



**Agencia de Tecnología
y Certificación Electrónica**

Política de Certificación de Certificados Cualificados en dispositivo seguro de pertenencia a empresa

| | |
|--|-------------------------------|
| Fecha: 15/06/2017 | Versión: 4.0 |
| Estado: APROBADO | Nº de páginas: 45 |
| OID: 1.3.6.1.4.1.8149.3.20.4.0 | Clasificación: PÚBLICO |
| Archivo: ACCV-CP-20V4.0.doc | |
| Preparado por: Agencia de Tecnología y Certificación Electrónica - ACCV | |

Este documento es propiedad del Institut Valencià de Finances - ACCV.
Queda prohibida su reproducción total o parcial sin autorización previa del
Institut Valencià de Finances - ACCV

Tabla de Contenido

| | |
|--|-----------|
| 1. INTRODUCCIÓN..... | 9 |
| 1.1. PRESENTACIÓN..... | 9 |
| 1.2. IDENTIFICACIÓN..... | 9 |
| 1.3. COMUNIDAD DE USUARIOS Y ÁMBITO DE APLICACIÓN..... | 10 |
| 1.3.1. <i>Autoridades de Certificación</i> | 10 |
| 1.3.2. <i>Autoridades de Registro</i> | 10 |
| 1.3.3. <i>Usuarios Finales</i> | 10 |
| 1.3.3.1. Suscriptores..... | 10 |
| 1.3.3.2. Partes confiantes..... | 10 |
| 1.4. USO DE LOS CERTIFICADOS..... | 10 |
| 1.4.1. <i>Usos Permitidos</i> | 10 |
| <i>Usos prohibidos</i> | 11 |
| 1.5. POLÍTICA DE ADMINISTRACIÓN DE LA ACCV..... | 11 |
| 1.5.1. <i>Especificación de la Organización Administradora</i> | 11 |
| 1.5.2. <i>Persona de Contacto</i> | 11 |
| 1.5.3. <i>Competencia para determinar la adecuación de la CPS a la Políticas</i> | 11 |
| 1.6. DEFINICIONES Y ACRÓNIMOS..... | 11 |
| 1.6.1. <i>Definiciones</i> | 11 |
| 1.6.2. <i>Acrónimos</i> | 11 |
| 2. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS..... | 12 |
| 2.1. REPOSITORIO DE CERTIFICADOS..... | 12 |
| 2.2. PUBLICACIÓN..... | 12 |
| 2.3. FRECUENCIA DE ACTUALIZACIONES..... | 12 |
| 2.4. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS..... | 12 |
| 3. IDENTIFICACIÓN Y AUTENTICACIÓN..... | 13 |
| 3.1. REGISTRO DE NOMBRES..... | 13 |
| 3.1.1. <i>Tipos de nombres</i> | 13 |
| 3.1.2. <i>Significado de los nombres</i> | 13 |
| 3.1.3. <i>Interpretación de formatos de nombres</i> | 13 |
| 3.1.4. <i>Unicidad de los nombres</i> | 13 |
| 3.1.5. <i>Resolución de conflictos relativos a nombres</i> | 13 |
| 3.1.6. <i>Reconocimiento, autenticación y función de las marcas registradas</i> | 13 |
| 3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD..... | 13 |
| 3.2.1. <i>Métodos de prueba de posesión de la clave privada</i> | 13 |

| | | |
|----------------------|--------------------------------|--------------|
| Cif.: PUBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 2 |

| | |
|--|-----------|
| 3.2.2. Autenticación de la identidad de una organización..... | 13 |
| 3.2.3. Autenticación de la identidad de un individuo..... | 13 |
| 3.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DEL PAR DE CLAVES..... | 14 |
| 3.3.1. Identificación y autenticación de las solicitudes de renovación rutinarias..... | 14 |
| 3.3.2. Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida..... | 14 |
| 3.4. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DEL PAR DE CLAVES..... | 14 |
| 4. EL CICLO DE VIDA DE LOS CERTIFICADOS..... | 16 |
| 4.1. SOLICITUD DE CERTIFICADOS..... | 16 |
| 4.2. TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADOS..... | 16 |
| 4.3. EMISIÓN DE CERTIFICADOS..... | 16 |
| 4.4. ACEPTACIÓN DE CERTIFICADOS..... | 17 |
| 4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO..... | 17 |
| 4.6. RENOVACIÓN DE CERTIFICADOS..... | 17 |
| 4.7. RENOVACIÓN DE CLAVES..... | 17 |
| 4.8. MODIFICACIÓN DE CERTIFICADOS..... | 17 |
| 4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS..... | 17 |
| 4.9.1. Circunstancias para la revocación..... | 17 |
| 4.9.2. Entidad que puede solicitar la revocación..... | 17 |
| 4.9.3. Procedimiento de solicitud de revocación..... | 17 |
| 4.9.3.1. Presencial..... | 17 |
| 4.9.3.2. Telemático..... | 17 |
| 4.9.3.3. Telefónico..... | 18 |
| 4.9.4. Periodo de gracia de la solicitud de revocación..... | 18 |
| 4.9.5. Circunstancias para la suspensión..... | 18 |
| 4.9.6. Entidad que puede solicitar la suspensión..... | 18 |
| 4.9.7. Procedimiento para la solicitud de suspensión..... | 18 |
| 4.9.8. Límites del período de suspensión..... | 18 |
| 4.9.9. Frecuencia de emisión de CRLs..... | 18 |
| 4.9.10. Requisitos de comprobación de CRLs..... | 18 |
| 4.9.11. Disponibilidad de comprobación on-line de revocación y estado..... | 18 |
| 4.9.12. Requisitos de comprobación on-line de revocación..... | 18 |
| 4.9.13. Otras formas de divulgación de información de revocación disponibles..... | 18 |
| 4.9.14. Requisitos de comprobación para otras formas de divulgación de información de revocación..... | 18 |
| 4.9.15. Requisitos especiales de renovación de claves comprometidas..... | 19 |
| 4.10. SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS..... | 19 |
| 4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN..... | 19 |
| 4.12. DEPÓSITO Y RECUPERACIÓN DE CLAVES..... | 19 |

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PUBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 3 |

| | |
|---|-----------|
| 4.13. CADUCIDAD DE LAS CLAVES DE CERTIFICADO DE CA..... | 19 |
| 5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES..... | 20 |
| 5.1. CONTROLES DE SEGURIDAD FÍSICA..... | 20 |
| 5.1.1. Ubicación y construcción..... | 20 |
| 5.1.2. Acceso físico..... | 20 |
| 5.1.3. Alimentación eléctrica y aire acondicionado..... | 20 |
| 5.1.4. Exposición al agua..... | 20 |
| 5.1.5. Protección y prevención de incendios..... | 20 |
| 5.1.6. Sistema de almacenamiento..... | 20 |
| 5.1.7. Eliminación de residuos..... | 20 |
| 5.1.8. Backup remoto..... | 20 |
| 5.2. CONTROLES DE PROCEDIMIENTOS..... | 20 |
| 5.2.1. Papeles de confianza..... | 20 |
| 5.2.2. Número de personas requeridas por tarea..... | 20 |
| 5.2.3. Identificación y autenticación para cada papel..... | 20 |
| 5.3. CONTROLES DE SEGURIDAD DE PERSONAL..... | 21 |
| 5.3.1. Requerimientos de antecedentes, calificación, experiencia, y acreditación..... | 21 |
| 5.3.2. Procedimientos de comprobación de antecedentes..... | 21 |
| 5.3.3. Requerimientos de formación..... | 21 |
| 5.3.4. Requerimientos y frecuencia de actualización de la formación..... | 21 |
| 5.3.5. Frecuencia y secuencia de rotación de tareas..... | 21 |
| 5.3.6. Sanciones por acciones no autorizadas..... | 21 |
| 5.3.7. Requerimientos de contratación de personal..... | 21 |
| 5.3.8. Documentación proporcionada al personal..... | 21 |
| 5.3.9. Controles periódicos de cumplimiento..... | 21 |
| 5.3.10. Finalización de los contratos..... | 21 |
| 5.4. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD..... | 21 |
| 5.4.1. Tipos de eventos registrados..... | 21 |
| 5.4.2. Frecuencia de procesado de logs..... | 21 |
| 5.4.3. Periodo de retención para los logs de auditoría..... | 21 |
| 5.4.4. Protección de los logs de auditoría..... | 22 |
| 5.4.5. Procedimientos de backup de los logs de auditoría..... | 22 |
| 5.4.6. Sistema de recogida de información de auditoría (interno vs externo)..... | 22 |
| 5.4.7. Notificación al sujeto causa del evento..... | 22 |
| 5.4.8. Análisis de vulnerabilidades..... | 22 |
| 5.5. ARCHIVO DE INFORMACIONES Y REGISTROS..... | 22 |
| 5.5.1. Tipo de informaciones y eventos registrados..... | 22 |
| 5.5.2. Periodo de retención para el archivo..... | 22 |

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PUBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 4 |

| | |
|--|-----------|
| 5.5.3. Protección del archivo..... | 22 |
| 5.5.4. Procedimientos de backup del archivo..... | 22 |
| 5.5.5. Requerimientos para el sellado de tiempo de los registros..... | 22 |
| 5.5.6. Sistema de recogida de información de auditoría (interno vs externo)..... | 22 |
| 5.5.7. Procedimientos para obtener y verificar información archivada..... | 22 |
| 5.6. CAMBIO DE CLAVE..... | 22 |
| 5.7. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O DE DESASTRE..... | 23 |
| 5.7.1. Alteración de los recursos hardware, software y/o datos..... | 23 |
| 5.7.2. La clave pública de una entidad se revoca..... | 23 |
| 5.7.3. La clave de una entidad se compromete..... | 23 |
| 5.7.4. Instalación de seguridad después de un desastre natural u otro tipo de desastre..... | 23 |
| 5.8. CESE DE UNA CA..... | 23 |
| 6. CONTROLES DE SEGURIDAD TÉCNICA..... | 24 |
| 6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES..... | 24 |
| 6.1.1. Generación del par de claves..... | 24 |
| 6.1.2. Entrega de la clave privada a la entidad..... | 24 |
| 6.1.3. Entrega de la clave pública al emisor del certificado..... | 24 |
| 6.1.4. Entrega de la clave pública de la CA a los usuarios..... | 24 |
| 6.1.5. Tamaño de las claves..... | 24 |
| 6.1.6. Parámetros de generación de la clave pública..... | 24 |
| 6.1.7. Comprobación de la calidad de los parámetros..... | 25 |
| 6.1.8. Hardware/software de generación de claves..... | 25 |
| 6.1.9. Fines del uso del par de claves..... | 25 |
| 6.2. PROTECCIÓN DE LA CLAVE PRIVADA..... | 25 |
| 6.2.1. Estándares para los módulos criptográficos..... | 25 |
| 6.2.2. Control multipersona de la clave privada..... | 25 |
| 6.2.3. Custodia de la clave privada..... | 25 |
| 6.2.4. Copia de seguridad de la clave privada..... | 26 |
| 6.2.5. Archivo de la clave privada..... | 26 |
| 6.2.6. Introducción de la clave privada en el módulo criptográfico..... | 26 |
| 6.2.7. Método de activación de la clave privada..... | 26 |
| 6.2.8. Método de desactivación de la clave privada..... | 26 |
| 6.2.9. Método de destrucción de la clave privada..... | 26 |
| 6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES..... | 26 |
| 6.3.1. Archivo de la clave pública..... | 26 |
| 6.3.2. Periodo de uso para las claves públicas y privadas..... | 26 |
| Los certificados emitidos al amparo de la presente política tienen una validez de tres (3) años..... | 26 |
| 6.4. DATOS DE ACTIVACIÓN..... | 26 |

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PUBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 5 |

| | |
|---|-----------|
| 6.4.1. Generación y activación de los datos de activación..... | 26 |
| 6.4.2. Protección de los datos de activación..... | 27 |
| 6.4.3. Otros aspectos de los datos de activación..... | 27 |
| 6.5. CONTROLES DE SEGURIDAD INFORMÁTICA..... | 27 |
| 6.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA..... | 27 |
| 6.7. CONTROLES DE SEGURIDAD DE LA RED..... | 27 |
| 6.8. CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS..... | 27 |
| 7. PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS..... | 28 |
| 7.1. PERFIL DE CERTIFICADO..... | 28 |
| 7.1.1. Número de versión..... | 28 |
| 7.1.2. Extensiones del certificado..... | 28 |
| 7.1.3. Identificadores de objeto (OID) de los algoritmos..... | 29 |
| 7.1.4. Formatos de nombres..... | 30 |
| 7.1.5. Identidad Empresarial..... | 30 |
| 7.1.6. Restricciones de los nombres..... | 31 |
| 7.1.7. Identificador de objeto (OID) de la Política de Certificación..... | 31 |
| 7.1.8. Uso de la extensión “Policy Constraints”..... | 31 |
| 7.1.9. Sintaxis y semántica de los cualificadores de política..... | 31 |
| 7.1.10. Tratamiento semántico para la extensión crítica “Certificate Policy”..... | 31 |
| 7.2. PERFIL DE CRL..... | 31 |
| 7.2.1. Número de versión..... | 31 |
| 7.2.2. CRL y extensiones..... | 32 |
| 7.3 LISTAS DE CERTIFICADOS REVOCADOS..... | 32 |
| 7.3.1 Límite Temporal de los certificados en las CRLs..... | 32 |
| 8. AUDITORÍA DE CONFORMIDAD..... | 33 |
| 8.1. FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD PARA CADA ENTIDAD..... | 33 |
| 8.2. IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR..... | 33 |
| 8.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA..... | 33 |
| 8.4. TÓPICOS CUBIERTOS POR EL CONTROL DE CONFORMIDAD..... | 33 |
| 8.5. ACCIONES A TOMAR COMO RESULTADO DE UNA DEFICIENCIA..... | 33 |
| 8.6. COMUNICACIÓN DE RESULTADOS..... | 33 |
| 9. REQUISITOS COMERCIALES Y LEGALES..... | 34 |
| 9.1. TARIFAS..... | 34 |
| 9.1.1. Tarifas de emisión de certificado o renovación..... | 34 |
| 9.1.2. Tarifas de acceso a los certificados..... | 34 |
| 9.1.3. Tarifas de acceso a la información de estado o revocación..... | 34 |

| | | |
|----------------------|--------------------------------|--------------|
| Cif.: PUBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 6 |

| | |
|---|----|
| 9.1.4. Tarifas de otros servicios como información de políticas..... | 34 |
| 9.1.5. Política de reintegros..... | 34 |
| 9.2. CAPACIDAD FINANCIERA..... | 34 |
| 9.2.1. Indemnización a los terceros que confían en los certificados emitidos por la ACCV..... | 34 |
| 9.2.2. Relaciones fiduciarias..... | 34 |
| 9.2.3. Procesos administrativos..... | 34 |
| 9.3. POLÍTICA DE CONFIDENCIALIDAD..... | 35 |
| 9.3.1. Información confidencial..... | 35 |
| 9.3.2. Información no confidencial..... | 35 |
| 9.3.3. Divulgación de información de revocación /suspensión de certificados..... | 35 |
| 9.4. PROTECCIÓN DE DATOS PERSONALES..... | 35 |
| 9.4.1. Plan de Protección de Datos Personales..... | 35 |
| 9.4.2. Información considerada privada..... | 35 |
| 9.4.3. Información no considerada privada..... | 35 |
| 9.4.4. Responsabilidades..... | 35 |
| 9.4.5. Prestación del consentimiento en el uso de los datos personales..... | 35 |
| 9.4.6. Comunicación de la información a autoridades administrativas y/o judiciales..... | 35 |
| 9.4.7. Otros supuestos de divulgación de la información..... | 35 |
| 9.5. DERECHOS DE PROPIEDAD INTELECTUAL..... | 35 |
| 9.6. OBLIGACIONES Y RESPONSABILIDAD CIVIL..... | 36 |
| 9.6.1. Obligaciones de la Entidad de Certificación..... | 36 |
| 9.6.2. Obligaciones de la Autoridad de Registro..... | 36 |
| 9.6.3. Obligaciones de los suscriptores..... | 36 |
| 9.6.4. Obligaciones de los terceros confiantes en los certificados emitidos por la ACCV..... | 36 |
| 9.6.5. Obligaciones del repositorio..... | 36 |
| 9.7. RENUNCIAS DE GARANTÍAS..... | 36 |
| 9.8. LIMITACIONES DE RESPONSABILIDAD..... | 36 |
| 9.8.1. Garantías y limitaciones de garantías..... | 36 |
| 9.8.2. Deslinde de responsabilidades..... | 36 |
| 9.8.3. Limitaciones de pérdidas..... | 36 |
| 9.9. PLAZO Y FINALIZACIÓN..... | 36 |
| 9.9.1. Plazo..... | 36 |
| 9.9.2. Finalización..... | 37 |
| 9.9.3. Supervivencia..... | 37 |
| 9.10. NOTIFICACIONES..... | 37 |
| 9.11. MODIFICACIONES..... | 37 |
| 9.11.1. Procedimientos de especificación de cambios..... | 37 |
| 9.11.2. Procedimientos de publicación y notificación..... | 37 |

| | | |
|----------------------|--------------------------------|--------------|
| Cif.: PUBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 7 |

| | |
|---|-----------|
| 9.11.3. Procedimientos de aprobación de la Declaración de Prácticas de Certificación..... | 37 |
| 9.12. RESOLUCIÓN DE CONFLICTOS..... | 37 |
| 9.12.1. Resolución extrajudicial de conflictos..... | 37 |
| 9.12.2. Jurisdicción competente..... | 37 |
| 9.13. LEGISLACIÓN APLICABLE..... | 37 |
| 9.14. CONFORMIDAD CON LA LEY APLICABLE..... | 37 |
| 9.15. CLÁUSULAS DIVERSAS..... | 37 |
| ANEXO I..... | 39 |
| ANEXO II – FORMULARIO DE SOLICITUD DE REVOCACIÓN DE CERTIFICADO..... | 42 |
| ANEXO III – FORMULARIO DE SOLICITUD DE ALTA DE ENTIDAD..... | 44 |
| ANEXO IV – FORMULARIO DE SOLICITUD DE CERTIFICADOS..... | 45 |

| | | |
|----------------------|--------------------------------|--------------|
| Cif.: PUBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 8 |

1 INTRODUCCIÓN

1.1 Presentación

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

La Política de Certificación referida en este documento se utilizará para la emisión de certificados cualificados de pertenencia a empresa, sobre dispositivo seguro de creación de firma –tarjeta criptográfica–. Mediante los certificados reconocidos y los dispositivos seguros de creación de firma asociados a esta Política de Certificación se generarán firmas electrónicas reconocidas

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

La Agencia de Tecnología y Certificación Electrónica (ACCV) se ajusta a la versión actual del documento “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”, publicada en <https://www.cabforum.org/>. En el caso de cualquier incompatibilidad entre esta Política de Certificación y los requisitos del CAB Forum, dichos requisitos prevalecerán sobre el presente documento.

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

1.2 Identificación

| | |
|---|--|
| Nombre de la política | Política de Certificación de Certificados Cualificados en dispositivo seguro de pertenencia a empresa |
| Calificador de la política | Certificado cualificado de pertenencia a empresa expedido por el Instituto Valenciano de Finanzas - ACCV (Plaza Nápoles y Sicilia, 6. Valencia CP 46003, ESPAÑA. CIF Q9650010C). CPS y CP en http://www.accv.es |
| Versión de la política | 3.0 |
| Estado de la política | APROBADO |
| Referencia de la política / OID (Object Identifier) | 1.3.6.1.4.1.8149.3.20.4.0 |
| Fecha de emisión | 15 de junio de 2017 |
| Fecha de expiración | No aplicable. |
| CPS relacionada | Declaración de Prácticas de Certificación (CPS) de la ACCV. Versión 4.0 OID: 1.3.6.1.4.1.8149.2.4.0 Disponible en http://www.accv.es/pdf-politicas |
| Localización | Esta Política de Certificación se puede encontrar en: http://www.accv.es/legislacion_c.htm |

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 9 |

1.3 Comunidad de usuarios y ámbito de aplicación

1.3.1 Autoridades de Certificación

La CA que puede emitir certificados acordes con esta política es “**ACCVCA-120**” perteneciente a la Agencia de Tecnología y Certificación Electrónica, cuya función es la emisión de certificados de entidad final para los suscriptores de ACCV. El certificado de “ACCVCA-120” es válido desde el día 13 de octubre de 2011 hasta el 1 de enero de 2027

1.3.2 Autoridades de Registro

La lista de Autoridades de Registro (Puntos de Registro de Usuario) que gestionan las solicitudes de certificados definidos en esta política se encuentra en la URL <http://www.accv.es>

1.3.3 Usuarios Finales

1.3.3.1 Suscriptores

El grupo de usuarios que pueden solicitar certificados definidos por esta política está compuesto por los empleados que trabajen para cualquier tipo de empresa, que cuenten con los mecanismos de identificación requeridos (DNI, NIE, Pasaporte español, etc.), y sean empleados estas organizaciones.

El soporte de claves y certificados es tarjeta criptográfica Giesecke & Devrient (G&D) Sm@rtCafé Expert 3.2 y versiones posteriores. En caso de acreditarse otros dispositivos criptográficos serán recogidos en el presente documento, en su punto 6.1.8 Hardware/software de generación de claves.

Se limita el derecho de solicitud de certificados definido en la presente Política de Certificación a personas físicas. No se aceptarán solicitudes de certificación realizadas en nombre de personas jurídicas, entidades u organizaciones.

1.3.3.2 Partes confiantes

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

- Los usuarios de clientes de correo electrónico S/MIME en el ámbito de la verificación de la identidad del emisor de mensajes de correo electrónico y del cifrado de los mismos.
- Las aplicaciones y servicios pertenecientes a entidades u organizaciones públicas o privadas que tengan acceso a los servicios de validación de la ACCV o de la Administración General del Estado o de otras entidades capaces de proporcionar información de validez de certificados expedidos por la ACCV.
- Las aplicaciones y servicios que se emplean en relaciones entre ciudadanos, empresas u otras Administraciones Públicas.

1.4 Uso de los certificados

1.4.1 Usos Permitidos

Los certificados emitidos por la Agencia de Tecnología y Certificación Electrónica bajo esta Política de Certificación, pueden utilizarse para la firma electrónica y cifrado de cualquier información o documento. Asimismo, pueden utilizarse como mecanismo de identificación ante servicios y aplicaciones informáticas.

| | | |
|----------------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 10 |

1.4.2 Usos prohibidos

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

1.5 Política de Administración de la ACCV

1.5.1 Especificación de la Organización Administradora

| | |
|--------------------|--|
| Nombre | <u>Agencia de Tecnología y Certificación Electrónica IVF</u> |
| Dirección de email | <u>accv@accv.es</u> |
| Dirección | <u>Plaza Napoles y Sicilia , 6 –46003 Valencia (Spain)</u> |
| Número de teléfono | <u>+34 902 482 481</u> |
| Número de fax | <u>+34-961 971 771</u> |

1.5.2 Persona de Contacto

| | |
|--------------------|--|
| Nombre | <u>Agencia de Tecnología y Certificación Electrónica IVF</u> |
| Dirección de email | <u>accv@accv.es</u> |
| Dirección | <u>Plaza Napoles y Sicilia , 6 –46003 Valencia (Spain)</u> |
| Número de teléfono | <u>+34 902 482 481</u> |
| Número de fax | <u>+34-961 971 771</u> |

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

La entidad competente para determinar la adecuación de esta CPS a las diferentes Políticas de Certificación de la ACCV, es la Subdirección de Entidades Financieras y Certificación Electrónica - IVF de conformidad con los Estatutos del Instituto Valenciano de Finanzas (IVF).

1.6 Definiciones y Acrónimos

1.6.1 Definiciones

No estipulado

1.6.2 Acrónimos

No estipulado

2 Publicación de información y repositorio de certificados

2.1 Repositorio de certificados

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

2.2 Publicación

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

2.3 Frecuencia de actualizaciones

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

2.4 Controles de acceso al repositorio de certificados.

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

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 12 |

3 Identificación y Autenticación

3.1 Registro de nombres

3.1.1 Tipos de nombres

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

3.1.2 Significado de los nombres

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

3.1.3 Interpretación de formatos de nombres

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

3.1.4 Unicidad de los nombres

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

3.1.5 Resolución de conflictos relativos a nombres

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

3.1.6 Reconocimiento, autenticación y función de las marcas registradas.

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

3.2 Validación inicial de la identidad

3.2.1 Métodos de prueba de posesión de la clave privada.

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

3.2.2 Autenticación de la identidad de una organización.

La solicitud de los certificados definidos en la presente Política de Certificación se encuentra limitada a organismos u empresas tanto públicas como privadas con las que se haya establecido convenio de certificación, contrato o alguna otra fórmula que instrumente la prestación del servicio por parte de la ACCV.

La identificación del organismo o empresa se realizará en el proceso de Alta de la Entidad que será suscrito por una persona física con capacidad de representar a dicho organismo o empresa.

3.2.3 Autenticación de la identidad de un individuo.

La identificación del suscriptor del certificado de pertenencia a empresa se realizará mediante su personación ante el Operador del Punto de Registro, acreditándose mediante presentación del

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 13 |

Documento Nacional de Identidad (DNI), pasaporte español, el Número de Identificación de Extranjeros (NIE) del solicitante u otros medios admitidos en Derecho.

La determinación de la condición de empleado es responsabilidad del organismo o empresa solicitante, la cual deberá comprobar dicha condición, bien en su base de datos, si está actualizada, o solicitando el documento por el que el suscriptor ha adquirido esa condición, si no le constare al propio organismo o empresa solicitante.

En este tipo de certificados se incluye la dirección de correo electrónico del suscriptor como elemento necesario para soportar operaciones de firma electrónica y cifrado de correo electrónico, pero la Agencia de Tecnología y Certificación Electrónica no garantiza que esta dirección de correo esté vinculada con el suscriptor del certificado, por lo que la confianza en que esta dirección sea la del suscriptor del certificado corresponde únicamente a la parte confiante. La Agencia de Tecnología y Certificación Electrónica únicamente garantiza que la dirección de correo que consta en el certificado fue la aportada por el organismo o empresa a la que pertenecía el suscriptor en el momento de la formalización de su solicitud y/o que consta como vinculada al suscriptor en las bases de datos de personal del organismo o empresa al que pertenezca el solicitante.

3.3 Identificación y autenticación de las solicitudes de renovación del par de claves.

3.3.1 Identificación y autenticación de las solicitudes de renovación rutinarias.

La identificación y autenticación para la renovación del certificado se puede realizar utilizando las técnicas para la autenticación e identificación inicial (descrita en el punto 3.2.3 *Autenticación de la identidad de un individuo*, de esta Política de Certificación). La primera renovación se podrá realizar a través del Área Personal de Servicios de Certificación (APSC), donde el usuario se identificará mediante un certificado cualificado personal de la ACCV o el DNle. Existen, por tanto, dos mecanismos alternativos para la renovación:

- Formularios web en APSC, disponible en www.accv.es.
- Solicitud de un nuevo certificado por parte del organismo o empresa a la que pertenezca el suscriptor (ver apartado 3.2.3. *Autenticación de la identidad de un individuo*, de esta Política de Certificación).

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

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

3.4 Identificación y autenticación de las solicitudes de revocación del par de claves

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

- Presencial. Es el mismo que para el registro inicial descrito en el punto 3.2.3. *Autenticación de la identidad de un individuo*, de esta Política de Certificación

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 14 |

- Telemática. Accediendo al Área Personal de Servicios de Certificación (APSC) identificándose mediante un certificado cualificado personal de la ACCV o el DNIe.
- Telefónica. Mediante la respuesta a las preguntas realizadas desde el servicio de soporte telefónico disponible en el número 902482481.

La Agencia de Tecnología y Certificación Electrónica o cualquiera de las entidades que la componen pueden solicitar de oficio la revocación de un certificado si tuvieran el conocimiento o sospecha del compromiso de la clave privada del suscriptor, o cualquier otro hecho que recomendará emprender dicha acción.

Deberán solicitar la revocación de los certificados las personas de contacto dadas de alta para la gestión de certificados de cada organismo o empresa en cuanto el suscriptor pierda su condición de empleado o cambie el cargo o puesto de trabajo recogido en el certificado

| | | |
|----------------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 15 |

4 El ciclo de vida de los certificados.

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

4.1 Solicitud de certificados

La solicitud de este tipo de certificados es responsabilidad del organismo o empresa, que deberá comprobar la condición de empleado de los titulares de los certificados mediante consulta a los registros de personal de la organización de su competencia.

El proceso comienza por dar de alta al organismo o empresa, a partir de un formulario de alta de entidad, como el que se recoge en el Anexo III de esta Política de Certificación. En ese formulario deben indicarse cuáles son las personas habilitadas para la gestión de certificados de pertenencia a empresa para el personal perteneciente a la entidad en cuestión.

Para llevar a cabo la solicitud de certificados debe emplearse el formulario del Anexo IV y remitirlo a la Agencia de Tecnología y Certificación Electrónica firmado por una de las personas habilitadas para llevar a cabo la gestión de certificados.

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 en el caso de la solicitud de certificado mediante medios telemáticos se exigirá que haya transcurrido un período de tiempo desde la identificación presencial menor a los cinco años.

4.2 Tramitación de la solicitud de certificados.

Tras recibir la solicitud de certificados por parte de las personas habilitadas al efecto y una vez aceptada, en su caso, la propuesta económica si fuera el caso, se procederá a la generación de los certificados y la preparación de la documentación asociada a éstos. Una vez concluido, se remitirá al organismo o empresa solicitante, a través de las personas habilitadas para la gestión.

Las personas habilitadas para la gestión de los certificados serán las responsables de la entrega de los certificados a sus suscriptores y de remitir los contratos de certificación a la Agencia de Tecnología y Certificación Electrónica.

4.3 Emisión de certificados

La Agencia de Tecnología y Certificación Electrónica 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 Agencia de Tecnología y Certificación Electrónica haya llevado a cabo las verificaciones necesarias para validar la solicitud de certificación. El mecanismo por el que determina la naturaleza y la forma de realizar dichas comprobaciones es esta Política de Certificación.

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

Es tarea de la Autoridad de Registro notificar al suscriptor de un certificado la emisión del mismo y proporcionarles una copia, o en su defecto, informarles del modo en que puede conseguirla.

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 16 |

4.4 Aceptación de certificados

La aceptación de los certificados por parte de los suscriptores se produce en el momento de la firma del contrato de certificación asociado a cada Política de Certificación. La aceptación del contrato implica el conocimiento y aceptación por parte del suscriptor de la Política de Certificación asociada.

El Contrato de Certificación es un documento que debe ser firmado por el suscriptor y por la persona adscrita al Punto de Registro de Usuarios, y cuyo fin es vincular a la persona a certificar con la acción de la solicitud, con el conocimiento de las normas de uso y con la veracidad de los datos presentados. El formulario del Contrato de Certificación se recoge en el Anexo I de esta Política de Certificación.

4.5 Uso del par de claves y del certificado.

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

4.6 Renovación de certificados.

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

4.7 Renovación de claves

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

4.8 Modificación de certificados.

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

4.9 Revocación y suspensión de certificados.

4.9.1 Circunstancias para la revocación

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

4.9.2 Entidad que puede solicitar la revocación

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

4.9.3 Procedimiento de solicitud de revocación

La Agencia de Tecnología y Certificación Electrónica acepta solicitudes de revocación por los siguientes procedimientos

4.9.3.1 Presencial

Mediante la presentación e identificación del suscriptor o del solicitante habilitado por cada entidad en un Punto de Registro de Usuario y la cumplimentación y firma, por parte del mismo, del "Formulario de Solicitud de Revocación" que se le proporcionará y del que se adjunta copia en el anexo II

4.9.3.2 Telemático

Existe un formulario de solicitud de revocación de certificados en la web de ACCV, en la URL <http://www.accv.es>.

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 17 |

4.9.3.3 Telefónico

Mediante llamada telefónica al número de soporte telefónico de la Agencia de Tecnología y Certificación Electrónica 902482481.

Cuando el suscriptor de un certificado de pertenencia a empresa deje de ser empleado de un organismo o empresa, el personal habilitado para la gestión de los certificados de dicho organismo o empresa, o en su defecto, el Registro de Personal o el departamento de RRHH de dicha Organización deberá solicitar la revocación del certificado digital.

4.9.4 Periodo de gracia de la solicitud de revocación

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

4.9.5 Circunstancias para la suspensión

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

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

4.9.6 Entidad que puede solicitar la suspensión

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

4.9.7 Procedimiento para la solicitud de suspensión

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

4.9.8 Límites del período de suspensión

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

4.9.9 Frecuencia de emisión de CRLs

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

4.9.10 Requisitos de comprobación de CRLs

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

4.9.11 Disponibilidad de comprobación on-line de revocación y estado

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

4.9.12 Requisitos de comprobación *on-line* de revocación

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

4.9.13 Otras formas de divulgación de información de revocación disponibles

Además de la consulta de revocados por medio de Listas de Certificados Revocados (CRL) y por medio del servicio OCSP, es posible comprobar la validez de los certificados por medio de un formulario web que, a partir del identificador (DNI o NIE) del ciudadano, devuelve los certificados que cumplan ese criterio y el estado de éstos. Este formulario se encuentra en el sitio web de la Autoridad de Certificación en la URL <http://www.accv.es>

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 18 |

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

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

4.9.15 Requisitos especiales de renovación de claves comprometidas

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

4.10 Servicios de comprobación de estado de certificados.

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

4.11 Finalización de la suscripción.

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

La ACCV informará al suscriptor, mediante correo electrónico firmado digitalmente, en un momento previo anterior a la publicación del certificado en la Lista de Certificados Revocados, acerca de la suspensión o revocación de su certificado, especificando los motivos, la fecha y la hora en que su certificado quedará sin efecto, y comunicándole que no debe continuar utilizándolo.

4.12 Depósito y recuperación de claves.

La ACCV no realiza el depósito de certificados y claves de cifrado.

4.13 Caducidad de las claves de certificado de CA.

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

5 Controles de seguridad física, de gestión y de operaciones

5.1 Controles de Seguridad Física

5.1.1 Ubicación y construcción

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

5.1.2 Acceso físico

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

5.1.3 Alimentación eléctrica y aire acondicionado

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

5.1.4 Exposición al agua

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

5.1.5 Protección y prevención de incendios

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

5.1.6 Sistema de almacenamiento

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

5.1.7 Eliminación de residuos

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

5.1.8 Backup remoto

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

5.2 Controles de procedimientos

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

5.2.1 Papeles de confianza

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

5.2.2 Número de personas requeridas por tarea

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

5.2.3 Identificación y autenticación para cada papel

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

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 20 |

5.3 Controles de seguridad de personal

Este apartado refleja el contenido del documento *Controles de Seguridad del Personal* de ACCV.

5.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación

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

5.3.2 Procedimientos de comprobación de antecedentes

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

5.3.3 Requerimientos de formación

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

5.3.4 Requerimientos y frecuencia de actualización de la formación

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

5.3.5 Frecuencia y secuencia de rotación de tareas

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

5.3.6 Sanciones por acciones no autorizadas

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

5.3.7 Requerimientos de contratación de personal

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

5.3.8 Documentación proporcionada al personal

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

5.3.9 Controles periódicos de cumplimiento

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

5.3.10 Finalización de los contratos

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

5.4 Procedimientos de Control de Seguridad

5.4.1 Tipos de eventos registrados

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

5.4.2 Frecuencia de procesado de logs

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

| | | |
|----------------------|--------------------------------|--------------|
| Clf.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 21 |

5.4.3 Periodo de retención para los logs de auditoría

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

5.4.4 Protección de los logs de auditoría

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

5.4.5 Procedimientos de backup de los logs de auditoría

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

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

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

5.4.7 Notificación al sujeto causa del evento

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

5.4.8 Análisis de vulnerabilidades

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

5.5 Archivo de informaciones y registros

5.5.1 Tipo de informaciones y eventos registrados

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

5.5.2 Periodo de retención para el archivo.

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

5.5.3 Protección del archivo.

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

5.5.4 Procedimientos de backup del archivo.

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

5.5.5 Requerimientos para el sellado de tiempo de los registros.

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

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

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

5.5.7 Procedimientos para obtener y verificar información archivada

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

| | | |
|----------------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 22 |

5.6 Cambio de Clave

No estipulado.

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

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

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

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

5.7.2 La clave pública de una entidad se revoca

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

5.7.3 La clave de una entidad se compromete

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

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

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

5.8 Cese de una CA

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

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 23 |

6 Controles de seguridad técnica

6.1 Generación e Instalación del par de claves

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

6.1.1 Generación del par de claves

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

6.1.2 Entrega de la clave privada a la entidad

La clave privada para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentra contenida en la tarjeta criptográfica que se entrega al suscriptor con su certificado en el momento de su registro.

6.1.3 Entrega de la clave pública al emisor del certificado

La clave pública a ser certificada es generada en el interior de la tarjeta criptográfica y es entregada a la Autoridad de Certificación por la Autoridad de Registro mediante el envío de una solicitud de certificación en formato PKCS#10, firmada digitalmente por el Operador de la Autoridad de Registro.

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

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

6.1.5 Tamaño de las claves

Las claves de la ACCVRAIZ1 y ACCVCA-120 son claves RSA de 4096 bits de longitud.

El tamaño de las claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación es de 2048 bits.

6.1.6 Parámetros de generación de la clave pública

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

Se utilizan los parámetros definidos en la suite criptográfica 001 especificada en el documento de ETSI TS 001 176-1 "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms". Se define ModLen=2048.

| Signature suite entry name | Signature algorithm | Signature algorithm parameters | Key generation algorithm | Padding method | Cryptographic hash function |
|----------------------------|---------------------|--------------------------------|--------------------------|-----------------|-----------------------------|
| Sha-256-with-rsa | rsa | MinModLen=2048 | rsagen1 | emsa-pkcs1-v1_5 | sha256 |

6.1.7 Comprobación de la calidad de los parámetros

Se utilizan los parámetros definidos en la suite criptográfica 001 especificada en el documento de ETSI TS 001 176-1 “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms”. Se define ModLen=2048.

| Signature suite entry name | Signature algorithm | Signature algorithm parameters | Key generation algorithm | Padding method | Cryptographic hash function |
|----------------------------|---------------------|--------------------------------|--------------------------|-----------------|-----------------------------|
| Sha-256-with-rsa | rsa | MinModLen=2048 | rsagen1 | emsa-pkcs1-v1_5 | sha256 |

6.1.8 Hardware/software de generación de claves

La generación de las claves se realiza en tarjeta criptográfica, por el chip criptográfico de la misma.

Las tarjetas certificadas para dar soporte a este tipo de certificados son las siguientes:

Tarjetas G&D:

- Giesecke & Devrient (G&D) SmartCafe Expert 3.2 72K FIPS 140-2 Level 2

6.1.9 Fines del uso del par de claves

Las claves definidas por la presente política se utilizarán para usos descritos en el punto de este documento *1.3 Comunidad de usuarios y ámbito de aplicación*.

La definición detallada del perfil de certificado y los usos de las claves se encuentra en el apartado 7 de este documento *“Perfiles de certificado y listas de certificados revocados”*.

6.2 Protección de la Clave Privada

En este punto se hace siempre referencia a las claves generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación. La información sobre las claves de las entidades que componen la Autoridad de Certificación se encuentra en el punto 6.2 de la Declaración de Prácticas de Certificación (CPS) de la Agencia de Tecnología y Certificación Electrónica.

6.2.1 Estándares para los módulos criptográficos

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

6.2.2 Control multipersona de la clave privada

Las claves privadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentran bajo el control exclusivo de los suscriptores de los mismos.

6.2.3 Custodia de la clave privada

No se custodian claves privadas de firma, autenticación ni cifrado de los suscriptores de los certificados definidos por la presente política.

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 25 |

6.2.4 Copia de seguridad de la clave privada

No se custodian claves privadas de firma, autenticación y cifrado de los suscriptores de los certificados definidos por la presente política, por lo que no es aplicable.

6.2.5 Archivo de la clave privada.

No se archivan las claves privadas.

6.2.6 Introducción de la clave privada en el módulo criptográfico.

La generación de las claves vinculadas al certificado se realiza en tarjeta criptográfica por el propio chip criptográfico de la misma y nunca la abandonan.

6.2.7 Método de activación de la clave privada.

La clave privada del suscriptor se activa mediante la introducción del PIN de la tarjeta que la contiene.

6.2.8 Método de desactivación de la clave privada

La desactivación de la clave privada del suscriptor se consigue mediante la extracción de la tarjeta que la contiene del lector PC/SC.

6.2.9 Método de destrucción de la clave privada

No estipulado.

6.3 Otros Aspectos de la Gestión del par de claves.

6.3.1 Archivo de la clave pública

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

6.3.2 Periodo de uso para las claves públicas y privadas

Los certificados emitidos al amparo de la presente política tienen una validez de tres (3) años.

La clave utilizada para la emisión de los certificados se crea para cada emisión, y por tanto también tienen una validez de tres (3) años.

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

6.4 Datos de activación

6.4.1 Generación y activación de los datos de activación

Los datos de activación de la clave privada consisten en el PIN de la tarjeta que la contiene y que se proporciona al suscriptor del certificado con el mismo.

La generación del PIN de la tarjeta se realiza en el momento de la inicialización de la misma. El PIN, junto con el código de desbloqueo –PUK–, se entregará al suscriptor.

Es responsabilidad y obligación del suscriptor la custodia de ese PIN (y PUK). Se aconseja al suscriptor el cambio de ese PIN preconfigurado por uno de su exclusivo conocimiento.

| | | |
|----------------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 26 |

6.4.2 Protección de los datos de activación

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

6.4.3 Otros aspectos de los datos de activación

No estipulado.

6.5 Controles de Seguridad Informática

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

6.6 Controles de Seguridad del Ciclo de Vida.

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

6.7 Controles de Seguridad de la Red

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

6.8 Controles de Ingeniería de los Módulos Criptográficos

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

| | | |
|----------------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 27 |

7 Perfiles de certificados y listas de certificados revocados

7.1 Perfil de Certificado

7.1.1 Número de versión

Esta política de certificación especifica el uso de un certificado con tres usos distintos; firma digital, autenticación del suscriptor y cifrado de datos.

7.1.2 Extensiones del certificado

Las extensiones utilizadas por los certificados emitidos bajo el amparo de la presente política son:

| Campo | Valor |
|---------------------------|--|
| Subject | |
| SerialNumber | NIF del suscriptor. 9 caracteres completados a ceros por la izquierda. |
| GivenName | Nombre de pila del empleado , tal como aparece en el DNI |
| SurName | Apellidos del suscriptor, tal como aparece en el DNI APELLIDO1 APELLIDO2 |
| CommonName | Cadena compuesta de la forma: NOMBRE APELLIDO1 APELLIDO2 – DNI NIFDELSUSSCRIPTOR |
| Title | Puesto o cargo de la persona física, que le vincula con el organismo o empresa suscriptora del certificado |
| OrganizationalUnit | Número de identificación del suscriptor del certificado (unívoco dentro de una organización) |
| OrganizationalUnit | Unidad, dentro del organismo o empresa, en la que está incluida el suscriptor del certificado |
| OrganizationalUnit | Cadena fija con el valor CERTIFICADO ELECTRONICO DE PERTENENCIA A EMPRESA |
| Organization | Denominación (nombre “oficial”) del organismo, empresa o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado |
| Country | Cadena fija con el valor ES |
| Version | V3 |
| SerialNumber | Identificador único del certificado. Menor de 32 caracteres hexadecimales. |
| Algoritmo de firma | sha256withRSAEncryption |
| Issuer (Emisor) | |
| CommonName | ACCVCA-120 |
| OrganizationalUnit | PKIACCV |
| Organization | ACCV |
| Country | ES |

| | |
|--------------------------------------|--|
| | |
| Válido desde | Fecha de Emisión |
| Válido hasta | Fecha de Caducidad |
| Clave Pública | Octet String conteniendo la clave pública del suscriptor |
| Extended Key Usage | |
| | Client Authentication |
| | Email Protection |
| CRL Distribution Point | http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl |
| SubjectAlternativeName | |
| RFC822Name | Correo electrónico del suscriptor |
| DirectoryName | |
| | CN=Nombre Apellido1 Apellido2 |
| | UID=NIF |
| | Identidad Empresarial (se desarrolla en el punto 7.1.5) |
| Certificate Policy Extensions | |
| Policy OID | QCP-n: certificate policy for EU qualified certificates issued to natural persons; Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural(0) |
| Policy OID | 1.3.6.1.4.1.8149.3.20.4.0 |
| Policy CPS Location | http://www.accv.es/legislacion_c.htm * |
| Policy Notice | Certificado cualificado de pertenencia a empresa expedido por el Instituto Valenciano de Finanzas - ACCV (Plaza Nápoles y Sicilia, 6. Valencia CP 46003, ESPAÑA. CIF Q9650010C). CPS y CP en http://www.accv.es |
| Authority Information Access | |
| Access Method | Id-ad-ocsp |
| Access Location | http://ocsp.accv.es |
| Access Method | Id-ad-calssuers |
| Access Location | http://www.accv.es/gestcert/ACCVCA120SHA2.cacert.crt |
| Fingerprint issuer | 48 72 a4 c3 df 17 4c ef 34 d7 7f e6 a3 b4 e7 be 7d f2 d2 5d |
| Algoritmo de hash | SHA-256 |
| KeyUsage (críticos) | |
| | Digital Signature Content Commitment |

| | | |
|--------------------|---|---|
| | Key Encipherment | |
| QcStatement | Campos QC (Qualified Certificate) | |
| QcCompliance | | El certificado es cualificado |
| QcType | eSign | Tipo particular de certificado cualificado |
| QcRetentionPeriod | 15y | Periodo de retención de la información material |
| QcPDS | https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-V1.0-EN.pdf | Ubicación de PKI Disclosure Statement |

7.1.3 Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

- SHA1withRSA (1.2.840.113549.1.1.5)
- SHA256withRSA (1.2.840.113549.1.1.11)

7.1.4 Formatos de nombres

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

Todos los campos del certificado del Subject y del Subject Alternative Name, exceptuando los que se refieren a nombre DNS o direcciones de correo, se cumplimentan obligatoriamente en mayúsculas, prescindiendo de acentos.

7.1.5 Identidad Empresarial

A efectos de facilitar la obtención de los datos se crea en el campo subjectAlternativeName dentro del objeto DirectoryName la siguiente estructura de datos de Identidad Empresarial.

| Campo | Contenido | Observaciones |
|-----------------------------------|---|--|
| Tipo de Certificado | Indica la naturaleza del certificado | Tipo= certificado electrónico de pertenencia a empresa OID.1.3.6.1.4.1.8149.4.2.1 |
| Nombre de la entidad suscriptora | La entidad propietaria de dicho certificado | Entidad Suscriptora = ie: ACCV OID.1.3.6.1.4.1.8149.4.2.2 |
| NIF entidad suscriptora | Número de identificación de la entidad | CIF entidad suscriptora ie: S-2833002 OID.1.3.6.1.4.1.8149.4.2.3 |
| NIF NIE del suscriptor | NIF o NIE del suscriptor | NIF NIE suscriptor= ie: 0000000G OID.1.3.6.1.4.1.8149.4.2.4 |
| Número de identificación personal | Número de identificación del suscriptor del certificado | Número identificativo = ie: |

| | | |
|----------------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 30 |

| | | |
|---------------------|---|---|
| | (supuestamente unívoco). Se corresponde con el NRP o NIP | A02APE1056 OID.1.3.6.1.4.1.8149.4.2.5 |
| Nombre de pila | Nombre de pila del responsable del certificado | N = Nombre de pila del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte OID.1.3.6.1.4.1.8149.4.2.6 |
| Primer apellido | Primer apellido del responsable del certificado | SN1 = Primer apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte OID.1.3.6.1.4.1.8149.4.2.7 |
| Segundo apellido | Segundo apellido del responsable del certificado | SN2 = Segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte OID.1.3.6.1.4.1.8149.4.2.8 |
| Correo electrónico | Correo electrónico del responsable del certificado | Correo electrónico de la persona responsable del certificado ie: jvalenciano@accv.es OID.1.3.6.1.4.1.8149.4.2.9 |
| Unidad organizativa | Unidad, dentro del organismo o empresa, en la que está incluida el suscriptor del certificado | Unidad = ie: AGENCIA DE TECNOLOGIA Y CERTIFICACION ELECTRONICA OID.1.3.6.1.4.1.8149.4.2.10 |
| Puesto o cargo | Puesto desempeñado por el suscriptor del certificado dentro del organismo o empresa | Puesto = ie: ANALISTA PROGRAMADOR OID.1.3.6.1.4.1.8149.4.2.11 |

7.1.6 Restricciones de los nombres

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

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

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

1.3.6.1.4.1.8149.3.20.4.0

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

| | | |
|----------------------|--------------------------------|--------------|
| Clf.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 31 |

0.4.0.194112.1.0 Política de certificación para certificados cualificados EU en soporte software emitidos a personas físicas

7.1.8 Uso de la extensión “Policy Constraints”

No se hace uso de la extensión “*Policy Constraints*” en los certificados emitidos bajo la presente Política de Certificación.

7.1.9 Sintaxis y semántica de los cualificadores de política

No estipulado

7.1.10 Tratamiento semántico para la extensión crítica “Certificate Policy”

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

7.2 Perfil de CRL

7.2.1 Número de versión

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 Política de Certificación soporta y utiliza CRLs conformes al estándar X.509.

7.3 Listas de Certificados Revocados

7.3.1 Límite Temporal de los certificados en las CRLs

Los números de serie de los certificados revocados aparecerán en las CRL hasta que alcance su fecha de expiración.

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 32 |

8 Auditoría de conformidad

8.1 Frecuencia de los controles de conformidad para cada entidad

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

8.2 Identificación/cualificación del auditor

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

8.3 Relación entre el auditor y la entidad auditada

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

8.4 Tópicos cubiertos por el control de conformidad

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

8.5 Acciones a tomar como resultado de una deficiencia.

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

8.6 Comunicación de resultados

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

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 33 |

9 Requisitos comerciales y legales

9.1 Tarifas

9.1.1 Tarifas de emisión de certificado o renovación

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

9.1.2 Tarifas de acceso a los certificados

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

9.1.3 Tarifas de acceso a la información de estado o revocación

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

9.1.4 Tarifas de otros servicios como información de políticas

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

9.1.5 Política de reintegros

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

9.2 Capacidad financiera

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

Tal y como se especifica en la Declaración de Prácticas de Certificación (CPS), la ACCV dispone de garantía de cobertura suficiente de responsabilidad civil a través de aval bancario 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 Agencia, 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

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

9.2.3 Procesos administrativos

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

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 34 |

9.3 Política de Confidencialidad

9.3.1 Información confidencial.

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

9.3.2 Información no confidencial

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

9.3.3 Divulgación de información de revocación /suspensión de certificados

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

9.4 Protección de datos personales

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

9.4.1 Plan de Protección de Datos Personales.

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

9.4.2 Información considerada privada.

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

9.4.3 Información no considerada privada.

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

9.4.4 Responsabilidades.

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

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

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

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

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

9.4.7 Otros supuestos de divulgación de la información.

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

| | | |
|----------------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 35 |

9.5 Derechos de propiedad Intelectual

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

9.6 Obligaciones y Responsabilidad Civil

9.6.1 Obligaciones de la Entidad de Certificación

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

9.6.2 Obligaciones de la Autoridad de Registro

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

9.6.3 Obligaciones de los suscriptores

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

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

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

9.6.5 Obligaciones del repositorio

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

9.7 Renuncias de garantías

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

9.8 Limitaciones de responsabilidad

9.8.1 Garantías y limitaciones de garantías

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

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

9.8.2 Deslinde de responsabilidades

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

9.8.3 Limitaciones de pérdidas

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

| | | |
|----------------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 36 |

9.9 Plazo y finalización.

9.9.1 Plazo.

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

9.9.2 Finalización.

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

9.9.3 Supervivencia.

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

9.10 Notificaciones.

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

Todos los correos que la ACCV envíe a los suscriptores de los certificados emitidos bajo esta Política de Certificación, en el ejercicio de la prestación del servicio de certificación, serán firmados digitalmente para garantizar su autenticidad e integridad.

9.11 Modificaciones.

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

9.11.1 Procedimientos de especificación de cambios

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

9.11.2 Procedimientos de publicación y notificación.

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

9.11.3 Procedimientos de aprobación de la Declaración de Prácticas de Certificación

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

9.12 Resolución de conflictos.

9.12.1 Resolución extrajudicial de conflictos.

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

9.12.2 Jurisdicción competente.

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

9.13 Legislación aplicable

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

| | | |
|----------------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 37 |

9.14 Conformidad con la Ley aplicable.

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

9.15 Cláusulas diversas.

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

| | | |
|----------------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 38 |

10 Anexo I

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.20

Secció 1 – Dades del subscriptor / Sección 1 – Datos del suscriptor

Cognoms/Apellidos:

Nom/Nombre:

DNI/NIF:

Tel.:

Càrrec/Puesto o cargo:

Unitat Organitzativa-Departament/Unidad Organizativa-Departamento:

Empresa-Organismo/Empresa-Organismo

CIF de la Organització/CIF de la Organización:

Adreça de correu electrònic/Dirección correo electrónico:

Adreça postal/Dirección postal:

PIN :

Tel. suport/ tel. soporte **902 482 481**

www.accv.es

Secció 2 – Dades del operador del Punt de Registre / Sección 2 – Datos del operador del Punto de Registro de Certificados de Empleado Público

Nom i cognoms/Nombre y Apellidos:

Secció 3 - Data i Firma / Sección 3 – Fecha y Firma

Subscribo el present contracte de certificació associat a la Política de Certificació de Certificats Qualificats de Pertinença a empresa amb codi 1.3.6.1.4.1.8149.3.20, emés per la Autoritat de Certificació de la Comunitat Valenciana. Declare que conec i accepte les normes d'utilització d'este tipus de certificats que es troben exposades en <http://www.accv.es>. Declare, així mateix, que les dades posades de manifest són certes.

Suscribo el presente contrato de certificación asociado a la Política de Certificación de Certificados Cualificados de Pertenencia a Empresa con código 1.3.6.1.4.1.8149.3.20, emitido por la Agencia de Tecnología y Certificación Electrónica. Declaro conocer y aceptar las normas de utilización de este tipo de certificados que se encuentran expuestas en <http://www.accv.es>. Declaro, asimismo, que los datos puestos de manifiesto son ciertos.

Firma del subscriptor
Firma del suscriptor

Firma i segell del Punt de Registre
Firma y sello del Punto de Registro

Firmat/Firmado:

Firmat/Firmado:

Exemplar per al subscriptor - Anvers / Ejemplar para el suscriptor - Anverso

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 39 |

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.20

Condiciones de utilización de los certificados

1. Los certificados asociados a la Política de Certificación para Certificados de Pertenencia a Empresa, emitidos por la ACCV son del tipo X.509v3 y se rigen por la Declaración de Prácticas de Certificación de la ACCV, en tanto que Prestador de Servicios de Certificación, así como por la Política de Certificación referida. Ambos documentos se deben interpretar según la legislación de la Comunidad Europea, el Ordenamiento Jurídico Español y la legislación propia de la Generalitat.
2. Los suscriptores de los certificados deberán ser personas físicas, en posesión de un NIF, un NIE u otro documento de identificación válido en Derecho, y deben estar empleados en el organismo o empresa a la que se vinculara en el certificado.
3. El solicitante de los certificados, especialmente habilitado para la gestión de éstos por parte de un organismo o empresa determinada, es responsable de la veracidad de los datos aportados en todo momento a lo largo del proceso de solicitud y registro. Será responsable de comunicar cualquier variación de los datos aportados para la obtención del certificado.
4. El suscriptor del certificado es responsable de la custodia de su clave privada y de comunicar a la mayor brevedad posible cualquier pérdida o sustracción de esta clave.
5. El suscriptor del certificado es responsable de limitar el uso del certificado a lo dispuesto en la Política de Certificación asociada, que es un documento público y que se encuentra disponible en <http://www.accv.es>.
6. La Agencia de Tecnología y Certificación Electrónica, no se responsabiliza del contenido de los documentos firmados haciendo uso de los certificados por ella emitidos.
7. La Agencia de Tecnología y Certificación Electrónica, es responsable del cumplimiento de las legislaciones Europea, Española y Valenciana, por lo que a Firma Electrónica se refiere. Es, asimismo, responsable del cumplimiento de lo dispuesto en la Declaración de Prácticas de Certificación de la ACCV y en la Política de Certificación asociada a este tipo de certificados.
8. El periodo de validez de estos certificados es de tres (3) años. Para su renovación deberán seguirse el mismo procedimiento que para la primera solicitud o bien los procedimientos previstos en la Política de Certificación asociada.
9. Los certificados emitidos perderán su eficacia, además de al vencimiento del periodo de validez, cuando se produzca una revocación, cuando se inutilice el soporte del certificado, ante resolución judicial o administrativa que ordene la pérdida de eficacia, por inexactitudes graves en los datos aportados por el solicitante y por fallecimiento del suscriptor del certificado. Otras condiciones para la pérdida de eficacia se recogen en la Declaración de Prácticas de Certificación y en la Política de Certificación asociada a este tipo de certificados.
10. La documentación a aportar para la identificación de los solicitantes será el Documento Nacional de Identidad, NIE o Pasaporte válido y vigente.
11. El cumplimiento de la ley 15/1.999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa al solicitante de la existencia de un fichero automatizado de datos de carácter personal creado bajo la responsabilidad de la Agencia de Tecnología y Certificación Electrónica, denominado "Usuarios de firma electrónica". La finalidad de dicho fichero es la servir a los usos relacionados con los servicios de certificación prestados por la Agencia de Tecnología y Certificación Electrónica. El suscriptor consiente expresamente la utilización de sus datos de carácter personal contenidos en dicho fichero, en la medida en que sea necesario para llevar a cabo las acciones previstas en la Política de Certificación.
12. La Agencia de Tecnología y Certificación Electrónica se compromete a poner los medios a su alcance para evitar la alteración, pérdida o acceso no autorizado a los datos de carácter personal contenidos en el fichero.
13. El solicitante podrá ejercer sus derechos de acceso, rectificación o cancelación sobre sus datos de carácter personal dirigiendo escrito a la Agencia de Tecnología y Certificación Electrónica, a través de cualquiera de los Registros de Entrada de la Generalitat indicando claramente esta voluntad.
14. Se aconseja al usuario realizar el cambio del PIN inicial que aparece en el presente contrato a través de las herramientas que pone a su disposición la Autoridad de Certificación, así como custodiar de forma segura el PUK
15. La Agencia de Tecnología y Certificación Electrónica ha constituido un aval bancario por un importe de tres millones de euros (3.000.000,00 €) para afrontar el riesgo por la responsabilidad por los daños y perjuicios que pudiera ocasionar el uso de los certificados expedidos y los servicios de certificación digital.

Ejemplar para el solicitante - Reverso

| | | |
|----------------|--------------------------------|--------------|
| Clf.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 40 |

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.20

Secció 1 – Dades del subscriptor / Sección 1 – Datos del suscriptor

Cognoms/Apellidos:

Nom/Nombre:

DNI/NIF:

Tel.:

Càrrec/Puesto o cargo:

Unitat Organitzativa-Departament/Unidad Organizativa-Departamento:

Empresa-Organismo/Empresa-Organismo

CIF de la Organització/CIF de la Organización:

Adreça de correu electrònic/Dirección correo electrónico:

Adreça postal/Dirección postal:

Secció 2 – Dades del operador del Punt de Registre / Sección 2 – Datos del operador del Punto de Registro

Nom i cognoms/Nombre y Apellidos:

Secció 3 - Data i Firma / Sección 3 – Fecha y Firma

Subscribo el present contracte de certificació associat a la Política de Certificació de Certificats Qualificats de Empleat Públic amb codi 1.3.6.1.4.1.8149.3.20, emés per la Generalitat. Declare que conec i accepto les normes d'utilització d'este tipus de certificats que es troben exposades en <http://www.accv.es>. Declare, així mateix, que les dades posades de manifest són certes.

Suscribo el presente contrato de certificación asociado a la Política de Certificación de Certificados Cualificados de Pertenencia a Empresa con código 1.3.6.1.4.1.8149.3.20, emitido por la Agencia de Tecnología y Certificación Electrónica. Declaro conocer y aceptar las normas de utilización de este tipo de certificados que se encuentran expuestas en <http://www.accv.es>. Declaro, asimismo, que los datos puestos de manifiesto son ciertos.

Firma del subscriptor
Firma del suscriptor

Firma i segell del Punt de Registre
Firma y sello del Punto de Registro

Firmat/*Firmado*:

Firmat/*Firmado*:

Nº de petició

Exemplar per a la ACCV / *Ejemplar para la ACCV*

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 41 |

13 Anexo IV – Formulario de solicitud de certificados

D'acord amb la Política de Certificació de Certificats Reconeguts de Pertenença a Empresa, es requereixen les següents dades per a la correcta emissió de certificats.
De acuerdo con la Política de Certificación de Certificados Reconocidos de Pertenencia a Empresa, se requieren los siguientes datos para la correcta emisión de certificados.

DADES COMUNES / DATOS COMUNES

NOM DE L'ORGANISME / NOMBRE DEL ORGANISMO:

CIF:

Domicilio:

Localidad:

DADES DEL PERSONAL / DATOS DEL PERSONAL (los campos con * son opcionales)

NIF/NIE Cognom1/Apellido1 Cognom2/Apellido2 Nom/Nombre Adreça electrònica/Correo electrónico Càrrec/Cargo* Unitat/Unidad* Identificació personal/IdeTelèfon/Teléfono*

| | | |
|----------------|--------------------------------|--------------|
| Cif.: PÚBLICO | Ref.: ACCV-CP-20V4.0.doc | Versión: 4.0 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.3.20.4.0 | Pág. 45 |