DATYS
SOLUCIONES TECNOLÓGICAS

AC DATYS
AUTORIDAD DE CERTIFICACIÓN

Política de Certificación: Certificado SSL Sitios Web

La Habana, Cuba

Hoja de control

Título	Política de Certificación de la AC DATYS: Certificado SSL Sitios Web
Autores	Especialista César A. Peláiz López Dr. C. Sacha Pelaiz Barranco
Versión	1.0.0
Fecha	06/03/2025

Registro de cambios

Versión	Fecha	Motivos de los cambios
1.0.0	06/03/2025	Versión inicial

Índice

1. Introducción

1.1. Generalidades

El presente documento: Política de Certificación de la AC DATYS: Certificado SSL Sitios Web (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 AC DATYS, el reglamento para la Infraestructura de Llave Pública (en lo adelante PKI, por sus siglas en inglés) de la República de Cuba, vigente por el Decreto Ley 79/2023, 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 AC DATYS, 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 AC DATYS 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 79/2023,
- 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 AC DATYS, 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 AC DATYS https://www.ac.datys.cu.

1.2. Nombre del documento e identificación

Nombre del documento	Políticas de Certificación de la AC DATYS: Certificado SSL Sitios Web
Versión del documento	1.0.0
Estado del documento	Aprobado
Fecha de emisión	06/03/2025
Disponible en:	https://www.ac.datys.cu/politicas

1.3. Entidades y personas participantes

Las entidades y personas participantes son:

- La empresa Datys como titular de la AC DATYS,
- La Autoridad de Certificación AC DATYS,
- La Autoridad de Registro AR DATYS,
- 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 AC DATYS,
- Los terceros aceptantes de los Certificados Digitales de Llave Pública emitidos por la AC DATYS.

1.3.1. Autoridad de Certificación AC DATYS

La AC DATYS 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 AC DATYS, 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 AR DATYS

De acuerdo con lo especificado en la DPC de la AC DATYS.

1.3.3. Autoridad de Validación

De acuerdo con lo especificado en la DPC de la AC DATYS.

1.3.4. Autoridad de Sellado de tiempo

De acuerdo con lo especificado en la DPC de la AC DATYS.

1.3.5. Repositorio de Certificados Digitales de Llave Pública

De acuerdo con lo especificado en la DPC de la AC DATYS.

1.3.6. Repositorio de llaves privadas

De acuerdo con lo especificado en la DPC de la AC DATYS.

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 jurídica a través de un representante acreditado 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 jurídica, propietario de un Certificado Digital, cuya identidad está vinculada a los datos de creación y verificación del Certificado SSL.

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 AC DATYS.

1.4. Uso de los Certificados Digitales de Llave Pública

1.4.1. Uso apropiado de los Certificados

Los Certificados Digitales de Llave Pública emitidos por la AC DATYS bajo esta PC, tienen bien definido y regulado su uso, restricciones y requerimientos específicos, para autenticar la identidad de un sitio web de alcance nacional y habilitar además una conexión cifrada.

El uso de un Certificado Digital de Llave Pública emitido conforme a la presente PC y a la DPC de la AC DATYS, 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 AC DATYS y la ACSCC, y sujetos a su aprobación, los Certificados Digitales emitidos por la AC DATYS 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 AC DATYS, 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 AC DATYS, según lo establecido en la presente PC y en la DPC de la AC DATYS, por parte de terceros, entidades o titulares, eximirá a la AC DATYS de cualquier responsabilidad.

1.5. Administración de la PC de la AC DATYS

1.5.1. Organización responsable de la PC

Nombre	Autoridad de Certificación AC DATYS
Correo electrónico	acdatys@datys.cu
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	cesar.pelaiz@datys.cu
Dirección	5ta y 34 No. 3401 Miramar, Playa, La Habana, Cuba
Teléfono	78830492 ext. 212

1.5.3. Procedimiento de aprobación

La AC DATYS 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 DPC se emplean las definiciones establecidas en el Decreto Ley 79/2023 “Sobre el desarrollo, la aplicación y uso de los dispositivos de

protección criptográfica y servicios de la esfera de la criptografía en la República de Cuba".

1.6.2. Acrónimos

AC: Autoridad de Certificación

AC DATYS: Autoridad de Certificación de la empresa Datys

ACSCC: Autoridad de Certificación del Servicio Central Cifrado

AR: Autoridad de Registro

AR DATYS: 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 Comon 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 Infraestructure

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 AC DATYS.

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

A los efectos de esta PC, la ACDATYS asume la responsabilidad de la generación del par de llaves criptográficas, pública y privada.

3.1. Registro de nombres

De acuerdo con lo especificado en la DPC de la AC DATYS.

3.2. Validación de la identidad inicial

Ante la solicitud, de manera presencial y por primera vez, de varios Certificados Digitales por una persona jurídica a través de un representante acreditado, la AR DATYS solicitará a la AC DATYS que emita un Certificado Digital de Firma Digital cuyo titular será el representante acreditado por la persona jurídica o entidad, de manera que, como parte del proceso de solicitud, el representante pueda enviar, vía correo electrónico, firmado digitalmente el Modelo de Solicitud que corresponda, empleando su Certificado Digital, emitido por la AC DATYS.

De esta forma, se evita la impresión de un Modelo de Solicitud de muchas hojas en correspondencia con la cantidad de Certificados Digitales solicitados.

3.2.1. Procedimiento de prueba de posesión de llave privada

No procede.

3.2.2. Autenticación de la Identidad de una persona jurídica

A los efectos de esta PC, el representante acreditado por la entidad o persona jurídica, deberá entregar a la AR DATYS la información que avale la existencia legal de la persona jurídica o entidad.

La AR DATYS verificará en los registros legales correspondientes la veracidad de la información entregada.

3.2.3. Autenticación de la Identidad individual

A los efectos de esta PC, la persona jurídica a través del representante acreditado, deberá realizar la solicitud de Certificado Digital, de manera presencial o a través de correo electrónico según lo especificado en 3.2, ante la AR DATYS, presentando los siguientes documentos:

- Carné de identidad (NIF) actualizado del representante acreditado,
- copia digital o impresa de documentación legal que avale la constitución de la entidad que representa,
- impreso y firmado por Autoridad facultada el documento de Contrato General de Prestación de Servicios de Certificado Digital establecido por la empresa DATYS,
- impreso y firmado por Autoridad facultada el documento de Ficha de Cliente establecido por la empresa DATYS,
- impreso y firmado por Autoridad facultada el documento que designa y acredita a un funcionario de una persona jurídica o entidad, que fungirá como su representante legal a los efectos de todo el proceso de solicitud y uso de los Certificados Digitales. Se entregará además una versión digital del documento,

- impreso y firmado el Modelo de Solicitud de Certificado Digital: Certificado SSL Sitios Web, que incluirá los datos identificativos de la persona jurídica, del representante acreditado y del responsable, así como otros datos técnicos requeridos. Se entregará además una versión digital del modelo,
- Modelo de Solicitud de Certificado Digital: Certificado SSL Sitios Web, firmado digitalmente por el representante. Solo en caso de que la solicitud se realice vía correo electrónico.

La AR DATYS 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

La ARDATYS realiza la verificación de pertenencia del solicitante o representante acreditado a la entidad en cuestión antes de la emisión del Certificado Digital de Llave Pública, a través de los registros legales correspondientes.

3.2.5. Información no verificada sobre el solicitante

De acuerdo con lo especificado en la DPC de la AC DATYS.

3.3. Identificación y autenticación en las solicitudes de renovación

A los efectos de esta PC, la persona jurídica a través del representante acreditado, deberá realizar la solicitud de renovación de llaves, de manera presencial o a través de correo electrónico, ante la AR DATYS, presentando los siguientes documentos:

- Carné de identidad (NIF) actualizado del representante acreditado, en caso de solicitud presencial,
- impreso y firmado el Modelo de Solicitud de Certificado Digital: Certificado SSL Sitios Web, que incluirá los datos identificativos de la persona jurídica, del

representante acreditado, y del responsable, así como otros datos técnicos requeridos. Se entregará además una versión digital del modelo,

- Modelo de Solicitud de Certificado Digital: Certificado SSL Sitios Web, firmado digitalmente por representante. Solo en caso que la solicitud se realice vía correo electrónico.

Si el representante acreditado 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, la persona jurídica a través del representante acreditado, deberá realizar la solicitud de revocación de Certificado Digital, de manera presencial o a través de correo electrónico, ante la AR DATYS, presentando los siguientes documentos:

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

Si el representante acreditado 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 AC DATYS 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 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 AR DATYS es el siguiente:

1. **Realizar solicitud**: la persona jurídica a través del representante acreditado, de manera presencial, solicita el Certificado Digital a un funcionario de la AR DATYS, presentando los documentos requeridos según se establece en la sección 3.2.3 de la presente PC.

2. **Recepcionar solicitud**: el funcionario de la AR DATYS recepciona los documentos presentados por el representante acreditado.

3. **Validar datos identificativos**: el funcionario de la AR DATYS valida los datos identificativos de la persona jurídica y del representante acreditado. En caso que se detecte algún problema con algún dato identificativo, el funcionario de la AR DATYS lo comunica al representante acreditado.

4. **Validar Contrato General**: el funcionario de la ARDATYS verifica que el Contrato General haya sido llenado correctamente y debidamente firmado en

todas sus hojas. En caso que se detecte algún problema con el Contrato General, el funcionario de la ARDATYS lo comunica al representante acreditado.

5. **Validar Ficha de Cliente**: el funcionario de la ARDATYS verifica que la Ficha de Cliente haya sido llenada correctamente y debidamente firmada. En caso que se detecte algún problema con la Ficha de Cliente, el funcionario de la ARDATYS lo comunica al representante acreditado.

6. **Validar Modelo de Solicitud**: el funcionario de la AR DATYS 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 AR DATYS lo comunica al representante acreditado.

7. **Solicitar consecutivo para Contrato General (si procede)**: el Director de la ACDATYS solicita al Departamento Legal de la empresa DATYS el consecutivo correspondiente al nuevo Contrato.

8. **Elaborar Contrato Específico**: el Director de la ACDATYS, una vez recibido el consecutivo correspondiente al nuevo Contrato General (si procede), elabora el Contrato Específico de Certificado Digital, que se corresponde con la solicitud presentada por el representante acreditado.

9. **Enviar Contrato Específico al Cliente**: el Director de la ACDATYS envía, vía correo electrónico, el Contrato Específico de Certificado Digital al representante acreditado, para que proceda a su firma y reenvío a la ACDATYS.

10. **Confirmar aceptación y firma del Contrato Específico**: el Director de la ACDATYS confirma la aceptación y firma por el Cliente del Contrato Específico. En caso que la firma del Contrato Específico no se concrete, se da por concluido el proceso de tramitación de la solicitud.

11. **Aprobar solicitud**: la ARDATYS aprueba la solicitud de Certificado Digital.

12. **Crear expediente técnico**: el funcionario de la AR DATYS crea el expediente técnico del solicitante y archiva todos los documentos presentados como parte de la solicitud.

13. **Registrar datos del solicitante**: el funcionario de la AR DATYS registra al solicitante en el sistema.

14. **Crear Orden de trabajo**: el funcionario de la AR DATYS crea una Orden de trabajo de la nueva solicitud.

15. **Firmar Orden de trabajo**: el funcionario de la AR DATYS firma digitalmente la Orden de trabajo de la nueva solicitud.

16. **Publicar Orden de trabajo**: el funcionario de la AR DATYS publica vía FTP (en la carpeta que corresponda) la Orden de trabajo correspondiente a la solicitud.

17. **Notificar a la AC DATYS**: el funcionario de la AR DATYS notifica al funcionario de la AC DATYS que fue creada una nueva Orden de trabajo para que este proceda a su tramitación y correspondiente emisión del Certificado Digital.

18. **Validar Orden de trabajo:** el funcionario de la AC DATYS 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 AC DATYS lo comunica al funcionario de la AR DATYS que creó y firmó la Orden de trabajo.

19. **Comprobar Orden de trabajo:** el funcionario de la AC DATYS 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 AR DATYS que creó la Orden de trabajo para que proceda a su corrección.

20. **Emitir Certificado Digital:** el funcionario de la AC DATYS emite el Certificado Digital correspondiente a la solicitud a partir de la CSR correspondiente.

21. **Firmar Orden de trabajo**: el funcionario de la AC DATYS firma digitalmente la Orden de trabajo de la solicitud como constancia de que fue tramitada y que se emitió el Certificado Digital correspondiente.

22. **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.

23. **Notificar a la AR DATYS**: el funcionario de la AC DATYS notifica al funcionario de la AR DATYS que la Orden de trabajo fue tramitada y que fue emitido el Certificado Digital correspondiente.

24. **Publicar Certificado Digital (si procede)**: el funcionario de la AC DATYS publica en el sitio web oficial de la AC DATYS el Certificado Digital emitido.

25. **Notificar al representante acreditado**: el funcionario de la AR DATYS notifica al representante acreditado que la solicitud fue tramitada y que el Certificado Digital fue publicado (si procedía) en el repositorio púbico de la ACDATYS, y que puede presentarse en la ACDATYS a recogerlo.

26. **Actualizar expediente técnico del titular**: el funcionario de la AR DATYS realiza las acciones pertinentes de actualización del expediente del titular del Certificado Digital.

27. **Validar expediente técnico**: el directivo de la AR DATYS 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 AR DATYS lo

comunica al funcionario que creó el expediente para que proceda a su corrección.

4.1.1. Proceso de registro y responsabilidades

La AR DATYS 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 AR DATYS verificar la identidad de la persona natural o jurídica, del representante acreditado, y del responsable; así como la autenticidad de la información tributada, que el solicitante haya consentido la solicitud de Certificado Digital mediante su firma, y que el Contrato General haya sido aprobado por las partes involucradas.

4.2.1. Aprobación o denegación de las solicitudes de Certificados Digitales

La AR DATYS puede denegar una solicitud de Certificado Digital, sin que ello implique contraer responsabilidad alguna por las consecuencias que pudieran derivarse para la persona jurídica, de tal decisión.

4.3. Emisión de Certificados Digitales de Llave Pública

Los Certificados Digitales emitidos por la AC DATYS entrarán en vigencia a partir del momento de su publicación en el sitio web oficial de la AC DATYS.

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 AC DATYS, se asegura mediante la firma del Contrato General, que precisa que el

solicitante conoce y acepta las condiciones de la presente PC y de la DPC de la AC DATYS.

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 la autenticación de servicios o servidores, y establecer una conexión segura para el acceso, de acuerdo con lo especificado en el campo KeyUsage del Certificado Digital. Además, de acuerdo con lo establecido en el campo ExtendedKeyUsage del Certificado Digital, su uso extendido permitirá Server Authentication.

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, 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 AC DATYS, 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 o representante acreditado 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 establecido por la AR DATYS y publicado en su sitio web oficial,
- que la AC DATYS 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 AR DATYS, de acuerdo a lo convenido en el Contrato General, podrá notificar al titular o representante acreditado, 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 AR DATYS es el siguiente:

1. **Realizar solicitud**: el representante acreditado, de manera presencial, solicita la renovación del Certificado Digital a un funcionario de la AR DATYS, presentando los documentos requeridos según se establece en la sección 3.3 de la presente PC.
2. **Recepcionar solicitud**: el funcionario de la AR DATYS recepciona los documentos presentados por el representante acreditado de la persona jurídica.
3. **Validar datos identificativos**: el funcionario de la AR DATYS valida los datos identificativos del representante acreditado y de la persona jurídica titular,

comparándolos además con sus datos registrados. Si alguna información del titular ha cambiado, ésta deberá ser nuevamente registrada con el acuerdo del representante acreditado. En caso que se detecte algún problema con algún dato, el funcionario de la AR DATYS lo comunica al representante acreditado.

4. **Validar Modelo de Solicitud**: el funcionario de la AR DATYS 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 AR DATYS lo comunica al titular o representante acreditado.

5. **Precisar causas de renovación**: el funcionario de la AR DATYS precisa las causas que motivaron la solicitud de renovación del Certificado Digital de acuerdo a lo establecido en el Modelo de Solicitud correspondiente.

6. **Elaborar Contrato Específico**: el Director de la ACDATYS elabora el Contrato Específico de Certificado Digital, que se corresponde con la solicitud presentada por el representante acreditado.

7. **Enviar Contrato Específico al Cliente**: el Director de la ACDATYS envía, vía correo electrónico, el Contrato Específico de Certificado Digital al representante acreditado, para que proceda a su firma y reenvío a la ACDATYS.

8. **Confirmar aceptación y firma del Contrato Específico**: el Director de la ACDATYS confirma la aceptación y firma por el Cliente del Contrato Específico. En caso que la firma del Contrato Específico no se concrete, se da por concluido el proceso de tramitación de la solicitud.

9. **Aprobar solicitud**: la ARDATYS aprueba la solicitud de renovación del Certificado Digital.

10. **Actualizar expediente técnico**: el funcionario de la AR DATYS actualiza el expediente técnico del titular.

11. **Actualizar datos del solicitante**: el funcionario de la AR DATYS actualiza en el sistema los datos del titular, si existen cambios previamente acordados con el titular o representante acreditado.

12. **Crear Orden de trabajo**: el funcionario de la AR DATYS crea una Orden de trabajo de la nueva solicitud.

13. **Firmar Orden de trabajo**: el funcionario de la AR DATYS firma digitalmente la Orden de trabajo de la nueva solicitud.

14. **Publicar Orden de trabajo**: el funcionario de la AR DATYS publica vía FTP (en la carpeta que corresponda) la Orden de trabajo.

15. **Notificar a la AC DATYS**: el funcionario de la AR DATYS notifica al funcionario de la AC DATYS que fue creada una nueva Orden de trabajo para que este proceda a su tramitación y correspondiente renovación del Certificado Digital.

16. **Validar Orden de trabajo:** el funcionario de la AC DATYS 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 AC DATYS lo comunica al funcionario de la AR DATYS que creó y firmó la Orden de trabajo.

17. **Comprobar Orden de trabajo:** el funcionario de la AC DATYS 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 AR DATYS que creó la Orden de trabajo para que proceda a su corrección.

18. **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.

19. **Renovar Certificado Digital:** el funcionario de la ACDATYS emite un nuevo Certificado Digital en correspondencia con la solitud de renovación en trámite, haciendo efectiva la renovación.

20. **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.

21. **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.

22. **Notificar a la AR DATYS**: el funcionario de la AC DATYS notifica al funcionario de la AR DATYS que la Orden de trabajo fue tramitada y que fue renovado el Certificado Digital correspondiente.

23. **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.

24. **Publicar Certificado Digital (si procede)**: el funcionario de la ACDATYS publica en el repositorio público de la ACDATYS el nuevo Certificado Digital emitido.

25. **Notificar al representante acreditado**: el funcionario de la ARDATYS notifica al representante acreditado que la solicitud fue tramitada y que el nuevo Certificado Digital fue publicado (si procedía) en el repositorio púbico 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.

26. **Actualizar expediente técnico del titular**: el funcionario de la ARDATYS realiza las acciones pertinentes de actualización del expediente técnico del titular.

27. **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 AC DATYS.

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 AR DATYS revisará los términos convenidos en el Contrato General.

La suspensión de un Certificado Digital de Llave Pública es efectiva por un período máximo de 30 días. Vencido este tiempo, la AR DATYS procederá a evaluar el

estado de la suspensión con el titular, y procederá a eliminar la suspensión del Certificado o tramitar con la AC DATYS su revocación.

Ante la solicitud de revocación de un Certificado Digital, la AR DATYS evalúa la solicitud, y en caso de proceder, gestiona la revocación con la AC DATYS, 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 AR DATYS es el siguiente:

1. **Realizar solicitud**: el representante acreditado, de manera presencial, solicita la revocación del Certificado Digital a un funcionario de la AR DATYS, presentando los documentos requeridos según se establece en la sección 3.4 de la presente PC.

2. **Recepcionar solicitud**: el funcionario de la AR DATYS recepciona los documentos presentados por el representante acreditado.

3. **Validar datos identificativos**: el funcionario de la AR DATYS valida los datos identificativos del representante acreditado y de la persona jurídica, comparándolos además con sus datos registrados. En caso que se detecte algún problema con algún dato, el funcionario de la AR DATYS lo comunica al representante acreditado.

4. **Validar Modelo de Solicitud**: el funcionario de la AR DATYS 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 AR DATYS lo comunica al representante acreditado.

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 representante acreditado**: el funcionario de la ARDATYS notifica al representante acreditado 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 AC DATYS,
- término de la relación del titular del Certificado Digital con la entidad,
- el Certificado Digital de la AC DATYS 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 General,
- 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 o representante acreditado, así como por la AC DATYS, 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 AR DATYS 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 AR DATYS.

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 AR DATYS.

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

4.8.4. Plazo en que la AC DATYS debe resolver la solicitud de revocación

La AC DATYS 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 AC DATYS.

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

De acuerdo con lo especificado en la DPC de la AC DATYS.

4.8.8. Disponibilidad de verificación de la revocación

De acuerdo con lo especificado en la DPC de la AC DATYS.

4.8.9. Requerimientos especiales de revocación de llave privada comprometida

De acuerdo con lo especificado en la DPC de la AC DATYS.

4.9. Servicios de verificación del estado de los Certificados Digitales

De acuerdo con lo especificado en la DPC de la AC DATYS.

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 o representante acreditado no solicita la renovación de un Certificado Digital tras el término de su validez, la AR DATYS procederá a la revisión de los términos establecidos en el Contrato General 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 AC DATYS.

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

De acuerdo con lo especificado en la DPC de la AC DATYS.

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

De acuerdo a lo especificado en la DPC de la AC DATYS.

6.1.2. Entrega de la llave privada al titular

El archivo contenedor de la llave privada le será entregado al representante acreditado en formato PKCS#12 en un dispositivo de almacenamiento USB (facilitado por el titular o el representante acreditado) o en un disco compacto (CD por sus siglas en inglés).

La contraseña de protección de la llave privada le será entregada al representante acreditado, impresa en sobre de seguridad y será tratada como información oficial clasificada.

6.1.3. Entrega de la llave pública de la AC DATYS a los titulares

La llave pública de la AC DATYS 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 4096 bits de longitud para el esquema criptográfico RSA y de 384 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 AC DATYS no eximen al titular de ser el principal responsable de proteger su llave privada.

6.2.1. Custodia de la llave privada

La ACDATYS asumirá 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 AC DATYS 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 AC DATYS son de un (1) año o de dos (2) años.

En casos excepcionales y sujeto a condiciones particulares, la AC DATYS 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 AC DATYS.

6.5. Controles de seguridad del ciclo de vida

De acuerdo con lo especificado en la DPC de la AC DATYS.

6.6. Controles de seguridad de la red

De acuerdo con lo especificado en la DPC de la AC DATYS.

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 AC DATYS 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,
- Decreto Ley 79/2023.

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

Campo	Valor
Versión	V3
Número de Serie	Valor único generado por la AC DATYS
Algoritmo de firma	SHA512WithRSAEncryption
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 llave es 4096 bits para el algoritmo RSA y de 384 bits para el algoritmo ECDSA

7.1.1. Número de versión

La AC DATYS 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 AC DATYS tendrán las siguientes extensiones:

Campo	Descripción	Crítico
KeyUsage	Content Commitment Key encipherment	Si
ExtendedKeyUsage	Server Authentication	Si
CRLDistributionsPoints	Especifica las URL de descarga de las CRL	No
AuthorityKeyIdentifier	Identificador de la llave pública de la AC DATYS	No
CertificatePolicies	Especifica la URL de publicación de la presente PC	No
AuthorityInformationAccess	Especifica la URL de publicación de la DPC de la AC DATYS	No

7.1.3. Identificadores de objetos (OID) de los algoritmos

De acuerdo con lo especificado en la DPC de la AC DATYS.

7.1.4. Formato de nombres

De acuerdo con lo especificado en la DPC de la AC DATYS.

7.2. Perfil de CRL

De acuerdo con lo especificado en la DPC de la AC DATYS.

7.3. Listas de revocación de Certificados (CRL)

De acuerdo con lo especificado en la DPC de la AC DATYS.

8. Auditorías de cumplimiento y otros controles

De acuerdo con lo especificado en la DPC de la AC DATYS.

9. Cuestiones legales y comerciales

De acuerdo con lo especificado en la DPC de la AC DATYS y en el Contrato General que se suscriba por las partes.

Firmado digitalmente por Autoridad de Certificación de DATYS (SELLO)
Fecha: 2025.03.14 10:53:08 -04'00'