Número de CRL secuencial

Issuer Key Identifier: Huella digital del emisor de la CA

Revoked Certificates: Lista de certificados revocados.

reasonCode (OID 2.5.29.21)

Si está presente, esta extensión no se marca como crítica.

Si una entrada de CRL es para un certificado de CA raíz o CA subordinada, esta extensión de entrada de CRL está presente. En los certificados de suscriptor se omite su extensión de entrada CRL cuando el CRLReason indicado no se especifica (0).

La ACCV hará todo lo posible para que la CRLReason indique el motivo más adecuado para la revocación del Certificado.

Sólo las siguientes CRLReason pueden estar presentes en la extensión CRL reasonCode para los certificados de suscriptor:

- Compromiso de clave (RFC 5280 CLR Razón #1): Indica que se sabe o se sospecha que la clave privada del suscriptor se ha visto comprometida.

- Modificación de datos (RFC 5280 CRL Razón #3): Indica que el nombre del sujeto u otra información de identidad del sujeto en el certificado ha cambiado, pero no hay motivo para sospechar que la clave privada del certificado se ha visto comprometida.
- Reemplazo (RFC 5280 CRL Razón #4): Indica que el Certificado se está reemplazando porque: el Suscriptor ha solicitado un nuevo Certificado.
- Cese de operación (RFC 5280 CRL Razón #5): Indica que el sitio web con el Certificado se cierra antes del vencimiento del Certificado, o si el Suscriptor ya no posee o controla el Nombre de dominio en el Certificado antes del vencimiento del Certificado.
- Privilegio retirado (RFC 5280 CRL Razón #9): indica que ha habido una infracción por parte del suscriptor que no ha dado lugar a un Compromiso de clave, como que el Suscriptor del certificado proporcionó información engañosa en su Solicitud de certificado o no ha cumplido con sus obligaciones materiales en virtud del Acuerdo del suscriptor. o Condiciones de uso.

ACCV informará a los Suscriptores sobre las opciones de motivo de revocación enumeradas anteriormente y brinda una explicación sobre cuándo elegir cada opción. Las herramientas que la ACCV pone a disposición del Suscriptor permiten especificar fácilmente estas opciones cuando el Suscriptor solicita la revocación de su Certificado, siendo el valor por defecto que no se indica el motivo de la revocación.

El código de motivo de Privilegio retirado no está disponible para el suscriptor como una opción de motivo de revocación, porque el uso de este código de motivo lo determina la CA y no el suscriptor.

7.3. Perfil OCSP

ACCV también publica información sobre el estado de los certificados mediante el Protocolo de Estado de los Certificados en Línea (OCSP). Este servicio OCSP funciona según el estándar definido en el RFC 6960 y el RFC 5019.

Concretamente se garantiza que si el respondedor de OCSP recibe una solicitud de estado de un certificado que no ha sido emitido, no responderá con un estado "bueno". La respuesta debe ser "revocada", con especificación del motivo de revocación certificateHold (6), y debe especificar el revocationTime 1 de enero de 1970.

Si la respuesta OCSP se basa en una entrada de OCSP el código del motivo de revocación de la respuesta será el mismo que el obtenido de la CRL.

ACCV proporciona su servicio OCSP en http://ocsp.accv.es, de forma continuada 24x7

7.3.1. Número de versión

El servicio OCSP opera acorde al estándar definido en el RFC-6960 y RFC-5019. Los certificados utilizados en el servicio son conformes al estándar X509 versión 3

7.3.2. Extensiones del OCSP

El servicio OCSP proporcionado pr ACCV soporta al menos las siguientes extensiones:

- NONCE (optional)
- Archive Cutoff
- Extended Revoked Definition

Las Extensiones individuales de las respuestas OCSP de la ACCV no contienen la extensión ReasonCode (OID 2.5.29.21) de las entradas CRL.

8. Auditoría de conformidad

ACCV lleva a cabo los controles necesarios para garantizar que

- Emite los certificados y explota los servicios de acuerdo con toda la legislación aplicable a su actividad

- Cumple con los requisitos técnicos establecidos

- Cumple con los requisitos de auditoría establecidos en esta sección

8.1. Frecuencia de los controles de conformidad para cada entidad

Al menos una vez al año se llevará a cabo una auditoría completa de ACCV para garantizar la conformidad de sus procedimientos de funcionamiento y operación con las disposiciones incluidas en esta DPC.

Los certificados capaces de emitir nuevos certificados y todas sus operaciones entran en el ámbito de la auditoría, estas operaciones se dividen en una secuencia ininterrumpida de períodos de auditoría. La duración de un período de auditoría no debe ser superior a un año.

Otras auditorías técnicas y de seguridad se llevarán a cabo de acuerdo con lo estipulado en la Política de Auditoría de ACCV, que incluye una auditoría sobre el cumplimiento de la legislación en materia de protección de datos personales.

Si la ACCV no cuenta con un Informe de Auditoría válido que indique el cumplimiento de uno de los esquemas de auditoría enumerados en la Sección 8.4, entonces, antes de emitir Certificados de Confianza Pública, se completará con éxito una evaluación de preparación en un punto en el tiempo realizada de acuerdo con los estándares aplicables bajo uno de los esquemas de auditoría enumerados en la Sección 8.4. La evaluación de preparación en un punto en el tiempo se completará no antes de los doce (12) meses anteriores a la emisión de los Certificados de Confianza Pública y será seguida por una auditoría completa bajo dicho esquema dentro de los noventa (90) días posteriores a la emisión del primer Certificado de Confianza Pública.

8.2. Identificación/cualificación del auditor

El auditor se seleccionará en el momento de realizar cada auditoría.

La auditoría de la CA será realizada por un Auditor Cualificado. Un Auditor Cualificado significa una persona física, Entidad Legal, o grupo de personas físicas o Entidades Legales que colectivamente poseen las siguientes calificaciones y habilidades:

- Independencia del objeto de la auditoría;
- La capacidad de realizar una auditoría que aborde los criterios especificados en un Esquema de Auditoría Elegible (consulte la Sección 8.4);
- Emplear a personas que tienen competencia en el examen de tecnología de infraestructura de clave pública, herramientas y técnicas de seguridad de la información, tecnología de la información y auditoría de seguridad, y la función de atestación de terceros;
- Para auditorías realizadas de acuerdo con el estándar WebTrust: con licencia de WebTrust;
- Obligado por ley, regulación gubernamental o código de ética profesional; y
- Excepto en el caso de una Agencia de Auditoría Interna Gubernamental, mantener un seguro de Responsabilidad Profesional/Errores y Omisiones con límites de póliza de al menos un millón de dólares estadounidenses en cobertura.

8.3. Relación entre el auditor y la entidad auditada

Al margen de la función de auditoría, el auditor y la parte auditada (ACCV) no deberán tener ninguna relación, actual o planificada, financiera, legal, o de cualquier otra clase que pueda derivar en un conflicto de intereses.

En cumplimiento de lo establecido en la normativa vigente en nuestro ordenamiento sobre protección de datos de carácter personal, y habida cuenta de que para el cumplimiento, por parte del auditor, de los servicios regulados en el contrato será preciso acceder a los datos de carácter personal de los ficheros titularidad de ACCV, el auditor tendrá la consideración de Encargado de Tratamiento, en virtud de lo previsto en el artículo 4.8 del Reglamento (UE) 2016/679, de 27 de abril de 2016.

8.4. Tópicos cubiertos por el control de conformidad

La auditoría determinará la conformidad de los servicios de ACCV con esta DPC y las CP's aplicables. También determinará los riesgos del no cumplimiento de la adecuación con la operativa definida por esos documentos.

Los aspectos cubiertos por una auditoría incluirá, pero no estará limitada a:

- Política de seguridad.
- Seguridad física
- Evaluación tecnológica
- Administración de los servicios de la CA
- Selección de personal
- DPC y CP's vigentes
- Contratos
- Política de privacidad

La ACCV realiza al menos una auditoría anual bajo estos esquemas:

• "WebTrust para CAs v2.1 o más reciente" y "WebTrust para CAs SSL Baseline con Network Security v2.3 o más reciente".

• Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 (eIDAS) y Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024 .

Además de las auditorías necesarias establecidas por la legislación vigente y por las normas técnicas de aplicación para el cumplimiento de sus funciones.

La ACCV incorpora procedimientos periódicos de seguimiento y/o rendición de cuentas para asegurar que sus auditorías continúan realizándose de acuerdo con los requisitos del esquema.

Las auditorías serán realizadas por un Auditor Cualificado, como se especifica en la Sección 8.2.

8.5. Acciones a tomar como resultado de una deficiencia.

La identificación de deficiencias en la auditoría dará lugar a la adopción de medidas correctoras. ACCV, en colaboración con el Auditor, será responsable de determinar estas medidas correctoras.

En caso de deficiencia grave, el ISTEC podrá decidir la suspensión temporal de las operaciones hasta que se subsanen las deficiencias, la revocación del certificado de la entidad, los cambios de personal, etc.

8.6. Comunicación de resultados

El auditor comunicará los resultados de la auditoría al Responsable de Seguridad de la ACCV, y a los responsables de las distintas áreas en las que se detecten no conformidades. El Informe de Auditoría deberá indicar explícitamente que cubre los sistemas y procesos relevantes utilizados en la emisión de todos los Certificados asociados a uno o más de los identificadores de política enumerados en la Sección 7.1.6.1.

El informe de auditoría debe contener al menos la siguiente información claramente etiquetada:

- nombre de la organización auditada;
- nombre y dirección de la organización que realiza la auditoría;
- la huella digital SHA-256 de todos los Certificados de CA Raíces y Subordinadas que están dentro del alcance de la auditoría;
- criterios de auditoría, con número(s) de versión, que se utilizaron para auditar cada uno de los certificados (y claves asociadas);
- una lista de los documentos de política de la CA, con números de versión, a los que se hace referencia durante la auditoría;
- si la auditoría evaluó un período de tiempo o un punto en el tiempo;
- la fecha de inicio y la fecha de finalización del Período de Auditoría, para aquellos que cubren un período de tiempo;
- la fecha del punto en el tiempo, para aquellos que son para un punto en el tiempo;
- la fecha de emisión del informe, que será necesariamente posterior a la fecha de finalización o fecha puntual.

El auditor cualificado debe proporcionar una versión autorizada en inglés de la información de auditoría disponible públicamente y, cuando sea posible, la ACCV mantendrá los informes de auditoría públicos y accesibles, asegurando que no pasen más de tres meses desde el final del período de auditoría anterior.

El informe de auditoría debe estar disponible en formato PDF y debe permitir la búsqueda de texto para toda la información requerida. Cada huella SHA-256 dentro del informe de auditoría debe estar en letras mayúsculas y no debe contener dos puntos, espacios ni saltos de línea.

8.7. Autoevaluación

ACCV vigila constantemente el cumplimiento de los procedimientos y políticas, estableciendo controles periódicos de los indicadores relevantes y realizando autoauditorías (de acuerdo con la Sección 8.7 de los Requisitos básicos de TLS del CABF). En el caso de certificados no personales de sitio web y sede electrónica al menos trimestralmente sobre una muestra seleccionada aleatoriamente del tres por ciento de los Certificados emitidos durante el periodo inmediatamente posterior a la toma de la muestra de autoauditoría anterior. En este análisis trimestral se utilizan herramientas de revisión para verificar la corrección técnica de los certificados emitidos independientemente de las revisiones realizadas en el proceso de emisión.

9. Requisitos comerciales y legales

9.1. Tarifas

9.1.1. Tarifas de emisión de certificado o renovación

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

9.1.2. Tarifas de acceso a los certificados

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

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

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

9.1.4. Tarifas de otros servicios como información de políticas

No se aplicará ninguna tarifa por el servicio de información sobre esta DPC ni las políticas de certificación administradas por ACCV ni por ningún otro servicio adicional del que se tenga conocimiento en el momento de la redacción del presente documento.

Esta disposición podrá ser modificada por la Política de Certificación aplicable en cada caso.

9.1.5. Política de reintegros

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

9.2. Responsabilidades financieras

9.2.1. Seguro de responsabilidad civil

ACCV ofrece una garantía de cobertura suficiente de la responsabilidad civil al ser un organismo público y responsable como tal de los daños y perjuicios, según lo establecido en el artículo 9, apartado 3, subapartado b) de la Ley 6/2020, de 11 de noviembre, por la que se regulan determinados aspectos de los servicios de confianza electrónica, que cubre el riesgo de la responsabilidad por los daños y perjuicios que pudieran ocasionarse por el uso de los certificados emitidos por esta Autoridad de Certificación.

9.2.2. Otros activos

No hay otros activos a considerar.

9.2.3. Seguros y garantías para entidades finales

No hay seguros o coberturas adicionales mas allá de las cubiertas por el seguro de responsabilidad civil definido en la sección 9.2.1.

9.3. Confidencialidad de la información

9.3.1. Alcance de la Información confidencial.

Se declara expresamente como información confidencial, que no podrá ser divulgada a terceros, excepto en aquellos supuestos previstos legalmente:

- Las claves privadas de las entidades que componen ACCV.
- Toda información relativa a las operaciones que lleve a cabo ACCV.
- Toda información relativa a los parámetros de seguridad, control y procedimientos de auditoría.
- Toda la información de carácter personal proporcionada a ACCV durante el proceso de registro de los suscriptores de certificados, con la salvedad de lo especificado por la Política de Certificación aplicable y el contrato de certificación.
- La información de negocio suministrada por sus proveedores y otras personas con las que ACCV tiene el deber de guardar secreto establecida legal o convencionalmente.
- Planes de continuidad de negocio y de emergencia.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Toda la información clasificada como “CONFIDENCIAL” o “ESTRICTAMENTE CONFIDENCIAL”

9.3.2. Información no confidencial

ACCV considera información de acceso público:

- La contenida en la Declaración de Prácticas de Certificación aprobada por ACCV.
- La contenida en las diferentes Políticas de Certificación aprobadas por ACCV.
- Los certificados emitidos así como las informaciones contenidas en éstos.
- La lista de certificados revocados (CRL)
- Toda aquella información que sea calificada como "PÚBLICA".

La DPC y las CP’s de ACCV no incluirán información calificada como confidencial en el punto 9.3.1 del presente documento.

Se permite el acceso a la información no considerada confidencial, sin perjuicio de que se establezcan por ACCV los controles de seguridad pertinentes con el fin de proteger la autenticidad e integridad de los documentos que albergan la información de acceso público e impedir así que personas no autorizadas puedan añadir, modificar o suprimir contenidos.

9.3.3. Responsabilidad para proteger la información confidencial

ACCV es responsable de la protección de la información confidencial generada o comunicada durante todas las operaciones.

En el caso de las entidades finales, los suscriptores del certificado son responsables de proteger su propia clave privada y toda la información de activación necesaria para acceder o utilizar la clave privada.

ACCV tendrá derecho a revelar la información confidencial en la medida en que lo exija la ley. En concreto, los registros que certifican la fiabilidad de la información incluida en el certificado se divulgarán si son requeridos como prueba en un procedimiento judicial. En estos casos, no se requiere el consentimiento del suscriptor del certificado.

La información relativa a la revocación de certificados se proporciona mediante la CRL en el servidor web que actúa como repositorio de ACCV.

Esta información también está disponible en el servidor de validación OCSP de ACCV en ocsp.accv.es:80.

9.4. Protección de datos personales

ACCV dispone de una Política de Privacidad, publicada en la web de la entidad, mediante la que se da cumplimiento a las disposiciones establecidas en la legislación de protección de datos de carácter personal vigente y en la que se informa sobre la política de protección de datos de carácter personal de ACCV.

9.4.1. Plan de Protección de Datos Personales.

En cumplimiento de los requisitos estipulados en cada una de las Políticas de Certificación y de acuerdo con el artículo 5 del Reglamento (UE) 910/2014 (eIDAS), cualquier información de carácter personal facilitada a ACCV por los suscriptores de sus certificados será tratada en los términos del "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales" y de la "Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales".

En este sentido, ACCV figura frente a la Agencia Española de Protección de Datos como responsable del fichero mixto "*Usuarios de Firma Electrónica*" y de su tratamiento. Dicho fichero fue creado y sus atributos modificados mediante las siguientes normas:

- Orden de 8 de marzo de 2002, de la Conselleria de Innovación y Competitividad, por la que se crean ficheros informatizados con datos de carácter personal (vid. DOGV nº 4.221de 4 de abril de 2002 y corrección de errores en el DOGV nº 4.304, de 31 de julio de 2002)
- Orden de 26 de mayo de 2004, de la Conselleria de Infraestructuras y Transporte, por la que se crean, modifican y cancelan ficheros de datos de carácter personal (DOGV 4.772, de 10 de junio de 2004)
- Decreto 149/2007, de 7 de septiembre, del Consell, por el que se aprueba el Estatuto del Ente Prestador de Servicios de Certificación Electrónica de la Comunitat Valenciana. (DOGV 5.596, de 11 de septiembre de 2007)
- Ley 5/2013, de 23 de diciembre, de Medidas Fiscales, de Gestión Administrativa y Financiera, y de Organización de la Generalitat. (DOCV 7.181 de 27 de diciembre de 2013)
- Decreto 15/2014, de 24 de enero, del Consell, por el que se aprueba el Reglamento de Organización y Funcionamiento del Institut Valencià de Finances (IVF). (DOCV 7.202 de 29 de enero de 2014)
- Ley 21/2017, de 28 de diciembre, de Medidas Fiscales, de Gestión Administrativa y Financiera, y de Organización de la Generalitat. (DOCV 8.202 de 30 de diciembre de 2017)
- Ley 27/2018, de 27 de diciembre, de Medidas Fiscales, de Gestión Administrativa y Financiera, y de Organización de la Generalitat. (DOCV 8.453 de 28 de diciembre de 2018)

En este fichero se registran principalmente aquellos datos de carácter identificativo (nombre, apellidos, DNI o equivalente) y de contacto (dirección postal, correo electrónico,) necesarios para la prestación de los servicios de certificación digital que ACCV oferta a personas físicas y jurídicas. Datos considerados legalmente por sus características como de NIVEL BÁSICO.

Adicionalmente, de acuerdo con las obligaciones establecidas por Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), ACCV dispone de un Registro de Actividades público en el que se describen las medidas técnicas y organizativas llevadas a cabo por la propia entidad con la intención de proteger los datos de carácter personal cedidos en la realización de sus funciones.

9.4.2. Información considerada privada.

De conformidad con lo dispuesto en el artículo 4.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, se considerará dato personal toda información relativa a personas físicas identificadas o identificables.

La información personal que no debe incluirse ni en los certificados ni en el sistema de verificación del estado de los certificados se considera información personal de carácter privado.

En cualquier caso, los siguientes datos son considerados como información privada:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados.
- Claves privadas generadas y/o almacenadas por ACCV.
- Toda otra información identificada como “Información privada”

Asimismo, los datos captados por el Prestador de Servicios de Certificación tienen la consideración legal de datos de nivel básico.

De acuerdo con el Reglamento (UE) 2016/679 de 27 de abril de 2016, la información confidencial está protegida contra la pérdida, la destrucción, el daño, la falsificación y el tratamiento ilegal o no autorizado (artículo 5.1.f)

En ningún caso ACCV incluye datos referidos en el artículo 9 del Reglamento (UE) 2016/679 de 27 de abril de 2016, en los certificados digitales emitidos.

9.4.3. Información no considerada privada.

Esta información hace referencia a la información personal que se incluye en los certificados y en el referido mecanismo de comprobación del estado de los certificados, de acuerdo con la sección 3.1 de este documento.

La información no tiene carácter privado, por imperativo legal (“datos públicos”), pero solo se publica en el depósito si lo consiente el suscriptor.

En todo caso, es considerada no confidencial la siguiente información:

a. Los certificados emitidos o en trámite de emisión

b. La sujeción del suscriptor a un certificado emitido por ACCV.

c. El nombre y los apellidos del suscriptor del certificado, así como cualesquiera otras circunstancias o datos personales del titular, en el supuesto que sean significativas en función de la finalidad del certificado, de acuerdo con este documento.

d. La dirección electrónica del suscriptor del certificado.

e. Los usos y límites económicos reseñados en el certificado.

f. El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.

g. El número de serie del certificado.

h. Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.

i. Las listas de revocación de certificados (CRLs), así como el resto de informaciones de estado de revocación.

j. La información contenida en el Depósito de ACCV.

9.4.4. Responsabilidades.

ACCV garantiza el cumplimiento de sus obligaciones legales como prestador de servicios de certificación, de acuerdo con el Reglamento (UE) 910/2014 (eIDAS) y su modificación en el Reglamento (UE) 2024/1183, y en virtud de ello, y de acuerdo con el artículo 24 del citado Reglamento, será responsable de los daños y perjuicios que cause en el desarrollo de su propia actividad, por el incumplimiento de los requisitos contenidos en el artículo 8 de la Ley 6/2020, de 11 de noviembre, relativo a la protección de datos de carácter personal.

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

Para la prestación del servicio, ACCV habrá de obtener el consentimiento de los titulares de los datos necesarios para prestación los servicios de certificación. Se entenderá obtenido el consentimiento con la firma del contrato de certificación y la retirada de los certificados por parte del usuario.

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

ACCV sólo podrá comunicar informaciones calificadas como confidenciales o que contengan datos de carácter personal en aquellos supuestos en los que así se le requiera por la autoridad pública competente y en los supuestos previstos legalmente.

En concreto, ACCV está obligada a revelar la identidad de los firmantes cuando así lo soliciten las autoridades judiciales en el ejercicio de las funciones que tienen atribuidas, y en el resto de los supuestos previstos en el artículo 52 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y Garantía de los Derechos Digitales, en los que se requiera esta comunicación.

9.4.7. Otros supuestos de divulgación de la información.

ACCV incluye, en la política de privacidad prevista al inicio de la sección 9.4, prescripciones para permitir la divulgación de la información del poseedor de claves, directamente a los mismos o a terceros.

9.5. Derechos de propiedad Intelectual

Todos los derechos de propiedad intelectual, incluidos los referentes a los certificados y CRL emitidos por ACCV, los OID y cualquier otro documento que no se mencione explícitamente, ya sea electrónico o de cualquier otro tipo, propiedad de ACCV, pertenecen a ACCV.

Las DPC y las Políticas de Certificación son emitidas por ACCV, y tienen una licencia de Creative Commons Attribuion-NoDerivatives 4.0 (CC BY-ND 4.0).

Las claves privadas y las claves públicas son propiedad del suscriptor, independientemente del soporte físico utilizado para almacenarlas.

El suscriptor conservará cualquier derecho que pueda tener sobre la marca del producto o el nombre comercial registrado en el certificado.

9.6. Obligaciones y Garantías

9.6.1. Obligaciones y garantías de la Autoridad de Certificación

La Agencia de Tecnología y Certificación Electrónica está obligada:

- Realizar sus operaciones en conformidad con esta DPC.
- Proteger sus claves privadas.
- Emitir certificados en conformidad con las Políticas de Certificación que les sean de aplicación.
- Tras la recepción de una solicitud válida de certificado, emitir certificados conformes con el estándar X.509 y con los requerimientos de la solicitud.

- Emitir certificados que sean conformes con la información conocida en el momento de su emisión, y libres de errores de entrada de datos.
- Garantizar la confidencialidad en el proceso de generación de datos de creación de firma y su entrega por un procedimiento seguro al firmante.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte
- Utilizar sistemas fiables para almacenar certificados cualificados que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.
- Garantizar que puede determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia.
- Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica.
- Revocar los certificados en los términos de la sección *Suspensión y Revocación de Certificados* de este documento y publicar los certificados revocados en la CRL del repositorio de ACCV (www.accv.es), con la frecuencia estipulada en el punto *Frecuencia de emisión de CRLs* de este documento.
- Publicar esta DPC y las CP aplicables en el sitio web www.accv.es/DPC, garantizando el acceso a las versiones actuales así como a las versiones anteriores.
- Notificar con prontitud, por correo electrónico, a los suscriptores de certificados en el caso que la CA proceda a la revocación o suspensión del mismo y el motivo que la hubiera producido.
- Colaborar con las auditorias dirigidas por ACCV para validar la renovación de sus propias claves.
- Operar de acuerdo con la legislación aplicable. En concreto con:

.1.1. Decreto 220/2014, de 12 de diciembre, del Gobierno Valenciano, por el que se regula el uso de la firma electrónica avanzada en la Generalitat Valenciana.

.1.2. Ley 6/2020, de 11 de noviembre, por la que se regulan determinados aspectos de los servicios de confianza electrónica.

.1.3. Reglamento (UE) número 910/2014 del Parlamento Europeo y del Consejo, sobre la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y su modificación en el Reglamento (UE) 2024/1183.

.1.4. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

.1.5. Decreto 15/2014, de 24 de enero, del Consell, por el que se aprueba el Reglamento de Organización y Funcionamiento del Institut Valencià de Finances (IVF)

.1.6. Ley 21/2017, de 28 de diciembre de 2017 Generalitat Valenciana, por la que se aprueba la integración en la Generalitat Valenciana de las funciones y competencias en materia de certificación y firma electrónica desarrolladas por el Institut Valencià de Finances (IVF)

.1.7. Ley 27/2018, de 27 de diciembre de 2018 de la Generalitat Valenciana, por la que se aprueba la creación del nuevo organismo, ISTEC

.1.8. Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados

.1.9. Orden ETD/743/2022, de 26 de julio, por la que se modifica la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

.1.10. Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

- Proteger, en caso de haberlas, las claves bajo su custodia.
- Garantizar la disponibilidad de las CRLs de acuerdo con las disposiciones de la sección 4.9.9 *Frecuencia de emisión de CRLs*, de la presente DPC.
- En caso de cesar en su actividad, deberá comunicarlo con una antelación mínima de dos meses al cese efectivo, a los titulares de los certificados emitidos por ACCV, así como al Ministerio competente (a la fecha de redacción de este documento es el Ministerio de Industria, Turismo y Comercio), comunicando el destino que va a dar a los certificados.
- Cumplir las especificaciones contenidas en la normativa sobre Protección de Datos de Carácter Personal
- Conservar registrada toda la información y documentación relativa a un certificado cualificado y las declaraciones de prácticas de certificación vigentes en cada momento durante quince años desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo

Las CA raíz serán responsables del desempeño y las garantías de las CA subordinadas, del cumplimiento de las CA subordinadas con estos Requisitos y de todas las responsabilidades y obligaciones de indemnización de las CA subordinadas en virtud de estos Requisitos, como si las CA raíz fueran las CA subordinadas que emiten los Certificados.

9.6.2. Obligaciones de la Autoridad de Registro

Las personas que operan en las RAs integradas en la jerarquía de ACCV –operadores de Punto de Registro de Usuario– están obligadas a:

- Realizar sus operaciones en conformidad con esta DPC.
- Realizar sus operaciones de acuerdo con la Política de Certificación que sea de aplicación para el tipo de certificado solicitado en cada ocasión.
- Comprobar exhaustivamente la identidad de las personas a las que se les concede el certificado digital por ellos tramitado, para lo que requerirán la presencia del solicitante y la exhibición del DNI original y en vigor, pasaporte español, o documento admitido en derecho. En caso de usuarios extranjeros deberán mostrar el documento que les identifique y deberán estar en posesión de un Numero de Identificación de Extranjero (NIE).
- No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios.
- Informar, antes de la emisión de un certificado, a la persona que solicite sus servicios, de las obligaciones que asume, la forma que debe custodiar los datos de creación de firma, el procedimiento que debe seguir para comunicar la pérdida o utilización indebida de los datos o dispositivos de creación y de verificación de firma, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial, y de la página web donde puede consultar cualquier información de ACCV, la DPC y las CP vigentes y anteriores, la legislación aplicable, las certificaciones obtenidas y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de la actividad.

- Validar y enviar de forma segura a la CA a la que está subordinada la RA una solicitud de certificación debidamente cumplimentada con la información aportada por el subscriptor y firmada digitalmente, y recibir los certificados emitidos de acuerdo con esa solicitud.
- Almacenar de forma segura y hasta el momento de su remisión a la Agencia de Tecnología y Certificación Electrónica, tanto la documentación aportada por el subscriptor como la generada por la propia RA, durante el proceso de registro o revocación
- Formalizar el Contrato de Certificación con el subscriptor según lo establecido por la Política de Certificación aplicable.
- Solicitar la revocación de un certificado cuando tenga conocimiento o sospecha del compromiso de una clave privada.
- Autentificar las solicitudes de usuarios finales para la renovación o revocación de sus certificados, generar solicitudes de renovación o revocación firmadas digitalmente y enviarlas a su CA superior.
- En el caso de la aprobación de una solicitud de certificación notificar al subscriptor la emisión de sus certificados y la forma de obtenerlo.
- En el caso del rechazo de una solicitud de certificación, notificar al solicitante dicho rechazo y el motivo del mismo.
- Mantener bajo su estricto control las herramientas de tramitación de certificados digitales y notificar a la Agencia de Tecnología y Certificación Electrónica cualquier malfuncionamiento u otra eventualidad que pudiera salirse del comportamiento normal esperado.
- Remitir copia firmada del contrato de certificación y de las solicitudes de revocación a Agencia de Tecnología y Certificación Electrónica.
- Recibir y tramitar las solicitudes de revocación que reciba de manera inmediata, después de haber llevado a cabo una identificación fiable.
- Colaborar en cuantos aspectos de la operación, auditoría o control del Punto de Registro de Usuario se le soliciten por parte de la Agencia de Tecnología y Certificación Electrónica.
- A la más general y amplia obligación de confidencialidad, durante y con posterioridad a la prestación del servicio como Autoridad de Registro, respecto de la información recibida por ACCV y respecto de la información y documentación en que se haya concretado el servicio. En el mismo sentido, no transmitir a terceros dicha información, bajo ningún concepto, sin autorización expresa, escrita y con carácter previo de ACCV, en cuyo caso trasladará a dichos terceros idéntica obligación de confidencialidad.

9.6.3. Obligaciones de los suscriptores

Es obligación de los suscriptores de los certificados emitidos bajo la presente política:

- Limitar y adecuar el uso del certificado a propósitos lícitos y acordes con los usos permitidos por la Política de Certificación pertinente y la presente DPC.
- Poner el cuidado y medios necesarios para garantizar la custodia de su clave privada.
- Solicitar inmediatamente la revocación de un certificado en caso de tener conocimiento o sospecha del compromiso de la clave privada correspondiente a la clave pública contenida en el certificado. Los modos en el que puede realizarse esta solicitud se encuentran especificados en este documento en el apartado 4.9.3 *Procedimientos de solicitud de revocación*.
- No utilizar un certificado digital que hubiera perdido su eficacia, por haber sido suspendido, revocado o por haber expirado el periodo de validez del certificado.

- Suministrar a las Autoridades de Registro información que consideren exacta y completa con relación a los datos que éstas les soliciten para realizar el proceso de registro, así como informar a los responsables de ACCV de cualquier modificación de esta información.
- Abonar en su caso los importes que se devenguen por los servicios de certificación que soliciten.
- Los certificados con el uso de clave serverAuthentication están sujetos a lo definido por el CA/Browser Forum en https://cabforum.org/working-groups/server/baseline-requirements/documents/. Entre la condiciones establecidas se encuentra la obligatoriedad de revocar los certificados si se detecta que la emisión u operación no cumple con lo definido en la normativa. Esta revocación se debe hacer en un plazo máximo de cinco (5) días naturales y no es posible aplazamiento de ningún tipo.Si no es posible cumplir esta condición no se deben utilizar nunca certificados emitidos bajo esta normativa.

La ACCV requiere, como parte del Contrato de Suscriptor o Términos de Uso, que el Solicitante asuma los compromisos y garantías de esta sección en beneficio de la CA y los Beneficiarios del Certificado.

Con carácter previo a la emisión de un Certificado, la ACCV obtendrá, en beneficio expreso de la CA y de los Beneficiarios del Certificado, ya sea:

- La aceptación del Solicitante del Acuerdo de Suscriptor con la CA, y
- El reconocimiento por parte del Solicitante de las Condiciones de Uso.

La ACCV implementará un proceso para garantizar que cada Acuerdo de Suscriptor o Términos de Uso sea legalmente exigible contra el Solicitante. En cualquier caso, el Acuerdo debe aplicarse al Certificado que se emitirá conforme a la solicitud de certificado. La ACCV puede utilizar un Acuerdo electrónico o "click-through" siempre que la CA haya determinado que dichos acuerdos son legalmente exigibles. Se utilizará un Acuerdo separado para cada solicitud de certificado.

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

Es obligación de las partes que confíen en los certificados emitidos por ACCV:

- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y la Política de Certificación pertinente.
- Verificar la validez de los certificados en el momento de realizar o verificar cualquier operación basada en los mismos.
- Asumir su responsabilidad en la correcta verificación de las firmas digitales
- Asumir su responsabilidad en la comprobación de la validez, revocación o suspensión de los certificados en que confía.
- Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.
- En el caso de certificados cualificados verificar que el identificador del servicio se encuentra incluido en la versión mas reciente de la ***Trusted Service List*** publicada por el organismo responsable de la Comisión Europea.

9.6.5. Obligaciones de otros participantes

No se consideran garantías ni representaciones para otros participantes.

9.7. Renuncias de garantías

ACCV podrá denegar todas las garantías de servicio que no estén vinculadas a las obligaciones estipuladas por la Ley 6/2020, de 11 de noviembre, por la que se regulan determinados aspectos de los servicios de confianza electrónica, y el Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y a los servicios de confianza para las transacciones electrónicas en el mercado interior, especialmente las garantías de adecuación a una finalidad concreta o las garantías de uso de los certificados con fines comerciales.

9.8. Limitaciones de responsabilidad

ACCV será responsable de los daños y perjuicios que cause a cualquier persona en el ejercicio de su actividad, cuando incumpla las obligaciones impuestas por la Ley 6/2020, de 11 de noviembre, por la que se regulan determinados aspectos de los servicios de confianza electrónica, el Decreto 220/2014, de 12 de diciembre, del Gobierno Valenciano, y el Reglamento (UE) número 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, o actúe de forma negligente.

ACCV responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado emitido por ACCV, una vez tenga conocimiento de ello.

ACCV asume toda la responsabilidad frente a terceros por la actuación de las personas que realicen las funciones necesarias para la prestación del servicio de certificación.

ACCV es la Agencia de Tecnología y Certificación Electrónica, que es una Subdirección de Infraestructures I Serveis De Telecomunicacions I Certificacio SA, Entidad de Derecho Público. La responsabilidad de la Administración se asienta sobre bases objetivas y cubre toda lesión que los particulares sufran siempre que sea consecuencia del funcionamiento normal o anormal de los servicios públicos.

ACCV sólo responderá de los daños y perjuicios causados por el uso indebido del certificado cualificado, cuando no haya consignado en él, de forma claramente reconocible por terceros, el limite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo, No responderá cuando el firmante supere los límites que figuran en el certificado en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizase con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por ACCV Tampoco responderá ACCV si el destinatario de los documentos firmados electrónicamente no comprueba y tiene en cuenta las restricciones que figuran en el certificado en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.

Las Entidades de Registro de ACCV no asumen ninguna responsabilidad en caso de pérdida o perjuicio:

- De los servicios que prestan, en caso de guerra, desastres naturales o cualquier otro caso de fuerza mayor.
- Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos, la Política de Certificación pertinente y esta DPC.
- Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por ACCV.
- Ocasionados al firmante o terceros de buena fe si el destinatario de los documentos firmados electrónicamente no comprueba ni tiene en cuenta las restricciones que figuren en el certificado en cuanto a sus posibles usos, o cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado publicada en la CRL, o cuando no verifique la firma electrónica

A excepción de lo establecido por las disposiciones de la presente DPC, ACCV no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asumen ninguna otra responsabilidad ante suscriptores o partes confiantes.

9.9. Indemnizaciones

ACCV es una entidad gubernamental, por lo que no es aplicable.

No hay seguros o coberturas adicionales mas allá de las cubiertas por el seguro de responsabilidad civil definido en la sección 9.2.1.

9.10. Plazo y finalización.

9.10.1. Plazo.

ACCV establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, una cláusula que determina el período de vigencia de la relación jurídica en virtud de la que suministran certificados a los suscriptores.

La DPC, las PDS y las distintas CP entran en vigor en el momento de su publicación.

9.10.2. Finalización.

ACCV establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, una cláusula que determina las consecuencias de la finalización de la relación jurídica en virtud de la que suministran certificados a los suscriptores.

La presente DPC, las PDS y las distintas DPC serán derogadas en el momento que una nueva versión del documento sea publicada. La nueva versión sustituirá íntegramente el documento anterior.

9.10.3. Supervivencia.

ACCV establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, cláusulas de supervivencia, en virtud de la que ciertas reglas continúan vigentes después de la finalización de la relación jurídica reguladora del servicio entre las partes.

Para los certificados vigentes emitidos bajo una Declaración de Prácticas y Políticas de Certificación anterior, la nueva versión prevalecerá a la anterior en todo lo que no se oponga a ésta.

9.11. Notificaciones individuales y comunicación con los participantes

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las practicas descritas en esta DPC se realizará mediante documento o mensaje electrónico de conformidad con esta última o por escrito mediante correo certificado dirigido a cualquiera de las direcciones contenidas en el punto *1.5* de este documento. Las comunicaciones electrónicas se harán efectivas una vez que las reciba el destinatario al que van dirigidas.

9.12. Modificaciones

ACCV puede modificar unilateralmente este documento, sujetándose al siguiente procedimiento:

- La modificación tiene que estar justificada desde el punto de vista técnico y legal.
- La modificación propuesta por ACCV no puede vulnerar las disposiciones contenidas en las políticas de certificación establecidas por ACCV.
- Se establece un control de modificaciones, basado en la Política de Gestión del Cambio de ACCV.
- Se establecen las implicaciones que el cambio de especificaciones tiene sobre el usuario, y se prevé la necesidad de notificarle dichas modificaciones.

9.12.1. Procedimiento para las modificaciones

La entidad con atribuciones para realizar y aprobar cambios sobre la DPC y las CP's de ACCV es Subdirección de Certificación Electrónica de ISTEC, cuyos datos de contacto se encuentran en el apartado 1.5.1. de esta DPC.

En aquellos supuestos en los que se considere por la Subdirección de Certificación Electrónica que la modificación de la DPC no reduce materialmente la confianza que una Política de Certificación o su implementación proporcionan, ni altera la aceptabilidad de los certificados que soporta la política para los propósitos para los que se han usado, se procederá al incremento del número menor de versión del documento y el último número de Identificador de Objeto (OID) que lo representa, manteniendo el número mayor de la versión del documento, así como el resto de su OID asociado. No se considera necesario comunicar este tipo de modificaciones a los suscriptores de los certificados correspondientes a la CP o DPC modificada.

En el supuesto de que la Subdirección de Certificación Electrónica juzgue que los cambios a la especificación vigente afectan a la aceptabilidad de los certificados para propósitos específicos se procederá al incremento del número mayor de versión del documento y la puesta a cero del número menor de la misma. También se modificarán los dos últimos números del Identificador de Objeto (OID) que lo representa.

9.12.2. Procedimientos de publicación y notificación.

Toda modificación de esta Declaración de Prácticas de Certificación o de los Documentos de Políticas de Certificación se publicará en el sitio web de ACCV www.accv.es sirviendo este mecanismo como notificación a los suscriptores, usuarios o terceras partes.

Las RA podrán ser notificadas directamente mediante correo electrónico o telefónicamente en función de la naturaleza de los cambios realizados.

9.12.3. Circunstancias en las que el OID debe ser cambiado

La Subdirección de Certificación Electrónica de ISTEC es la entidad competente para acordar la aprobación de la presente Declaración de Prácticas de Certificación, así como de las Políticas de Certificación asociadas a cada tipo de certificado.

Asimismo compete a la Subdirección de Certificación Electrónica de ISTEC la aprobación y autorización de las modificaciones de dichos documentos.

9.13. Resolución de conflictos.

ACCV podrá establecer, a través de los instrumentos jurídicos mediante los que se articule su relación con suscriptores y verificadores, los procedimientos de mediación, arbitraje y resolución de conflictos que se consideren oportunos, todo ello sin perjuicio de la legislación de procedimiento administrativo.

Los conflictos que se plateen en la prestación por ACCV de los servicios de certificación, se someterán a la jurisdicción contencioso-administrativa, conforme a lo dispuesto en la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-Administrativa.

9.14. Legislación aplicable

El funcionamiento y operaciones de ACCV, así como la presente DPC están regidos por la legislación comunitaria, estatal y valenciana vigente en cada momento.

Explícitamente se asumen como de aplicación las siguientes normas:

1..1. Decreto 220/2014, de 12 de diciembre, del Gobierno Valenciano, por el que se regula el uso de la firma electrónica avanzada en la Generalitat Valenciana

1..2. Ley 6/2020, de 11 de noviembre, por la que se regulan determinados aspectos de los servicios de confianza electrónica

1..3. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

1..4. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público

1..5. Ley 5/2013, de 23 de diciembre, de Medidas Fiscales, de Gestión Administrativa y Financiera, y de Organización de la Generalitat.

1..6. Ley 21/2017, de 28 de diciembre de 2017 Generalitat Valenciana, por la que se aprueba la integración en la Generalitat Valenciana de las funciones y competencias en materia de certificación y firma electrónica desarrolladas por el Institut Valencià de Finances (IVF)

1..7. Ley 27/2018, de 27 de diciembre de 2018 de la Generalitat Valenciana, por la que se aprueba la creación del nuevo organismo, ISTEC

1..8. Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

1..9. Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.° 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital

1..10. Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados

1..11. Orden ETD/743/2022, de 26 de julio, por la que se modifica la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

1..12. Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

9.15. Conformidad con la Ley aplicable.

ACCV declara que esta DPC cumple con la legislación indicada en el apartado 9.14.

9.16. Cláusulas diversas.

9.16.1. Acuerdo integro

Esta DPC y todos los documentos a los que se hace referencia en ella constituyen el acuerdo completo entre las partes, sustituyendo a todos los demás acuerdos que puedan existir con respecto a la misma materia.

Todos los terceros que confíen en los certificados asumen en su totalidad el contenido de la última versión de este documento, los PDS y las Políticas correspondientes.

9.16.2. Asignación

La presente DPC será vinculante para los sucesores, albaceas, herederos, representantes, administradores y cesionarios, expresos, tácitos o aparentes de las partes.

La nulidad de una de las cláusulas contenidas en esta DPC no afectará al resto de las cláusulas. En tal caso, dicha cláusula se considerará sin aplicación.

9.16.3. Severabilidad

En caso de conflicto de cualquier parte de este documento con la legislación vigente de cualquier jurisdicción en la que una Autoridad de Certificación opere o emita certificados, tras la correspondiente revisión legal, ACCV podrá modificar los puntos conflictivos en la medida mínima necesaria para cumplir con dicha legislación.

En tal caso, (antes de emitir un certificado bajo los requisitos modificados) ACCV incluirá en los subapartados de esta Sección información sobre la Ley que requiere la modificación y el cambio específico implementado por ACCV.

ACCV también informará a las partes interesadas, como el CAB Forum, de la información relevante recién añadida antes de emitir un certificado bajo los cambios realizados.

9.16.4. Cumplimiento (honorarios de los abogados y renuncia a los derechos)

ACCV podrá reclamar a una de las partes una indemnización y los honorarios de los abogados por los daños, pérdidas y gastos relacionados con la conducta de dicha parte. El hecho de que ACCV no aplique una disposición de esta DPC no supone una renuncia al derecho de ACCV a aplicar la misma disposición más adelante o al derecho a aplicar cualquier otra disposición de esta DPC. Para que sean efectivas, las renuncias deben ser por escrito y estar firmadas por ACCV.

9.16.5. Fuerza Mayor

ACCV no aceptará ninguna responsabilidad por el incumplimiento o el retraso en el cumplimiento de cualquiera de las obligaciones contenidas en la DPC, si dicho incumplimiento o retraso es consecuencia de un acontecimiento de fuerza mayor, circunstancias imprevisibles o cualquier circunstancia sobre la que no se pueda ejercer un control directo.

El funcionamiento de Internet está fuera del control razonable de ACCV.

9.17. Otras estipulaciones.

En caso de pérdida de la certificación QSCD de alguno de los dispositivos cualificados que ACCV utiliza para los certificados de entidad final, ACCV tomará las medidas necesarias para minimizar el posible impacto, informando de ello al organismo supervisor y paralizando la emisión de certificados sobre los dispositivos afectados.

10. Anexo I

10.1. Certificados Cualificados de Autenticación de Sitios Web

CONTRATO DE CERTIFICACIÓN - CÓDIGO 1.3.6.1.4.1.8149.3.3
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 del dominio Nombre cualificado: Alias: 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 Autenticación de Sitios Web con código 1.3.6.1.4.1.8149.3.3, 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 1.3.6.1.4.1.8149.3.3

Condiciones de utilización de los certificados

1. Los certificados asociados a la la Política de Certificación de certificados para servidores con soporte SSL , emitidos por la Agencia de Tecnología y Certificación Electrónica son del tipo X.509v3 y se rigen por la Declaración de Prácticas de Certificación de la Agencia de Tecnología y Certificación Electrónica, en tanto que Prestador de Servicios de Certificación, así como por la Política de Certificación referida. Ambos documentos se deben interpretar según la legislación de la Comunidad Europea, el Ordenamiento Jurídico Español y la legislación propia de la Generalitat Valenciana.

2. El solicitante de los certificados debe ser una persona física, en posesión de un certificado cualificado de la ACCV o del DNIe. El solicitante deberá aportar los datos relativos a su relación con el Organismo o Empresa en nombre del que solicita el certificado utilizando las herramientas puestas a su disposición por la ACCV.

3. El solicitante de los certificados, especialmente habilitado para la gestión de éstos por parte de un Organismo o Empresa determinada, es responsable de la veracidad de los datos aportados en todo momento a lo largo del proceso de solicitud y registro. Será responsable de comunicar cualquier variación de los datos aportados para la obtención del certificado.

4. El suscriptor del certificado es responsable de la custodia de su clave privada y de comunicar a la mayor brevedad posible cualquier pérdida o sustracción de esta clave.

5. El suscriptor del certificado es responsable de limitar el uso del certificado a lo dispuesto en la Política de Certificación asociada, que es un documento público y que se encuentra disponible en http://www.accv.es.

6. La Agencia de Tecnología y Certificación Electrónica no se responsabiliza del funcionamiento de los servidores informáticos que hacen uso de los certificados emitidos.

7. La Agencia de Tecnología y Certificación Electrónica es responsable del cumplimiento de las legislaciones Europea, Española y Valenciana, por lo que a Firma Electrónica se refiere. Es, asimismo, responsable del cumplimiento de lo dispuesto en la Declaración de Prácticas de Certificación de la Agencia de Tecnología y Certificación Electrónica y en la Política de Certificación asociada a este tipo de certificados.

8. El periodo de validez de estos certificados es de 12 meses como máximo. Para su renovación deberá seguirse el mismo procedimiento que para la primera solicitud o bien los procedimientos previstos en la Política de Certificación asociada.

9. Los certificados emitidos perderán su eficacia, además de al vencimiento del periodo de validez, cuando se produzca una revocación, cuando se inutilice el soporte del certificado, ante resolución judicial o administrativa que ordene la pérdida de eficacia, por inexactitudes graves en los datos aportados por el solicitante y por fallecimiento del suscriptor del certificado. Otras condiciones para la pérdida de eficacia se recogen en la Declaración de Prácticas de Certificación y en la Política de Certificación asociada a este tipo de certificados.

10. La identificación de los solicitantes se hará en base a su certificado digital personal expedido por la Agencia de Tecnología y Certificación Electrónica o su DNIe.

11. En cumplimiento de la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos de Carácter Personal, se informa al solicitante de la existencia de un fichero automatizado de datos de carácter personal, creado bajo la responsabilidad de la Agencia de Tecnología y Certificación Electrónica. La finalidad de este fichero es servir a los usos relacionados con los servicios de certificación que presta la Agencia de Tecnología y Certificación Electrónica. El suscriptor autoriza expresamente el uso de sus datos personales que contiene el fichero, en la medida en que sean necesarios para llevar a cabo las acciones previstas en la Política de Certificación.

12. La Agencia de Tecnología y Certificación Electrónica se compromete a poner los medios a su alcance para evitar la alteración, pérdida o acceso no autorizado a los datos de carácter personal contenidos en el fichero.

13. El solicitante podrá ejercer sus derechos de acceso, rectificación o cancelación sobre sus datos de carácter personal dirigiendo escrito a la Agencia de Tecnología y Certificación Electrónica, a través de cualquiera de los Registros de Entrada de la Generalitat Valenciana e indicando claramente esta voluntad.

Motivos de revocación

Estos son los motivos que podrá utilizar para revocar su certificado:

No reason or unspecified

El suscriptor no está obligado a proporcionar un motivo de revocación, a menos que su clave privada se haya visto comprometida.

affiliationChanged

Se DEBERÍA elegir este motivo de revocación cuando el nombre de su organización u otra información de la organización en el certificado haya cambiado.

superseded

Se DEBERÍA elegir este motivo de revocación cuando se solicita un nuevo certificado para reemplazar un certificado existente.

cessationOfOperation

Se DEBERÍA elegir este motivo de revocación cuando ya no sea propietario de todos los nombres de dominio en el certificado o cuando ya no vaya a utilizar el certificado porque el sitio web vaya a dejar de estar operativo.

keyCompromise

Se DEBE elegir este motivo de revocación cuando el suscriptor tenga conocimiento o tenga motivos para creer que la clave privada de su certificado se ha visto comprometida. Por ejemplo si una persona no autorizada ha tenido acceso a la clave privada de su certificado. Si se selecciona este motivo SE REVOCARÁN TODOS LOS CERTIFICADOS DEL ORGANISMO EMITIDOS CON LAS MISMAS CLAVES y la ACCV puede contactar con el solicitante para recabar mas información y requerir evidencias adicionales.

privilegeWithdrawn

La CA detecta que ha habido una infracción del lado del suscriptor que no ha resultado en compromiso de clave, como que el suscriptor del certificado proporcionó información engañosa en su solicitud de certificado o no ha cumplido con sus obligaciones materiales bajo el acuerdo del suscriptor o los términos de uso.

Los certificados con el uso de clave serverAuthentication están sujetos a lo definido por el CA/Browser Forum en https://cabforum.org/working-groups/server/baseline-requirements/documents/. Entre la condiciones establecidas se encuentra la obligatoriedad de revocar los certificados si se detecta que la emisión u operación no cumple con lo definido en la normativa. Esta revocación se debe hacer en un plazo máximo de entre uno (1) y cinco (5) días naturales dependiendo del tipo de incidente y no es posible aplazamiento de ningún tipo. Si no es posible cumplir esta condición no se deben utilizar nunca certificados emitidos bajo esta normativa.

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.

10.2. Certificados Cualificados de sede electrónica administrativa en dispositivo seguro

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.14
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 dispositivo seguro con código 1.3.6.1.4.1.8149.3.14, 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 1.3.6.1.4.1.8149.3.14
Condiciones de utilización de los certificados

1. Los certificados asociados a la Política de Certificación para Certificados Cualificados de Sede Electrónica Administrativa en dispositivo seguro, 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 reconocido de la Agencia de Tecnología y Certificación Electrónica, 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 pública determinada, es responsable de la veracidad de los datos aportados en todo momento a lo largo del proceso de solicitud y registro. Será responsable de comunicar cualquier variación de los datos aportados para la obtención del certificado.

4. El suscriptor del certificado es responsable de la custodia de su clave privada y de comunicar a la mayor brevedad posible cualquier pérdida o sustracción de esta clave.

5. El suscriptor del certificado es responsable de limitar el uso del certificado a lo dispuesto en la Política de Certificación asociada, que es un documento público y que se encuentra disponible en http://www.accv.es.

6. La Agencia de Tecnología y Certificación Electrónica, no se responsabiliza del contenido de los documentos firmados haciendo uso de los certificados por ella emitidos.

7. La Agencia de Tecnología y Certificación Electrónica, es responsable del cumplimiento de las legislaciones Europea, Española y Valenciana, por lo que a Firma Electrónica se refiere. Es, asimismo, responsable del cumplimiento de lo dispuesto en la Declaración de Prácticas de Certificación de la ACCV y en la Política de Certificación asociada a este tipo de certificados.

8. El periodo de validez de estos certificados es de 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 el Documento Nacional de Identidad, NIE o Pasaporte válido y vigente. 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. En cumplimiento de la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos de Carácter Personal, se informa al solicitante de la existencia de un fichero automatizado de datos de carácter personal, creado bajo la responsabilidad de la Agencia de Tecnología y Certificación Electrónica. La finalidad de este fichero es servir a los usos relacionados con los servicios de certificación que presta la Agencia de Tecnología y Certificación Electrónica. El suscriptor autoriza expresamente el uso de sus datos personales que contiene el fichero, en la medida en que sean necesarios para llevar a cabo las acciones previstas en la Política de Certificación.

12. La Agencia de Tecnología y Certificación Electrónica se compromete a poner los medios a su alcance para evitar la alteración, pérdida o acceso no autorizado a los datos de carácter personal contenidos en el fichero.

13. El solicitante podrá ejercer sus derechos de acceso, rectificación o cancelación sobre sus datos de carácter personal dirigiendo escrito a la Agencia de Tecnología y Certificación Electrónica, a través de cualquiera de los Registros de Entrada de la Generalitat indicando claramente esta voluntad.

Motivos de revocación

Estos son los motivos que podrá utilizar para revocar su certificado:

No reason or unspecified

El suscriptor no está obligado a proporcionar un motivo de revocación, a menos que su clave privada se haya visto comprometida.

affiliationChanged

Se DEBERÍA elegir este motivo de revocación cuando el nombre de su organización u otra información de la organización en el certificado haya cambiado.

superseded

Se DEBERÍA elegir este motivo de revocación cuando se solicita un nuevo certificado para reemplazar un certificado existente.

cessationOfOperation

Se DEBERÍA elegir este motivo de revocación cuando ya no sea propietario de todos los nombres de dominio en el certificado o cuando ya no vaya a utilizar el certificado porque el sitio web vaya a dejar de estar operativo.

keyCompromise

Se DEBE elegir este motivo de revocación cuando el suscriptor tenga conocimiento o tenga motivos para creer que la clave privada de su certificado se ha visto comprometida. Por ejemplo si una persona no autorizada ha tenido acceso a la clave privada de su certificado. Si se selecciona este motivo SE REVOCARÁN TODOS LOS CERTIFICADOS DEL ORGANISMO EMITIDOS CON LAS MISMAS CLAVES y la ACCV puede contactar con el solicitante para recabar mas información y requerir evidencias adicionales.

privilegeWithdrawn

La CA detecta que ha habido una infracción del lado del suscriptor que no ha resultado en compromiso de clave, como que el suscriptor del certificado proporcionó información engañosa en su solicitud de certificado o no ha cumplido con sus obligaciones materiales bajo el acuerdo del suscriptor o los términos de uso.

Los certificados con el uso de clave serverAuthentication están sujetos a lo definido por el CA/Browser Forum en https://cabforum.org/working-groups/server/baseline-requirements/documents/. Entre la condiciones establecidas se encuentra la obligatoriedad de revocar los certificados si se detecta que la emisión u operación no cumple con lo definido en la normativa. Esta revocación se debe hacer en un plazo máximo de entre uno (1) y cinco (5) días naturales dependiendo del tipo de incidente y no es posible aplazamiento de ningún tipo. Si no es posible cumplir esta condición no se deben utilizar nunca certificados emitidos bajo esta normativa.

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.

10.3. Certificados Cualificados de sede electrónica administrativa en soporte software

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. En cumplimiento de la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos de Carácter Personal, se informa al solicitante de la existencia de un fichero automatizado de datos de carácter personal, creado bajo la responsabilidad de la Agencia de Tecnología y Certificación Electrónica. La finalidad de este fichero es servir a los usos relacionados con los servicios de certificación que presta la Agencia de Tecnología y Certificación Electrónica. El suscriptor autoriza expresamente el uso de sus datos personales que contiene el fichero, en la medida en que sean necesarios 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.

Motivos de revocación

Estos son los motivos que podrá utilizar para revocar su certificado:

No reason or unspecified

El suscriptor no está obligado a proporcionar un motivo de revocación, a menos que su clave privada se haya visto comprometida.

affiliationChanged

Se DEBERÍA elegir este motivo de revocación cuando el nombre de su organización u otra información de la organización en el certificado haya cambiado.

superseded

Se DEBERÍA elegir este motivo de revocación cuando se solicita un nuevo certificado para reemplazar un certificado existente.

cessationOfOperation

Se DEBERÍA elegir este motivo de revocación cuando ya no sea propietario de todos los nombres de dominio en el certificado o cuando ya no vaya a utilizar el certificado porque el sitio web vaya a dejar de estar operativo.

keyCompromise

Se DEBE elegir este motivo de revocación cuando el suscriptor tenga conocimiento o tenga motivos para creer que la clave privada de su certificado se ha visto comprometida. Por ejemplo si una persona no autorizada ha tenido acceso a la clave privada de su certificado. Si se selecciona este motivo SE REVOCARÁN TODOS LOS CERTIFICADOS DEL ORGANISMO EMITIDOS CON LAS MISMAS CLAVES y la ACCV puede contactar con el solicitante para recabar mas información y requerir evidencias adicionales.

privilegeWithdrawn

La CA detecta que ha habido una infracción del lado del suscriptor que no ha resultado en compromiso de clave, como que el suscriptor del certificado proporcionó información engañosa en su solicitud de certificado o no ha cumplido con sus obligaciones materiales bajo el acuerdo del suscriptor o los términos de uso.

Los certificados con el uso de clave serverAuthentication están sujetos a lo definido por el CA/Browser Forum en https://cabforum.org/working-groups/server/baseline-requirements/documents/. Entre la condiciones establecidas se encuentra la obligatoriedad de revocar los certificados si se detecta que la emisión u operación no cumple con lo definido en la normativa. Esta revocación se debe hacer en un plazo máximo de entre uno (1) y cinco (5) días naturales dependiendo del tipo de incidente y no es posible aplazamiento de ningún tipo. Si no es posible cumplir esta condición no se deben utilizar nunca certificados emitidos bajo esta normativa.

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.

10.4. Certificados de Autenticación de Servidor

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.36
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 del dominio Nombre cualificado: Alias: Dirección de correo de contacto:
Sección 3 – *Fecha y Firma* *Suscribo el presente contrato de certificación asociado a la Política de Certificación de Certificados de Autenticación de Sitios Web con código 1.3.6.1.4.1.8149.3.36, 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 1.3.6.1.4.1.8149.3.36

Condiciones de utilización de los certificados

1. Los certificados asociados a la la Política de Certificación de certificados para servidores con soporte SSL , emitidos por la Agencia de Tecnología y Certificación Electrónica son del tipo X.509v3 y se rigen por la Declaración de Prácticas de Certificación de la Agencia de Tecnología y Certificación Electrónica, en tanto que Prestador de Servicios de Certificación, así como por la Política de Certificación referida. Ambos documentos se deben interpretar según la legislación de la Comunidad Europea, el Ordenamiento Jurídico Español y la legislación propia de la Generalitat Valenciana.
2. El solicitante de los certificados debe ser una persona física, en posesión de un certificado cualificado de la ACCV o del DNIe. El solicitante deberá aportar los datos relativos a su relación con el Organismo o Empresa en nombre del que solicita el certificado utilizando las herramientas puestas a su disposición por la ACCV.
3. El solicitante de los certificados, especialmente habilitado para la gestión de éstos por parte de un Organismo o Empresa determinada, es responsable de la veracidad de los datos aportados en todo momento a lo largo del proceso de solicitud y registro. Será responsable de comunicar cualquier variación de los datos aportados para la obtención del certificado.
4. El suscriptor del certificado es responsable de la custodia de su clave privada y de comunicar a la mayor brevedad posible cualquier pérdida o sustracción de esta clave.
5. El suscriptor del certificado es responsable de limitar el uso del certificado a lo dispuesto en la Política de Certificación asociada, que es un documento público y que se encuentra disponible en http://www.accv.es.
6. La Agencia de Tecnología y Certificación Electrónica no se responsabiliza del funcionamiento de los servidores informáticos que hacen uso de los certificados emitidos.
7. La Agencia de Tecnología y Certificación Electrónica es responsable del cumplimiento de las legislaciones Europea, Española y Valenciana, por lo que a Firma Electrónica se refiere. Es, asimismo, responsable del cumplimiento de lo dispuesto en la Declaración de Prácticas de Certificación de la Agencia de Tecnología y Certificación Electrónica y en la Política de Certificación asociada a este tipo de certificados.
8. El periodo de validez de estos certificados es de 12 meses como máximo. Para su renovación deberá seguirse el mismo procedimiento que para la primera solicitud o bien los procedimientos previstos en la Política de Certificación asociada.
9. Los certificados emitidos perderán su eficacia, además de al vencimiento del periodo de validez, cuando se produzca una revocación, cuando se inutilice el soporte del certificado, ante resolución judicial o administrativa que ordene la pérdida de eficacia, por inexactitudes graves en los datos aportados por el solicitante y por fallecimiento del suscriptor del certificado. Otras condiciones para la pérdida de eficacia se recogen en la Declaración de Prácticas de Certificación y en la Política de Certificación asociada a este tipo de certificados.
10. La identificación de los solicitantes se hará en base a su certificado digital personal expedido por la Agencia de Tecnología y Certificación Electrónica o su DNIe.
11. En cumplimiento de la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos de Carácter Personal, se informa al solicitante de la existencia de un fichero automatizado de datos de carácter personal, creado bajo la responsabilidad de la Agencia de Tecnología y Certificación Electrónica. La finalidad de este fichero es servir a los usos relacionados con los servicios de certificación que presta la Agencia de Tecnología y Certificación Electrónica. El suscriptor autoriza expresamente el uso de sus datos personales que contiene el fichero, en la medida en que sean necesarios para llevar a cabo las acciones previstas en la Política de Certificación.
12. La Agencia de Tecnología y Certificación Electrónica se compromete a poner los medios a su alcance para evitar la alteración, pérdida o acceso no autorizado a los datos de carácter personal contenidos en el fichero.
13. El solicitante podrá ejercer sus derechos de acceso, rectificación o cancelación sobre sus datos de carácter personal dirigiendo escrito a la Agencia de Tecnología y Certificación Electrónica, a través de cualquiera de los Registros de Entrada de la Generalitat Valenciana e indicando claramente esta voluntad.

Motivos de revocación

Estos son los motivos que podrá utilizar para revocar su certificado:

No reason or unspecified

El suscriptor no está obligado a proporcionar un motivo de revocación, a menos que su clave privada se haya visto comprometida.

affiliationChanged

Se DEBERÍA elegir este motivo de revocación cuando el nombre de su organización u otra información de la organización en el certificado haya cambiado.

superseded

Se DEBERÍA elegir este motivo de revocación cuando se solicita un nuevo certificado para reemplazar un certificado existente.

cessationOfOperation

Se DEBERÍA elegir este motivo de revocación cuando ya no sea propietario de todos los nombres de dominio en el certificado o cuando ya no vaya a utilizar el certificado porque el sitio web vaya a dejar de estar operativo.

keyCompromise

Se DEBE elegir este motivo de revocación cuando el suscriptor tenga conocimiento o tenga motivos para creer que la clave privada de su certificado se ha visto comprometida. Por ejemplo si una persona no autorizada ha tenido acceso a la clave privada de su certificado. Si se selecciona este motivo SE REVOCARÁN TODOS LOS CERTIFICADOS DEL ORGANISMO EMITIDOS CON LAS MISMAS CLAVES y la ACCV puede contactar con el solicitante para recabar mas información y requerir evidencias adicionales.

privilegeWithdrawn

La CA detecta que ha habido una infracción del lado del suscriptor que no ha resultado en compromiso de clave, como que el suscriptor del certificado proporcionó información engañosa en su solicitud de certificado o no ha cumplido con sus obligaciones materiales bajo el acuerdo del suscriptor o los términos de uso.

Los certificados con el uso de clave serverAuthentication están sujetos a lo definido por el CA/Browser Forum en https://cabforum.org/working-groups/server/baseline-requirements/documents/. Entre la condiciones establecidas se encuentra la obligatoriedad de revocar los certificados si se detecta que la emisión u operación no cumple con lo definido en la normativa. Esta revocación se debe hacer en un plazo máximo de entre uno (1) y cinco (5) días naturales dependiendo del tipo de incidente y no es posible aplazamiento de ningún tipo. Si no es posible cumplir esta condición no se deben utilizar nunca certificados emitidos bajo esta normativa.

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.