Agencia de Tecnología
y Certificación Electrónica

Declaración de Prácticas de Certificación (CPS) de la ACCV

Fecha: 19/10/2011	**Versión:** 3.0
Estado: APROBADO	**Nº de páginas:** 57
OID: 1.3.6.1.4.1.8149.2.3.0	**Clasificación: PUBLICO**
Archivo: ACCV-CPS-V3.0.doc	
Preparado por: **Agencia de Tecnología y Certificación Electrónica**	

Tabla de Contenido

1. INTRODUCCIÓN

1.1. Presentación

El presente documento contiene la preceptiva *Declaración de Prácticas de Certificación (CPS)* de la Agencia de Tecnología y Certificación Electrónica.

La Agencia de Tecnología y Certificación Electrónica es una entidad de derecho público, con personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus fines, que se rige por sus Estatutos contenidos en el Decreto 21/2011, de 4 de marzo, del Consell, por el que se aprueba el Estatuto de la Agencia de Tecnología y Certificación Electrónica.

De acuerdo con lo anterior y en cumplimiento de la previsión legal contenida en el artículo 19 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, la presente Declaración de Prácticas de Certificación (CPS) 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.

Así pues, la presente Declaración de Prácticas de Certificación constituye el compendio general de normas aplicables a toda actividad certificadora de la Agencia de Tecnología y Certificación Electrónica en tanto que Prestador de Servicios de Certificación. Sin embargo, las distintas especialidades aplicables a cada uno de los diferentes tipos de certificados que se emitan se establecen en las distintas Políticas de Certificación que, como normas complementarias y específicas, prevalecerán sobre la presente Declaración de Prácticas de Certificación en lo que se refiera a cada tipo de certificado.

Asimismo cabe indicar que la presente Declaración de Prácticas de Certificación está redactada siguiendo las especificaciones del RFC 3647 "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*" propuesto por *Network Working Group* para este tipo de documentos.

1.2. Nombre del documento e identificación

Nombre del documento	Declaración de Prácticas de Certificación (CPS) de la ACCV
Versión del documento	3.0
Estado del documento	APROBADO
Referencia de la CPS/ OID (Object Identifier)	1.3.6.1.4.1.8149.2.3.0
Fecha de emisión	19 de octubre de 2011
Fecha de expiración	No aplicable.
Localización	Esta CPS se puede encontrar en http://www.accv.es/pdf-politicas

1.3. Comunidad de usuarios de los servicios de la ACCV

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 la ACCV se estructuran en dos jerarquías de certificación independientes, cada una con su autoridad de certificación raíz.

La jerarquía primera está formada por las siguientes autoridades de certificación:

- “Root CA GVA" como Autoridad de Certificación de primer nivel de la jerarquía más antigua de la ACCV. Esta CA no emite certificados para entidades finales. Esta Autoridad de Certificación de primer nivel se auto-firma, emitiendo un certificado cuyo firmante es “Root CAGVA”, y que contiene la clave pública (o datos de verificación de firma) de “Root CAGVA” firmada con los datos de creación de firma (clave privada) de “Root CAGVA”. La huella digital o fingerprint de la esta Root CA expresado en hexadecimal, es:

  A073 E5C5 BD43 610D 864C 2113 0A85 5857 CC9C EA46

  Con esta clave se verifica el certificado autofirmado de la Autoridad de Certificación raíz Root CA, que es válido desde el 6 de julio de 2001 al 1 de julio de 2021.

- “ACCV-CA1” Como Autoridad de Certificación subordinada de Root CA GVA. Su función es la emisión de certificados de para entidades con o sin personalidad jurídica. El certificado de “ACCV-CA1” es válido desde el día 4 de mayo de 2006 hasta el 1 de mayo de 2016.

- “ACCV-CA2” Como Autoridad de Certificación subordinada de Root CA GVA. Su función es la emisión de certificados de entidad final para los suscriptores de la ACCV. El certificado de “ACCV-CA2” es válido desde el día 4 de mayo de 2006 hasta el 1 de mayo de 2016.

- “ACCV-CA3” Como Autoridad de Certificación subordinada de Root CA GVA. Su función es la emisión de certificados para la identificación de usuarios de dominio de Windows y para la identificación de los controladores de dominio de Windows. El certificado de “ACCV-CA3” es válido desde el día 17 de junio de 2006 hasta el 14 de junio de 2016.

La segunda jerarquía de autoridades de certificación se ha desarrollado para sustituir progresivamente a la jerarquía de PKI anterior, cuya raíz y componentes se describen en párrafos anteriores. Esta jerarquía está formada por los siguientes componentes:

- “ACCVRAIZ1” como 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 “ACCVRAIZ1”, y que contiene la clave pública (o datos de verificación de firma) de “ACCVRAIZ1” firmada con los datos de creación de firma (clave privada) de “ACCVRAIZ1”. La huella digital o fingerprint de esta nueva CA raíz es:

  9305 7A88 15C6 4FCE 882F FA91 1652 2878 BC53 6417

  Con esta clave se verifica el certificado autofirmado de ACCVRAIZ1, que es válido desde el 5 de mayo de 2011 al 31 de diciembre de 2030.

- "ACCVCA-110" Como Autoridad de Certificación subordinada de ACCVRAIZ1. Su función es la emisión de certificados de para entidades con o sin personalidad jurídica. El certificado de "ACCVCA-110" es válido desde el día 13 de octubre de 2011 hasta el 1 de enero de 2027.
- "ACCVCA-120" Como Autoridad de Certificación subordinada de ACCVRAIZ1. Su función es la emisión de certificados de entidad final para los suscriptores de la ACCV. El certificado de "ACCVCA-120" es válido desde el día 13 de octubre de 2011 hasta el 1 de enero de 2027.
- "ACCVCA-130" Como Autoridad de Certificación subordinada de ACCVRAIZ1. Su función es la emisión de certificados para la identificación de usuarios de dominio de Windows y para la identificación de los controladores de dominio de Windows El certificado de "ACCVCA-130" es válido desde el día 14 de octubre de 2011 hasta el 1 de enero de 2027.

1.3.2. Autoridades de Registro

Las Autoridades de Registro son aquellas personas físicas o jurídicas a las que la ACCV encomienda la identificación y comprobación de las circunstancias personales de los solicitantes de certificados. A tal efecto, las Autoridades de Registro se encargarán de garantizar que la solicitud del certificado contiene información veraz y completa del solicitante, y que la misma se ajusta a los requisitos exigidos en la correspondiente Política.

Pueden ser Autoridades de Registro aquellas entidades con las que se haya formalizado el correspondiente convenio de colaboración o suscrito el contrato de prestación de servicio. Estas Autoridades de Registro se denominan Puntos de Registro de Usuario o PRUs en la documentación relativa a la Agencia de Tecnología y Certificación Electrónica. Las funciones básicas de estas Autoridades de Registro, que actúan por cuenta de la ACCV, 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 reconocido.
- 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.

1.3.3. Usuarios finales

Las Entidades finales o Usuarios son las personas físicas o jurídicas que tienen capacidad para solicitar y obtener un certificado electrónico en las condiciones que se establecen en la presente Declaración de Prácticas de Certificación y en las Políticas de Certificación vigentes para cada tipo de certificado.

A los efectos de la presente Declaración de Prácticas de Certificación, y de las Políticas de Certificación que la desarrollan, son Entidades finales del sistema de certificación de la ACCV, las siguientes:

- Solicitantes
- Suscriptores
- Terceros de confianza

1.3.3.1. Solicitantes

Solicitante es la persona física que, en nombre propio o en representación de tercero, y previa identificación, solicita la emisión de un *Certificado*.

En el supuesto de tratarse de un Solicitante de Certificado cuyo Suscriptor sea una persona jurídica dicha persona física sólo podrá ser un administrador o un representante, legal o voluntario con poder bastante a estos efectos, de la persona jurídica que vaya a ser el suscriptor del certificado.

1.3.3.2. Suscriptores

A los efectos de la presente CPS, el suscriptor de los certificados de la ACCV se corresponde con el término firmante previsto en el artículo 6 de la Ley 59/2003 de Firma Electrónica.

Tendrá la condición de suscriptor el titular del certificado. Es la persona física o jurídica cuya identidad personal queda vinculada a los datos de creación y verificación de firma, firmados electrónicamente, a través de una clave pública certificada por el Prestador de Servicios de Certificación.

El suscriptor asume la responsabilidad de custodia de los datos de creación de firma, sin que pueda ceder su uso a cualquier otra persona bajo ningún concepto.

El grupo de usuarios que pueden solicitar la emisión de certificados de la ACCV se encuentra definido y limitado por cada Política de Certificación.

De forma genérica, y sin perjuicio de lo establecido por la Política de Certificación aplicable en cada caso, se establece que los posibles suscriptores son el conjunto de ciudadanos que dispongan de los mecanismos de identificación requeridos en las diferentes Políticas de Certificación,.

1.3.3.3. Partes confiantes

Tendrán la consideración de partes confiantes o terceras partes confiantes, todas aquellas personas que, de forma voluntaria, confían en los certificados emitidos por la ACCV.

Las Políticas de Certificación aplicables en cada caso limitan el derecho a confiar en los certificados emitidos por la ACCV.

De forma genérica, y sin perjuicio de lo establecido por la Política de Certificación aplicable en cada caso, se establecen como terceros que confían en los certificados de la ACCV cualesquiera Administraciones públicas, empresas o ciudadanos españoles.

1.4. Uso de los certificados

Las Políticas de Certificación correspondientes a cada tipo de certificado emitido por la ACCV constituyen los documentos en los que se determinan los usos y limitaciones de cada certificado. No se fijan pues, en esta CPS, los usos y limitaciones de los diferentes tipos de certificados que emite la ACCV.

1.4.1. Usos prohibidos

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

1.5. Política de Administración de la ACCV

1.5.1. Especificación de la Organización Administradora

Nombre	*Agencia de Tecnología y Certificación Electrónica*
Dirección de email	*accv@accv.es*
Dirección	*Plaza de Cánovas del Castillo, 1 – 46005 Valencia (Spain)*
Número de teléfono	*+34·961 923 150*

Número de fax	*+34·961 923 151*

1.5.2. Persona de Contacto

Nombre	*Agencia de Tecnología y Certificación Electrónica*
Dirección de email	*accv@accv.es*
Dirección	*Plaza de Cánovas del Castillo, 1 – 46005 Valencia (Spain)*
Número de teléfono	*+34·961 923 150*
Número de fax	*+34·961 923 151*

1.5.3. Competencia para determinar la adecuación de la CPS con las diferentes Políticas de certificación.

La entidad competente para determinar la adecuación de esta CPS a las diferentes Políticas de Certificación de la ACCV, es la Gerencia de la Agencia de Tecnología y Certificación Electrónica de conformidad con los Estatutos de la Agencia.

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, y en las distintas Políticas 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 la 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 la ACCV reciben también el nombre de Puntos de Registro del Usuario o PRU.
- Cadena de certificación: lista de certificados que contiene al menos un certificado y el certificado raíz de la 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 la ACCV.
- Certificado raíz: Certificado cuyo suscriptor es la ACCV y pertenece a la jerarquía de la 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 reconocido: Certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley 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, de conformidad con lo que dispone el capítulo II del Título II de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- 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 la 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 que establece el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Directorio de Certificados: repositorio de información que sigue el estándar X.500 del ITU-T.
- Documento electrónico: conjunto de registros lógicos almacenado en soporte susceptible de ser leído por equipos electrónicos de procesamiento de datos, que contiene información.
- Documento de seguridad: documento exigido por la Ley Orgánica 15/99 de Protección de Datos de Carácter Personal cuyo objetivo es establecer las medidas de seguridad implantadas, a los efectos de este documento, por la 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 del tratamiento de los ficheros.
- Firma electrónica reconocida: es aquella firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro 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 la ACCV.
- 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 la ACCV.
- Política de Certificación: documento que completa la Declaración de Prácticas de Certificación, estableciendo las condiciones de uso y los procedimientos seguidos por la 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.
- 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.
- 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.
- SHA-1: Secure Hash Algorithm (algoritmo seguro de resumen –hash-). Desarrollado por el NIST y revisado en 1994 (SHA-1). El algoritmo consiste en tomar mensajes de menos de 264 bits y generar un resumen de 160 bits de longitud. 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 previa identificación, 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 y permite la generación de firma electrónica reconocida.
- Terceras partes confiantes o partes confiantes: aquellas personas que depositan su confianza en un certificado de la 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
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
FIPS	Federal Information Processing Standard
IETF	Internet Engineering Task Force
OID	Object identifier
OCSP	On-line Certificate Status Protocol
OPRU	Operador de Punto de Registro
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
Sub CA	Subordinate Certification Authority

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 la ACCV está compuesto por un servicio de directorio LDAP, en alta disponibilidad, accesible en: ldap://ldap.accv.es:389.

El repositorio de la ACCV no contiene ninguna información de naturaleza confidencial.

La ACCV no utiliza ningún otro repositorio operado por ninguna organización distinta a la ACCV.

2.2. Publicación

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

La presente CPS es pública y se encuentra disponible en el sitio web de la ACCV http://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-CPS-V3.0.pdf, en formato PDF.

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

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

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

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

2.3. Frecuencia de actualizaciones

La CPS y las Políticas de Certificación se publicarán cada vez que sean modificadas.

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 la ACCV y de su sitio web es libre y gratuito.

Sólo la ACCV está autorizada a modificar, sustituir o eliminar información de su repositorio y sitio web. En este sentido, la 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.

El *distinguished name* se incluye en el campo Common Name (CN) y se corresponde con el nombre que aparece identificado en el DNI, Pasaporte o Documento que identifique al firmante del certificado.

3.1.2. Significado de los nombres

En todos los casos los nombres distintivos deben tener sentido. Si la Política de Certificación aplicable al tipo de certificado no indica lo contrario, se utilizan el nombre y NIF del solicitante.

La ACCV no permite el uso de seudónimos en los certificados que emite.

3.1.3. Interpretación de formatos de nombres

Las reglas utilizadas por la ACCV para interpretar los nombres distintivos de los certificados que emite son las contenidas en la ISO/IEC 9595 (X.500) Distinguished Name (DN)

3.1.4. Unicidad de los nombres

Los nombres distintivos deben ser únicos y no inducirán a ambigüedad.

Para ello se incluirá como parte del nombre común (common name) del nombre distintivo (distinguished name) el nombre del subscriptor seguido de su NIF, con el formato "*nombre* - NIF *número de NIF*".

Las Políticas de Certificación pueden disponer la sustitución de este mecanismo de unicidad.

3.1.5. Resolución de conflictos relativos a nombres

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.

La 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.

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

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

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

- "Autoritat de Certificació de la Comunitat Valenciana", marca mixta nº 2.591.232, con fecha de concesión 15 de septiembre de 2004, publicación 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 mixta nº 2.943.180, solicitado ante la Oficina Española de Patentes y Marcas el 13 de agosto de 2010.

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) este 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 en formato PKCS #10.

Esta norma podrá verse revocada por lo establecido en cada caso en la Política de Certificación aplicable para cada solicitud.

3.2.2. Autenticación de la identidad de una organización.

En el caso que una Política de Certificación considere necesaria la autenticación de la identidad de una organización, dicha política será la responsable del establecimiento de los métodos necesarios para la verificación de la mencionada identidad.

Explícitamente se prohíbe en esta CPS el uso de métodos de identificación remota de organizaciones.

3.2.3. Autenticación de la identidad de un individuo.

El proceso de identificación individual se define por la Política de Certificación aplicable a cada tipo de certificado.

Como norma general no se emplearán métodos de identificación remota distintos a la firma digital realizada con certificados emitidos por la propia ACCV o por algún otro Prestador de Servicios de Certificación reconocido.

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 o utilizando solicitudes firmadas digitalmente mediante el certificado original que se pretende renovar, siempre que este no haya vencido ni se haya procedido a su revocación. Existen, por tanto, dos mecanismos alternativos para la renovación:

- Formularios web firmados en el Área Personal de Servicios de Certificación, disponible en www.accv.es.
- Personación en cualquier Punto de Registro de Usuario, con los documentos de identificación suficientes (ver apartado 3.2.3. de esta CPS).

Asimismo, y de conformidad con lo establecido en el art. 13.4 b) de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica la renovación del certificado mediante solicitudes firmadas digitalmente exigirá que haya transcurrido un período de tiempo desde la identificación personal menor a los cinco años.

3.3.2. Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida.

La política de identificación y autenticación para la renovación de un certificado después de una revocación sin compromiso de la clave será la misma que para el registro inicial, o bien se empleará algún método electrónico que garantice de manera fiable e inequívoca la identidad del solicitante y la autenticidad de la solicitud.

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

El proceso de solicitud de revocación viene definido por la Política de Certificación aplicable a cada tipo de certificado.

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.

En cualquier caso, las distintas Políticas de Certificación pueden definir otras políticas de identificación menos severas.

La 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.

Las distintas Políticas de Certificación pueden definir la creación de una contraseña de revocación en el momento del registro del certificado.

4. El ciclo de vida de los certificados.

Las especificaciones contenidas en este apartado lo son sin perjuicio de las estipulaciones previstas en cada una de las distintas Políticas de Certificación para los distintos tipos de certificados emitidos por la ACCV.

4.1. Solicitud de certificados

La Autoridad de Registro de la ACCV que reciba la solicitud le compete el determinar que el tipo de certificado solicitado se adecue a las características concretas del solicitante, de conformidad con el contenido de la Política de Certificación aplicable a dicho certificado y, de este modo, resolver la solicitud formulada.

En cada Política de Certificación se especifica la información que debe suministrarse con carácter previo, a quien solicite un certificado.

4.2. Tramitación de la solicitud de certificados.

Compete a la Autoridad o Entidad de Registro la comprobación de la identidad del solicitante, la verificación de la documentación y la constatación de que el solicitante ha firmado el documento de comparecencia. Una vez completa la solicitud, la Autoridad de Registro la remitirá a la ACCV.

4.3. Emisión de certificados

La 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.

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

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

Es tarea de la RA notificar al subscriptor de un certificado la emisión del mismo y proporcionarle una copia, o en su defecto, informarle del modo en que puede conseguirla.

Todo lo especificado en este apartado queda supeditado a lo estipulado por las distintas Políticas de Certificación para la emisión de cada tipo de certificados.

4.4. Aceptación de certificados

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.

4.5. Uso del par de claves y del certificado.

Los certificados emitidos por la ACCV se utilizan para las relaciones de suscriptores con las Administraciones Públicas españolas. Además, los certificados pueden utilizarse, por parte de los titulares de éstos, en cualesquiera otras relaciones telemáticas con otras entidades públicas o privadas, organismos, personas jurídicas o físicas que acepten los certificados.

Los certificados pueden emplearse para identificar al suscriptor de manera segura, para firmar documentos electrónicos, correo electrónico, etc.

Pueden emplearse, asimismo, para cifrar información en formato electrónico de forma permanente.

4.6. Renovación de certificados.

En cada una de las Políticas de Certificación asociadas a cada tipo de certificado emitido por la Agencia de Tecnología y Certificación Electrónica se detalla la posibilidad o no de renovar los certificados, así como las condiciones para proceder a su renovación.

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.

4.8. Modificación de certificados.

Únicamente se pueden acordar durante el ciclo de vida de un certificado la modificación de los campos relativos a la dirección postal y teléfono del suscriptor.

4.9. Revocación y suspensión de certificados.

4.9.1. Circunstancias para la revocación

Un certificado se revoca cuando:

- 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 subscripción, la CP asociada o de la presente CPS.
- Se produce la emisión defectuosa de un certificado debido a:
  - Que no se ha satisfecho un prerrequisito material para la emisión del certificado.
  - Que un factor fundamental en el certificado se sepa o crea razonablemente que puede ser falso.
  - Un error de entrada de datos u otro error de proceso.
- El par de claves generado por un usuario final se revela como “débil”.
- La información contenida en un certificado o utilizada para realizar su solicitud se convierte en inexacta, por ejemplo cuando el dueño de un certificado cambia su nombre.
- Una solicitud de revocación válida se recibe de un usuario final.
- Una solicitud de revocación válida se recibe de una tercera parte autorizada, por ejemplo una orden judicial.
- El certificado de una RA o CA superior en la jerarquía de confianza del certificado es revocado.

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 la ACCV.

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

El procedimiento para la solicitud de la revocación de cada tipo de certificado se definirá en la Política de Certificación correspondiente.

De forma general, y sin perjuicio de lo definido en las Políticas de Certificación:

- Se aceptarán solicitudes de revocación remotas si están firmadas digitalmente con un certificado de la ACCV o de algún otro Prestador de Servicios de Certificación reconocido, y presenciales si se cumplen los requisitos de identificación del usuario establecidos para el registro inicial.
- En el caso de producirse una solicitud de revocación sin posible verificación de la identidad del solicitante (telefónica, correo electrónico sin firma digital,…), se procederá a la suspensión del certificado durante un plazo máximo de 30 días naturales, durante los que se procederá a verificar la veracidad de la solicitud. En el caso de no poder verificar la solicitud en dicho plazo, se procederá a la revocación del certificado. Es importante reseñar que el certificado no será utilizable desde el momento del procesamiento de la solicitud.
- Tras la revocación del certificado el suscriptor del mismo deberá destruir la clave privada que se corresponda con el mismo, y no hacer uso del certificado revocado.

Existe un formulario de solicitud de revocación de certificados en la web de la ACCV, en la URL http://www.accv.es, dentro del Área Personal de Servicios de Certificación

Una solicitud de revocación tanto si se realiza en papel o de forma electrónica (v.gr. correo electrónico) debe contener la información que se describe en el formulario de solicitud de revocación, recogido en cada una de las Políticas de Certificación.

4.9.4. Periodo de gracia de la solicitud de revocación

La revocación se realizará de forma inmediata al procesamiento de cada solicitud verificada como válida. Por tanto no existe ningún periodo de gracia asociado a este proceso.

4.9.5. Circunstancias para la suspensión

La suspensión implica invalidez del certificado durante el tiempo que permanece suspendido.

La suspensión únicamente se puede declarar de oficio por la propia ACCV, cuando se ha producido una solicitud de revocación de un certificado sin posible verificación inmediata de la identidad del solicitante (telefónica, por correo electrónico sin firma digital...), o cuando la ACCV sospecha que se haya podido comprometer la clave privada asociada al certificado de un usuario, o si la ACCV tiene dudas sobre la veracidad de los datos asociados al certificado. El plazo máximo que puede quedar suspendido un certificado por alguna de estas causas será de 30 días.

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

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

4.9.6. Entidad que puede solicitar la suspensión

Tanto el suscriptor del mismo como la propia Agencia de Tecnología y Certificación Electrónica podrán solicitar la suspensión de un certificado emitido por ésta.

4.9.7. Procedimiento para la solicitud de suspensión

La suspensión de un certificado iniciada por el suscriptor deberá realizarse por vía telefónica, mediante llamada telefónica al número de soporte telefónico de la Agencia de Tecnología y Certificación Electrónica 902482481.

4.9.8. Límites del período de suspensión

El período de suspensión de la vigencia de los certificados será normalmente de 15 días, salvo que la resolución judicial o administrativa que lo dictamine imponga un plazo superior o inferior, para lo cual, se estará al mismo.

4.9.9. Frecuencia de emisión de CRLs

La ACCV publicará una nueva CRL en su repositorio en intervalos de máximo 3 horas, aunque no se hayan producido modificaciones en la misma (cambios de estado de certificados) durante el citado periodo.

4.9.10. Requisitos de comprobación de CRLs

La verificación del estado de los certificados es obligatoria para cada uso de los certificados de entidades finales. Esta comprobación puede hacerse a través de la consulta de la CRL o de otros mecanismos dispuestos por la ACCV.

Los terceros confiantes deberán comprobar la validez de la CRL previamente a cada uno de sus usos y descargarse la nueva CRL del repositorio de la ACCV al finalizar el periodo de validez de la que posean.

Los certificados revocados permanecen en la CRL hasta que alcanzan su fecha de expiración. Alcanzada ésta, se eliminan de la Lista de Certificados Revocados, ante su imposibilidad de ser utilizados por estar caducados.

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

La ACCV proporciona un servidor OCSP para la verificación on-line del estado de los certificados en la URL ocsp.accv.es:80

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

El servidor OCSP es de libre acceso y no existe ningún requisito para su uso excepto los derivados del uso del propio protocolo OCSP según se define en el RFC 2560.

La ACCV dispone también de servicios web de consulta del estado de validez de los certificados expedidos.

4.9.13. Otras formas de divulgación de información de revocación disponibles

Algunas Políticas de Certificación pueden dar soporte a otras formas de información sobre el estado de revocación, como los Puntos de Distribución de CRLs (CDP).

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

Cuando la Política de Certificación que sea de aplicación soporte otras formas de divulgación de información de revocación, los requerimientos para la comprobación de dicha información se especificarán en la propia Política de Certificación.

4.9.15. Requisitos especiales de renovación de claves comprometidas

No hay ninguna variación en las cláusulas anteriores cuando la revocación sea debida al compromiso de la clave privada.

4.10. Servicios de comprobación de estado de certificados.

Los sistemas CRLs y de consulta en línea del estado de los certificados están disponibles durante las 24 horas los 7 días de la semana.

4.11. Finalización de la suscripción.

La suscripción finaliza con la expiración o revocación del certificado.

4.12. Depósito y recuperación de claves.

La ACCV podrá realizar el depósito de los certificados y claves de cifrado, para determinado tipo de certificado personal y nunca los empleados para la identificación del suscriptor o la firma electrónica de documentos.

La ACCV almacenará estas claves cifradas e implementará aquellas medidas adicionales que puedan ser necesarias para impedir cualquier recuperación indebida de las mismas. El cifrado de las claves se realizará mediante algoritmos de seguridad contrastada.

Los detalles particulares se recogen en las Políticas de Certificación asociadas a cada tipo de certificado.

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 la 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.

5.1.2. Acceso físico

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

5.2.1.1. 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 la 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.

5.2.1.2. 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.

5.2.1.3. Administrador de Seguridad.

Debe cumplir y hacer cumplir las políticas de seguridad de la ACCV, y debe encargarse de cualquier aspecto relativo a la seguridad de la 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 la ACCV y de hacer cumplir las normas y políticas de seguridad. Debe colaborar con los Auditores en todo aquello que les sea requerido.

5.2.1.4. 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.

5.2.1.5. Operador de Punto de Registro de Usuario

Se encarga única y exclusivamente 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.

Dentro de este perfil, existe un subgrupo denominado “Operadores de Suspensión de CallCenter” que únicamente tienen privilegios para suspender certificados, tras recibir la solicitud telefónica de revocación por el titular del certificado.

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

5.2.1.6. 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 la 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 la 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.

5.2.1.7. Responsable de Seguridad

Debe cumplir y hacer cumplir las políticas de seguridad de la ACCV, y debe encargarse de cualquier aspecto relativo a la seguridad de la 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 la 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.

5.2.1.8. 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 la ACCV y personal de la ACCV, como en los PRUs.

5.2.1.9. 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.

5.2.1.10. Responsable de Documentación

Se encargará de mantener el repositorio de documentación electrónica de la 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 será el único habilitado para almacenar, borrar o modificar documentos en el repositorio de documentación de la 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.

5.2.1.11. 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 la 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.

5.2.1.12. 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 la 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 la ACCV.

5.3. Controles de seguridad de personal

Este apartado refleja el contenido del documento *Controles de Seguridad del Personal* de la 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 especifica para su puesto.
- Titulo académico o experiencia en la industria equivalente

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.

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, la ACCV suspenderá el acceso de las personas involucradas a todos los sistemas de información de la 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. Requerimientos de contratación de personal

Todo el personal de la ACCV está sujeto al deber de secreto mediante la firma del acuerdo de confidencialidad al incorporarse a su puesto. En dicho acuerdo, además, se obliga a desarrollar sus tareas de acuerdo con esta Declaración de Prácticas de Certificación, la Política de Seguridad de la Información de la ACCV y los procedimientos aprobados de la ACCV.

5.3.8. Documentación proporcionada al personal

Al personal que se incorpora a la 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 la 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 en Nixval
- Supresión privilegio acceso al CPD secundario en CETESI
- Supresión privilegio acceso a salas de informática y despachos de Pl . Cánovas del Castillo, 1

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 la 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 la 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 la ACCV de la marcha de individuo y de que ya no representa a la ACCV.

5.3.10.6. Devolución de material

Se deberá verificar la devolución del material proporcionado por la 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 XRAO

5.4. Procedimientos de Control de Seguridad

5.4.1. Tipos de eventos registrados

La 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

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

La ACCV retendrá todos los registros de auditoría 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

Cada histórico de auditoría que contenga esos registros se cifra usando la clave pública de un certificado que se emitirá para la función de auditoría de la . Las copias de backup de dichos registros se almacenan en un archivo ignífugo cerrado dentro de las instalaciones seguras de la ACCV.

La destrucción de un archivo de auditoría solo se puede llevar a cabo con la autorización del Administrador del Sistema, el Responsable de Seguridad y del Auditor de ACCV. Tal destrucción se puede iniciar por la recomendación por escrito de cualquiera de estas tres entidades o del administrador del servicio auditado.

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 la 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 la ACCV es una combinación de procesos automáticos y manuales ejecutados por los sistemas operativos, las aplicaciones de la ACCV, y por el personal que las opera.

5.4.7. Notificación al sujeto causa del evento

No estipulado.

5.4.8. Análisis de vulnerabilidades

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

Es responsabilidad de los coordinadores de los equipos de análisis el informar a la 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 la 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 la 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 la 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 la 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 vidad de los certificados emitidos por la 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 la 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 la 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 la ACCV.

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

Los sistemas de la 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 la 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 la 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

Los procedimientos para proporcionar una nueva clave pública a los usuarios de una CA se especificarán en la Política de Certificación correspondiente a cada tipo de certificado.

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

En el caso de una indisponibilidad de las instalaciones de la ACCV por un periodo superior a seis horas, se procederá a la activación del Plan de Continuación del Servicio de la ACCV. El Plan de Continuidad garantiza que los servicios identificados como críticos por su requerimiento de disponibilidad, estén disponibles en el CPD de continuidad en menos de 12 horas, tras la activación del Plan.

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

Si los recursos hardware, software, y/o datos se alteran o son sospechosos de haber sido alterados se detendrá el funcionamiento de los servicios de la ACCV hasta el restablecimiento de un entorno

seguro con la incorporación de nuevos componentes de eficiencia acreditable. De forma paralela se realizará una auditoría para identificar la causa de la alteración y asegurar la no reproducción de la misma.

En el caso de verse afectados certificados emitidos, se notificará del hecho a los suscriptores de los mismos y se procederá a su recertificación.

5.7.2. La clave pública de una entidad se revoca

En el caso de la revocación del certificado de una entidad de la ACCV se generará y publicará la correspondiente CRL, se detendrá el funcionamiento de la entidad y se procederá a la generación, certificación y puesta en marcha de una nueva entidad con la misma denominación que la eliminada y con un nuevo par de claves.

En el caso que la entidad afectada sea una CA el certificado revocado de la entidad permanecerá accesible en el repositorio de la ACCV con objeto de continuar permitiendo la verificación de los certificados emitidos durante su periodo de funcionamiento.

Las entidades componentes de la ACCV dependientes de la entidad renovada serán informadas del hecho y conminadas a solicitar su recertificación por la nueva instancia de la entidad.

5.7.3. La clave de una entidad se compromete

En el caso de compromiso de la clave de una entidad se procederá a su revocación inmediata según lo expuesto en el punto anterior y se informará del hecho al resto de entidades que componen la ACCV dependientes o no de la entidad afectada.

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

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

En caso de desastre natural que afecte a las instalaciones del Centro de Proceso de Datos principal de la ACCV y, por tanto, a los servicios que desde éste se prestan, se activará el Plan de Continuidad del Servicio, garantizándose que los servicios identificados como críticos por su requerimiento de disponibilidad, estén disponibles en el CPD de continuidad en menos de 12 horas, tras la activación del Plan, y el resto de servicios imprescindibles dentro de 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 la ACCV son:

- Compromiso de la clave privada de la CA
- Decisión política por parte del Consejo de Dirección de la Agencia de Tecnología y Certificación Electrónica

En caso de cese de su actividad como Prestador de Servicios de Certificación, la ACCV realizará, con una antelación mínima de dos meses, las siguientes acciones:

- Informar a todos los suscriptores de sus certificados y extinguir la vigencia de los mismos revocándolos.
- Informar a todas las terceras partes con las que tenga que haya firmado un convenio de certificación.

- Comunicar al Ministerio competente en materia de Sociedad de la Información y firma electrónica 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 materia de Sociedad de la Información y firma electrónica toda la información relativa a los certificados electrónicos revocados para que éste se haga cargo de su custodia.

6. Controles de seguridad técnica

6.1. Generación e Instalación del Par de Claves

6.1.1. Generación del par de claves

Los pares de claves para todos los componentes internos de la ACCV se generan en módulos de hardware criptográficos con certificación FIPS 140-1 Nivel 4.

Los pares de claves para entidades finales se generan en función de lo estipulado en la Política de Certificación aplicable.

6.1.2. Entrega de la clave privada a la entidad

En los casos en los que la generación de las claves no se realice mediante medios bajo control de la propia entidad final será la Política de Certificación correspondiente la que especifique el procedimiento a emplear para realizar la entrega de la clave privada a las entidades finales.

6.1.3. Entrega de la clave publica al emisor del certificado

Las claves públicas generadas por medios bajo el control de las entidades finales se envían a la ACCV como parte de una solicitud de certificación en formato PKCS#10, firmado digitalmente con la clave privada correspondiente a la clave pública que se solicita certificar.

6.1.4. Entrega de la clave pública de la CA a los usuarios

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

6.1.5. Tamaño de las claves

Las claves de la Root CA y las autoridades de certificación que se encuentran en la misma jerarquía son claves RSA de 2048 bits de longitud.

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.

El tamaño de las claves para cada tipo de certificado emitido por la ACCV se establece en la Política de Certificación que le es de aplicación. En todo caso, su tamaño nunca será inferior a 1.024 bits.

6.1.6. Parámetros de generación de la clave pública

Las claves de las autoridades de certificación Root CA y ACCVRAIZ1, así como las diferentes CAs integradas en cada una de las dos jerarquías están creadas con el algoritmo RSA

Los parámetros de generación de claves para cada tipo de certificado emitido por la ACCV vienen definidos por la Política de Certificación que le sea de aplicación.

6.1.7. Comprobación de la calidad de los parámetros

Los procedimientos y medios de comprobación de la calidad de los parámetros de generación de claves para cada tipo de certificado emitido por la ACCV vienen definidos por la Política de Certificación que le sea de aplicación.

6.1.8. Hardware/software de generación de claves

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

Los dispositivos hardware o software a utilizar en la generación de claves para cada tipo de certificado emitido por la ACCV viene definido por la Política de Certificación que le sea de aplicación.

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

6.1.9. Fines del uso de la clave

Los fines del uso de la clave para cada tipo de certificado emitido por la ACCV vienen definidos por la Política de Certificación que le sea de aplicación.

Todos los certificados emitidos por la ACCV contienen las extensiones *KEY USAGE* y *EXTENDED KEY USAGE* definidas por el estándar X.509 v3 para la definición y limitación de tales fines.

6.2. Protección de la Clave Privada

6.2.1. Estándares para los módulos criptográficos

Se requiere que los módulos utilizados para la creación de claves utilizadas por las diferentes autoridades de certificación de ambas jerarquías dispongan de un nivel de certificación de seguridad suficiente para la funcionalidad y seguridad que se exige.

6.2.2. Control multipersona 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.

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 la ACCV se encuentran alojadas en dispositivos de hardware criptográfico con certificación FIPS 140-1 de nivel 4.

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

6.2.4. Copia de seguridad de la clave privada

Las copias de backup de las claves privadas de componentes de la ACCV se almacenan cifradas en archivos seguros ignífugos.

6.2.5. Archivo de la clave privada.

Las copias de backup de las claves privadas en custodia cifradas en archivos seguros ignífugos.

6.2.6. Introducción de la clave privada en el módulo criptográfico.

Las claves privadas se crean en el módulo criptográfico en el momento de la creación de cada una de las entidades de la ACCV que hacen uso de dichos módulos.

6.2.7. Método de activación de la clave privada.

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. Método de desactivación de la clave privada

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

6.2.9. 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 sustraido.

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

6.2.9.1. 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.

6.2.9.2. 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.

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

6.3.1. Archivo de la clave pública

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

6.3.2. Periodo de uso para las claves públicas y privadas

El certificado de Root CA GVA tiene una validez de veinte (20) años y el de sus CAs subordinadas de diez (10) años. 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. Las Autoridades de Registro y el resto de entidades de la ACCV de tres (3) años.

El periodo de validez de los certificados de entidades finales vendrá establecido por la Política de Certificación aplicable en cada caso, y en ningún caso superará los cuatro (4) años de validez máxima.

6.4. Datos de activación

6.4.1. Generación y activación de los datos de activación

Los datos de activación de las Autoridades de Certificación de la ACCV se generan y almacenan en smart cards criptográficas en posesión de personal autorizado.

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.

6.4.3. Otros aspectos de los datos de activación

No estipulado.

6.5. Controles de Seguridad Informática

Los datos concernientes a este apartado se considera información confidencial y solo se proporciona a quien acredite la necesidad de conocerlos.

6.6. Controles de Seguridad del Ciclo de Vida.

La datos concernientes a este apartado se considera información confidencial y solo se proporciona a quien acredite la necesidad de conocerlos.

6.7. Controles de Seguridad de la Red

La datos concernientes a este apartado se considera información confidencial y solo se proporciona a quien acredite la necesidad de conocerlos.

6.8. Controles de Ingeniería de los Módulos Criptográficos

La ACCV utiliza módulos criptográficos hardware y software disponibles comercialmente desarrollados por terceros.

La ACCV únicamente utiliza módulos criptográficos con un nivel de certificación de seguridad suficiente para la funcionalidad y seguridad que se exige.

7. Perfiles de certificados y listas de certificados revocados

7.1. Perfil de Certificado

7.1.1. Número de versión

La 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

Las extensiones utilizadas de forma genérica en los certificados son:

- Key Usage. Marcada como crítica.
- Basic Constraint. Marcada como critica.
- Certificate Policies. Marcada como critica.
- Subject Alternative Name. Marcada como no critica.
- CRL Distribution Point. Marcada como no crítica.

Las Políticas de Certificación de la ACCV pueden establecer variaciones en conjunto de las extensiones utilizadas por cada tipo de certificado.

7.1.3. Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

- md5withRSAEncryption (1.2.840.113549.1.1.4)
- SHA1withRSAEncryption (1.2.840.113549.1.1.5)

7.1.4. Formatos de nombres

Los certificados emitidos por la ACCV contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

7.1.5. Restricciones de los nombres

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

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

A definir por cada Política de Certificación.

La 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 la ACCV comienzan con el prefijo 1.3.6.1.4.1.8149.3

7.1.7. Uso de la extensión "Policy Constraints"

No estipulado

7.1.8. Sintaxis y semántica de los cualificadores de política

No estipulado

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

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

7.2. Perfil de CRL

7.2.1. Número de versión

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

7.2.2. CRL y extensiones

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

8. Auditoría de conformidad

8.1. Frecuencia de los controles de conformidad para cada entidad

Se llevará a cabo una auditoría sobre la ACCV, al menos una vez al año, para garantizar la adecuación de su funcionamiento y operativa con las disposiciones incluidas en esta CPS.

Se llevarán a cabo otras auditorías técnicas y de seguridad según lo establecido en la Política de Auditoría de la ACCV, entre las que se incluye una auditoría de cumplimiento de la legislación de protección de datos de carácter personal.

8.2. Identificación/cualificación del auditor

El auditor será seleccionado en el momento de la realización de cada auditoría.

Cualquier empresa o persona contratada para realizar una auditoría de seguridad sobre la ACCV deberá cumplir con los siguientes requisitos:

- Adecuada y acreditada capacitación y experiencia en PKI, seguridad y procesos de auditoría de sistemas de información.
- Independencia a nivel organizativo de la autoridad de la ACCV, para el caso de auditorías externas.

8.3. Relación entre el auditor y la entidad auditada

Al margen de la función de auditoría, el auditor y la parte auditada (la 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 la ACCV, el auditor tendrá la consideración de Encargado de Tratamiento, en virtud de lo previsto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de Diciembre.

8.4. Tópicos cubiertos por el control de conformidad

La auditoría determinará la conformidad de los servicios de la ACCV con esta CPS 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
- CPS y CP's vigentes
- Contratos
- Política de privacidad

8.5. Acciones a tomar como resultado de una deficiencia.

La identificación de deficiencias en la auditoría dará lugar a la adopción de medidas correctivas. La Gerencia de la Agencia de Tecnología y Certificación Electrónica, en colaboración con el auditor será la responsable de la determinación de las mismas.

En el caso de una deficiencia grave, la Gerencia de la Agencia de Tecnología y Certificación Electrónica podrá determinar la suspensión temporal de las operaciones de la ACCV hasta que las deficiencias se corrijan, la revocación del certificado de la entidad, cambios en el personal, etc.

8.6. Comunicación de resultados

El auditor comunicará los resultados de la auditoría a la Gerencia de la Agencia de Tecnología y Certificación Electrónica, en tanto que responsable de la dirección y gestión de las actividades de la ACCV, al Responsable de Seguridad de la ACCV, así como a los responsables de las distintas áreas en las que se detecten no conformidades.

9. Requisitos comerciales y legales

9.1. Tarifas

9.1.1. Tarifas de emisión de certificado o renovación

Las tarifas de emisión y revocación de cada certificado se especifican en la Política de Certificación que le sea de aplicación.

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 CPS ni las políticas de certificación administradas por la 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

En el caso que alguna Política de Certificación especifique alguna tarifa aplicable a la prestación de servicios de certificación o revocación por parte de la ACCV para el tipo de certificados que defina, será obligación de esa política la especificación de la política de reintegros correspondiente.

9.2. Capacidad financiera

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

La ACCV dispone de garantía de cobertura suficiente de responsabilidad civil a través de aval bancario emitido por la Caja de Ahorros de Valencia, Castellón y Alicante, Bancaja, por importe de Tres Millones de Euros (3.000.000 €) que cubre el riesgo de la responsabilidad por los daños y perjuicios que pudiera ocasionar el uso de los certificados expedidos por esta Autoridad de Certificación, cumpliendo así con la obligación establecida en el artículo 20.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

9.2.2. Relaciones fiduciarias

La ACCV no se desempeña como agente fiduciario ni representante en forma alguna de suscriptores ni de terceros que confían en los certificados emitidos por la ACCV.

9.2.3. Procesos administrativos

La ACCV garantiza la realización de auditorías de los procesos y procedimientos establecidos de manera regular. Estas auditorías se llevarán a cabo tanto de manera interna como externa.

9.3. Política de Confidencialidad

9.3.1. 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 la ACCV.
- Las claves privadas de suscriptores de las que la ACCV mantenga en custodia.
- Toda información relativa a las operaciones que lleve a cabo la ACCV.
- Toda información relativa a los parámetros de seguridad, control y procedimientos de auditoría.
- Toda la información de carácter personal proporcionada a la 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 la 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

La ACCV considera información de acceso público:

- La contenida en la Declaración de Prácticas de Certificación aprobada por la ACCV.
- La contenida en las diferentes Políticas de Certificación aprobadas por la 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 CPS y las CP’s de la 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 la 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. Divulgación de información de revocación /suspensión de certificados

La información relativa a la revocación o suspensión de certificados se proporciona vía CRL en el directorio LDAP que actúa como repositorio de la ACCV

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

9.4. Protección de datos personales

La 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 la ACCV.

9.4.1. Plan de Protección de Datos Personales.

En cumplimiento con los requisitos establecidos por cada una de las Políticas de Certificación de la ACCV, y de acuerdo con lo dispuesto en el artículo 19 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, toda información de carácter personal proporcionada a la ACCV por los suscriptores de sus certificados será tratada de acuerdo con los términos de la "Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal".

En este sentido, la 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 modificado mediante las siguientes órdenes:

- 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)
- (Estamos pendientes de la aprobación de la última orden donde solicitamos figurar directamente nosotros como titulares)

En él 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 la 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 el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, la ACCV dispone de un Documento de Seguridad 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.

En cumplimiento de los requisitos establecidos por las concretas políticas de certificados de la ACCV, y de acuerdo con el artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, toda información de carácter personal proporcionada a la ACCV por los suscriptores de sus certificados será tratada de acuerdo con los términos de la "Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal".
En este sentido se informa que existe un fichero de Usuarios de Firma Electrónica, creado mediante Orden de 8 de marzo de 2002, (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), y modificado mediante 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).

La ACCV dispone de un Documento de Seguridad, que responde a la obligación establecida en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

9.4.2. Información considerada privada.

De conformidad con lo establecido en el artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se consideran datos de carácter personal cualquier información relativa a personas físicas identificadas o identificables.

Tanto la información personal que no haya de ser incluida en los certificados como el mecanismo de comprobación del estado de los certificados, se consideran 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 la 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 conformidad con la Ley Orgánica 15/1999 la información confidencial está protegida frente a su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

En ningún caso la ACCV incluye en los certificados electrónicos que expide, los datos a los que se hace referencia en el artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

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.

Dicha información, proporcionada en la solicitud de certificados en los términos que se prevén en el artículo 17.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, es incluida en sus certificados y en el mecanismo de comprobación del estado de los certificados.

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 la 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 la ACCV.

9.4.4. Responsabilidades.

La ACCV garantiza el cumplimento de sus obligaciones legales como prestador de servicios de certificación, de conformidad con la Ley 59/2003, de 19 de diciembre, y en virtud de esto, y de acuerdo con el artículo 22 de dicha Ley, responderá por los daños y perjuicios que cause en el ejercicio de la actividad que le es propia, por el incumplimiento de las prescripciones contenidas en el artículo 17 de la Ley 59/2003, relativas a la protección de datos personales.

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

Para la prestación del servicio, la 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.

La 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, la ACCV está obligada a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tengan atribuidas, y en el resto de supuestos previstos en el artículo 11.2 de la LOPD donde así se requiera.

9.4.7. Otros supuestos de divulgación de la información.

La 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 incluyendo los referidos a certificados y CRL's emitidos por la ACCV, OIDs, la presente CPS, las Políticas de Certificación que le son de aplicación, así como cualquier otro documento, electrónico o de cualquier otro tipo, propiedad de la ACCV, pertenecen a la ACCV.

Las claves privadas y las claves públicas son propiedad del usuario, independientemente del medio físico que se emplee para su almacenamiento.

El suscriptor conserva cualquier derecho que pudiere ostentar sobre la marca producto o nombre comercial contenido en el certificado.

9.6. Obligaciones y Responsabilidad Civil

9.6.1. Obligaciones de la Entidad de Certificación

La Agencia de Tecnología y Certificación Electrónica está obligada:

- Realizar sus operaciones en conformidad con esta CPS.
- 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 reconocidos 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.
- Publicar sin alteración los certificados emitidos en el directorio LDAP de la ACCV (ldap.accv.es).
- 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 directorio LDAP de la ACCV (ldap.accv.es), con la frecuencia estipulada en el punto *Frecuencia de emisión de CRLs* de este documento.
- Publicar esta CPS y las CP aplicables en el sitio web www.accv.es/cps, 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 la ACCV para validar la renovación de sus propias claves.
- Operar de acuerdo con la legislación aplicable. En concreto con:

    1. Decreto 87/2002, de 30 de mayo, del Gobierno Valenciano, por el que se regula la utilización de la firma electrónica avanzada en la Generalitat Valenciana.
    2. Decreto 96/1998 de 6 de julio del Gobierno Valenciano, por el que se regulan la organización de la función informática, la utilización de sistemas de información y el Registro de Ficheros informatizados en el ámbito de la administración de la Generalitat Valenciana.
    3. Orden de 3 de diciembre de 1999, de la Conselleria de Justicia y Administraciones Públicas por la que se aprueba el Reglamento Técnico de Medidas

de Seguridad para la Aprobación y Homologación de Aplicaciones y Medios de Tratamiento Automatizado de la Información

4. Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

5. La Orden de 21 de febrero de 2000 por la que se aprueba el reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de forma electrónica.

6. La Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica

7. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos

8. Ley 3/010, de 5 de mayo, de la Generalitat, de Administración Electrónica de la Comunitat Valenciana.

9. Decreto 21/2011, de 4 de marzo, del Consell, por el que se aprueba el Estatuto de la Agencia de Tecnología y Certificación Electrónica.

- 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 CPS.
- 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 la ACCV, así como al 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 reconocido 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

9.6.2. Obligaciones de la Autoridad de Registro

Las personas que operan en las RAs integradas en la jerarquía de la ACCV –operadores de Punto de Registro de Usuario– están obligadas a:

- Realizar sus operaciones en conformidad con esta CPS.
- 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 física del solicitante y la exhibición del DNI original y en vigor, o pasaporte español. En caso de usuarios extranjeros deberán mostrar la Tarjeta de Residencia / 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 la ACCV, la CPS 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.

- Cuando se trata de certificados personales, utilizar las herramientas de solicitud y tramitación de certificados en presencia de la persona para la que se realizará la solicitud, tras haber realizado una identificación fiable.

- 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 presenciales que reciba de manera inmediata, después de haber llevado a cabo una identificación fiable basada en el DNI del demandante, o en el NIE en el caso de extranjeros.

- 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 la 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 la 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 CPS.
- 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 la ACCV de cualquier modificación de esta información.
- Abonar en su caso los importes que se devenguen por los servicios de certificación que soliciten.

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

Es obligación de las partes que confíen en los certificados emitidos por la 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.

9.6.5. Obligaciones del repositorio

- Mantener accesible para las entidades finales el conjunto de certificados emitidos por la ACCV
- Mantener accesible para las entidades finales la información de los certificados que han sido revocados, en formato CRL.

9.7. Renuncias de garantías

La ACCV puede rechazar todas las garantías del servicio que no se encuentren vinculadas a obligaciones establecidas por la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, especialmente aquellas garantías de adaptación para un propósito particular o garantía de uso mercantil del certificado.

9.8. Limitaciones de responsabilidad

9.8.1. Garantías y limitaciones de garantías

La ACCV responderá por los daños y perjuicios que causen a cualquier persona, en el ejercicio de su actividad, cuando incumplan las obligaciones que le impone el Decreto 87/2002, de 30 de mayo, del Gobierno Valenciano, sobre Firma Electrónica Avanzada, y la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, o actúe con negligencia.

La 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 la ACCV, una vez tenga conocimiento de ello.

La 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.

La ACCV es la Agencia de Tecnología y Certificación Electrónica, que es una 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.

La ACCV sólo responderá de los daños y perjuicios causados por el uso indebido del certificado reconocido, 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 la ACCV Tampoco responderá la 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.

9.8.2. Deslinde de responsabilidades

Las Entidades de Registro de la 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 CPS.
- Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por la 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

9.8.3. Limitaciones de pérdidas

A excepción de lo establecido por las disposiciones de la presente CPS, la 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. Plazo y finalización.

9.9.1. Plazo.

La 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.

9.9.2. Finalización.

La 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.

9.9.3. Supervivencia.

La 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.

9.10. Notificaciones.

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las practicas descritas en esta CPS se realizará mediante documento o mensaje electrónico firmado digitalmente de conformidad con esta última o por escrito mediante correo certificado dirigido a cualquiera de las direcciones contenidas en el punto *1.5 Datos de contacto*. Las comunicaciones electrónicas se harán efectivas una vez que las reciba el destinatario al que van dirigidas.

9.11. Modificaciones.

La 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 la ACCV no puede vulnerar las disposiciones contenidas en las políticas de certificación establecidas por la ACCV.
- Se establece un control de modificaciones, basado en la Política de Gestión del Cambio de la ACCV.
- Se establecen las implicaciones que el cambio de especificaciones tiene sobre el usuario, y se prevé la necesidad de notificarle dichas modificaciones.

9.11.1. Procedimientos de especificación de cambios

La entidad con atribuciones para realizar y aprobar cambios sobre la CPS y las CP's de la ACCV es la Gerencia de la Agencia de Tecnología y Certificación Electrónica, cuyos datos de contacto se encuentran en el apartado 1.5.1. de esta CPS.

En aquellos supuestos en los que se considere por la Gerencia de la Agencia de Tecnología y Certificación Electrónica que la modificación de la CPS 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 CPS modificada.

En el supuesto de que la Gerencia de la Agencia de Tecnología y Certificación Electrónica juzgue que los cambios a la especificación vigente afecten 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 de Identificador de Objeto (OID) que lo representa. Este tipo de modificaciones se comunicará a los suscriptores de los certificados correspondientes a la CP o CPS modificada mediante el envío de una notificación a la dirección de correo electrónico que el usuario ha facilitado en la emisión del certificado, con una antelación de al menos 30 días a su publicación. El usuario puede aceptar las modificaciones o rechazarlas. En caso de rechazarlas, su certificado, emitido bajo las instrucciones de la anterior CPS será válido para los propósitos en ella incluidos, pero no para los propósitos específicos que se incluyen en la nueva CPS o CP modificada. Si transcurridos 15 días desde la

notificación al usuario no se tuviera respuesta del mismo, se considerará que el usuario no ha aceptado la modificación, aunque puede aceptarla en cualquier momento posterior.

9.11.2. 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 la ACCV www.accv.es.

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

La Gerencia de la Agencia de Tecnología y Certificación Electrónicaes 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 Gerencia de la Agencia de Tecnología y Certificación Electrónica la aprobación y autorización de las modificaciones de dichos documentos.

9.12. Resolución de conflictos.

9.12.1. Resolución extrajudicial de conflictos.

La 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.

9.12.2. Jurisdicción competente.

Los conflictos que se plateen en la prestación por la 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.

9.13. Legislación aplicable

El funcionamiento y operaciones de la ACCV, así como la presente CPS están regidos por la legislación comunitaria, estatal y valenciana vigente en cada momento.

Explícitamente se asumen como de aplicación las siguientes normas:

Decreto 87/2002, de 30 de mayo, del Gobierno Valenciano por el que se regula la utilización de la firma electrónica avanzada en la Generalitat Valenciana.

- Decreto 96/1998 de 6 de julio del Gobierno Valenciano, por el que se regulan la organización de la función informática, la utilización de sistemas de información y el Registro de Ficheros informatizados en el ámbito de la administración de la Generalitat Valenciana.

- Orden de 3 de diciembre de 1999, de la Conselleria de Justicia y Administraciones Públicas por la que se aprueba el Reglamento Técnico de Medidas de Seguridad para la Aprobación y Homologación de Aplicaciones y Medios de Tratamiento Automatizado de la Información

- Ley 59/2003, de 19 de diciembre, de firma electrónica.

- La Orden de 21 de febrero de 2000 por la que se aprueba el reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de forma electrónica.
- La Directiva 11999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos
- Ley 3/2010, de 5 de mayo, de la Generalitat, de Administración Electrónica de la Comunitat Valenciana
- Decreto 21/2011, de 4 de marzo, del Consell, por el que se aprueba el Estatuto de la Agencia de Tecnología y Certificación Electrónica.

9.14. . Conformidad con la Ley aplicable.

La ACCV declara que la presente CPS cumple con las prescripciones contenidas en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

9.15. Cláusulas diversas.

Sin estipulación adicional.