

# Política de Certificación

Proyecto e-firmaGV



**Certificados para  
Correo y Aplicaciones Seguras**

**Fecha:** 20 de enero de 2003

**Versión:** 1.0

**Archivo:** PKIGVA-CP-02V1.0.doc

**OID:** 1.3.6.1.4.1.8149.3.2.1.2.1.0

**Preparado por:** Proyecto e-firmaGV

## Tabla de Contenido

<b>1. INTRODUCCIÓN</b>	<b>7</b>
1.1. VISTA GENERAL	7
1.2. IDENTIFICACIÓN	7
1.3. COMUNIDAD Y ÁMBITO DE APLICACIÓN	8
1.3.1. Autoridades de Certificación	8
1.3.2. Autoridades de Registro	8
1.3.3. Entidades Finales	8
1.3.4. Ámbito de aplicación	9
1.4. DATOS DE CONTACTO	10
1.4.1. Persona de Contacto	10
1.4.2. Determinación de la adecuación de la CPS a la Política	10
<b>2. CLÁUSULAS GENERALES</b>	<b>11</b>
2.1. OBLIGACIONES	11
2.1.1. Obligaciones de la CA	11
2.1.2. Obligaciones de la RA	11
2.1.3. Obligaciones de los Subscriptores	11
2.1.4. Obligaciones de las partes confiantes	11
2.1.5. Obligaciones del repositorio	11
2.2. RESPONSABILIDAD	11
2.2.1. Responsabilidad de la CA	11
2.2.2. Responsabilidad de la RA	12
2.3. RESPONSABILIDAD FINANCIERA	12
2.3.1. Indemnización a las partes confiantes	12
2.3.2. Relaciones fiduciarias	12
2.3.3. Procesos administrativos	12
2.4. INTERPRETACIÓN Y EJECUCIÓN	12
2.4.1. Leyes gubernamentales	12
2.4.2. Extinción, subsistencia, fusión, y notificación	12
2.4.3. Procedimientos de resolución de disputas	12
2.5. TARIFAS	13
2.5.1. Tarifas de emisión de certificado o renovación	13
2.5.2. Tarifas de acceso a los certificados	13
2.5.3. Tarifas de acceso a la información de estado o revocación	13
2.5.4. Tarifas de otros servicios como información de políticas	13
2.5.5. Política de reintegros	13
2.6. PUBLICACIÓN Y REPOSITORIOS	13

2.6.1.	<i>Publicación de información de la CA</i> .....	13
2.6.2.	<i>Frecuencia de publicación</i> .....	13
2.6.3.	<i>Controles de acceso</i> .....	14
2.6.4.	<i>Repositorios</i> .....	14
2.7.	<b>CONTROL DE CONFORMIDAD</b> .....	14
2.7.1.	<i>Frecuencia de los controles de conformidad para cada entidad</i> .....	14
2.7.2.	<i>Identificación/cualificación del auditor</i> .....	14
2.7.3.	<i>Relación entre el auditor y la entidad auditada</i> .....	14
2.7.4.	<i>Tópicos cubiertos por el control de conformidad</i> .....	14
2.7.5.	<i>Acciones a tomar como resultado de una deficiencia</i> .....	14
2.7.6.	<i>Comunicación de resultados</i> .....	14
2.8.	<b>POLÍTICA DE CONFIDENCIALIDAD</b> .....	15
2.8.1.	<i>Tipo de información a mantener confidencial</i> .....	15
2.8.2.	<i>Tipo de información no considerada confidencial</i> .....	15
2.8.3.	<i>Divulgación de información de revocación /suspensión de certificados</i> .....	15
2.8.4.	<i>Envío a la autoridad judicial y/o policial</i> .....	15
2.8.5.	<i>Publicación como parte de un descubrimiento civil</i> .....	15
2.8.6.	<i>Divulgación a petición del propietario</i> .....	15
2.8.7.	<i>Otras circunstancias de publicación de información</i> .....	15
2.9.	<b>DERECHOS DE PROPIEDAD INTELECTUAL</b> .....	15
<b>3.</b>	<b>IDENTIFICACIÓN Y AUTENTIFICACIÓN</b> .....	<b>16</b>
3.1.	<b>REGISTRO INICIAL</b> .....	16
3.1.1.	<i>Tipos de nombres</i> .....	16
3.1.2.	<i>Necesidad de los nombres de ser significativos</i> .....	16
3.1.3.	<i>Reglas para interpretar varios formatos de nombres</i> .....	16
3.1.4.	<i>Unicidad de los nombres</i> .....	16
3.1.5.	<i>Procedimientos de resolución de disputas de nombres</i> .....	16
3.1.6.	<i>Reconocimiento, autenticación y función de las marcas registradas</i> .....	16
3.1.7.	<i>Métodos de prueba de posesión de la clave privada</i> .....	16
3.1.8.	<i>Autenticación de la identidad de una organización</i> .....	16
3.1.9.	<i>Autenticación de la identidad de un individuo</i> .....	17
3.2.	<b>RENOVACIÓN RUTINARIA DE LA CLAVE</b> .....	17
3.3.	<b>RENOVACIÓN DE CLAVE DESPUÉS DE UNA REVOCACIÓN – CLAVE NO COMPROMETIDA</b> .....	17
3.4.	<b>SOLICITUD DE REVOCACIÓN</b> .....	17
<b>4.</b>	<b>REQUERIMIENTOS OPERACIONALES</b> .....	<b>18</b>
4.1.	<b>SOLICITUD DE CERTIFICADOS</b> .....	18
4.2.	<b>EMISIÓN DE CERTIFICADOS</b> .....	18
4.3.	<b>ACEPTACIÓN DE CERTIFICADOS</b> .....	19
4.4.	<b>SUSPENSIÓN Y REVOCACIÓN DE CERTIFICADOS</b> .....	19

4.4.1.	<i>Circunstancias para la revocación</i> .....	19
4.4.2.	<i>Quién puede solicitar la revocación</i> .....	19
4.4.3.	<i>Procedimiento de solicitud de revocación</i> .....	19
4.4.4.	<i>Periodo de gracia de la solicitud de revocación</i> .....	21
4.4.5.	<i>Circunstancias para la suspensión</i> .....	21
4.4.6.	<i>Quien puede solicitar la suspensión</i> .....	21
4.4.7.	<i>Procedimiento para la solicitud de suspensión</i> .....	21
4.4.8.	<i>Limites del periodo de suspensión</i> .....	21
4.4.9.	<i>Frecuencia de emisión de CRLs (si aplicable)</i> .....	21
4.4.10.	<i>Requisitos de comprobación de CRLs</i> .....	21
4.4.11.	<i>Disponibilidad de comprobación on-line de revocación/estado</i> .....	21
4.4.12.	<i>Requisitos de comprobación on-line de revocación</i> .....	21
4.4.13.	<i>Otras formas de divulgación de revocación disponibles</i> .....	22
4.4.14.	<i>Requisitos de comprobación para otras formas de divulgación de revocación</i> .....	22
4.4.15.	<i>Requisitos especiales de renovación de claves comprometidas</i> .....	22
4.5.	PROCEDIMIENTOS DE CONTROL DE SEGURIDAD.....	22
4.5.1.	<i>Tipos de eventos registrados</i> .....	22
4.5.2.	<i>Frecuencia de procesado de logs</i> .....	22
4.5.3.	<i>Periodo de retención para los logs de auditoría</i> .....	22
4.5.4.	<i>Protección de los logs de auditoría</i> .....	22
4.5.5.	<i>Procedimientos de backup de los logs de auditoría</i> .....	23
4.5.6.	<i>Sistema de recogida de información de auditoría (interno vs externo)</i> .....	23
4.5.7.	<i>Notificación al sujeto causa del evento</i> .....	23
4.5.8.	<i>Análisis de vulnerabilidades</i> .....	23
4.6.	ARCHIVO DE REGISTROS.....	23
4.6.1.	<i>Tipo de eventos registrados</i> .....	23
4.6.2.	<i>Periodo de retención para el archivo</i> .....	23
4.6.3.	<i>Protección del archivo</i> .....	23
4.6.4.	<i>Procedimientos de backup del archivo</i> .....	23
4.6.5.	<i>Requerimientos para el sellado de tiempo de los registros</i> .....	24
4.6.6.	<i>Sistema de recogida de información de auditoría (interno vs externo)</i> .....	24
4.6.7.	<i>Procedimientos para obtener y verificar información archivada</i> .....	24
4.7.	CAMBIO DE CLAVE.....	24
4.8.	RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O UN DESASTRE .....	24
4.8.1.	<i>Alteración de los recursos hardware, software y/o datos</i> .....	24
4.8.2.	<i>La clave publica de una entidad se revoca</i> .....	24
4.8.3.	<i>La clave de una entidad se compromete</i> .....	24
4.8.4.	<i>Instalación de seguridad después de un desastre natural u otro tipo de desastre</i> .....	24
4.9.	CESE DE UNA CA.....	25
<b>5.</b>	<b>CONTROLES DE SEGURIDAD FÍSICA, PROCEDURAL Y DE PERSONAL</b> .....	<b>26</b>

5.1.	CONTROLES DE SEGURIDAD FÍSICA .....	26
5.1.1.	<i>Ubicación y construcción</i> .....	26
5.1.2.	<i>Acceso físico</i> .....	26
5.1.3.	<i>Alimentación eléctrica y aire acondicionado</i> .....	26
5.1.4.	<i>Exposición al agua</i> .....	26
5.1.5.	<i>Protección y prevención de incendios</i> .....	26
5.1.6.	<i>Sistema de almacenamiento</i> .....	26
5.1.7.	<i>Eliminación de residuos</i> .....	26
5.1.8.	<i>Backup remoto</i> .....	27
5.2.	CONTROLES PROCEDIMENTALES .....	27
5.2.1.	<i>Papeles de confianza</i> .....	27
5.2.2.	<i>Numero de personas requeridas por tarea</i> .....	27
5.2.3.	<i>Identificación y autenticación para cada papel</i> .....	27
5.3.	CONTROLES DE SEGURIDAD DE PERSONAL .....	27
5.3.1.	<i>Requerimientos de antecedentes, calificación, experiencia, y acreditación</i> .....	27
5.3.2.	<i>Procedimientos de comprobación de antecedentes</i> .....	27
5.3.3.	<i>Requerimientos de formación</i> .....	27
5.3.4.	<i>Requerimientos y frecuencia de la actualización de la formación</i> .....	27
5.3.5.	<i>Frecuencia y secuencia de rotación de tareas</i> .....	28
5.3.6.	<i>Sanciones por acciones no autorizadas</i> .....	28
5.3.7.	<i>Requerimientos de contratación de personal</i> .....	28
5.3.8.	<i>Documentación proporcionada al personal</i> .....	28
<b>6.</b>	<b>CONTROLES DE SEGURIDAD TÉCNICA .....</b>	<b>29</b>
6.1.	GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES .....	29
6.1.1.	<i>Generación del par de claves</i> .....	29
6.1.2.	<i>Entrega de la clave privada a la entidad</i> .....	29
6.1.3.	<i>Entrega de la clave pública al emisor del certificado</i> .....	29
6.1.4.	<i>Entrega de la clave pública de la CA a los usuarios</i> .....	29
6.1.5.	<i>Tamaño de las claves</i> .....	29
6.1.6.	<i>Parámetros de generación de la clave pública</i> .....	29
6.1.7.	<i>Comprobación de la calidad de los parámetros</i> .....	29
6.1.8.	<i>Hardware/software de generación de claves</i> .....	30
6.1.9.	<i>Fines del uso de la clave</i> .....	30
6.2.	PROTECCIÓN DE LA CLAVE PRIVADA .....	30
6.2.1.	<i>Estándares para los módulos criptográficos</i> .....	30
6.2.2.	<i>Control multipersona (n de entre m) de la clave privada</i> .....	30
6.2.3.	<i>Custodia de la clave privada</i> .....	30
6.2.4.	<i>Copia de seguridad de la clave privada</i> .....	31
6.2.5.	<i>Archivo de la clave privada</i> .....	31
6.2.6.	<i>Introducción de la clave privada en el módulo criptográfico</i> .....	31

6.2.7.	<i>Método de activación de la clave privada</i> .....	31
6.2.8.	<i>Método de desactivación de la clave privada</i> .....	31
6.2.9.	<i>Método de destrucción de la clave privada</i> .....	31
6.3.	OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES .....	31
6.3.1.	<i>Archivo de la clave pública</i> .....	31
6.3.2.	<i>Periodo de uso para las claves públicas y privadas</i> .....	32
6.4.	DATOS DE ACTIVACIÓN .....	32
6.4.1.	<i>Generación y activación de los datos de activación</i> .....	32
6.4.2.	<i>Protección de los datos de activación</i> .....	32
6.4.3.	<i>Otros aspectos de los datos de activación</i> .....	32
6.5.	CONTROLES DE SEGURIDAD INFORMÁTICA .....	32
6.5.1.	<i>Requerimientos técnicos de seguridad informática específicos</i> .....	32
6.5.2.	<i>Valoración de la seguridad informática</i> .....	33
6.6.	CONTROLES DE SEGURIDAD DEL CICLO DE VIDA .....	33
6.6.1.	<i>Controles de desarrollo del sistema</i> .....	33
6.6.2.	<i>Controles de gestión de la seguridad</i> .....	33
6.6.3.	<i>Evaluación de la seguridad del ciclo de vida</i> .....	33
6.7.	CONTROLES DE SEGURIDAD DE LA RED .....	33
6.8.	CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS .....	33
<b>7.</b>	<b>PERFILES DE CERTIFICADO Y CRL .....</b>	<b>34</b>
7.1.	PERFIL DE CERTIFICADO.....	34
7.1.1.	<i>Número de versión</i> .....	34
7.1.2.	<i>Extensiones del certificado</i> .....	34
7.1.3.	<i>Identificadores de objeto (OID) de los algoritmos</i> .....	35
7.1.4.	<i>Formatos de nombres</i> .....	35
7.1.5.	<i>Restricciones de los nombres</i> .....	35
7.1.6.	<i>Identificador de objeto (OID) de la Política de certificación</i> .....	36
7.1.7.	<i>Uso de la extensión “Policy Constraints”</i> .....	36
7.1.8.	<i>Sintaxis y semántica de los cualificadores de política</i> .....	36
7.1.9.	<i>Tratamiento semántico para la extensión crítica “Certificate Policy”</i> .....	36
7.2.	PERFIL DE CRL .....	36
7.2.1.	<i>Número de versión</i> .....	36
7.2.2.	<i>CRL y extensiones</i> .....	36
<b>8.</b>	<b>ESPECIFICACIÓN DE LA ADMINISTRACIÓN .....</b>	<b>37</b>
8.1.	PROCEDIMIENTOS DE ESPECIFICACIÓN DE CAMBIOS .....	37
8.2.	PROCEDIMIENTOS DE PUBLICACIÓN Y NOTIFICACIÓN .....	37
8.3.	PROCEDIMIENTOS DE APROBACIÓN DE LA CPS .....	37
<b>ANEXO I.</b>	<b>.....</b>	<b>38</b>

## 1. INTRODUCCIÓN

La presente Política de Certificación es conforme con la especificación del RFC 2527 *“Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”* propuesto por S. Chokhani y W. Ford, del Internet Engineering Task Force (IETF), para este tipo de documentos. Se incluyen todas las secciones de la especificación a fin de dotar de consistencia al documento. Cuando no exista ninguna disposición o limitación respecto de una sección aparecerá la frase “No estipulado” contenida en dicha sección.

Esta Política de Certificación asume que el lector conoce los conceptos básicos de PKI, 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.

### 1.1. Vista General

Esta Política de certificación 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 PKI y las reglas de solicitud, adquisición gestión y uso de los certificados.

La Política de Certificación referida en este documento se utilizará para firma digital y cifrado de mensajes de correo electrónico S/MIME y para firma de documentos y formularios y autenticación de usuario en aquellas aplicaciones y servicios con capacidades de PKI pertenecientes al ámbito de la Generalitat Valenciana, a entidades y organismos vinculados a ella, o a alguna Administración Pública o Corporativa con la que haya establecido convenio de certificación, que sean autorizados por la Autoridad de Aprobación de Políticas de PKIGVA.

La entidad involucrada en el uso de los certificados emitidos bajo el amparo de la presente política es la propia Generalitat Valenciana así como las entidades y organismos vinculados a ella, y las Administraciones Públicas o Corporativas con la que haya establecido convenio de certificación.

### 1.2. Identificación

Nombre de la política	Certificados para Correo y Aplicaciones Seguras
Calificador de la política	El uso de este certificado está restringido a correo seguro y aplicaciones pertenecientes a la Generalitat Valenciana, a entidades y organismos vinculados a ella, o a alguna Administración Pública con la que haya establecido convenio de certificación.
Versión de la política	1.0
Estado de la política	Vigente

<b>e-firmagv</b>	<b>Política de certificación: Certificados para Correo y Aplicaciones Seguras</b>
Referencia de la política / OID (Object Identifier)	1.3.6.1.4.1.8149.3.2.1.2.1.0
Fecha de emisión	27 de enero de 2003
Fecha de expiración	No aplicable.
CPS relacionada	Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalitat Valenciana. Versión 1.0.  OID: 1.3.6.1.4.1.8149.2.1.0  Disponible en <a href="http://www.pki.gva.es/cps">http://www.pki.gva.es/cps</a>
Localización	Esta Política de certificación se puede encontrar en: <a href="http://www.pki.gva.es/cps/pol2101.htm">http://www.pki.gva.es/cps/pol2101.htm</a>

## 1.3. Comunidad y Ámbito de aplicación

### 1.3.1. Autoridades de Certificación

La CA que puede emitir certificados acordes con esta política es la “**CAGVA**” perteneciente a la PKI de la Generalitat Valenciana.

### 1.3.2. Autoridades de Registro

Las Autoridades de Registro que gestionan las solicitudes de certificados definidos en esta política estarán definidos en el documento "Ámbitos de Certificación y Puntos de Registro", que se puede consultar en <http://www.pki.gva.es/cp02/acpr.htm>.

### 1.3.3. Entidades Finales

#### 1.3.3.1. Subscriptores

El grupo de usuarios que pueden solicitar certificados definidos por esta política está compuesto por las personas que encajen en alguno de los ámbitos de certificación, determinados por la Dirección General de Telecomunicaciones y Modernización, a través del documento "Ámbitos de Certificación y Puntos de Registro", ubicado en <http://www.pki.gva.es/cp02/acpr.htm>.

El soporte de claves y certificados será smartcard, disquete o CDROM dependiendo del perfil de los solicitantes y de las aplicaciones a las que destine su uso más frecuente.

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 la Generalitat Valenciana, a alguna de las entidades u organizaciones vinculados a la Generalitat o a Administraciones Públicas o Corporativas con las que se haya firmado convenio de certificación, que sean autorizados por la Autoridad de Aprobación de Políticas de PKIGVA en el ámbito de firma y verificación de la firma de documentos y formularios, cifrado de documentos y autenticación de usuarios.
- Las aplicaciones y servicios que, sin pertenecer a la Generalitat Valenciana, entidades u organismos vinculados a ella, ni a Administraciones Públicas ni Corporativas con las que se haya establecido convenio de certificación, se emplean en relaciones entre ciudadanos, empresas u otras Administraciones Públicas con la Generalitat Valenciana, entidades u organismos vinculados a ella o Administraciones Públicas con las que se haya establecido convenio de certificación.

### 1.3.4. Ámbito de aplicación

#### 1.3.4.1. Usos Permitidos

Los certificados emitidos por la PKI de la Generalitat Valenciana bajo esta Política de Certificación, pueden utilizarse para la firma digital y cifrado de mensajes de correo electrónico S/MIME. Asimismo, pueden utilizarse como mecanismo de identificación ante servicios y para la firma electrónica de documentos.

#### 1.3.4.2. Usos Restringidos

Los certificados emitidos por la PKI de la Generalitat Valenciana bajo esta Política de Certificación pueden ser utilizados, de forma restringida por los usuarios de aplicaciones y servicios pertenecientes al ámbito de la Generalitat Valenciana o al de otras Administraciones Públicas o Corporativas con las que se haya establecido convenio de certificación, para la firma o cifrado de documentos y formularios, la comprobación de firma y la autenticación de usuario.

#### 1.3.4.3. Usos Prohibidos

Esta prohibido el uso de los certificados emitidos por la PKI de la Generalitat Valenciana bajo esta Política de certificación para cualquier uso no especificados por los puntos “1.3.4.1 Usos Permitidos” y “1.3.4.2 Usos Restringidos” del presente documento.

## 1.4. Datos de contacto

Esta Política de Certificación es propiedad de la “Direcció General de Telecomunicacions i Modernització”.

Nombre	<i>Direcció General de Telecomunicacions i Modernització</i>
Dirección de email	<a href="mailto:dgtm@gva.es">dgtm@gva.es</a>
Dirección	<i>C/ Colón, 66 – 46004 Valencia (Spain)</i>
Número de teléfono	<i>+34-96-196 1061</i>
Número de fax	<i>+34-96-196 1001</i>

Esta Política de Certificación está administrada por la Autoridad de Aprobación de Políticas (AAP) de la PKI de la Generalitat Valenciana.

Nombre	<i>AAP PKI de la Generalitat Valenciana</i>
Dirección de email	<a href="mailto:aap@pki.gva.es">aap@pki.gva.es</a>
Dirección	<i>C/ Colón, 66 – 46004 Valencia (Spain)</i>
Número de teléfono	<i>+34-902-482-481</i>
Número de fax	<i>+34-96-196-1001</i>

### 1.4.1. Persona de Contacto

Para más información relacionada con la presente Política de Certificación por favor contacte con:

Nombre	<i>Proyecto e-firmaGV</i>
Dirección de email	<a href="mailto:firma@gva.es">firma@gva.es</a>
Dirección	<i>C/ Colón, 66 – 46004 Valencia (Spain)</i>
Número de teléfono	<i>+34-902 482 481</i>
Número de fax	<i>+34-96 196 1001</i>

### 1.4.2. Determinación de la adecuación de la CPS a la Política

La Autoridad de Aprobación de Políticas (AAP) de la PKI de la Generalitat Valenciana es la entidad que determina la adecuación de esta política a la CPS de su PKI

## 2. Cláusulas Generales

### 2.1. Obligaciones

#### 2.1.1. Obligaciones de la CA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

Adicionalmente, las CAs especificadas en el punto 1.3.1 “Autoridades de Certificación” están obligadas a:

- Adaptar sus operaciones para cumplir lo estipulado por esta Política de Certificación.
- Emitir certificados en conformidad con esta Política de Certificación.

#### 2.1.2. Obligaciones de la RA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 2.1.3. Obligaciones de los Subscriptores

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 2.1.4. Obligaciones de las partes confiantes

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 2.1.5. Obligaciones del repositorio

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.2. Responsabilidad

#### 2.2.1. Responsabilidad de la CA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

## 2.2.2. Responsabilidad de la RA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

## 2.3. Responsabilidad Financiera

### 2.3.1. Indemnización a las partes confiantes

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.3.2. Relaciones fiduciarias

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.3.3. Procesos administrativos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

## 2.4. Interpretación y Ejecución

### 2.4.1. Leyes gubernamentales

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.4.2. Extinción, subsistencia, fusión, y notificación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.4.3. Procedimientos de resolución de disputas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

## 2.5. Tarifas

### 2.5.1. Tarifas de emisión de certificado o renovación

No se aplica ninguna tarifa sobre la emisión o renovación de certificados bajo el amparo de la presente Política de certificación.

### 2.5.2. Tarifas de acceso a los certificados

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

### 2.5.3. Tarifas de acceso a la información de estado o revocación

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

### 2.5.4. Tarifas de otros servicios como información de políticas

No se aplicará ninguna tarifa por el servicio de información sobre esta política ni por ningún otro servicio adicional del que se tenga conocimiento en el momento de la redacción del presente documento.

### 2.5.5. Política de reintegros

Al no existir ninguna tarifa de aplicación para esta Política de certificación no es necesaria ninguna política de reintegros.

## 2.6. Publicación y Repositorios

### 2.6.1. Publicación de información de la CA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

La presente Política de Certificación es pública y se encuentra disponible, en formato PDF, en la ubicación especificada en el apartado localización del punto "1.2 Identificación" del presente documento.

### 2.6.2. Frecuencia de publicación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.6.3. Controles de acceso

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.6.4. Repositorios

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

## 2.7. Control de conformidad

### 2.7.1. Frecuencia de los controles de conformidad para cada entidad

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.7.2. Identificación/cualificación del auditor

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.7.3. Relación entre el auditor y la entidad auditada

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.7.4. Tópicos cubiertos por el control de conformidad

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.7.5. Acciones a tomar como resultado de una deficiencia

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.7.6. Comunicación de resultados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

## 2.8. Política de Confidencialidad

### 2.8.1. Tipo de información a mantener confidencial

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.8.2. Tipo de información no considerada confidencial

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.8.3. Divulgación de información de revocación /suspensión de certificados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.8.4. Envío a la autoridad judicial y/o policial

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.8.5. Publicación como parte de un descubrimiento civil

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.8.6. Divulgación a petición del propietario

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 2.8.7. Otras circunstancias de publicación de información

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

## 2.9. Derechos de propiedad Intelectual

Todos los derechos de propiedad intelectual de la presente Política de Certificación pertenecen y permanecerán en propiedad de la Generalitat Valenciana.

## **3. IDENTIFICACIÓN Y AUTENTIFICACIÓN**

### **3.1. Registro inicial**

#### **3.1.1. Tipos de nombres**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **3.1.2. Necesidad de los nombres de ser significativos**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **3.1.3. Reglas para interpretar varios formatos de nombres**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **3.1.4. Unicidad de los nombres**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **3.1.5. Procedimientos de resolución de disputas de nombres**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **3.1.7. Métodos de prueba de posesión de la clave privada**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **3.1.8. Autenticación de la identidad de una organización**

El derecho de solicitud de certificados definido en la presente Política de Certificación se encuentra limitado a personas físicas. No se aceptarán solicitudes de certificación realizadas en nombre de

personas jurídicas, entidades u organizaciones. Por tanto, no se considera necesaria la identificación de ninguna organización.

### 3.1.9. Autenticación de la identidad de un individuo

La autenticación de la identidad del solicitante de un certificado se realizará mediante la presentación del Documento Nacional de Identidad (DNI) del solicitante ante el Operador de Registro en el momento de recoger el certificado.

Es necesario hacer notar que en este tipo de certificados se incluye la dirección de correo electrónico del suscriptor como elemento necesario para soportar el protocolo S/MIME, pero que PKIGVA no garantiza que esta dirección de correo esté vinculada con el suscriptor del certificado, por lo que la confianza o no en que esta dirección sea la del titular del certificado corresponde únicamente a la parte confiante. PKIGVA únicamente garantiza que la dirección de correo que consta en el certificado fue la aportada por el suscriptor en el momento de la formalización de su solicitud y/o que consta como vinculada al titular en las bases de datos de personal de la Generalitat Valenciana.

## 3.2. Renovación rutinaria de la clave

La autenticación para la renovación del certificado se puede realizar utilizando las técnicas para la autenticación e identificación inicial o bien utilizando solicitudes firmadas digitalmente u otros sistemas en los que quede perfectamente identificado el solicitante de la renovación, mediante el certificado original que se pretende renovar, siempre que este no haya vencido ni se haya procedido a su revocación.

## 3.3. 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.

## 3.4. Solicitud de revocación

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

PKIGVA 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.

## 4. REQUERIMIENTOS OPERACIONALES

### 4.1. Solicitud de certificados

El solicitante de un certificado acogido a la presente Política de Certificación deberá cumplimentar una solicitud de certificación a través de un formulario web ubicado en <http://www.pki.gva.es>, apartado "Gestión de Certificados", subapartado "Gestión de Certificados para Correo y Aplicaciones Seguras".

Una vez cumplimentado el formulario de solicitud, ésta se envía, automáticamente, a la Autoridad de Registro de PKIGVA.

Es atribución de la Autoridad de Registro de PKIGVA el determinar la adecuación de un tipo de certificado a las características del solicitante, en función de las disposiciones de la Política de Certificación aplicable, y de este modo acceder o denegar la gestión de la solicitud de certificación del mismo.

En el caso de denegación de la solicitud de certificación por parte del Operador de la Autoridad de Registro, el solicitante recibirá un correo electrónico en la dirección que hizo constar en su solicitud, informándole de los motivos del rechazo de la misma.

Las solicitudes de certificación una vez aceptadas son enviadas a la Autoridad de Certificación por la Autoridad de Registro de PKIGVA.

### 4.2. Emisión de certificados

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

Tras la emisión del certificado la Autoridad de Registro lo notificará al subscriptor del mismo mediante la presentación de una página html de retorno de solicitud o el envío de un correo electrónico firmado a la dirección que figure en la solicitud, en el que además le informará sobre la dirección de la oficina *–Punto de Registro de Usuario–*, en la que debe recoger el certificado, para lo cual deberá presentar documento acreditativo de identidad (DNI, pasaporte o carta de residencia) y firmar el Contrato de Certificación.

El Contrato de Certificación es un documento que debe ser firmado manualmente por el solicitante y por la persona adscrita al 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.

### 4.3. Aceptación de certificados

El suscriptor demuestra su aceptación del certificado con la firma del Contrato de Certificación y la recogida del mismo.

### 4.4. Suspensión y revocación de certificados

#### 4.4.1. Circunstancias para la revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 4.4.2. Quién puede solicitar la revocación

La revocación de un certificado se puede iniciar tanto por el suscriptor del mismo como por parte de PKIGVA.

Los suscriptores de certificados pueden solicitar su revocación por cualquier razón o sin ninguna razón y deben solicitar la revocación bajo las condiciones especificadas en el siguiente apartado.

#### 4.4.3. Procedimiento de solicitud de revocación

Se determina que:

- Se aceptarán solicitudes de revocación remotas si están firmadas digitalmente con un certificado de PKIGVA y presenciales si se cumplen los requisitos de identificación del usuario establecidos para el registro inicial (personación en algún *Punto de Registro de Usuario* y presentación de DNI, pasaporte o carta de residencia).
- 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 15 días naturales, durante los que se procederá a verificar la veracidad de la solicitud. En el caso de no poder verificar la falsedad de 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 la pública contenida en el certificado.

Una solicitud de revocación tanto si se realiza en papel o de forma electrónica (ej.: correo electrónico) debe contener la información siguiente:

Solicitud de revocación de certificado

Fecha : \_\_\_\_\_

**Sección 1 - Detalles del certificado (si se conocen)**

ID certificado: .....

Número de serie del certificado: .....

Tipo de certificado: .....

**Sección 2 - Datos del suscriptor del certificado**

Nombre: .....

NIF: .....

**Sección 3 - Motivo de la revocación \***

.....  
.....  
.....  
.....  
.....

\* La simple voluntad de revocación del suscriptor del certificado es un motivo válido para la solicitud de la misma.

**Sección 4 - Autorización**

Autorizado por:  Suscriptor del certificado  
 Tercera parte autorizada (especificar)

.....

Firma: .....

#### **4.4.4. Periodo de gracia de la solicitud de revocación**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **4.4.5. Circunstancias para la suspensión**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **4.4.6. Quien puede solicitar la suspensión**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **4.4.7. Procedimiento para la solicitud de suspensión**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **4.4.8. Límites del periodo de suspensión**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **4.4.9. Frecuencia de emisión de CRLs (si aplicable)**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **4.4.10. Requisitos de comprobación de CRLs**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **4.4.11. Disponibilidad de comprobación on-line de revocación/estado**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **4.4.12. Requisitos de comprobación on-line de revocación**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 4.4.13. Otras formas de divulgación 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 de una dirección de correo electrónico, devuelve los certificados vinculados a esa dirección y el estado de éstos. Este formulario se encuentra en el sitio web de la Autoridad de Certificación (<http://www.pki.gva.es>).

#### 4.4.14. Requisitos de comprobación para otras formas de divulgación de revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 4.4.15. Requisitos especiales de renovación de claves comprometidas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 4.5. Procedimientos de Control de Seguridad

#### 4.5.1. Tipos de eventos registrados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 4.5.2. Frecuencia de procesado de logs

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 4.5.3. Periodo de retención para los logs de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 4.5.4. Protección de los logs de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **4.5.5. Procedimientos de backup de los logs de auditoría**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **4.5.6. Sistema de recogida de información de auditoría (interno vs externo)**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **4.5.7. Notificación al sujeto causa del evento**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **4.5.8. Análisis de vulnerabilidades**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### **4.6. Archivo de registros**

#### **4.6.1. Tipo de eventos registrados**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **4.6.2. Periodo de retención para el archivo**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **4.6.3. Protección del archivo**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **4.6.4. Procedimientos de backup del archivo**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 4.6.5. Requerimientos para el sellado de tiempo de los registros

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 4.6.6. Sistema de recogida de información de auditoría (interno vs externo)

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 4.6.7. Procedimientos para obtener y verificar información archivada

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 4.7. Cambio de Clave

No estipulado.

### 4.8. Recuperación en caso de compromiso de una clave o un desastre

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 4.8.2. La clave publica de una entidad se revoca

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 4.8.3. La clave de una entidad se compromete

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 4.8.4. 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 PKI de la Generalidad Valenciana.

#### 4.9. Cese de una CA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

## **5. CONTROLES DE SEGURIDAD FÍSICA, PROCEDURAL Y DE PERSONAL**

### **5.1. Controles de Seguridad Física**

#### **5.1.1. Ubicación y construcción**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **5.1.2. Acceso físico**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **5.1.3. Alimentación eléctrica y aire acondicionado**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **5.1.4. Exposición al agua**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **5.1.5. Protección y prevención de incendios**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **5.1.6. Sistema de almacenamiento**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **5.1.7. Eliminación de residuos**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 5.1.8. Backup remoto

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 5.2. Controles procedimentales

#### 5.2.1. Papeles de confianza

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 5.2.2. Numero de personas requeridas por tarea

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 5.2.3. Identificación y autenticación para cada papel

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 5.3. Controles de seguridad de personal

#### 5.3.1. Requerimientos de antecedentes, calificación, experiencia, y acreditación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 5.3.2. Procedimientos de comprobación de antecedentes

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 5.3.3. Requerimientos de formación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 5.3.4. Requerimientos y frecuencia de la actualización de la formación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 5.3.5. Frecuencia y secuencia de rotación de tareas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 5.3.6. Sanciones por acciones no autorizadas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 5.3.7. Requerimientos de contratación de personal

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### 5.3.8. Documentación proporcionada al personal

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

## 6. CONTROLES DE SEGURIDAD TÉCNICA

### 6.1. Generación e Instalación del Par de Claves

#### 6.1.1. Generación del par de claves

El par de claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación se generan por la Autoridad de Certificación de la Generalitat Valenciana o en tarjeta criptográfica del usuario.

#### 6.1.2. Entrega de la clave privada a la entidad

La clave privada se encuentra contenida en la smartcard que se entrega al suscriptor con su certificado en el momento de su registro.

En caso de soporte disquete o CDRom, la clave privada se encuentra en el fichero PKCS#12. Este fichero contiene las claves y el certificado de usuario en un fichero cifrado.

#### 6.1.3. Entrega de la clave pública al emisor del certificado

La clave pública a ser certificada es generada por la Autoridad de Registro y entregada a la Autoridad de Certificación 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

La clave pública de la Autoridad de Certificación que emite el certificado del suscriptor se pueden descargar del sitio web <http://www.pki.gva.es>.

Adicionalmente las claves públicas de todas las CA's pertenecientes a la jerarquía de confianza de PKIGVA se pueden descargar del sitio web <http://www.pki.gva.es>.

#### 6.1.5. Tamaño de las claves

El tamaño de las claves es de 1024 bits.

#### 6.1.6. Parámetros de generación de la clave pública

No aplicable.

#### 6.1.7. Comprobación de la calidad de los parámetros

No aplicable.

### 6.1.8. Hardware/software de generación de claves

La generación de la clave se realiza en smartcards criptográficas en caso de soporte smartcard.

En caso de que el continente del certificado y las claves sea disquete o CDROM, se generarán en un sistema perteneciente al núcleo protegido de la PKI.

### 6.1.9. Fines del uso de la clave

La clave definida por la presente política se utilizará para la verificación de la identidad de los usuarios ante aplicaciones y servicios internos al ámbito de la Generalitat Valenciana. Además, esta clave se empleará con el propósito de proporcionar "Correo Seguro". Para los certificados X.509 v3, este propósito se mapeará en los parámetros de "Key Usage" y "Extended Key Usage" del siguiente modo:

Key Usage:

- Digital Signature
- Data Encipherment
- Key Encipherment

Extended Key Usage

- Client Authentication

La definición detallada del perfil de certificado y los usos de las claves se encuentra en el apartado 7 "Perfiles de certificado y CRL" de este documento.

## 6.2. Protección de la Clave Privada

### 6.2.1. Estándares para los módulos criptográficos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 6.2.2. Control multipersona (n de entre m) de la clave privada

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 6.2.3. Custodia de la clave privada

No se custodian claves privadas de firma de los subscriptores de los certificados definidos por la presente política. Sí se hace custodia de las claves vinculadas a los certificados de cifrado.

#### **6.2.4. Copia de seguridad de la clave privada**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **6.2.5. Archivo de la clave privada**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

#### **6.2.7. Método de activación de la clave privada**

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

En caso de que el soporte sea disquete o CDROM, la activación de la clave privada se realizará a través de la introducción de la palabra de paso de acceso a esta clave, contenida en el fichero PKCS#12.

#### **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 smartcard que la contiene del lector PC/SC.

En caso de que el soporte sea disquete o CDROM, la desactivación se realizará cerrando la aplicación que la utiliza o cerrando el módulo criptográfico asociado.

#### **6.2.9. Método de destrucción de la clave privada**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### **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 PKI de la Generalidad Valenciana.

### 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.

El par de claves utilizado para la emisión de los certificados se crea para cada emisión, y por tanto también tienen una validez de tres (3) años.

## 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 smartcard que la contiene y que se proporciona al suscriptor del certificado con el mismo.

La generación del PIN de la smartcard se realiza en el momento de la inicialización de la misma, comunicándose el dato al suscriptor en el momento en que se le hace entrega. Es responsabilidad y obligación del suscriptor la modificación de ese PIN preconfigurado por uno de su exclusivo conocimiento de forma inmediata a la recepción de la smartcard y previa a su primer uso.

En caso de que el soporte sea disquete o CDROM, se proporcionará al suscriptor la palabra de paso de acceso a la clave privada o de protección del fichero que contiene el PKCS#12. Igualmente es responsabilidad y obligación del suscriptor la modificación de esa palabra de paso preconfigurada por una de su exclusivo conocimiento de forma inmediata a la recepción del fichero PKCS#12 y previa a su primer uso.

### 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

### 6.5.1. Requerimientos técnicos de seguridad informática específicos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 6.5.2. Valoración de la seguridad informática

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

## 6.6. Controles de Seguridad del Ciclo de Vida

### 6.6.1. Controles de desarrollo del sistema

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 6.6.2. Controles de gestión de la seguridad

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 6.6.3. Evaluación de la seguridad del ciclo de vida

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

## 6.7. Controles de Seguridad de la Red

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

## 6.8. Controles de Ingeniería de los Módulos Criptográficos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

## 7. PERFILES DE CERTIFICADO Y CRL

### 7.1. Perfil de Certificado

Esta política de certificación especifica el uso de dos certificados distintos para firma digital y cifrado de datos. El perfil de ambos certificados es idéntico excepto en el apartado 7.1.2 Extensiones del certificado. En dicho punto se especifica cuando existen diferencias entre ambos certificados.

#### 7.1.1. Número de versión

La presente política se implementa sobre certificados X.509 versión 3 (X.509 v3).

#### 7.1.2. Extensiones del certificado

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

- Key Usage {joint-iso-itu-t(2) ds(5) certificateExtension(29) keyUsage(15)}
  - Marcada como crítica y con la siguiente combinación de valores:
    - Para el certificado de firma:
      - Digital Signature
    - Para el certificado de cifrado
      - Data Enciphement
      - Key Enciphement
  
- Extended Key Usage {joint-iso-itu-t(2) ds(5) certificateExtension(29) extKeyUsage(37)}
  - Marcada como crítica y con la siguiente combinación de valores:
    - Para ambos certificados:
      - Email Protection
      - Client Autentication
  
- Certificate Policies. {joint-iso-itu-t(2) ds(5) certificateExtension(29) certificatePolicies(32)}
  - Marcada como crítica y con la siguiente combinación de valores:
    - Policy OID: 1.3.6.1.4.1.8149.3.2.1.2.1.0
    - Policy CPS Location: <http://pki.gva.es/cps/pol2101.htm>

- Policy Notice: El uso de este certificado está restringido a correo seguro y aplicaciones pertenecientes a la Generalitat Valenciana, a entidades y organismos vinculados a ella, o a alguna Administración Pública con la que haya establecido convenio de certificación. Este certificado se ha emitido como *Certificado Reconocido* de acuerdo con el Real Decreto-Ley 14/1999, de 17 de septiembre.
  
- Subject Alternative Name {joint-iso-itu-t(2) ds(5) certificateExtension(29) subjectAltName(17)}  
Marcada como no crítica y con el valor:
  - Nombre RFC822: Dirección de correo electrónico del subscriptor.
  - Directory name: uid=*NIF*, cn=Nombre|Primer apellido|Segundo apellido
  
- CRL Distribution Point {joint-iso-itu-t(2) ds(5) certificateExtension(29) cRLDistributionPoints(31)}  
Marcada como no crítica.

### 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 bajo la presente política contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

- Subject name: cn=*NOMBRE APELLIDO1 APELLIDO2* – NIF:*nif*, ou=Ciudadanos, o=Generalitat Valenciana, c=ES

El campo cn del subject name se cumplimenta obligatoriamente en mayúsculas, prescindiendo de acentos y sustituyendo la letra “Ñ” por la “N” y la letra “Ç” por la “C”.

- Issuer name: cn=CAGVA, ou=PKIGVA, o=Generalitat Valenciana, c=ES

### 7.1.5. Restricciones de los nombres

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

#### 7.1.6. Identificador de objeto (OID) de la Política de certificación

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

1.3.6.1.4.1.8149.3.2.1.2.1.0

#### 7.1.7. Uso de la extensión “Policy Constraints”

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

#### 7.1.8. Sintaxis y semántica de los cualificadores de política

No estipulado.

#### 7.1.9. Tratamiento semántico para la extensión crítica “Certificate Policy”

La extensión “*Certificate Policy*” identifica la política que define las Prácticas que PKIGVA asocia explícitamente con el certificado. Adicionalmente la extensión contiene un cualificador de la política y una dirección URL de localización de la misma.

### 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 (v2).

#### 7.2.2. CRL y extensiones

La presente Política de Certificación soporta y utiliza CRLs conformes al estándar ITU - X.509.

## 8. ESPECIFICACIÓN DE LA ADMINISTRACIÓN

### 8.1. Procedimientos de Especificación de Cambios

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalidad Valenciana.

### 8.2. Procedimientos de Publicación y Notificación

Cuando se realicen modificaciones significativas en la presente Política de Certificación éstas se notificarán mediante correo electrónico, a los subscriptores de los certificados afectados.

En el caso de modificaciones significativas en la Declaración de Prácticas de Certificación de PKIGVA la notificación se hará extensiva a los subscriptores de todos los certificados emitidos.

Adicionalmente las modificaciones se harán públicas en el sitio web PKIGVA en <http://www.pki.gva.es>

Esta notificación se realizará con anterioridad a la entrada en vigor de la modificación que la haya producido.

### 8.3. Procedimientos de Aprobación de la CPS

La Autoridad de Aprobación de Políticas (AAP) de PKIGVA es la entidad encargada de la aprobación en el momento de su creación de la presente Política de Certificación (CP), así como de la Declaración de Prácticas de Certificación (CPS).

La AAP también se encarga de aprobar y autorizar las modificaciones de dichos documentos.

**Anexo I****CONTRATO DE CERTIFICACIÓN - CÓDIGO 1.3.6.1.4.1.8149.3.2.1.2.1.0****Sección 1 - Datos del solicitante**

Apellidos: .....

Nombre: ..... DNI/NIF: .....

Organismo: .....

Organización (si es diferente a Generalitat Valenciana): .....

Dirección correo electrónico: .....

Dirección postal: ..... Tel: .....

**Sección 2 - Datos del funcionario adscrito a Registro**

Nombre y apellidos: .....

DNI/NIF: .....

**Sección 3 - Fecha y Firma**

Solicito el Certificado asociado a la Política de Certificación con código 1.3.6.1.4.1.8149.3.2.1.2.0.6, para *Correo y Aplicaciones Seguras*, emitido por la Generalitat Valenciana. Declaro conocer y aceptar las normas de utilización de este tipo de certificados que se encuentran expuestos en <http://www.pki.gva.es>. Declaro, asimismo, que los datos expuestos son verdaderos.

En ..... a ..... de ..... de 2.00...

Firma del solicitante

Firma del funcionario de Registro

Fdo.:

Fdo.:

Ejemplar para el solicitante - Anverso

**CONTRATO DE CERTIFICACIÓN - CÓDIGO 1.3.6.1.4.1.8149.3.2.1.2.1.0****Condiciones de utilización de los certificados**

1. Los certificados asociados a la Política de Certificación para *Correo y Aplicaciones Seguras*, emitidos por la Generalitat Valenciana son del tipo X.509v3 y se rigen por la Declaración de Prácticas de Certificación de la Generalitat Valenciana, en tanto que Prestador de Servicios de Certificación, así como por la Política de Certificación referida. Ambos documentos se deben interpretar según la legislación de la Comunidad Europea, el Ordenamiento Jurídico Español y la legislación propia de la Generalitat Valenciana.
2. Los solicitantes deberán ser personas físicas, pertenecientes a alguno de los ámbitos de certificación descriptos en <http://www.pki.gva.es/cp02/acpr.htm> y en posesión de un NIF.
3. El solicitante 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 titular 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 titular 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.pki.gva.es>.
6. La Generalitat Valenciana, en tanto que Prestador de Servicios de Certificación, no se responsabiliza del contenido de los documentos firmados haciendo uso de los certificados por ella emitidos.
7. La Generalitat Valenciana, en tanto que Prestador de Servicios de Certificación, 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 Generalitat Valenciana 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 titular 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 o Pasaporte válido y vigente.

Ejemplar para el solicitante - Reverso

**CONTRATO DE CERTIFICACIÓN - CÓDIGO 1.3.6.1.4.1.8149.3.2.1.2.1.0****Sección 1 - Datos del solicitante**

Apellidos: .....

Nombre: ..... DNI/NIF: .....

Organismo: .....

Organización (si es diferente a Generalitat Valenciana): .....

Dirección correo electrónico: .....

Dirección postal: ..... Tel: .....

**Sección 2 - Datos del funcionario adscrito a Registro**

Nombre y apellidos: .....

DNI/NIF: .....

**Sección 3 - Fecha y Firma**

Solicito el Certificado asociado a la Política de Certificación con código 1.3.6.1.4.1.8149.3.2.1.2.0.6, para *Correo y Aplicaciones Seguras*, emitido por la Generalitat Valenciana. Declaro conocer y aceptar las normas de utilización de este tipo de certificados que se encuentran expuestos en <http://www.pki.gva.es>. Declaro, asimismo, que los datos expuestos son verdaderos.

En ..... a ..... de ..... de 2.00...

Firma del solicitante

Firma del funcionario de Registro

Fdo.:

Fdo.:

Ejemplar para la Generalitat Valenciana