



AC DATYS

AUTORIDAD DE CERTIFICACIÓN

---

Política de Certificación  
Certificado Digital Multipropósito Ciudadano

La Habana, Cuba

## Hoja de control

<b>Título</b>	Política de Certificación ACDATYS: Certificado Digital Multipropósito Ciudadano
<b>Autores</b>	Especialista César A. Peláiz López Dr. C. Sacha Pelaiz Barranco
<b>Versión</b>	1.0.0
<b>Fecha</b>	20/05/2023

## Registro de cambios

<b>Versión</b>	<b>Fecha</b>	<b>Motivos de los cambios</b>
1.0.0	20/05/2023	Versión inicial

## Índice

1.	Introducción .....	4
1.1.	Generalidades .....	4
1.2.	Nombre del documento e identificación .....	5
1.3.	Entidades y personas participantes .....	6
1.3.1.	Autoridad de Certificación ACDATYS.....	6
1.3.2.	Autoridad de Registro ARDATYS .....	7
1.3.3.	Autoridad de Validación.....	7
1.3.4.	Autoridad de Sellado de tiempo .....	7
1.3.5.	Repositorio de Certificados Digitales de Llave Pública.....	7
1.3.6.	Repositorio de llaves privadas.....	7
1.3.7.	Solicitantes y titulares de Certificados Digitales de Llave Pública.....	7
1.3.8.	Terceros que confían.....	8
1.4.	Uso de los Certificados Digitales de Llave Pública .....	8
1.4.1.	Uso apropiado de los Certificados .....	8
1.4.2.	Usos prohibidos de los Certificados .....	8
1.5.	Administración de la PC de la ACDATYS.....	9
1.5.1.	Organización responsable de la PC .....	9
1.5.2.	Personal de contacto con relación a la DPC.....	9
1.5.3.	Procedimiento de aprobación.....	9
1.6.	Definiciones y acrónimos .....	9
1.6.1.	Definiciones.....	9
1.6.2.	Acrónimos .....	10
2.	Publicación de información y repositorio de Certificados Digitales de Llave Pública.....	12
3.	Identificación y autenticación de los solicitantes y titulares de Certificados Digitales de Llave Pública .....	12
3.1.	Registro de nombres .....	12
3.2.	Validación de la identidad inicial.....	12
3.2.1.	Procedimiento de prueba de posesión de llave privada.....	12

3.2.2.	Autenticación de la Identidad de una persona jurídica .....	13
3.2.3.	Autenticación de la Identidad individual.....	13
3.2.4.	Autenticación de la pertenencia del solicitante a la entidad.....	14
3.2.5.	Información no verificada sobre el solicitante.....	14
3.3.	Identificación y autenticación en las solicitudes de renovación.....	14
3.4.	Identificación y autenticación en las solicitudes de revocación .....	15
4.	Requisitos y operaciones para el ciclo de vida de los Certificados Digitales .....	16
4.1.	Solicitud de un Certificado Digital.....	16
4.1.1.	Proceso de registro y responsabilidades.....	20
4.2.	Tramitación de las solicitudes de Certificados Digitales de Llave Pública .....	20
4.2.1.	Aprobación o denegación de las solicitudes de Certificados Digitales .....	21
4.3.	Emisión de Certificados Digitales de Llave Pública .....	21
4.4.	Aceptación de un Certificado Digital.....	21
4.5.	Uso de la llave privada y del Certificado Digital de Llave Pública .....	21
4.6.	Renovación de un Certificado Digital.....	22
4.7.	Modificación de un Certificado Digital de Llave Pública.....	27
4.8.	Suspensión y revocación de un Certificado Digital de Llave Pública.....	27
4.8.1.	Causas de revocación de un Certificado Digital de Llave Pública .....	31
4.8.2.	Quién puede solicitar la revocación de un Certificado Digital de Llave Pública .....	32
4.8.3.	Periodo de gracia de la solicitud de revocación.....	33
4.8.4.	Plazo en que la ACDATYS debe resolver la solicitud de revocación.....	33
4.8.5.	Requisitos de verificación de las revocaciones por los terceros aceptantes .....	33
4.8.6.	Frecuencia de emisión de las CRL .....	33
4.8.7.	Tiempo máximo entre la generación y la publicación de las CRL .....	33
4.8.8.	Disponibilidad de verificación de la revocación.....	33
4.8.9.	Requerimientos especiales de revocación de llave privada comprometida.....	34
4.9.	Servicios de verificación del estado de los Certificados Digitales.....	34
4.10.	Finalización de la suscripción .....	34
4.11.	Custodia y recuperación de llaves.....	34
5.	Controles de seguridad física, instalaciones, gestión y operacionales .....	34
6.	controles de seguridad técnica .....	35

6.1.	Generación e instalación del par de llaves.....	35
6.1.1.	Generación del par de llaves y el Certificado Digital de Llave Pública .....	35
6.1.2.	Entrega de la llave privada al titular.....	35
6.1.3.	Entrega de la llave pública de la ACDATYS a los titulares .....	36
6.1.4.	Tamaños de llaves .....	36
6.2.	Protección de la llave privada .....	36
6.2.1.	Custodia de la llave privada.....	36
6.3.	Otros aspectos de la gestión del par de llaves .....	36
6.3.1.	Archivo de llave pública .....	36
6.3.2.	Periodo de validez de los Certificados Digitales.....	37
6.4.	Controles de seguridad informática.....	37
6.5.	Controles de seguridad del ciclo de vida.....	37
6.6.	Controles de seguridad de la red .....	37
7.	Perfiles de los Certificados Digitales, las CRL y el OCSP .....	38
7.1.	Perfil de Certificado Digital de Llave Pública.....	38
7.1.1.	Número de versión.....	39
7.1.2.	Extensiones del Certificado Digital de Llave Pública .....	39
7.1.3.	Identificadores de objetos (OID) de los algoritmos .....	39
7.1.4.	Formato de nombres.....	39
7.2.	Perfil de CRL .....	39
7.3.	Listas de revocación de Certificados (CRL).....	39
8.	Auditorías de cumplimiento y otros controles.....	40
9.	Cuestiones legales y comerciales .....	40

## **1. Introducción**

### **1.1. Generalidades**

El presente documento: Política de Certificación de la ACDATYS: Certificado Digital Multipropósito Ciudadano (en lo adelante PC) constituye un documento de regulaciones, normas, reglas y procedimientos, que se establecen para el uso de los Certificados Digitales de Llave Pública, con requerimientos precisos y rigurosos de seguridad y control criptográfico.

La presente PC, de conjunto con la Declaración de Prácticas de Certificación (en lo adelante DPC) de la ACDATYS, el reglamento para la Infraestructura de Llave Pública (en lo adelante PKI, por sus siglas en inglés) de la República de Cuba, vigente por la Resolución 2/2016 del Ministro del Interior, así como con las regulaciones y disposiciones especiales emitidas por la Dirección de Criptografía (en lo adelante DC) del Ministerio del Interior (en lo adelante Minint) y la Autoridad de Certificación del Servicio Central Cifrado (en lo adelante ACSCC), son los documentos oficiales que establecen las reglas y normas aplicables para la solicitud, validación, aceptación, emisión, entrega, uso, suspensión, renovación y revocación de los Certificados Digitales de Llave Pública emitidos por la ACDATYS, así como las restricciones, aplicaciones, responsabilidades, obligaciones, deberes y derechos de las partes participantes, sujetos a las cuales se pueden utilizar eficaz y eficientemente dichos Certificados Digitales.

La ACDATYS asume que los titulares de Certificados Digitales de Llave Pública conocen y dominan los conceptos básicos de una PKI, el uso de un Certificado Digital de Llave Pública y cómo realizar la firma digital de un documento o archivo; no obstante, recomienda que todo titular de Certificado Digital, para disponer del adecuado conocimiento relativo a una PKI, consulte los documentos regulatorios posteriormente señalados, que sustentan la presente PC.

La presente PC está redactada siguiendo las especificaciones de la RFC 2527 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, y valorando además aspectos de interés incluidos en:

- ETSI TS 101 456: “Policy Requirements for certification authorities issuing qualified certificates”,
- ETSI TS 101 862: “Qualified Certificate Profile”,
- ETSI TS 102 042: “Policy Requirements for certification authorities issuing public key certificates”.

También se tuvieron en cuenta los siguientes documentos regulatorios oficiales de la República de Cuba:

- Decreto Ley 199/1999,
- Resolución 2/2016 del Ministerio del Interior,
- Declaración de Prácticas de Certificación de la ACSCC.

Para brindar el conocimiento a los titulares de Certificados Digitales de Llave Pública de las prácticas y reglas específicas que se aplican en el sistema de certificación de la ACDATYS, se ponen a su disposición esta PC, la DPC y demás documentos afines y documentación complementaria, los que estarán disponibles en el sitio web oficial de la ACDATYS <https://ac.datys.cu>.

## 1.2. Nombre del documento e identificación

Nombre del documento	Política de Certificación ACDATYS: Certificado Digital Multipropósito Ciudadano
Versión del documento	1.0.0
Estado del documento	Aprobado
Fecha de emisión	20/05/2023
Disponible en:	<a href="https://ac.datys.cu/politicas">https://ac.datys.cu/politicas</a>

### **1.3. Entidades y personas participantes**

Las entidades y personas participantes son:

- La empresa Datys como titular de la ACDATYS,
- La Autoridad de Certificación ACDATYS,
- La Autoridad de Registro ARDATYS,
- La Autoridad de Validación,
- La Autoridad de Sellado de Tiempo,
- Repositorio de Certificados Digitales de Llave Pública,
- Repositorio de llaves privadas,
- Los solicitantes y suscriptores de los Certificados Digitales de Llave Pública emitidos por la ACDATYS,
- Los terceros aceptantes de los Certificados Digitales de Llave Pública emitidos por la ACDATYS.

#### **1.3.1. Autoridad de Certificación ACDATYS**

La ACDATYS está destinada para emitir, renovar, suspender, revocar y firmar Certificados Digitales de Llave Pública en interés de los OACE, OSDE, entidades, empresas, organizaciones y ciudadanos naturales, para lo cual asume la responsabilidad de emitir y mantener actualizadas sus PC y la DPC; así como emitir y mantener actualizada la información del estado de los Certificados Digitales de Llave Pública que emite, a través de la publicación de las Listas de Revocación de Certificados (en lo adelante CRL, por sus siglas en inglés) y del servicio de validación en línea OCSP.



El Certificado Digital de Llave Pública de la ACDATYS, con el cual legaliza y mantiene un entorno certificado, seguro y confiable a todos los servicios que brinda, es generado por la ACSCC.

### **1.3.2. Autoridad de Registro ARDATYS**

De acuerdo con lo especificado en la DPC de la ACDATYS.

### **1.3.3. Autoridad de Validación**

De acuerdo con lo especificado en la DPC de la ACDATYS.

### **1.3.4. Autoridad de Sellado de tiempo**

De acuerdo con lo especificado en la DPC de la ACDATYS.

### **1.3.5. Repositorio de Certificados Digitales de Llave Pública**

De acuerdo con lo especificado en la DPC de la ACDATYS.

### **1.3.6. Repositorio de llaves privadas**

De acuerdo con lo especificado en la DPC de la ACDATYS.

### **1.3.7. Solicitantes y titulares de Certificados Digitales de Llave Pública**

A los efectos de la presente PC se entenderá como solicitante a toda persona natural en su condición de Ciudadano que presente una solicitud de Certificado Digital y que establezca una relación contractual con la ARDATYS.

Así mismo, se entenderá como titular a toda persona natural en su condición de Ciudadano, propietario de un Certificado Digital, cuya identidad está vinculada a los datos de creación y verificación de firma, firma de correo electrónico y Autenticación de Cliente.

### **1.3.8. Terceros que confían**

Los terceros que confían son las personas naturales o jurídicas que deciden aceptar y confiar en los Certificados Digitales de Llave Pública emitidos por la ACDATYS.

## **1.4. Uso de los Certificados Digitales de Llave Pública**

### **1.4.1. Uso apropiado de los Certificados**

Los Certificados Digitales de Llave Pública Multipropósito Ciudadano, emitidos por la ACDATYS bajo esta PC, tienen bien definido y regulado su uso, restricciones y requerimientos específicos, para la firma digital de documentos y archivos digitales y para el no repudio de la operación de firma digital.

El uso de un Certificado Digital de Llave Pública emitido conforme a la presente PC y a la DPC de la ACDATYS, solo tendrá validez legal si es utilizado acorde con las disposiciones vigentes en el país sobre la seguridad de la información y la protección criptográfica.

### **1.4.2. Usos prohibidos de los Certificados**

Los Certificados Digitales deben emplearse de acuerdo con las funciones y finalidades definidas en la presente PC, sin que puedan utilizarse legalmente para otras tareas y otros fines no contemplados en la misma.

Salvo en casos muy específicos, previamente convenidos con la ACDATYS y la ACSCC, y sujetos a su aprobación, los Certificados Digitales emitidos por la ACDATYS no podrán ser utilizados para actuar ni como Autoridad de Registro ni como Autoridad de Certificación.

Se considerarán aplicaciones no permitidas para el uso de los Certificados Digitales de Llave Pública emitidos por la ACDATYS, aquellas que se encuentran restringidas por los documentos legales vigentes relativos al secreto estatal y las que no estén contempladas en los servicios que se ejecutan a través de la PKI del país.

El uso no autorizado o indebido de un Certificado Digital de Llave Pública emitido por la ACDATYS, según lo establecido en la presente PC y en la DPC de la ACDATYS, por parte de terceros, entidades o titulares, eximirá a la ACDATYS de cualquier responsabilidad.

## **1.5. Administración de la PC de la ACDATYS**

### **1.5.1. Organización responsable de la PC**

Nombre	Autoridad de Certificación ACDATYS
Correo electrónico	<a href="mailto:acdatys@datys.cu">acdatys@datys.cu</a>
Dirección	5ta y 34 No. 3401 Miramar, Playa, La Habana, Cuba
Teléfono	78830492 ext. 212

### **1.5.2. Personal de contacto con relación a la DPC**

Nombre	César Augusto Peláiz López
Correo electrónico	<a href="mailto:cesar.pelaiz@datys.cu">cesar.pelaiz@datys.cu</a>
Dirección	5ta y 34 No. 3401 Miramar, Playa, La Habana, Cuba
Teléfono	78830492 ext. 212

### **1.5.3. Procedimiento de aprobación**

La ACDATYS es la responsable de la elaboración, modificación, actualización y presentación de la presente PC.

La DC del Minint es la entidad facultada para la aprobación de la presente PC.

## **1.6. Definiciones y acrónimos**

### **1.6.1. Definiciones**

En el ámbito de esta PC se emplean las definiciones establecidas en la Resolución 02/2016 del Ministerio del Interior: “Requerimientos técnicos, organizativos y de seguridad provisionales para el servicio criptográfico basado en la infraestructura de llave pública”.

## 1.6.2. Acrónimos

**AC:** Autoridad de Certificación

**ACDATYS:** Autoridad de Certificación de la empresa Datys

**ACSCC:** Autoridad de Certificación del Servicio Central Cifrado

**AR:** Autoridad de Registro

**ARDATYS:** Autoridad de Registro de la empresa Datys

**AV:** Autoridad de Validación

**C:** País, del inglés country. Atributo del DN de un objeto dentro de la estructura de directorio X.500

**CN:** Nombre común, del inglés Common Name. Atributo del DN de un objeto dentro de la estructura de directorio X.500

**CRL:** Lista de Certificados Digitales revocados, del inglés Certificate Revocation Lists

**CSR:** Solicitud firmada de certificado, del inglés Certificate Signing Request. Conjunto de datos, que contienen una llave pública y su firma digital utilizando la llave privada asociada, enviado a la Autoridad de Certificación para la emisión de un Certificado Digital que contenga dicha llave pública.

**DC:** Dirección de Criptografía del Ministerio del Interior

**DN:** Nombre distintivo, del inglés distinguished name. Atributo del DN de un objeto dentro de la estructura de directorio X.500

**DNS:** Nombre de dominio de sistema, del inglés Domain Name System

- DPC:** Declaración de Prácticas de Certificación
- IETF:** Organismo de estandarización de Internet, del inglés Internet Engineering Task Force
- NIF:** Número de identificación fiscal
- O:** Organización, del inglés Organization. Atributo del DN de un objeto dentro de la estructura de directorio X.500
- OACE:** Organismos de la Administración Central del Estado
- OCSP:** Protocolo de verificación en línea del estado de un Certificado Digital, del inglés Online Certificate Status Protocol
- OID:** Identificador de objeto único, del inglés Object Identifier.
- OU:** Unidad organizativa, del inglés Organization Unit. Atributo del DN de un objeto dentro de la estructura de directorio X.500
- PC:** Política de Certificación
- PKCS:** Estándares de PKI desarrollados por RSA Laboratories y aceptados internacionalmente, del inglés Public Key Certificate Standards
- PKI:** Infraestructura de Llave Pública, del inglés Public Key Infrastructure
- PSCC:** Prestador de Servicios Criptográficos de Certificación
- RFC:** Estándares de la IETF, del inglés Request for Comments

## **2. Publicación de información y repositorio de Certificados Digitales de Llave Pública**

De acuerdo con lo especificado en la DPC de la ACDATYS.

## **3. Identificación y autenticación de los solicitantes y titulares de Certificados Digitales de Llave Pública**

A los efectos de esta PC y como regla general, según lo especificado en la Resolución 2/2016 del Minint y en la Norma Técnica 000241.23-O.230425, el par de llaves criptográficas, pública y privada, será generado por el solicitante del Certificado Digital.

En casos excepcionales, de acuerdo con lo especificado en la Resolución y en la Norma Técnica, la persona natural en su condición de Ciudadano puede solicitar oficialmente, siendo refrendado además en el Modelo de Solicitud de Certificado Digital, que la ACDATYS asuma la responsabilidad de la generación del par de llaves criptográficas, pública y privada, del solicitante.

### **3.1. Registro de nombres**

De acuerdo con lo especificado en la DPC de la ACDATYS.

### **3.2. Validación de la identidad inicial**

#### **3.2.1. Procedimiento de prueba de posesión de llave privada**

En caso que el par de llaves criptográficas, pública y privada, sea generado por el solicitante del Certificado Digital, este deberá demostrar la correspondencia de la llave privada generada y resguardada por él, con la llave pública, también generada por él.

Para su confirmación, el solicitante deberá presentar la CSR, en formato PKCS#10, que se corresponde con la llave pública generada por él, firmada con la llave privada asociada, de manera que la ARDATYS pueda comprobar que efectivamente posee la llave privada.

### **3.2.2. Autenticación de la Identidad de una persona jurídica**

No procede.

### **3.2.3. Autenticación de la Identidad individual**

A los efectos de esta PC, la persona natural solicitante en su condición de Ciudadano, deberá realizar la solicitud de Certificado Digital, de manera presencial, según lo especificado en [3.2](#), ante la ARDATYS, presentando los siguientes documentos:

- Carné de identidad (NIF) actualizado del solicitante,
- impreso y firmado el Modelo de Solicitud de Certificado Digital: Certificado Digital Multipropósito Ciudadano, que incluirá los datos identificativos del solicitante. Se entregará además una versión digital del modelo,
- la Solicitud firmada de Certificado (CSR) en formato PKCS#10 correspondiente a la llave pública del solicitante. Solo en caso que el solicitante haya asumido la generación de su par de llaves criptográficas, pública y privada.

Si el solicitante es un ciudadano extranjero, representante oficial y reconocido legalmente de una firma extranjera acreditada en Cuba, deberá presentar entonces su pasaporte o Carné de residente temporal.

La ARDATYS podrá solicitar información adicional a la establecida en el Modelo de Solicitud, según lo considere necesario.

### **3.2.4. Autenticación de la pertenencia del solicitante a la entidad**

No procede.

### **3.2.5. Información no verificada sobre el solicitante**

De acuerdo con lo especificado en la DPC de la ACDATYS.

## **3.3. Identificación y autenticación en las solicitudes de renovación**

A los efectos de esta PC, el titular deberá realizar la solicitud de renovación de llaves, de manera presencial o a través de correo electrónico, ante la ARDATYS, presentando los siguientes documentos:

- Carné de identidad (NIF) actualizado del titular en caso de solicitud presencial,
- impreso y firmado el Modelo de Solicitud de Certificado Digital: Certificado Digital Multipropósito Ciudadano, que incluirá los datos identificativos del titular. Se entregará además una versión digital del modelo,
- Modelo de Solicitud de Certificado Digital: Certificado Digital Multipropósito Ciudadano, firmado digitalmente por el titular. Solo en caso que la solicitud se realice vía correo electrónico,
- la Solicitud firmada de Certificado (CSR) en formato PKCS#10 correspondiente a la nueva llave pública. Solo en caso que el titular haya asumido la generación de su nuevo par de llaves criptográficas, pública y privada.

Si el titular es un ciudadano extranjero, representante oficial y reconocido legalmente de una firma extranjera acreditada en Cuba, deberá presentar entonces su pasaporte o Carné de residente temporal, en caso de solicitud presencial.



### **3.4. Identificación y autenticación en las solicitudes de revocación**

A los efectos de esta PC, el titular deberá realizar la solicitud de revocación de Certificado Digital, de manera presencial o a través de correo electrónico, ante la ARDATYS, presentando los siguientes documentos:

- Carné de identidad (NIF) actualizado del titular en caso de solicitud presencial,
- impreso y firmado el Modelo de Solicitud de Revocación de Certificado Digital, que incluirá los datos identificativos del titular. Se entregará además una versión digital del modelo,
- Modelo de Solicitud de Revocación de Certificado Digital, firmado digitalmente por el titular. Solo en caso que la solicitud se realice vía correo electrónico.

Si el titular es un ciudadano extranjero, representante oficial y reconocido legalmente de una firma extranjera acreditada en Cuba, deberá presentar entonces su pasaporte o Carné de residente temporal, en caso de solicitud presencial.

La ACDATYS se reserva la facultad de revocar un Certificado Digital, ante sospecha o conocimiento del comprometimiento de la llave privada asociada, o cualquier otra causa determinante de revocación, según lo establecido en su DPC.

## 4. Requisitos y operaciones para el ciclo de vida de los Certificados Digitales

### 4.1. Solicitud de un Certificado Digital

A los efectos de esta PC, el procedimiento para solicitar, de manera presencial, un Certificado Digital a la ARDATYS es el siguiente:

1. **Realizar solicitud**: la persona natural en su condición de Ciudadano, de manera presencial, solicita el Certificado Digital a un funcionario de la ARDATYS, presentando los documentos requeridos según se establece en la sección [3.2.3](#) de la presente PC.
2. **Recepcionar solicitud**: el funcionario de la ARDATYS recepciona los documentos presentados por la persona natural solicitante en su condición de Ciudadano.
3. **Validar datos identificativos**: el funcionario de la ARDATYS valida los datos identificativos de la persona natural solicitante en su condición de Ciudadano. En caso que se detecte algún problema con algún dato identificativo, el funcionario de la ARDATYS lo comunica a la persona natural solicitante en su condición de Ciudadano.
4. **Validar Modelo de Solicitud**: el funcionario de la ARDATYS verifica que el Modelo de Solicitud en cuestión haya sido llenado correctamente. En caso que se detecte algún problema con el Modelo de Solicitud, el funcionario de la ARDATYS lo comunica a la persona natural solicitante en su condición de Ciudadano.
5. **Validar formato de la CSR (si procede)**: el funcionario de la ARDATYS valida que la CSR entregada por la persona natural solicitante en su condición de Ciudadano cumpla con el formato estándar PKCS#10. En caso que la CSR no

cumple con el formato PKCS#10 o exista algún problema que evite su validación, el funcionario de la ARDATYS lo comunica a la persona natural solicitante en su condición de Ciudadano.

6. **Validar posesión de llave privada (si procede)**: el funcionario de la ARDATYS comprueba la validez de la firma digital de la CSR presentada por la persona natural solicitante en su condición de Ciudadano. En caso de que la firma digital sea no válida o que no pueda ser comprobada su validez, el funcionario de la ARDATYS lo comunica a la persona natural solicitante en su condición de Ciudadano.
7. **Completar Modelo de Información a la Dirección Comercial**: el directivo de la ARDATYS completa el Modelo de Información a la Dirección Comercial de la empresa Datys.
8. **Enviar Modelo de Información a la Dirección Comercial**: el directivo de la ARDATYS envía, vía correo electrónico, firmado digitalmente, el Modelo de Información a la Dirección Comercial de la empresa Datys, para que un especialista comercial proceda con las acciones de carácter comercial, jurídico y económico.
9. **Elaborar Cotización (si procede)**: el funcionario de la ARDATYS elabora la Cotización de Servicio Criptográfico Especializado, que se corresponde con la solicitud presentada por la persona natural en su condición de Ciudadano.
10. **Enviar Cotización a la Dirección Comercial (si procede)**: el directivo de la ARDATYS envía, vía correo electrónico, la Cotización de Servicio Criptográfico Especializado a la Dirección Comercial de la empresa Datys, para que un especialista comercial proceda a su firma y envío al Cliente.
11. **Confirmar aceptación y firma de la Cotización**: el directivo de la ARDATYS espera la respuesta de la Dirección Comercial relacionada con la aceptación

y firma por el Cliente de la Cotización de Servicio Criptográfico Especializado. En caso que la firma de la Cotización de Servicio Criptográfico Especializado no se concrete, se da por concluido el proceso de tramitación de la solicitud.

12. **Confirmar aceptación y firma del Contrato**: el directivo de la ARDATYS espera la respuesta de la Dirección Comercial relacionada con la aceptación y firma por el Cliente del Contrato. En caso que la firma del Contrato no se concrete, se da por concluido el proceso de tramitación de la solicitud.
13. **Aprobar solicitud**: la ARDATYS aprueba la solicitud de Certificado Digital.
14. **Crear expediente técnico**: el funcionario de la ARDATYS crea el expediente técnico del solicitante y archiva todos los documentos presentados como parte de la solicitud.
15. **Registrar datos del solicitante**: el funcionario de la ARDATYS registra al solicitante en el sistema.
16. **Crear Orden de trabajo**: el funcionario de la ARDATYS crea la Orden de trabajo de la nueva solicitud.
17. **Firmar Orden de trabajo**: el funcionario de la ARDATYS firma digitalmente la Orden de trabajo de la nueva solicitud.
18. **Publicar Orden de trabajo**: el funcionario de la ARDATYS publica vía FTP (en la carpeta que corresponda) la Orden de trabajo correspondiente a la solicitud.
19. **Publicar la CSR (si procede)**: el funcionario de la ARDATYS publica vía FTP (en la carpeta que corresponde) la CSR asociada a la solicitud.

20. **Notificar a la ACDATYS:** el funcionario de la ARDATYS notifica al funcionario de la ACDATYS que fue creada una nueva Orden de trabajo para que este proceda a su tramitación y correspondiente emisión del Certificado Digital.
21. **Validar Orden de trabajo:** el funcionario de la ACDATYS valida la integridad y autenticidad de la Orden de trabajo verificando la validez de la firma digital. En caso que la firma digital sea no válida o que no pueda ser comprobada su validez, el funcionario de la ACDATYS lo comunica al funcionario de la ARDATYS que creó y firmó la Orden de trabajo para que proceda a su corrección.
22. **Comprobar Orden de trabajo:** el funcionario de la ACDATYS comprueba que la Orden de trabajo sea correcta, comprobando que contiene todos los datos requeridos para proceder a la emisión del Certificado Digital. En caso que detecte algún error o faltante, lo comunica de manera inmediata al funcionario de la ARDATYS que creó la Orden de trabajo para que proceda a su corrección.
23. **Emitir Certificado Digital:** el funcionario de la ACDATYS emite el Certificado Digital correspondiente a la solicitud.
24. **Firmar Orden de trabajo:** el funcionario de la ACDATYS firma digitalmente la Orden de trabajo de la solicitud como constancia de que fue tramitada y que se emitió el Certificado Digital correspondiente.
25. **Publicar Orden de trabajo:** el funcionario de la ACDATYS publica vía FTP (en la carpeta que corresponda) la Orden de trabajo tramitada correspondiente a la solicitud.
26. **Notificar a la ARDATYS:** el funcionario de la ACDATYS notifica al funcionario de la ARDATYS que la Orden de trabajo fue tramitada y que fue emitido el Certificado Digital correspondiente.

27. **Publicar Certificado Digital (si procede)**: el funcionario de la ACDATYS publica en el repositorio público de la ACDATYS el Certificado Digital emitido.
28. **Notificar al solicitante**: el funcionario de la ARDATYS notifica a la persona natural solicitante en su condición de Ciudadano que la solicitud fue tramitada y que el Certificado Digital fue publicado (si procedía) en el repositorio público de la ACDATYS, y que puede presentarse en la ACDATYS a recogerlo.
29. **Actualizar expediente técnico del titular**: el funcionario de la ARDATYS realiza las acciones pertinentes de actualización del expediente del titular del Certificado Digital.
30. **Validar expediente técnico**: el directivo de la ARDATYS revisa el expediente técnico del solicitante y valida que esté completo y correctamente conformado. En caso que detecte algún error o faltante, el directivo de la ARDATYS lo comunica al funcionario de la ARDATYS que actualizó el expediente para que proceda a su corrección.

#### **4.1.1. Proceso de registro y responsabilidades**

La ARDATYS podrá aprobar o denegar la solicitud de un Certificado Digital de acuerdo con lo establecido en su DPC.

#### **4.2. Tramitación de las solicitudes de Certificados Digitales de Llave Pública**

Es competencia y responsabilidad de la ARDATYS verificar la identidad de la persona natural solicitante en su condición de Ciudadano, la autenticidad de la información tributada, que el solicitante haya consentido la solicitud de Certificado Digital mediante su firma, y que el Contrato de prestación de servicios criptográficos especializados haya sido aprobado y firmado por las partes involucradas.

#### **4.2.1. Aprobación o denegación de las solicitudes de Certificados Digitales**

La ARDATYS puede denegar una solicitud de Certificado Digital, sin que ello implique contraer responsabilidad alguna por las consecuencias que pudieran derivarse para la persona natural en su condición de Ciudadano, de tal decisión.

#### **4.3. Emisión de Certificados Digitales de Llave Pública**

Los Certificados Digitales emitidos por la ACDATYS entrarán en vigencia a partir del momento de su publicación en el repositorio público de la ACDATYS.

#### **4.4. Aceptación de un Certificado Digital**

La aceptación formal por parte del nuevo titular de sus responsabilidades y obligaciones relacionadas con la tenencia y uso del Certificado Digital emitido por la ACDATYS, se asegura mediante la firma del Contrato de prestación de servicios criptográficos especializados, que precisa que el titular conoce y acepta las condiciones de la presente PC y de la DPC de la ACDATYS.

#### **4.5. Uso de la llave privada y del Certificado Digital de Llave Pública**

A los efectos de esta PC, el titular sólo podrá utilizar su llave privada y su Certificado Digital de Llave Pública para firma digital y no repudio, de acuerdo con lo especificado en el campo KeyUsage del Certificado Digital.

La llave privada y el Certificado Digital de Llave Pública serán legalmente válidos solo durante el periodo de vigencia establecido en el propio Certificado. Tras la expiración o revocación del Certificado Digital, el titular está obligado, de acuerdo a lo estipulado en el Contrato de prestación de servicios criptográficos especializados, a no seguir haciendo uso de su llave privada.

En su condición de terceras partes que confían, antes de aceptar y confiar en un Certificado Digital de Llave Pública emitido por la ACDATYS, la parte que confía debe asegurarse que, el Certificado es apropiado para el uso al que ha sido destinado y que se encuentra vigente.

#### **4.6. Renovación de un Certificado Digital**

La renovación de un Certificado Digital es el procedimiento mediante el cual el titular solicita un nuevo Certificado Digital, sujeto a las mismas condiciones de uso que el Certificado Digital en cuestión.

Un Certificado Digital puede ser renovado, entre otros, por los siguientes motivos:

- Expiración o cercanía a la fecha de expiración,
- cambios en los datos contenidos en el Certificado Digital,
- llaves comprometidas o pérdida de fiabilidad de las mismas.

En cualquier caso, la renovación de un Certificado Digital está supeditada a:

- Que se realice atendiendo al Modelo de Solicitud de Certificado Digital Firma Digital Ciudadano establecido por la ACDATYS y publicado en su sitio web oficial,
- que la ACDATYS no tenga conocimiento de la concurrencia de ninguna causa de revocación o suspensión del Certificado Digital,
- que la solicitud de renovación se refiera al mismo tipo de Certificado Digital emitido inicialmente al titular.

La ARDATYS, de acuerdo a lo convenido en el Contrato de prestación de servicios criptográficos especializados, podrá notificar al titular, con la debida antelación, la proximidad de la fecha de expiración del Certificado Digital.



A los efectos de esta PC, el procedimiento para solicitar, de manera presencial, la renovación de un Certificado Digital a la ARDATYS es el siguiente:

1. **Realizar solicitud**: el titular, de manera presencial, solicita la renovación del Certificado Digital a un funcionario de la ARDATYS, presentando los documentos requeridos según se establece en la sección [3.3](#) de la presente PC.
2. **Recepcionar solicitud**: el funcionario de la ARDATYS recepciona los documentos presentados por el titular.
3. **Validar datos identificativos**: el funcionario de la ARDATYS valida los datos identificativos del titular, comparándolos además con sus datos registrados. Si alguna información del titular ha cambiado, ésta deberá ser nuevamente registrada con el acuerdo del titular. En caso que se detecte algún problema con algún dato, el funcionario de la ARDATYS lo comunica al titular.
4. **Validar Modelo de Solicitud**: el funcionario de la ARDATYS verifica que el Modelo de Solicitud en cuestión haya sido llenado correctamente. En caso que se detecte algún problema con el Modelo de Solicitud, el funcionario de la ARDATYS lo comunica al titular.
5. **Precisar causas de renovación**: el funcionario de la ARDATYS precisa las causas que motivaron la solicitud de renovación del Certificado Digital de acuerdo a lo establecido en el Modelo de Solicitud correspondiente.
6. **Validar formato de la CSR (si procede)**: el funcionario de la ARDATYS valida que la nueva CSR entregada por el titular cumpla con el formato estándar PKCS#10. En caso que la nueva CSR no cumpla con el formato PKCS#10 o exista algún problema que evite su validación, el funcionario de la ARDATYS lo comunica al titular.

7. **Validar posesión de llave privada (si procede)**: el funcionario de la ARDATYS comprueba la validez de la firma digital de la nueva CSR presentada por el titular. En caso de que la firma digital sea no válida o que no pueda ser comprobada su validez, el funcionario de la ARDATYS lo comunica al titular.
8. **Completar Modelo de Información a la Dirección Comercial**: el directivo de la ARDATYS completa el Modelo de Información a la Dirección Comercial de la empresa Datys.
9. **Enviar Modelo de Información a la Dirección Comercial**: el directivo de la ARDATYS envía, vía correo electrónico, firmado digitalmente, el Modelo de Información a la Dirección Comercial de la empresa Datys, para que un especialista comercial proceda con las acciones de carácter comercial, jurídico y económico.
10. **Elaborar Cotización (si procede)**: el funcionario de la ARDATYS elabora la Cotización de Servicio Criptográfico Especializado, que se corresponde con la solicitud de renovación presentada por el titular.
11. **Enviar Cotización a la Dirección Comercial (si procede)**: el directivo de la ARDATYS envía, vía correo electrónico, la Cotización de Servicio Criptográfico Especializado a la Dirección Comercial de la empresa Datys, para que un especialista comercial proceda a su firma y envío al Cliente.
12. **Confirmar aceptación y firma de la Cotización**: el directivo de la ARDATYS espera la respuesta de la Dirección Comercial relacionada con la aceptación y firma por el Cliente de la Cotización de Servicio Criptográfico Especializado. En caso que la firma de la Cotización de Servicio Criptográfico Especializado no se concrete, se da por concluido el proceso de tramitación de la solicitud.

13. **Aprobar solicitud**: la ARDATYS aprueba la solicitud de renovación del Certificado Digital.
14. **Actualizar expediente técnico**: el funcionario de la ARDATYS actualiza el expediente técnico del titular.
15. **Actualizar datos del solicitante**: el funcionario de la ARDATYS actualiza en el sistema los datos del titular, si existen cambios previamente acordados con el titular.
16. **Crear Orden de trabajo**: el funcionario de la ARDATYS crea la Orden de trabajo de la nueva solicitud de renovación.
17. **Firmar Orden de trabajo**: el funcionario de la ARDATYS firma digitalmente la Orden de trabajo de la nueva solicitud de renovación.
18. **Publicar Orden de trabajo**: el funcionario de la ARDATYS publica vía FTP (en la carpeta que corresponda) la Orden de trabajo correspondiente a la solicitud de renovación.
19. **Publicar la CSR (si procede)**: el funcionario de la ARDATYS publica vía FTP (en la carpeta que corresponde) la CSR asociada a la solicitud de renovación.
20. **Notificar a la ACDATYS**: el funcionario de la ARDATYS notifica al funcionario de la ACDATYS que fue creada una nueva Orden de trabajo para que este proceda a su tramitación y correspondiente renovación del Certificado Digital.
21. **Validar Orden de trabajo**: el funcionario de la ACDATYS valida la integridad y autenticidad de la Orden de trabajo verificando la validez de la firma digital. En caso que la firma digital sea no válida o que no pueda ser comprobada su validez, el funcionario de la ACDATYS lo comunica al funcionario de la ARDATYS que creó y firmó la Orden de trabajo.

22. **Comprobar Orden de trabajo:** el funcionario de la ACDATYS comprueba que la Orden de trabajo sea correcta, comprobando que contiene todos los datos requeridos para proceder a la emisión del Certificado Digital. En caso que detecte algún error o faltante, lo comunica de manera inmediata al funcionario de la ARDATYS que creó la Orden de trabajo para que proceda a su corrección.
23. **Revocar Certificado Digital:** el funcionario de la ACDATYS revoca en el sistema el Certificado Digital vigente del titular, que se corresponde con la solicitud de renovación.
24. **Renovar Certificado Digital:** el funcionario de la ACDATYS emite un nuevo Certificado Digital en correspondencia con la solicitud de renovación en trámite, haciendo efectiva la renovación.
25. **Firmar Orden de trabajo:** el funcionario de la ACDATYS firma digitalmente la Orden de trabajo de la solicitud de renovación como constancia de que fue tramitada y que se renovó el Certificado Digital correspondiente.
26. **Publicar Orden de trabajo:** el funcionario de la ACDATYS publica vía FTP (en la carpeta que corresponda) la Orden de trabajo tramitada correspondiente a la solicitud de renovación.
27. **Notificar a la ARDATYS:** el funcionario de la ACDATYS notifica al funcionario de la ARDATYS que la Orden de trabajo fue tramitada y que fue renovado el Certificado Digital correspondiente.
28. **Revocar Certificado Digital en repositorio público (si procede):** el funcionario de la ACDATYS revoca en el repositorio público de la ACDATYS el Certificado Digital vigente del titular, que se corresponde con la solicitud de renovación.

29. **Publicar Certificado Digital (si procede)**: el funcionario de la ACDATYS publica en el repositorio público de la ACDATYS el nuevo Certificado Digital emitido.
30. **Notificar al titular**: el funcionario de la ARDATYS notifica al titular que la solicitud fue tramitada y que el nuevo Certificado Digital fue publicado (si procedía) en el repositorio público de la ACDATYS, y que puede presentarse en la ACDATYS a recogerlo. También le notifica que el Certificado Digital hasta ese momento vigente fue revocado.
31. **Actualizar expediente técnico del titular**: el funcionario de la ARDATYS realiza las acciones pertinentes de actualización del expediente técnico del titular.
32. **Validar expediente técnico**: el directivo de la ARDATYS revisa y valida los cambios realizados al expediente técnico del titular. En caso que detecte algún error o faltante, el directivo de la ARDATYS lo comunica al funcionario que actualizó el expediente para que proceda a su corrección.

#### **4.7. Modificación de un Certificado Digital de Llave Pública**

De acuerdo con lo especificado en la DPC de la ACDATYS.

#### **4.8. Suspensión y revocación de un Certificado Digital de Llave Pública**

Los Certificados Digitales de Llave Pública se suspenden o revocan cuando existen circunstancias por las cuales dejan de ser operativos o fiables. La suspensión o revocación de un Certificado Digital limita el uso legítimo del mismo por parte de su titular y el reconocimiento de las terceras partes confiables.

A los efectos de esta PC, todo titular de un Certificado Digital de Llave Pública podrá decidir y solicitar, en cualquier momento o circunstancia, la suspensión o revocación de su Certificado Digital. En todo caso la ARDATYS revisará los términos convenidos en el Contrato de prestación de servicios criptográficos especializados.

La suspensión de un Certificado Digital de Llave Pública es efectiva por un período máximo de 30 días. Vencido este tiempo, la ARDATYS procederá a evaluar el estado de la suspensión con el titular, y procederá a eliminar la suspensión del Certificado o tramitar con la ACDATYS su revocación.

Ante la solicitud de revocación de un Certificado Digital, la ARDATYS evalúa la solicitud, y en caso de proceder, gestiona la revocación con la ACDATYS, la cual procederá a hacerla efectiva con inmediatez.

La suspensión o revocación de un Certificado Digital implica su publicación en las CRL, precisando además las causas que determinaron su revocación. Al expirar el periodo de validez de un Certificado revocado, éste dejará de estar incluido en las CRL.

A los efectos de esta PC, el procedimiento para solicitar, de manera presencial, la revocación de un Certificado Digital a la ARDATYS es el siguiente:

1. **Realizar solicitud**: el titular, de manera presencial, solicita la revocación del Certificado Digital a un funcionario de la ARDATYS, presentando los documentos requeridos según se establece en la sección [3.4](#) de la presente PC.
2. **Recepcionar solicitud**: el funcionario de la ARDATYS recepciona los documentos presentados por el titular.
3. **Validar datos identificativos**: el funcionario de la ARDATYS valida los datos identificativos del titular, comparándolos además con sus datos registrados.

En caso que se detecte algún problema con algún dato, el funcionario de la ARDATYS lo comunica al titular.

4. **Validar Modelo de Solicitud**: el funcionario de la ARDATYS verifica que el Modelo de Solicitud de Revocación haya sido llenado correctamente. En caso que se detecte algún problema con el Modelo de Solicitud, el funcionario de la ARDATYS lo comunica al titular.
5. **Precisar causas de revocación**: el funcionario de la ARDATYS precisa las causas que motivaron la solicitud de revocación del Certificado Digital de acuerdo a lo establecido en el Modelo de Solicitud de Revocación.
6. **Aprobar solicitud**: la ARDATYS aprueba la solicitud de revocación del Certificado Digital.
7. **Actualizar expediente técnico**: el funcionario de la ARDATYS actualiza el expediente técnico del titular.
8. **Crear Orden de trabajo**: el funcionario de la ARDATYS crea la Orden de trabajo de la nueva solicitud de revocación.
9. **Firmar Orden de trabajo**: el funcionario de la ARDATYS firma digitalmente la Orden de trabajo de la nueva solicitud de revocación.
10. **Publicar Orden de trabajo**: el funcionario de la ARDATYS publica vía FTP (en la carpeta que corresponda) la Orden de trabajo correspondiente a la solicitud de revocación.
11. **Notificar a la ACDATYS**: el funcionario de la ARDATYS notifica al funcionario de la ACDATYS que fue creada una nueva Orden de trabajo para que este proceda a su tramitación y correspondiente revocación del Certificado Digital.

12. **Validar Orden de trabajo:** el funcionario de la ACDATYS valida la integridad y autenticidad de la Orden de trabajo verificando la validez de la firma digital. En caso que la firma digital sea no válida o que no pueda ser comprobada su validez, el funcionario de la ACDATYS lo comunica al funcionario de la ARDATYS que creó y firmó la Orden de trabajo para que proceda a su corrección.
13. **Comprobar Orden de trabajo:** el funcionario de la ACDATYS comprueba que la Orden de trabajo sea correcta, comprobando que contiene todos los datos requeridos para proceder a la revocación del Certificado Digital. En caso que detecte algún error o faltante, lo comunica de manera inmediata al funcionario de la ARDATYS que creó la Orden de trabajo para que proceda a su corrección.
14. **Revocar Certificado Digital:** el funcionario de la ACDATYS revoca en el sistema el Certificado Digital del titular, que se corresponde con la solicitud de revocación.
15. **Revocar Certificado Digital en repositorio público (si procede):** el funcionario de la ACDATYS revoca en el repositorio público de la ACDATYS el Certificado Digital del titular, que se corresponde con la solicitud de renovación.
16. **Firmar Orden de trabajo:** el funcionario de la ACDATYS firma digitalmente la Orden de trabajo de la solicitud como constancia de que fue tramitada y que se revocó el Certificado Digital correspondiente.
17. **Publicar Orden de trabajo:** el funcionario de la ACDATYS publica vía FTP (en la carpeta que corresponda) la Orden de trabajo tramitada correspondiente a la solicitud de revocación.



18. **Notificar a la ARDATYS**: el funcionario de la ACDATYS notifica al funcionario de la ARDATYS que la Orden de trabajo fue tramitada y que fue revocado el Certificado Digital correspondiente.
19. **Notificar al titular**: el funcionario de la ARDATYS notifica al titular que la solicitud fue tramitada y que el Certificado Digital fue revocado. También le informa que el Certificado Digital revocado será incluido en la CRL delta de la ACDATYS, que será publicada en el sitio web oficial de la ACDATYS con efecto inmediato.
20. **Actualizar expediente del titular**: el funcionario de la ARDATYS realiza las acciones pertinentes de actualización del expediente del titular del Certificado Digital.
21. **Validar expediente**: el directivo de la ARDATYS revisa y valida los cambios realizados al expediente. En caso que detecte algún error, el directivo de la ARDATYS lo comunica al funcionario que actualizó el expediente para que proceda a su corrección.

#### **4.8.1. Causas de revocación de un Certificado Digital de Llave Pública**

Las principales causas que determinan la revocación de un Certificado Digital son:

- Comprometimiento de la llave privada asociada al Certificado Digital,
- comprometimiento de la llave privada de la ACDATYS,
- término de la relación del titular del Certificado Digital con la entidad,
- el Certificado Digital de la ACDATYS fue renovado,
- No especificada.

Otras causas que pueden implicar la revocación de un Certificado Digital, que serían tratadas como No especificada, son:

- Incumplimiento por parte del titular de sus obligaciones de conformidad con la DPC y lo estipulado en el Contrato de prestación de servicios criptográficos especializados,
- por Resolución judicial o administrativa que lo disponga,
- a solicitud de la dirección de la entidad a la que pertenece el titular,

#### **4.8.2. Quién puede solicitar la revocación de un Certificado Digital de Llave Pública**

A los efectos de esta PC, la revocación de un Certificado Digital de Llave Pública puede ser solicitada por el titular, así como por la ACDATYS, quien se reserva la facultad de revocar un Certificado Digital, ante sospecha o conocimiento demostrados del comprometimiento de la llave privada asociada, o cualquier otra causa determinante de revocación, según lo establecido en la presente PC.

Las autoridades jurídicas, por disposición legal, también podrán solicitar la revocación de un Certificado Digital.

En cualquier caso, la ARDATYS comunicará, a quien corresponda, en un término no mayor a las veinticuatro (24) en días laborales, que se ejecutó la revocación solicitada del Certificado Digital.

La solicitud de revocación de un Certificado Digital recibida con posterioridad a su fecha de caducidad no será atendida por la ARDATYS.

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

La revocación de un Certificado Digital se realizará de manera inmediata, una vez verificados los datos presentados en el Modelo de Solicitud de Revocación y que haya sido aprobada por la ARDATYS.

No se establece un periodo de gracia asociado a este proceso.

#### **4.8.4. Plazo en que la ACDATYS debe resolver la solicitud de revocación**

La ACDATYS establece que la tramitación efectiva de una solicitud de revocación no excederá las cuarenta y ocho (48) horas en días laborables.

#### **4.8.5. Requisitos de verificación de las revocaciones por los terceros aceptantes**

La verificación de las revocaciones, ya sea mediante consulta directa de las CRL o el protocolo OCSP, es responsabilidad directa de las terceras partes que confían.

#### **4.8.6. Frecuencia de emisión de las CRL**

De acuerdo con lo especificado en la DPC de la ACDATYS.

#### **4.8.7. Tiempo máximo entre la generación y la publicación de las CRL**

De acuerdo con lo especificado en la DPC de la ACDATYS.

#### **4.8.8. Disponibilidad de verificación de la revocación**

De acuerdo con lo especificado en la DPC de la ACDATYS.

#### **4.8.9. Requerimientos especiales de revocación de llave privada comprometida**

De acuerdo con lo especificado en la DPC de la ACDATYS.

#### **4.9. Servicios de verificación del estado de los Certificados Digitales**

De acuerdo con lo especificado en la DPC de la ACDATYS.

#### **4.10. Finalización de la suscripción**

Se dará por finalizada la suscripción de un Certificado Digital de Llave Pública:

- Por término de su vigencia,
- por su revocación.

Si el titular no solicita la renovación de un Certificado Digital tras el término de su validez, la ARDATYS procederá a la revisión de los términos establecidos en el Contrato de prestación de servicios criptográficos especializados y actuará en consecuencia.

Toda la documentación generada durante los procesos anteriormente descritos, será archivada por un período de 15 años.

#### **4.11. Custodia y recuperación de llaves**

De acuerdo con lo especificado en la DPC de la ACDATYS.

### **5. Controles de seguridad física, instalaciones, gestión y operacionales**

De acuerdo con lo especificado en la DPC de la ACDATYS.

## **6. Controles de seguridad técnica**

### **6.1. Generación e instalación del par de llaves**

#### **6.1.1. Generación del par de llaves y el Certificado Digital de Llave Pública**

En caso que el solicitante haya asumido la generación de su par de llaves criptográficas, pública y privada, él será el único poseedor de su llave privada, ya que como parte del procedimiento de solicitud de un Certificado Digital no se requiere que la llave privada sea entregada a la ARDATYS.

La ACDATYS provee una aplicación para la generación de manera segura y confiable del par de llaves pública y privada, y está disponible para su descarga en su sitio web oficial <https://ac.datys.cu/descargas>. Esta aplicación ha sido certificada y autorizada para su uso por la DC del Minint.

#### **6.1.2. Entrega de la llave privada al titular**

En caso que la persona natural en su condición de Ciudadano haya solicitado oficialmente y refrendado en el Modelo de Solicitud y en la Cotización de Servicio Criptográfico Especializado, que la ACDATYS asuma la responsabilidad de la generación del par de llaves criptográficas, pública y privada, del solicitante, el archivo contenedor de la llave privada le será entregada al titular en formato PKCS#12 en un dispositivo de almacenamiento USB (facilitado por el titular) o en un disco compacto (CD por sus siglas en inglés).

La contraseña de protección de la llave privada le será entregada a su titular, impresa en sobre de seguridad y será tratada como información oficial clasificada.

### **6.1.3. Entrega de la llave pública de la ACDATYS a los titulares**

La llave pública de la ACDATYS está disponible para ser descargada desde su sitio web oficial.

### **6.1.4. Tamaños de llaves**

A los efectos de esta PC, las llaves criptográficas serán de 2048 bits de longitud para el esquema criptográfico RSA y de 256 bits para el esquema criptográfico ECDSA soportado en la Teoría de Curvas Elípticas.

## **6.2. Protección de la llave privada**

Las políticas y procedimientos para la protección de la llave privada indicadas en la DPC de la ACDATYS no eximen al titular de ser el principal responsable de proteger su llave privada.

### **6.2.1. Custodia de la llave privada**

En caso que el titular haya asumido la generación de su par de llaves criptográficas, pública y privada, él será el único responsable del resguardo y custodia de su llave privada.

En caso que la ACDATYS haya asumido la responsabilidad de la generación del par de llaves criptográficas, pública y privada, del titular; la ACDATYS asumirá también el resguardo y custodia de la llave privada del titular.

## **6.3. Otros aspectos de la gestión del par de llaves**

### **6.3.1. Archivo de llave pública**

La ACDATYS mantiene un repositorio de todos los Certificados Digitales emitidos, por un período de 15 años, para que puedan ser consultados en cualquier momento

y validada la cadena de confianza. Igualmente, los mantiene almacenados en las copias de respaldo.

### **6.3.2. Periodo de validez de los Certificados Digitales**

A los efectos de esta PC, el periodo de validez de los Certificados Digitales emitidos por la ACDATYS es de un (1) año o de dos (2) años.

En casos excepcionales y sujeto a condiciones particulares, la ACDATYS podrá emitir Certificados Digitales de Llave Pública cuyo período de validez sea inferior a un (1) año.

### **6.4. Controles de seguridad informática**

De acuerdo con lo especificado en la DPC de la ACDATYS.

### **6.5. Controles de seguridad del ciclo de vida**

De acuerdo con lo especificado en la DPC de la ACDATYS.

### **6.6. Controles de seguridad de la red**

De acuerdo con lo especificado en la DPC de la ACDATYS.

## 7. Perfiles de los Certificados Digitales, las CRL y el OCSP

### 7.1. Perfil de Certificado Digital de Llave Pública

Los certificados emitidos por la ACDATYS se ajustan a las siguientes normas:

- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework,
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) profile,
- Resolución 2/2016 del Minint.

A los efectos de esta PC, los Certificados Digitales de Llave Pública emitidos por la ACDATYS son x.509 versión 3 e incluyen los siguientes campos:

<b>Campo</b>	<b>Valor</b>
Versión	V3
Número de Serie	Valor único generado por la ACDATYS
Algoritmo de firma	SHA512WithRSAEncryption o ECDSAWithSHA512
Algoritmo HASH	SHA512
Emisor	CN = Autoridad de Certificación DATYS OU = Empresa Desarrollo de Aplicaciones Tecnologías y Sistemas DATYS O = Grupo Empresarial MININT L = Playa ST = La Habana C = CU
Válido desde	Especifica la fecha y hora a partir de la cual el Certificado es válido
Válido hasta	Especifica la fecha y hora a partir de la cual el Certificado deja de ser válido
Sujeto	De acuerdo al tipo de suscriptor
Llave pública	Se codifica de acuerdo con la RFC 5280. La longitud de la llave es de 2048 bits para el algoritmo RSA y de 256 bits para el algoritmo ECDSA



### 7.1.1. Número de versión

La ACDATYS soporta y utiliza Certificados X.509 versión 3 (X.509 v3).

### 7.1.2. Extensiones del Certificado Digital de Llave Pública

A los efectos de esta PC, los Certificados Digitales de Llave Pública emitidos por la ACDATYS tendrán las siguientes extensiones:

<b>Campo</b>	<b>Descripción</b>	<b>Crítico</b>
SubjectAlternativeName	Dirección de correo electrónico (RFC822 Name)	Si
KeyUsage	Content Commitment Digital Signature Key Encipherment	Si
ExtendedKeyUsage	Email Protection Client Authentication	Si
CRLDistributionsPoints	Especifica las URL de descarga de las CRL	No
AuthorityKeyIdentifier	Identificador de la llave pública de la ACDATYS	No
CertificatePolicies	Especifica la URL de publicación de la presente PC	No
AuthorityInformationAccess	Especifica la URL de publicación de la DPC de la ACDATYS	No

### 7.1.3. Identificadores de objetos (OID) de los algoritmos

De acuerdo con lo especificado en la DPC de la ACDATYS.

### 7.1.4. Formato de nombres

De acuerdo con lo especificado en la DPC de la ACDATYS.

## 7.2. Perfil de CRL

De acuerdo con lo especificado en la DPC de la ACDATYS.

## 7.3. Listas de revocación de Certificados (CRL)

De acuerdo con lo especificado en la DPC de la ACDATYS.

## **8. Auditorías de cumplimiento y otros controles**

De acuerdo con lo especificado en la DPC de la ACDATYS.

## **9. Cuestiones legales y comerciales**

De acuerdo con lo especificado en la DPC de la ACDATYS y en el Contrato de prestación de servicios criptográficos especializados que se suscriba por las partes.