AC DATYS

AUTORIDAD DE CERTIFICACIÓN

Declaración de Prácticas de Certificación

La Habana, Cuba

Hoja de control

Título	Declaración de Prácticas de Certificación de la ACDATYS
Autores	Especialista César A. Peláiz López Dr. C. Sacha Pelaiz Barranco
Versión	1.0.0
Fecha	1/11/2021

Registro de cambios

Versión	Fecha	Motivos de los cambios
1.0.0	1/11/2021	Versión inicial
1.1.0	20/05/2023	Norma Técnica 000241.23-O.23230425

Índice

1. Introducción

1.1. Generalidades

El presente documento: Declaración de Prácticas de Certificación (en lo adelante DPC) describe, precisa y regula las prácticas, reglas y procedimientos, facultades, responsabilidades, obligaciones, deberes y derechos de la empresa DATYS, al constituirse como Autoridad de Certificación Intermedia de Certificados Digitales de Llave Pública (en lo adelante ACDATYS) en el contexto de la Infraestructura de Llave Pública (en lo adelante PKI) de la República de Cuba, para proporcionar seguridad y protección al intercambio de información entre los Organismos de la Administración Central del Estado (en lo adelante OACE) y entidades del país, así como a su conservación; garantizando la identidad, autenticidad, integridad, confidencialidad y no repudio, de sus archivos y documentos digitales; asegurando la fiabilidad, transparencia y seguridad en la generación y emisión de Certificados Digitales de Llave Pública.

La presente DPC constituye la identificación y la caracterización de la ACDATYS, y está destinada para la comprensión y uso por los directivos y funcionarios de los OACE y entidades del país, que necesitan y requieren evaluar y confirmar la fiabilidad de la ACDATYS, a fin de determinar y conciliar que los Certificados Digitales de Llave Pública que esta emite, satisfacen los requisitos de protección para su información digital y se corresponden con las Políticas de Certificación (en lo adelante PC), emitida por la ACDATYS. De igual forma ordena y dispone el régimen jurídico y comercial que se establece entre las entidades, los titulares y la ACDATYS.

Esta DPC y los documentos relacionados regulan todo el ciclo de vida de los Certificados Digitales, desde su solicitud hasta su extinción o revocación, así como las relaciones que se establecen entre el solicitante y titular del certificado, la ACDATYS y las terceras partes que confían.

En la presente DPC se establece la delimitación de responsabilidades de las diferentes partes intervinientes, así como las limitaciones de las mismas ante posibles daños y perjuicios.

La presente DPC está redactada siguiendo las especificaciones de:

- RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”,
- 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”.

Su estructura y contenido está basada en 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 Autoridad Raíz ACSCC,

así como en buenas prácticas de experimentadas Autoridades de Certificación externas.

Para la ACDATYS constituirse como una Autoridad de Certificación de Certificados Digitales de Llave Pública confiable y segura, garantiza que:

- Sus operaciones se desenvuelven en un ambiente de seguridad y control,
- sus responsabilidades y obligaciones están bien definidas,

- sus procesos de trabajo están bien identificados y se ejecutan correctamente,
- sus titulares estén bien informados,
- se aplica una adecuada y rigurosa identificación, autenticación y acreditación de los solicitantes,
- sus directivos y especialistas son profesionales experimentados y están debidamente preparados y certificados.

La ACDATYS asume que las entidades y 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 los directivos y funcionarios de los OACE y entidades del país, para disponer del adecuado conocimiento relativo a una PKI, consulten los documentos regulatorios anteriormente señalados, que sustentan la presente DPC.

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 DPC, las PC y demás documentos afines y documentación complementaria, los que estarán disponibles en el sitio web oficial de la ACDATYS https://ac.datys.cu.

En la medida que la ACDATYS incorpore otros niveles de aseguramientos, servicios y reglamentaciones, la presente DPC será objeto de modificación para describir las nuevas prácticas correspondientes, las que serán oportunamente notificadas a las entidades y a los titulares de Certificados Digitales de Llave Pública y publicadas en su sitio web oficial.

1.2. Nombre del documento e identificación

Nombre del documento	Declaración de Prácticas de Certificación de la ACDATYS
Versión del documento	1.1.0
Estado del documento	Aprobado
Fecha de emisión	20/05/2023
Disponible en:	https://ac.datys.cu/politicas

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, revocar y firmar Certificados Digitales de Llave Pública en interés de los OACE, OSDE, entidades, empresas,

organizaciones y personas naturales, para lo cual asume la responsabilidad de emitir y mantener actualizadas sus PC y la presente 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.

Los datos más significativos del Certificado Digital de Llave Pública de la ACDATYS son:

Versión	X.509 v3
Número de serie	00975704e401
Algoritmo de firma	SHA512WithRSAEncryption
Nombre distintivo del sujeto	CN = Autoridad de Certificación DATYS OU = Empresa Desarrollo Aplicaciones Tecnologías y Sistemas DATYS O = Grupo Empresarial MININT L = Playa ST = La Habana C = CU
Nombre distintivo del Emisor	CN = Autoridad de Certificación Servicio Central Cifrado OU = Autoridad Raíz O = Infraestructura de Llave Pública de la República de Cuba L = Boyeros ST = La Habana C = CU E = admonpki@mail.mn.co.cu
Periodo de validez	Desde: 03-08-2021 hasta: 01-08-2028
Limitaciones básicas	AC, sin restricción de longitud de ruta
Usos de llave	Firma digital, firma de Certificados, firma de CRL
Huella digital (SHA1)	FEFD1D851D1DE6B14E56284B01C57681A537C74A
Huella digital (SHA 256)	F2152FFC71CFAB03DFF6CC5F40EC4715 58D63C18D008C9AAA8C6FB4EB5279ED2
Algoritmo criptográfico	RSA
Longitud de llave	4096 bits

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

La Autoridad de Registro ARDATYS está destinada para registrar, comprobar, gestionar y controlar Certificados Digitales de Llave Pública, en interés de los OACE, OSDE, entidades, empresas y organizaciones del país y personas naturales, para lo cual asume la responsabilidad de cumplir con las PC y la presente DPC de la ACDATYS.

La ARDATYS para el cumplimiento de sus responsabilidades asegura se ejecuten las siguientes acciones:

- Recepcionar las solicitudes de Certificados Digitales de Llave Pública de las entidades y solicitantes, y comprobar la validez de la documentación presentada mediante rigurosos procedimientos de identificación y autenticación,
- emitir la certificación oficial de aprobación de la identificación y autenticación realizada a la información del solicitante,
- recepcionar en el soporte digital y formato convenido en la presente DPC y las PC, la llave pública del titular del Certificado Digital de Llave Pública, si ese es el caso, para la emisión de su Certificado Digital,
- gestionar con la ACDATYS la emisión del Certificado Digital de Llave Pública solicitado,
- alertar a las entidades y titulares de Certificados Digitales de Llave Pública bajo su control, la proximidad de la fecha de caducidad del mismo y el procedimiento a seguir para la renovación de este,

- activar los planes y medidas para la continuidad de funcionamiento de la ARDATYS, a fin de restablecer las operaciones en un tiempo razonable, en caso de interrupción o falla de los procesos críticos,
- describir el entorno de seguridad y protección en que se encuentran enmarcados los servicios de registro y validación que brinda y otros,
- ejecutar auditorías internas y poner en conocimiento de la ACDATYS las situaciones anormales detectadas, no compatibles con lo establecido en la presente DPC.

1.3.3. Autoridad de Validación

La Autoridad de Validación de la ACDATYS tiene como objetivo proveer un servicio de validación del estado de los Certificados Digitales de Llave Pública emitidos por la ACDATYS. El servicio implementa el protocolo de validación en línea del estado de un Certificado Digital (OCSP por sus siglas en inglés) conforme a lo establecido en la RFC 2560.

Este mecanismo de validación es complementario a la emisión y publicación de las CRL.

1.3.4. Autoridad de Sellado de tiempo

La Autoridad de Sellado de Tiempo de la ACDATYS cumple con la RFC 3161.

1.3.5. Repositorio de Certificados Digitales de Llave Pública

El repositorio de Certificados Digitales de Llave Pública emitidos por la ACDATYS es un almacén público y de libre acceso, que permite la visualización, búsqueda y descarga de los Certificados.

1.3.6. Repositorio de llaves privadas

El repositorio de llaves privadas de la ACDATYS garantiza la confidencialidad de las llaves almacenadas, así como su recuperación, de acuerdo a lo regulado en la presente DPC y en las PC, con relación a los procedimientos de solicitud y tramitación de recuperación de llaves.

El acceso al repositorio de llaves privadas de la ACDATYS no es público ni libre, y está sujeto a las políticas y regulaciones internas de la ACDATYS.

1.3.7. Solicitantes y titulares de Certificados Digitales de Llave Pública

A los efectos de la presente DPC se entenderá como solicitante a toda persona natural en su condición de Ciudadano, a persona natural en su condición de Funcionario, y a 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 o persona natural en su condición de Ciudadano o Funcionario, propietario de un Certificado Digital, cuya identidad está vinculada a los datos de creación y verificación de firma.

1.3.8. Terceros que confían

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

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, que se encuentra vigente y conocer sus características expresadas en la

PC y la presente DPC, según las cuales se emitió el Certificado Digital de Llave Pública.

1.4. Uso de los Certificados Digitales de Llave Pública

1.4.1. Usos apropiados de los certificados

Los Certificados Digitales de Llave Pública emitidos por la ACDATYS tienen bien definidos y regulados sus usos, restricciones y requerimientos específicos, lo que queda establecido en las PC de la ACDATYS.

El uso de un Certificado Digital de Llave Pública emitido conforme a esta DPC, 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 deben emplearse de acuerdo con las funciones y finalidades definidas en las PC de la ACDATYS, sin que puedan utilizarse para otras tareas y otros fines no contemplados en la misma.

Los Certificados, salvo en los casos en que así lo especifiquen las PC, no pueden utilizarse para actuar ni como Autoridad de Registro ni como Autoridad de Certificación, firmando certificados de llave pública de ningún tipo, ni CRL.

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 de un Certificado Digital de Llave Pública emitido por la ACDATYS, según lo establecido en la PC correspondiente y en la presente DPC, por parte de terceros, entidades o titulares, eximirá a la ACDATYS de cualquier responsabilidad.

1.5. Administración de la DPC de la ACDATYS

1.5.1. Organización responsable de la DPC

Nombre	Autoridad de Certificación ACDATYS
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 ACDATYS es la responsable de la elaboración, modificación, actualización y presentación de la presente DPC y las correspondientes PC.

Su aprobación es facultad de la Dirección de Criptografía (en lo adelante DC) del Ministerio del Interior (en lo adelante MININT).

1.6. Definiciones y acrónimos

1.6.1. Definiciones

En el ámbito de esta DPC 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

ACRAIZ: Autoridad de Certificación de la República de Cuba

ACSCC: Autoridad de Certificación del Servicio Central Cifrado

AR: Autoridad de Registro

ARI: Autoridad de Registro Intermedia

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 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

FIPS: Estándar de Estados Unidos, del inglés Federal Information Processing Standard

IETF: Organismo de estandarización de Internet, del inglés Internet Engineering Task Force

NIF: Número de identificación fiscal

Nonce: valor aleatorio de un solo uso.

O: Organización, del inglés Organization. Atributo del DN de un objeto dentro de la estructura de directorio X.500

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

PIN: Clave personal de identificación, del inglés Personal Identification Number.

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

RFC: Estándares de la IETF, del inglés Request for Comments

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

2.1. Repositorios de Certificados Digitales de Llave Pública

La ACDATYS hace uso de los siguientes repositorios:

- Un sitio web (https://ac.datys.cu) accesible desde Internet con acceso libre, que publica la presente DPC, las PC de la ACDATYS, el Certificado Digital de Llave Pública de la ACDATYS, el Certificado Digital de Llave Pública de la ACSCC, los Certificados Digitales de Llave Pública de los titulares, así como otros documentos normativos y regulatorios de la República de Cuba en materia de PKI,

- Listas de Certificados revocados CRL, las que pueden ser descargadas desde la dirección URL https://ac.datys.cu/crls

- Un servicio de validación en línea del estado de los Certificados Digitales de Llave Pública, que implementa el protocolo OCSP, con acceso libre a través de Internet http://ocsp.datys.cu

Los repositorios de la ACDATYS estarán disponibles las 24 horas del día, los 7 días de la semana; y en caso de interrupción por causas de fuerza mayor, los servicios se restablecerán en el menor tiempo posible.

Los repositorios cuentan con un servicio de asistencia operativa de 8 horas al día durante los 5 días laborables de la semana.

Los repositorios de la ACDATYS no contienen, en ningún caso, información de naturaleza confidencial.

La ACDATYS se reserva hasta un máximo de una (1) hora diaria de lunes a viernes para ejecutar acciones de mantenimiento, salvas del sistema, etc.

Si existen problemas funcionales u operativos relacionados con los servicios de los repositorios, la ACDATYS lo comunicará a los representantes oficiales de los titulares y precisará el tiempo previsto para su solución.

2.2. Publicación de información de certificación

Es obligación de la ACDATYS publicar la información relativa a sus prácticas, a sus certificados y al estado actual de dichos certificados.

La presente DPC es pública y se encuentra disponible en el sitio web oficial de la ACDATYS https://ac.datys.cu/politicas.

Las PC de la ACDATYS son públicas y se encuentran disponibles en formato PDF en: https://ac.datys.cu/politicas.

El Certificado Digital de Llave Pública de la ACDATYS es público y se encuentra disponible en: https://ac.datys.cu/certificados.

Las CRL emitidas por la ACDATYS son públicas y se encuentran disponibles en formato CRL v2 en: https://ac.datys.cu/crls.

Las CRL estarán firmadas digitalmente por la ACDATYS.

La información sobre el estado de los Certificados Digitales de Llave Pública emitidos por la ACDATYS se podrá consultar accediendo directamente a las CRL o mediante el servicio de validación en línea disponible que implementa el protocolo OCSP.

2.3. Frecuencia de publicación

La DPC y las PC de la ACDATYS se publicarán en el momento de su aprobación y se volverán a publicar una vez se apruebe cualquier modificación sobre las mismas. Las modificaciones se harán públicas en el sitio web oficial de la ACDATYS.

La ACDATYS incorporará los Certificados revocados a la CRL pertinente dentro del periodo de tiempo definido en la presente DPC.

La actualización de las bases de datos del servicio de validación en línea que implementa el protocolo OCSP, se realiza de manera inmediata a la emisión, suspensión o revocación de un certificado.

2.4. Controles de acceso a los repositorios

El acceso para la lectura y descarga de la DPC, las PC, las CRL y los Certificados Digitales de Llave Pública, es libre; pero sólo la ACDATYS está autorizada a modificar, sustituir o eliminar información de sus repositorios y de su sitio web. Para ello la ACDATYS establecerá controles y medidas que impidan a personas no autorizadas manipular la información contenida en los repositorios.

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

3.1. Registro de nombres

3.1.1. Tipos de nombres

Los titulares de Certificados Digitales emitidos por la ACDATYS requieren un nombre distintivo (DN) conforme con el estándar X.500.

El DN es conformado de acuerdo a lo estipulado en el artículo 12 de la Resolución 2/2016 del MININT y a la Norma Técnica 000241.23-O.230425, que incluyen como campos obligatorios:

- nombres y apellidos (CN),
- el número de identidad (NIF),
- entidad principal a la que pertenece el solicitante (O),
- entidad específica a la que pertenece el solicitante (OU),
- cargo que ostenta el solicitante en la entidad (T) de conjunto con el Registro del documento oficial de nombramiento,
- el país (C),
- provincia donde radica el solicitante (S) y
- municipio donde radica el solicitante (L).

Los campos O, OU y T son obligatorios para las Personas Naturales en su condición de Funcionarios, mientras que los campos S y L son obligatorios para las Personas Naturales en su condición de Ciudadanos.

3.1.2. Necesidad de que los nombres sean significativos

Se establece que los DN deben tener sentido, no permitiéndose el uso de seudónimos ni el anonimato en los Certificados Digitales de Llave Pública emitidos por la ACDATYS.

La ACDATYS garantiza que los DN de los Certificados Digitales emitidos por ella son significativos, lo que permite establecer una identificación unívoca del titular del Certificado Digital y vincular su identidad con la llave pública.

3.1.3. Interpretación de varios formatos de nombres

La ACDATYS interpretará los DN de los Certificados Digitales de Llave Pública sobre la base de lo definido en “ISO/IEC 9595 (x.500) Distinguished Name (DN)” y en el artículo 12 de la Resolución 2/2016 del MININT.

3.1.4. Unicidad de los nombres

El nombre del sujeto del Certificado Digital de Llave Pública emitido por la ACDATYS es único.

La ARDATYS se encarga de comprobar la unicidad del NIF del titular, así como de los Nombres de Dominio (DNS por sus siglas en inglés) para el caso de Certificados del tipo Servidor SSL/TLS.

En el DN se utiliza una combinación de valores que permite garantizar su unicidad.

3.1.5. Resolución de conflictos sobre nombres

La ACDATYS y la ARDATYS no actúan como árbitros o mediadores, ni resuelven disputa alguna respecto a la titularidad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales, etc. Ambas autoridades se reservan el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

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 por él, con la llave pública, también generada por él y entregada a la ARDATYS como parte de la solicitud de su Certificado Digital de Llave Pública. En tal caso, el Modelo de solicitud de Certificado Digital de Llave Pública deberá ir acompañado de una CSR en formato PKCS#10, firmada con su llave privada, de manera que la ACDATYS pueda comprobar que el solicitante efectivamente posee la llave privada.

3.2.2. Autenticación de la Identidad de una persona jurídica

Cuando una persona jurídica o entidad solicite el servicio de Certificado Digital, deberá hacerlo a través de un representante acreditado por ella, y este deberá entregar a la ARDATYS sus datos identificativos, según lo establece el Modelo de Solicitud de Certificados que corresponda; así como la información que avale la existencia legal de la entidad.

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

3.2.3. Autenticación de la Identidad individual

La ACDATYS emite Certificados Digitales de Llave Pública a personas naturales, ya sea por interés personal o institucional. En el último caso la solicitud se realiza a través de un representante acreditado por la entidad a la que pertenece el solicitante.

La ARDATYS realiza la verificación de la identidad del solicitante a través de los registros legales correspondientes.

3.2.4. Autenticación de la pertenencia del solicitante a una entidad

La ARDATYS realiza la verificación de pertenencia del solicitante 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

La ARDATYS verificará toda la información entregada por el titular o representante acreditado, que vaya a ser incluida en el Certificado Digital.

3.3. Identificación y autenticación en las solicitudes de renovación de llaves

Solamente serán reconocidas como válidas aquellas solicitudes de renovación de llaves que sean tramitadas por representantes acreditados de una entidad, salvo el caso de personas naturales en interés personal.

3.4. Identificación y autenticación en las peticiones de revocación de llaves

Solamente serán reconocidas como válidas aquellas solicitudes de revocación de llaves que sean tramitadas por representantes acreditados de una entidad, salvo el caso de personas naturales en interés personal.

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 la presente DPC.

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

4.1. Solicitud de un Certificado Digital de Llave Pública

El procedimiento para solicitar un Certificado Digital a la ARDATYS se establece en las PC. Además, se especifica quién puede solicitar un Certificado y la información que debe tributar.

La ARDATYS podrá solicitar información adicional a la establecida en las PC, según lo considere necesario.

4.1.1. Registro de las solicitudes de certificados y responsabilidades de los solicitantes

La solicitud de un Certificado Digital se realiza mediante el Modelo de Solicitud de Certificado Digital que se corresponda con el tipo de Certificado solicitado, que están disponibles para su descarga en el sitio web oficial de la ACDATYS.

La información tributada como parte del Modelo de Solicitud de Certificado Digital será conservada de manera protegida por la ARDATYS.

La ARDATYS podrá aprobar o denegar la solicitud de un Certificado Digital.

La solicitud del Certificado Digital, una vez aprobada por la ARDATYS, será enviada a la ACDATYS.

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

Es competencia y responsabilidad de la ARDATYS verificar la identidad del solicitante y del representante acreditado, la autenticidad de la información tributada, que el solicitante haya consentido la solicitud de Certificado Digital y la Cotización de Servicios Criptográficos Especializados mediante su firma, y que el

Contrato de prestación de servicios criptográficos especializados haya sido aprobado por las partes involucradas.

4.2.1. Aprobación o denegación de las solicitudes de certificados

La ARDATYS puede denegar una solicitud de Certificado Digital, sin que ello implique contraer responsabilidad alguna por las consecuencias que pudieran derivarse, para solicitantes, representantes acreditados o entidades, de tal decisión.

4.3. Emisión de Certificados Digitales de Llave Pública

Una vez aprobada por la ARDATYS una solicitud de Certificado Digital, esta envía la Orden de Trabajo a la ACDATYS para que proceda a la emisión del Certificado Digital correspondiente.

Una vez la ACDATYS emita el Certificado Digital, lo comunica a la ARDATYS, lo incorpora al repositorio de Certificados y lo publica en el sitio web oficial de la ACDATYS.

La ARDATYS comunica al representante acreditado de la entidad o a la persona natural en interés personal, que la solicitud de Certificado Digital ha sido satisfecha y que, si procede, debe presentarse para recoger la llave privada asociada al Certificado Digital.

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

4.4. Aceptación de un Certificado Digital de Llave Pública

La aceptación formal por parte del nuevo titular o por el representante oficial de la entidad, de sus responsabilidades y obligaciones relacionadas con la tenencia y uso del Certificado Digital de Llave Pública emitido por la ACDATYS, se asegura mediante la firma del Contrato de prestación de servicios criptográficos

especializados, que precisa que el solicitante conoce y acepta las condiciones de la presente DPC y de las PC.

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

El titular sólo podrá utilizar su llave privada y su Certificado Digital de Llave Pública para los usos autorizados en la PC correspondiente y en la presente DPC, de acuerdo con lo establecido en los campos KeyUsage y ExtendedKeyUsage del Certificado.

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, el titular está obligado 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 Digital es apropiado para el uso al que ha sido destinado, que se encuentra vigente y conocer sus características expresadas en la PC correspondiente y en la presente DPC.

4.6. Renovación de un Certificado Digital de Llave Pública

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.

Todas las renovaciones de Certificados Digitales en el ámbito de esta DPC se realizarán con cambio de llaves.

La ARDATYS comprobará como parte del proceso de renovación, que la información utilizada para verificar la identidad y atributos del titular es todavía válida. Si alguna información del titular ha cambiado ésta deberá ser nuevamente verificada y registrada, con el acuerdo del titular o representante acreditado.

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

- Que se realice atendiendo al Modelo de Solicitud de Renovación establecido por la ARDATYS,
- que la ACDATYS no tenga conocimiento de la concurrencia de ninguna causa de revocación o suspensión del Certificado,
- que la solicitud de renovación se refiera al mismo tipo de Certificado Digital emitido inicialmente.

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

4.7. Modificación de un Certificado Digital de Llave Pública

Todas las modificaciones de Certificados Digitales realizadas en el ámbito de esta DPC se tratarán como una renovación.

La modificación de un Certificado Digital está sujeta a cambios en la información incluida en el Certificado, no relacionados con su llave pública o expiración del periodo de validez.

Las modificaciones de los Certificados Digitales pueden venir dadas por motivos tales como:

- Cambio de nombre,
- cambio de organización,
- cambio en las funciones dentro de la organización,
- reorganización como resultado del cambio en el DN.

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 de las terceras partes confiables.

Toda entidad o titular de un Certificado Digital de Llave Pública podrá decidir y solicitar, en cualquier momento o circunstancia, la suspensión o revocación de su Certificado. 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 o representante acreditado, 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.

Los procesos de solicitud de suspensión y revocación de un Certificado Digital se realizan a través de los correspondientes modelos establecidos por la ARDATYS y publicados en el sitio web oficial de la ACDATYS.

La 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 Digital revocado, éste dejará de estar incluido en las CRL.

Son circunstancias para la suspensión de un Certificado Digital, las mismas que se establecen para la revocación en la sección siguiente.

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,
- comprometimiento de la llave privada de la ACDATYS,
- término de la relación del titular del Certificado con la entidad,
- el Certificado de la ACDATYS fue renovado o revocado,
- 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 presente DPC y lo estipulado en el Contrato de prestación de servicios criptográficos especializados con la ARDATYS,
- 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

La revocación de un Certificado Digital de Llave Pública puede ser solicitada por su titular, por el representante acreditado de su entidad o por la dirección de la entidad, así como por la ACDATYS, quien 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 la presente DPC.

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

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

El procedimiento para solicitar la revocación de un Certificado Digital se establece en las PC.

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 correspondiente.

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 resolución 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

La ACDATYS publicará sus CRL en su sitio web oficial.

Con frecuencia diaria, en días laborables, la ACDATYS publicará una CRL de tipo delta, siempre y cuando se produzcan suspensiones o revocaciones de Certificados.

Con frecuencia semanal, todos los viernes, en el horario comprendido entre las 09:00 y las 10:00 horas, la ACDATYS publicará una CRL acumulativa.

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

La máxima latencia entre la generación de una CRL y su publicación es de dos (2) horas.

4.8.8. Disponibilidad de verificación de la revocación

La verificación de la revocación de un Certificado Digital de Llave Pública puede realizarse a través de las CRL disponibles en el sitio web oficial de la ACDATYS y mediante el servicio de validación en línea del estado de los Certificados, que implementa el protocolo OCSP.

4.8.9. Requerimientos especiales de revocación de llave privada comprometida

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

4.9. Servicios de verificación del estado de los Certificados

Para la consulta y verificación del estado de un Certificado Digital de Llave Pública, la ACDATYS provee un servicio de consulta en línea que implementa el protocolo OCSP; y además, publica en su sitio web oficial las CRL.

Para hacer uso del servicio de validación en línea, las terceras partes que confían deben disponer de un Cliente OCSP que cumpla la RFC 6960 o RFC 5019.

4.9.1. Disponibilidad del servicio

El servicio de consulta en línea del estado de un Certificado Digital de Llave Pública, de la ACDATYS, estará disponible las 24 horas del día, los 7 días de la semana. Igual disponibilidad tendrá la descarga de las CRL desde el sitio web oficial de la ACDATYS.

La ACDATYS se reserva hasta un máximo de 1 hora diaria de lunes a viernes en el momento de mínima actividad, para efectuar tareas de mantenimiento a sus servicios.

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 ARDATYS procederá a la revisión de los términos establecidos en el Contrato de prestación de servicios criptográficos especializados y actuará en consecuencia.

4.11. Custodia y recuperación de llaves

La llave privada asociada a un Certificado Digital de Llave Pública que haya sido generada por la ACDATYS, y sea resguardada de acuerdo a lo refrendado en el Contrato de prestación de servicios criptográficos especializados, puede recuperarse de presentarse alguna de las situaciones siguientes:

- A solicitud del titular,
- a solicitud del representante acreditado de la entidad a la que pertenece el titular,
- a solicitud de la dirección de la entidad a la que pertenece el titular,
- a solicitud de una Autoridad jurídica.

Las razones para la recuperación de la llave privada de un titular no pueden estar relacionadas con el comprometimiento de la misma. Ante tal situación se impone una revocación del certificado.

La ACDATYS resolverá la solicitud de recuperación de una llave privada en un tiempo no superior a las cuarenta y ocho (48) horas en días laborables.

El procedimiento de entrega de la llave privada recuperada será el mismo que el ejecutado para la entrega de la llave original.

4.11.1. Causas de recuperación de llave privada

Las causas admisibles para solicitar la recuperación de una llave privada asociada a un Certificado Digital de Llave Pública, que haya sido generada y resguardada por la ACDATYS se circunscriben a:

- El titular olvidó la contraseña de protección de la llave privada,
- el titular dañó el archivo contenedor de llave privada,
- el titular dañó el soporte digital de almacenamiento de la llave privada,
- la dirección de la entidad a la que pertenece o perteneció el titular requiere disponer de la llave privada,
- por Resolución judicial o administrativa que lo disponga.

4.12. Recuperación de llaves privadas en caso de catástrofes

La ACDATYS dispone de un Plan de Recuperación de llaves privadas para el caso de presentarse una catástrofe natural, tecnológica, provocada o no, donde se describen los pasos a seguir.

La ACDATYS contará con copias de seguridad de las llaves privadas generadas y conservadas por ella, de acuerdo a lo refrendado en el Contrato de prestación de servicios criptográficos especializados, en un lugar apropiado y bajo mecanismos adecuados de seguridad y protección.

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

5.1. Controles físicos

La ACDATYS valora como de trascendental importancia las medidas y controles para su seguridad y protección, razón por la cual dispone de un sistema integral de seguridad y protección a las tecnologías, medios y sistemas para su funcionamiento eficiente, eficaz y seguro.

Por considerarse partes significativas de este sistema de carácter confidencial, solo se refrendarán sus aspectos públicos.

5.1.1. Ubicación física y construcción de las instalaciones

Las instalaciones donde se encuentra ubicada la infraestructura de la ACDATYS disponen de medidas de seguridad y de control de acceso, siendo limitado a personal no autorizado. Las instalaciones se mantendrán cerradas y tendrán vigilancia electrónica y custodia profesional, las 24 horas del día y los 7 días de la semana.

Todas las operaciones críticas se llevan a cabo en recintos físicamente seguros e independientes de otros elementos de la empresa DATYS.

Así mismo, los repositorios públicos están desplegados en el Centro de Datos de DATYS, que cuenta con niveles de protección y solidez constructiva.

5.1.2. Acceso físico

Las instalaciones de la ACDATYS se mantendrán protegidas y cerradas con llave y solamente se permitirá el acceso a personal autorizado y debidamente registrado. Solo se permitirá el acceso libre a la ACDATYS a los directivos y funcionarios acreditados de esta, que cumplan con los rigores de control.

La infraestructura tecnológica de la ACDATYS estará situada en locales de acceso restringido y controlado dentro de sus instalaciones.

5.1.3. Alimentación eléctrica y aire acondicionado

Las instalaciones de la ACDATYS y la ARDATYS poseen suministro eléctrico y acondicionamiento idóneos para crear un entorno fiable de funcionamiento, adecuados a los requisitos de los equipos en ellas instalados.

Las áreas destinadas a los directivos y funcionarios, están adecuadamente equipadas para satisfacer las necesidades operativas de higiene y de seguridad.

La infraestructura está protegida contra caídas de tensión o cualquier anomalía en el suministro eléctrico.

5.1.4. Exposición al agua

Las instalaciones de la ACDATYS y la ARDATYS no corren ningún riesgo de exposición al agua.

5.1.5. Protección y prevención contra incendios

Las instalaciones de la ACDATYS y la ARDATYS poseen un sistema de prevención y extinción de incendios conforme a la legislación vigente al respecto en el país.

5.1.6. Almacenamiento de los soportes de datos

La ACDATYS ha establecido los procedimientos necesarios para disponer de copias de respaldo de toda la información de su infraestructura productiva.

La información se conserva durante un período mínimo de 15 años, en archivos protegidos con técnicas criptográficas de cifrado y control de acceso.

Los soportes de información sensible se almacenan de forma segura en cajas fuertes, de acuerdo a la clasificación y significación de la información. El acceso a estos soportes está restringido a personal autorizado.

5.1.7. Eliminación de residuos

Los soportes digitales utilizados para el almacenamiento de los archivos de datos de la ACDATYS se borran, mediante tecnologías de borrado seguro, o se destruyen antes de su eliminación.

La depuración de las copias de respaldo de la información relativa a los Certificados Digitales emitidos por la ACDATYS, se realiza en un acto con la participación de los funcionarios designados de la autoridad, y previa notificación a las entidades clientes involucradas.

La destrucción de los materiales y medios se realiza por una comisión designada por el Jefe de la ACDATYS, registrando los medios y materiales destruidos.

Los residuos normales de oficina que son o hayan sido portadores de información sensible, se eliminarán o destruirán de conformidad con lo dispuesto en el país para la información confidencial.

5.1.8. Copia de respaldo fuera de la instalación

Las instalaciones destinadas a la conservación de las copias de respaldo, disponen de medidas, controles y seguridad equivalentes a las instalaciones principales y son además independientes a estas.

5.2. Controles de procedimiento

La ACDATYS garantiza que toda la gestión, tanto la relativa a los procedimientos operacionales como a la de administración, se lleve a cabo de forma segura, conforme a lo establecido en la presente DPC, realizando auditorías periódicas.

Asimismo, se garantiza la segregación de funciones para evitar que un solo funcionario o directivo de la ACDATYS, pueda tener el control total de la infraestructura crítica productiva.

5.2.1. Roles responsables del control y gestión de la ACDATYS

La ACDATYS establece los siguientes roles:

Especialista de Producción Criptográfica: es el encargado de la emisión, suspensión, revocación, renovación y publicación de los Certificados Digitales, así como de la generación, actualización y publicación de las CRL.

Jefe de la ACDATYS: es el encargado de la elaboración y actualización de la DPC y las PC, así como de otros documentos de regulación y procedimientos de trabajo en el marco de la infraestructura de la ACDATYS. También es el encargado de la definición de los perfiles de certificado y los perfiles de entidad final. Además, es el encargado de velar por el cumplimiento del código de ética, los reglamentos internos, las regulaciones y procedimientos de trabajo establecidos y la administración de los roles. En casos excepcionales y si así se requiere, puede asumir el rol de Operario de ARDATYS.

Operador de la ARDATYS: es el encargado de tramitar, proponer aprobar o denegar las solicitudes de Certificado Digital y de registrar las entidades finales en la infraestructura de la ARDATYS.

Especialista en seguridad de la ACDATYS: es el encargado del monitoreo y control de los sistemas informáticos y criptográficos relacionados con el ciclo de vida de los Certificados Digitales, que se emplean en el marco de la infraestructura crítica de la ACDATYS, respondiendo por su seguridad, mantenimiento y actualización. En casos excepcionales y si así se requiere, puede asumir el rol de Especialista de Producción Criptográfica.

Cualquiera de los roles definidos puede además asumir la responsabilidad de custodio de llave, como portador de una secuencia de llave aleatoria, que conforma los datos de activación de la llave privada de la ACDATYS.

5.2.2. Número de personas requerido por tarea

Para poder llevar a cabo los procesos relacionados con el ciclo de vida de los Certificados Digitales deben estar cubiertos al menos con una (1) persona los siguientes roles:

- Operador de la ARDATYS,
- Especialista de Producción Criptográfica y
- Jefe de la ACDATYS.

5.2.3. Identificación y autenticación para cada rol

Los procesos de identificación, autenticación y autorización en el marco de la infraestructura de la ACDATYS se llevarán a cabo mediante el uso de Certificados Digitales de Llave Pública emitidos por la propia ACDATYS.

5.3. Controles de personal

Los directivos y funcionarios de la ACDATYS y la ARDATYS son procesados sistemáticamente, respecto a su integridad y confiabilidad, de acuerdo con las disposiciones vigentes en el país para las personas que trabajan con información clasificada.

5.3.1. Requisitos relativos a la calificación, conocimiento y experiencia

Los directivos y funcionarios de la ACDATYS y la ARDATYS deben ser profesionales, debidamente preparados, con la experiencia requerida y acreditados por la ACSCC, para el desempeño de sus funciones, las que son consideradas de críticas y sensibles, portadoras de alto y/o moderado riesgo.

Es de carácter obligatorio que sean trabajadores de la empresa DATYS y posean no menos de tres (3) años de experiencia en la actividad de seguridad de la información y/o la criptografía.

5.3.2. Requerimientos de capacitación y formación

Los directivos y funcionarios de la ACDATYS y la ARDATYS, recibirán una preparación especializada relativa a:

- Funcionamiento y objetivos del software y hardware utilizados en los sistemas tecnológicos, criptográficos, informáticos y de seguridad integral de la ACDATYS y la ARDATYS, en especial los correspondientes a su Rol específico,
- la formación legal para las tareas que deben desempeñar en su Rol,
- lo estipulado en la presente DPC y en las PC de ACDATYS,
- los conocimientos básicos de una PKI, de ciberseguridad y de los SPC,
- las normativas vigentes en Cuba en materia de seguridad de la información oficial y criptografía,
- el código de ética de la ACDATYS y la ARDATYS,
- los planes de enfrentamiento a contingencias naturales o tecnológicas,
- los procedimientos relacionados con el enfrentamiento a las contingencias.

Para ser acreditado como funcionario o directivo de la ACDATYS y la ARDATYS es un requisito necesario haber cursado y aprobado con resultados satisfactorios, el Programa de capacitación elaborado por la ACDATYS. Además, deben estar avalados y certificados por la ACSCC.

5.3.3. Frecuencia de actualización de la formación

La ACDATYS prevé la recalificación del personal cuando se produzcan cambios en las normativas en materia de seguridad de la información oficial y la criptografía; en las políticas de seguridad, de certificación digital y DPC; en los procedimientos de seguridad, criptográficos, de operación y administración y de enfrentamiento a contingencias; en la operación de los medios computacionales y/o electrónicos y aplicaciones informáticas, o cualquier otro tema que resulte relevante para la ACDATYS y que involucre los aspectos funcionales de los roles establecidos.

5.3.4. Sanciones por acciones no autorizadas

Los directivos y funcionarios de la ACDATYS y la ARDATYS están en la obligación de ejecutar solo las acciones para las que están facultados y autorizados, de acuerdo al Rol que desempeñan.

La realización de acciones no autorizadas, o presuntas acciones no autorizadas, en el marco de la infraestructura de la ACDATYS, estarán sujetas a la adopción de medidas disciplinarias, las que estarán en correspondencia con la gravedad y consecuencias de la acción.

El incumplimiento de lo establecido en la presente DPC o de las PC de la ACDATYS, ya sea por negligencia o dolo, dará lugar a la revisión y/o revocación de los privilegios, a medidas disciplinarias administrativas y/o jurídicas, o conjuntas.

5.3.5. Documentación suministrada al personal

La ACDATYS pone a disposición de sus directivos y funcionarios, toda la documentación necesaria para el correcto desempeño de sus obligaciones y responsabilidades, de acuerdo al Rol en que se desempeñan.

Entre la documentación que se pone a disposición está:

- Código de ética de la empresa DATYS,
- Código de ética de la ACDATYS y la ARDATYS,
- Las PC y la DPC de la ACDATYS,
- Los manuales de operación, administración e instalación de las herramientas informáticas y electrónicas de la ACDATYS,
- La documentación relativa a las funciones y procedimientos de cada rol,
- Los planes de medidas ante contingencias,
- Los aspectos esenciales del sistema de seguridad y protección,
- La resolución 02/2016 del MININT sobre la PKI.

5.3.6. Terminación del contrato de trabajo

Al término de la relación laboral de un funcionario o directivo de la ACDATYS o la ARDATYS, se ejecutan las siguientes acciones:

- Revocación del Certificado Digital del funcionario o directivo,
- si el funcionario o directivo cumple el rol de custodio de llave, se asigna esta responsabilidad en otro funcionario o directivo de la ACDATYS y se procede a la generación de nuevos Datos de Activación de la llave privada de la ACDATYS,
- se eliminan sus privilegios y permisos de acceso a las instalaciones de la ACDATYS,

- se eliminan los privilegios y permisos de acceso a los sistemas y componentes informáticos y criptográficos que forman parte de la infraestructura de la ACDATYS.

5.4. Procedimiento de auditoría de seguridad

La ACDATYS y la ARDATYS están sujetas a ser auditadas en cualquier momento y circunstancias que los organismos competentes lo consideren oportuno.

Se aplicarán además auditorías internas con personal propio de la ACDATYS y la ARDATYS, así como auditorías externas por entidades especializadas.

5.4.1. Tipos de eventos registrados

Todos los eventos significativos en la seguridad de las operaciones que se realizan en el marco de la ACDATYS se registrarán automáticamente, con la fecha y hora, en archivos de registro de auditoría.

Los principales eventos registrados son:

- Inicio y parada de los sistemas de la ACDATYS,
- interacciones malogradas con los sistemas criptográficos o informáticos, incluidos intentos exitosos o fracasados de conexión y operaciones de lectura y escritura,
- intentos exitosos o fracasados de crear, eliminar y cambiar contraseñas, así como de otorgar o revocar privilegios y permisos,
- intentos exitosos o fracasados de modificar, eliminar o recuperar información de los titulares, sus llaves privadas o Certificados Digitales,
- intentos exitosos o fracasados de recuperar llaves privadas de funcionarios o directivos de la ACDATYS o la ARDATYS y de titulares de certificados,

- todos los eventos relacionados con la emisión, renovación, suspensión y revocación de Certificados Digitales,
- intentos exitosos o fracasados de modificar o eliminar información asociada a los titulares de Certificados Digitales,
- intentos exitosos o fracasados de generación o eliminación de las CRL,
- modificaciones de las PC y la DPC,
- modificaciones a los procedimientos, reglamentos y metodologías de trabajo,
- registros de auditoría y control,
- informes de discrepancias y violaciones de seguridad.

5.4.2. Frecuencia de procesamiento de los registros

Los registros de auditoría serán validados con una frecuencia mensual, comprobando la integridad de los archivos de datos.

Cada proceso de validación dejará evidencia de las acciones ejecutadas, así como de los resultados y posibles alertas o irregularidades encontradas.

5.4.3. Período de conservación de los registros de auditoría

Los registros de auditoría de la ACDATYS y la ARDATYS se conservarán por un periodo no menor a quince (15) años en formato electrónico. El procedimiento a aplicar para esta conservación se corresponderá con lo establecido en la presente DPC.

Vencido el tiempo de conservación de los registros de auditoría, la ACDATYS y la ARDATYS, adoptarán a discreción, la decisión de borrado seguro.

5.4.4. Protección de los registros de auditoría

Los registros de auditoria se conservan protegidos criptográficamente.

5.4.5. Procedimiento de respaldo de los registros de auditoría

A los registros de auditoría se les realiza una copia de respaldo con frecuencia mensual y son almacenados de manera segura y confiable empleando mecanismos de protección criptográfica.

5.4.6. Sistema de recopilación de los registros de auditoría

En el sistema de recopilación de los registros de auditoría de la ACDATYS intervienen procesos automáticos referidos a las aplicaciones y sistemas informáticos que forman parte de la infraestructura, así como procesos manuales ejecutados por personal autorizado.

5.4.7. Confidencialidad de los registros de auditoría

El sistema de recopilación y control de los registros de auditoría es clasificado como confidencial. Los directivos y funcionarios responsables de la realización de un evento solo conocerán si el mismo se ejecutó o no.

5.4.8. Análisis de vulnerabilidades

La ACDATYS realiza, con frecuencia trimestral, un análisis de vulnerabilidades de las aplicaciones, sistemas informáticos y criptográficos, y los servicios que forman parte de su infraestructura; así como de los sistemas de control de acceso y monitoreo de sus instalaciones. Como resultado se elabora un informe detallado de los resultados, las deficiencias o vulnerabilidades detectadas y un plan de medidas para solucionarlas.

5.5. Archivo de registros

5.5.1. Tipo de eventos archivados

La ACDATYS y la ARDATYS conservan toda la información relevante y crítica, relativa al ciclo de vida de los Certificados Digitales, manteniendo un registro de eventos y cumpliendo con los periodos establecidos en la presente DPC.

5.5.2. Periodo de conservación de registros

Los periodos de conservación de la información relacionada con los eventos registrados se presentan en la siguiente tabla:

Información	Tiempo de conservación (años)
Registros e informes de auditoría	15
Llaves privadas de titulares de Certificados, incluidas las de la ACDATYS y la ARDATYS	25
Solicitudes y aprobaciones de Certificados	15 años posteriores al tiempo de vigencia
Identificación y autenticación de titulares y entidades	15 años posteriores al tiempo de vigencia
Suspensiones y revocaciones de certificados	15 años posteriores al tiempo de vigencia
Llaves criptográficas de los SPC	25
Registros de ataques, amenazas, debilidades e irregularidades detectadas o conocidas	15
Riesgos identificados	10
Expedientes del personal	15 años posteriores al final de su vida laboral activa
Certificados emitidos	15
Políticas, regulaciones, normativas, reglamentos, etc.	permanente

5.5.3. Sellado de tiempo de los archivos de registros

Las copias de respaldo en formato digital, de los archivos de registro y de la información relacionada con el ciclo de vida de los Certificados Digitales, llevan el sello de tiempo de la Autoridad de Sellado de tiempo de la ACDATYS.

5.5.4. Protección de los archivos de registros

Los archivos de registros son protegidos empleando mecanismos de protección criptográfica. Su borrado o destrucción estará sujeta a reglamentaciones internas de la ACDATYS.

5.5.5. Procedimiento de copia de respaldo de los archivos de registros

El procedimiento de copias de respaldo de los archivos de registro está sujeto a reglamentaciones internas de la ACDATYS.

5.6. Cambio de llave de la ACDATYS

Al hacerse efectivo el cambio de la llave privada de la ACDATYS y su correspondiente Certificado Digital, este será publicado de manera inmediata en el sitio web oficial de la ACDATYS y se notificará además el cambio en el propio sitio.

La ACDATYS continuará emitiendo CRL firmadas con su llave privada previa, hasta que expire el periodo de validez del último Certificado Digital emitido y firmado por esa llave.

5.7. Recuperación en caso de compromiso de llave o catástrofe

5.7.1. Procedimientos para la gestión de incidentes y comprometimiento

La ACDATYS cuenta con un Plan de Contingencias, donde se especifican los riesgos, recursos y acciones a realizar, ante la ocurrencia de un evento o catástrofe, accidental o intencional, que afecte o inhabilite el correcto funcionamiento de alguno o de todos los sistemas o componentes informáticos y criptográficos que conforman su infraestructura productiva crítica, para garantizar la continuidad de la prestación de sus servicios esenciales.

El Plan de Contingencia contempla, entre otros aspectos:

- La redundancia de los componentes y sistemas críticos,
- la puesta en marcha inmediata de un sistema de respaldo,
- el chequeo completo y periódico de los servicios de copias de respaldo.

En el caso del comprometimiento de la llave privada de la ACDATYS, se comunicará a los titulares y terceras partes que confían, que los Certificados Digitales y las CRL emitidos y firmados con la llave privada comprometida dejan de ser válidos. Así mismo, se publicará una notificación en el sitio web oficial de la ACDATYS.

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

En caso de existir alguna sospecha de que los recursos de hardware, software o los datos, han sido alterados o modificados, la ACDATYS detendrá sus operaciones, hasta tanto se restablezcan los parámetros de seguridad de la infraestructura.

De forma simultánea se realizará una auditoría para identificar las causas y condiciones que dieron lugar a la alteración o modificación de los componentes en cuestión, con el objetivo de evitar una futura reproducción.

5.7.3. Comprometimiento de la llave privada de la ACDATYS

Ante el comprometimiento o sospecha de comprometimiento de la llave privada de la ACDATYS, se sigue el siguiente procedimiento:

- se revoca de manera inmediata el Certificado Digital de la ACDATYS,
- se genera y publica la correspondiente CRL,
- se comunica a los titulares, representantes acreditados y terceras partes que confían que los Certificados Digitales y las CRL emitidos y firmados con la llave privada comprometida dejan de ser válidos,
- cesan las operaciones de la ACDATYS,
- se solicita a la ACSCC un nuevo par de llaves para la ACDATYS.

La ACDATYS mantendrá en los repositorios su Certificado Digital revocado, garantizando así la verificación, por parte de titulares y terceras partes que confían, de los Certificados y las CRL emitidas durante el período de validez de la llave privada comprometida.

5.7.4. Continuidad de funcionamiento de la ACDATYS tras un desastre natural u otra catástrofe

En caso de producirse un desastre natural u otra catástrofe que limite o afecte la disponibilidad de los servicios de la ACDATYS, se activa el Plan de Recuperación de Desastres, garantizando la disponibilidad y operatividad de los servicios esenciales en el menor tiempo posible.

El tiempo de recuperación operativa de la ACDATYS dependerá de la severidad de las afectaciones sufridas en las instalaciones y en la infraestructura productiva crítica.

5.8. Cese de operaciones de la ACDATYS

La ACDATYS cesará sus operaciones por las siguientes causas:

- comprometimiento de su llave privada,
- por Ley o Resolución de autoridad competente que así lo determine,
- por dudas o sospechas demostradas de la integridad operacional de la infraestructura productiva crítica.

Cualquiera sea la causa, la ACDATYS comunicará a la ACSCC sobre el cese de sus operaciones y esta supervisará todo el proceso.

Ante el cese operacional definitivo de la ACDATYS se ejecutarán las siguientes acciones:

- Informar a todos los titulares y representantes acreditados que los Certificados Digitales emitidos por la ACDATYS serán revocados,
- destruir las llaves privadas generadas y resguardadas por la ACDATYS,
- destruir la llave privada de la ACDATYS.

La comunicación a los titulares y representantes acreditados, deberá ejecutarse, siempre que sea posible, con al menos dos (2) meses de antelación al cese definitivo de la ACDATYS.

Transcurridos los dos (2) meses, la ACDATYS procederá a la revocación de los Certificados Digitales y a la destrucción de las llaves privadas.

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

El par de llaves y el Certificado Digital de Llave Pública de la ACDATYS son generados por la ACSCC, y este último también es firmado por la ACSCC.

El par de llaves de un titular es generado de acuerdo a lo establecido en las PC de la ACDATYS y previo Contrato de prestación de servicios criptográficos especializados firmado por ambas partes.

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 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 el par de llaves criptográficas, pública y privada, sea generado por la ACDATYS, la llave privada será entregada al titular como se establece en las PC.

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

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

El Certificado Digital de Llave pública de la ACDATYS está disponible para su descarga desde su sitio web oficial.

6.1.4. Tamaños de llaves

Las llaves criptográficas de la ACDATYS son RSA de 4096 bits de longitud.

Las longitudes de las llaves generadas por la ACDATYS para los titulares de Certificados Digitales de Llave Pública varían de acuerdo al uso del certificado. Ver 6.1.5.

6.1.5. Generación de parámetros de llave pública/privada

Los Certificados Digitales emitidos por la ACDATYS cumplen el estándar X.509 v3.

Parámetros de generación de llaves criptográficas por la ACDATYS			
Esquema criptográfico		RSA longitud en bits	ECDSA longitud en bits
Tipo de Certificado Digital	Certificado ACDATYS	4096	
	Firma digital	2048	256
	Sello electrónico	2048	256
	Firma digital de Código	2048	256
	OCSP Signer	4096	384
	Sellado de tiempo	4096	384
	Autenticación Cliente	2048	256
	Servidor SSL/TLS	4096	384

6.1.6. Usos admitidos de llave (campo KeyUsage de X.509 v3)

Los Certificados Digitales emitidos por la ACDATYS contienen la extensión *KeyUsage* definida por el estándar X.509 v3, la que se califica como crítica. Asimismo, pueden establecerse usos y limitaciones adicionales mediante la extensión *ExtendedKeyUsage*.

Es importante tener en cuenta que la eficacia de las limitaciones basadas en las extensiones que se incluyen en los Certificados depende, en ocasiones, de la operatividad de las aplicaciones informáticas que hacen uso de los Certificados Digitales y que estas no son desarrolladas ni controladas por la ACDATYS.

6.2. Protección de la llave privada

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

6.2.1. Normas para los módulos criptográficos

El módulo criptográfico utilizado en la infraestructura de la ACDATYS se encuentra físico y lógicamente aislado dentro del sistema y en él se realiza y garantiza:

- La generación de las llaves criptográficas,
- la generación aleatoria de los datos de activación de las llaves privadas,
- el cifrado de las llaves privadas y su almacenamiento en formato PKCS#12,
- la generación y firma de los Certificados Digitales de Llave Pública,
- la revocación de los Certificados,
- la generación y firma de las CRL.

El módulo criptográfico de la ACDATYS cumple los requisitos operacionales, eficacia, eficiencia y de seguridad establecidos por la DC del Minint.

6.2.2. Control multipersona de la llave privada de la ACDATYS

La llave privada de la ACDATYS se encuentra bajo control multipersona.

Tanto para acceder a la copia de seguridad de la llave privada como a sus Datos de Activación se requiere la participación de tres (3) custodios de llave, cada uno en posesión exclusiva de una sucesión de llave aleatoria.

6.2.3. Custodia de la llave privada

La ACDATYS asume el almacenamiento y custodia de su llave privada, así como de su copia de respaldo o seguridad.

Además, la ACDATYS asume, el almacenamiento y custodia de las llaves privadas de titulares que hayan sido generadas por la ACDATYS, de acuerdo a lo refrendado en el Contrato de prestación de servicios criptográficos especializados.

El titular que asume la generación de su par de llaves criptográficas, pública y privada, es el único responsable del resguardo y custodia de su llave privada.

6.2.4. Copia de seguridad de la llave privada de la ACDATYS

Al recibir su par de llaves, generado por la ACSCC, la ACDATYS crea una copia de respaldo y la almacena protegida criptográficamente en un dispositivo digital de almacenamiento específico. Este dispositivo, a su vez es almacenado en una caja fuerte con control de acceso multipersona.

6.2.5. Acceso a la copia de seguridad de la llave privada de la ACDATYS

La solicitud de acceso a la copia de seguridad de la llave privada de la ACDATYS y sus datos de activación, solo procede en caso de hacerlo el Jefe de la ACDATYS y en presencia de dos (2) operadores o directivos de la ACDATYS que se desempeñen como custodios de llave.

6.2.6. Almacenamiento de la llave privada de la ACDATYS en el módulo criptográfico

La llave privada de la ACDATYS se integra al módulo criptográfico en el momento de puesta en funcionamiento inicial de la Autoridad de Certificación que la empleará para la firma de los Certificados Digitales y de las CRL.

La llave privada de la ACDATYS se almacena cifrada en el módulo criptográfico y solamente se descifra en el momento preciso de su uso.

6.2.7. Método de activación de la llave privada de la ACDATYS

La llave privada de la ACDATYS se activa en el momento de inicialización del software de la ACDATYS por medio de la combinación de dos (2) operadores de la ACDATYS. Éste es el único método de activación de dicha llave privada.

6.2.8. Método de desactivación de la llave privada de la ACDATYS

La desactivación de la llave privada de la ACDATYS se produce inmediatamente y de manera automática, cuando concluyen los procesos que hacen uso de la misma.

6.2.9. Método de destrucción de la llave privada de la ACDATYS

La eliminación permanente de la llave privada de la ACDATYS del módulo criptográfico se realiza mediante borrado seguro.

Para la destrucción de la copia de respaldo de la llave privada de la ACDATYS, el Jefe de la ACDATYS designa una comisión, que realizará el borrado seguro del medio de almacenamiento donde se encuentra la copia y posteriormente lo destruirá físicamente.

Así mismo, el Jefe de la ACDATYS designa una comisión que procederá a la incineración de los Sobre-PIN donde se encuentra los datos de activación de la llave privada.

Ambas comisiones harán constar en acta las acciones realizadas.

6.2.10. Clasificación de los módulos criptográficos

El módulo criptográfico empleado por la ACDATYS para la generación del par de llaves pública/privada cumple con los requerimientos establecidos por la DC del MININT.

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 quince (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

El Certificado Digital de la ACDATYS tiene una validez de diez (10) años.

Los períodos de validez de los Certificados Digitales emitidos por la ACDATYS se establecen en las PC.

6.4. Datos de activación

6.4.1. Generación de los datos de activación

Una vez entregada por la ACSCC a la ACDATYS su llave privada, se procede al cambio de los datos de activación iniciales (contraseña de protección) por nuevos datos. Este proceso requiere y exige la participación de al menos tres (3) funcionarios o directivos de la ACDATYS que asumirán el rol de custodios de llave.

El procedimiento es el siguiente:

- De manera independiente cada custodio de llave genera una sucesión llave de manera aleatoria que se resguarda en un Sobre-PIN, y estos a su vez son resguardados en caja fuerte,
- la combinación de las sucesiones llaves aleatorias generadas se constituye como los nuevos datos de activación de la llave privada de la ACDATYS,
- se hace efectivo el cambio de los datos de activación.

El procedimiento de activación de las llaves privadas de los titulares de Certificados Digitales emitidos por la ACDATYS se establece en las PC.

6.4.2. Protección de los datos de activación

Los Sobre-PIN que contienen las sucesiones llaves aleatorias, cuya combinación determina los datos de activación de la llave privada de la ACDATYS son resguardados en caja fuerte.

Es responsabilidad de los funcionarios de la ACDATYS que actúan como custodios de la llave privada, la seguridad y protección de sus respectivas sucesiones llaves aleatorias.

6.5. Controles de seguridad informática

La ACDATYS tiene aprobado su reglamento de seguridad informática que es de estricto cumplimiento para todos sus funcionarios y directivos.

Todos los equipos con SO Windows de la infraestructura de la ACDATYS, poseen protección contra virus y malware, que se actualiza diariamente. Además, existen controles de accesos físicos y lógicos a los mismos.

Todos los dispositivos de almacenamiento extraíble que se utilizan como parte del procedimiento de registro y copias de respaldo, son sometidos a control antivirus, de manera automática, antes de su uso.

6.5.1. Requisitos técnicos específicos de seguridad informática

El sistema de la ACDATYS dispondrá, a través del sistema operativo y de una combinación de los controles del sistema operativo, físicos y del software de la ACDATYS, de un protocolo de seguridad de acceso, basado en el uso de Certificados Digitales de Llave Pública, que regula y verifica:

- El control y validación del acceso a los servicios de la ACDATYS y la ARDATYS y a los roles de directivos y funcionarios,
- la identificación y autenticación de los roles autorizados y otras restricciones,
- la auditoría de los eventos relacionados con la seguridad de los procesos críticos,
- la protección criptográfica de la sesión de comunicación,
- el uso del archivo histórico de datos de registros de auditoría de la ACDATYS y la ARDATYS,
- los mecanismos de recuperación de llaves y del sistema de la ACDATYS,
- la independencia de las facultades y obligaciones de cada rol identificado para la PKI.

6.6. Controles de seguridad del ciclo de vida

Para garantizar y controlar la seguridad de los procesos clave que conforman el ciclo de vida de los Certificados Digitales emitidos por la ACDATYS, se establecen mecanismos y normas de control dirigidos a:

- Supervisar sistemática y permanentemente la configuración e integridad de los sistemas y procesos de la ACDATYS,
- supervisar que las tecnologías, medios y sistemas de la ACDATYS, no se usan para cuestiones ajenas al ciclo de vida de los Certificados Digitales de Llave Pública,
- supervisar que en la infraestructura de la ACDATYS, no se encuentran instalados aplicaciones ni componentes de software, que no sean utilizados como parte del ciclo de vida de los Certificados Digitales,
- asegurar que las actualizaciones de las tecnologías, medios y sistemas de la ACDATYS, son instaladas por funcionarios facultados y autorizados

En cualquier circunstancia se dejará evidencia oficial de estas acciones.

6.6.1. Controles de desarrollo de sistemas

En la ACDATYS se utilizan procedimientos específicos de control para cambios de nuevas versiones y actualizaciones de sus componentes.

Todo el hardware y software que se emplea en el marco de la infraestructura productiva crítica de la ACDATYS, así como sus configuraciones y principales flujos de trabajo, fueron sometidos a pruebas intensivas en un polígono.

6.6.2. Controles de gestión de seguridad

La gestión de la seguridad en el marco de la infraestructura de la ACDATYS responde a regulaciones y procedimientos internos, que son considerados como información confidencial.

6.7. Controles de seguridad de la red

La infraestructura de la ACDATYS que comprende la generación de las llaves criptográficas y los Certificados Digitales, así como de las CRL, está en una red privada.

El sitio web oficial de la ACDATYS, así como los servicios OCSP y de Sellado de tiempo se encuentran desplegados en el Centro de Datos de DATYS, por lo que heredan los mecanismos de seguridad y de control de acceso establecidos en dicho centro.

Otros datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos.

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.

Los Certificados Digitales de Llave Pública emitidos por la ACDATYS son x.509 versión 3 e incluyen los siguientes campos:

Campo	Valor
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 mínima de la llave es de 2048 bits para el algoritmo RSA y de 256 bits para algoritmos de Curvas elípticas

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

Los Certificados Digitales de Llave Pública emitidos por la ACDATYS tendrán las siguientes extensiones:

Campo	Descripción	Crítico
KeyUsage	Especifica los usos permitidos de la llave	Si
ExtendedKeyUsage	Especifica otros usos de la llave	No
CRLDistributionsPoints	Especifica la URL de descarga de la CRL base	No
Freshest CRL	Especifica la URL de descarga de la CRL tipo delta	No
AuthorityKeyIdentifier	Identificador de la llave pública de la ACDATYS	No
AuthorityInformationAccess	Especifica la URL del servicio OCSP	No

Las PC de la ACDATYS pueden establecer variaciones en las extensiones utilizadas de acuerdo al tipo y uso del Certificado Digital.

7.1.3. Identificadores de objetos (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

- SHA-512-with-RSAEncryption (1.2.840.113549.1.1.13)
- ECDSA-with-SHA-512 (1.2.840.10045.4.3.4)

7.1.4. Formato de nombres

Fue definido en la sección 3.1 de la presente DPC.

7.2. Perfil de CRL

Las CRL emitidas por la ACDATYS cumplen con la RFC 5280 y contienen los siguientes elementos básicos:

Campo	Valor
Versión	V2
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
Fecha efectiva	Especifica la fecha de emisión de la CRL
Próxima actualización	Especifica la fecha en que será publicada la próxima CRL. La frecuencia de emisión es la establecida en el numeral de la presente DPC
Algoritmo de firma	SHA512WithRSAEncryption
Algoritmo HASH de firma	SHA512
Certificados revocados	CRL, incluyendo el número de serie, la fecha de revocación y las causas

7.2.1. Número de versión

La ACDATYS emite las CRL en formato x.509 versión 2.

7.2.2. CRL y extensiones

Las extensiones empleadas en las CRL son:

Campo	Descripción
CRLNumber	Especifica el número de la CRL
CRLDistributionsPoints	Especifica la URL de descarga de la CRL base
Freshest CRL	Especifica la URL de descarga de la CRL delta
AuthorityKeyIdentifier	Identificador de la llave pública asociada a la llave privada de la ACDATYS, como Autoridad que emite las CRL

7.3. Perfil de OCSP

Los Certificados Digitales del OCSP Responder son emitidos por la ACDATYS y conforme a las siguientes normas:

- RFC 6960: X.509 Internet Public Key Infraestructure Online Certificate Status Protocol – OCSP
- RFC 6066: Transport Layer Security Extensions: Extension Definitions

El periodo de validez de los mismos será de dos (2) años.

La ACDATYS incluirá en el Certificado Digital del OCSP responder la extensión “id-pkix-ocsp-nocheck”. De esta forma, la ACDATYS especifica que los clientes OCSP pueden confiar en el OCSP Responder mientras su Certificado Digital sea válido.

7.3.1. Número de versión

Los certificados de OCSP Responder se basan en el estándar X.509 versión 3 (X.509 v3). El perfil es el definido en la RFC 6960.

7.3.2. Campos y extensiones del Certificado Digital de firma del OCSP

El Perfil del Certificado Digital de firma digital del OCSP es:

Campo	Valor
Versión	X509 v3
Algoritmo de firma	SHA512WithRSAEncryption
DN 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
Validez	1 año
DN Sujeto	CN = OCSP ACDATYS OU = ACDATYS O = DATYS L = Playa ST = La Habana C = CU
Información de llave del sujeto	RSA 4096
Identificador de llave del Sujeto	Derivada de aplicar la función resumen SHA1 a la llave pública del Sujeto
Identificador de llave de la Autoridad	Derivada de aplicar la función resumen SHA1 a la llave pública de la ACDATYS
Usos de la llave	Firma Digital
Usos extendidos de la llave	OCSP Signer

7.3.3. Formato de las peticiones y respuestas OCSP

El OCSP Responder de la ACDATYS admite respuestas del tipo id-pkix-ocsp-basic.

Además, admite el empleo de un valor “nonce” tanto para las peticiones como para las respuestas, para prevenir ataques del tipo “replay attacks”. El OID es id-pkix-ocsp-nonce.

Las posibles respuestas del servicio OCSP sobre el estado de Certificado Digital son:

- “Revoked”: cuando el Certificado Digital está revocado,
- “Good”: cuando el Certificado Digital no está revocado.
- “unknown”: si la petición se corresponde con una Autoridad de Certificación desconocida.

8. Auditorías de cumplimiento y otros controles

8.1. Frecuencia de las auditorías o controles

La ACDATYS efectuará anualmente una auditoría interna de desempeño integral sobre su funcionamiento. Así mismo podrá efectuar auditorías o controles parciales cuando lo considere pertinente.

El director general de la Empresa DATYS puede disponer una auditoría de desempeño a la ACDATYS o la ARDATYS y que esta se realice por una comisión de auditoría externa, en cualquier momento que lo considere pertinente.

El director general de la empresa DATYS se reserva el derecho de exigir inspecciones de las instalaciones, procedimientos, sistema de seguridad y de control y acceso a la ACDATYS o la ARDATYS, para validar que se encuentran funcionando de acuerdo con las prácticas y procedimientos de seguridad establecidos en la presente DPC.

Las especialidades autorizadas del Minint se reservan el derecho de realizar controles u auditorías a la ACDATYS cuando lo consideren necesario.

8.2. Autorización, identificación y calificación del auditor

El director general de la empresa DATYS dará su aprobación a las comisiones de auditoría externa, teniendo en cuenta su demostrada experiencia con las tecnologías PKI y criptográficas, con el funcionamiento del software PKI correspondiente y su conocimiento con las políticas, normativas, reglamentaciones y documentos legales de la ACDATYS.

8.3. Relación entre el auditor y la Autoridad auditada

Los auditores integrantes de la comisión de auditoría externa aprobada no podrán tener relación alguna con la ACDATYS, evitando así cualquier conflicto de intereses.

Los auditores internos no podrán tener relación funcional con el área objeto de la auditoría.

8.4. Aspectos cubiertos por los controles

La auditoría de desempeño abordará la aplicación por parte de la ACDATYS y la ARDATYS asociada, de las prácticas técnicas, de procedimientos, de seguridad y de personal, descritas en la presente DPC.

Las principales áreas en las que se debe centrar una auditoría son las siguientes:

- Mecanismos de identificación y autenticación en la tramitación de solicitudes,
- políticas de seguridad,
- administración de los servicios,
- controles de seguridad física,
- controles de procedimientos,
- controles de seguridad técnica, criptográfica e informática,
- evaluación tecnológica,
- selección y acreditación del personal,
- contratos y servicios especializados.

8.5. Acciones a emprender derivadas de la auditoría

Al término de la auditoría y una vez analizado de manera conjunta con la dirección de la ACDATYS sus resultados, se elaborará e implementará un Plan de Medidas, para dar solución a las deficiencias e insuficiencias señaladas por la comisión auditora.

La ACDATYS deberá informar periódicamente, al director general de la empresa DATYS, sobre el estado de implementación de las acciones derivadas del Plan de Medidas.

El director general de la empresa DATYS determinará cuándo deba realizarse una nueva evaluación.

8.6. Comunicación de los resultados de una auditoría

Una síntesis de los resultados de toda auditoría interna o externa realizada a la ACDATYS se informa a la ACSCC. De requerirse por la ACSCC, se le hará entrega íntegra del documento informe final de la auditoría, previa autorización por el Director general de la Empresa DATYS.

El director general de la empresa DATYS, la ACSCC y el Jefe de la ACDATYS, evaluarán y precisarán que aspectos de la auditoría requieren ser informados a las entidades y titulares de Certificados Digitales.

Ante cualquier circunstancia, la ACSCC y la ACDATYS, se asegurarán de que todas las entidades y titulares de Certificados Digitales emitidos por la ACDATYS reciban de forma fiable la información correspondiente.

9. Cuestiones legales y comerciales

9.1. Tarifas

9.1.1. Tarifas de emisión de Certificado o renovación

Las tarifas de emisión y renovación de un Certificado Digital se encuentran publicadas en https://ac.datys.cu/politicas.

9.1.2. Tarifas de acceso a los Certificados

El acceso a los Certificados Digitales emitidos por la ACDATYS es libre y gratuito, dada su naturaleza pública, y por tanto no se le aplica ninguna tarifa.

9.1.3. Tarifas de acceso a la información de estado o revocación

El acceso a la información de estado o revocación de los Certificados Digitales emitidos por la ACDATYS, ya sea a través de las CRL o del servicio OCSP, es libre y gratuito y por tanto no se le aplica ninguna tarifa.

9.1.4. Tarifas de otros servicios como información de políticas

No se aplica tarifa alguna por el servicio de información y publicación de la presente DPC y las PC de la ACDATYS. Su acceso es libre y gratuito desde el sitio web oficial de la ACDATYS.

9.2. Política de Confidencialidad

9.2.1. Información confidencial

Toda la información que la ACSCC y la ACDATYS no consideren de dominio público se mantendrá clasificada como restringida, y por tanto, le será aplicada medidas seguras para su conservación y control de acceso.

Se declara expresamente como información confidencial:

- La llave privada de la ACDATYS,
- las llaves privadas de titulares que la ACDATYS haya generado y mantiene en custodia,
- la información relativa a las operaciones que realizan la ARDATYS y la ACDATYS,
- la información referida a los parámetros de seguridad, control y procedimientos de auditoría,
- la información de carácter personal proporcionada por los titulares de certificados a la ARDATYS durante el proceso de registro, de conformidad con lo dispuesto en la normativa sobre protección de datos de carácter personal.

Esta información no será divulgada ni compartida fuera del marco de la infraestructura de la ACDATYS, a menos que así lo exija la Ley o un documento legal.

9.2.2. Información no confidencial

Se considera información pública y por lo tanto accesible por terceros:

- La contenida en la presente DPC,
- la incluida en las PC de la ACDATYS,
- los certificados emitidos por la ACDATYS,
- las listas de certificados suspendidos o revocados.

9.2.3. Deber de secreto profesional

Los funcionarios y directivos de la ACDATYS y la ARDATYS están obligados al deber de secreto profesional y por lo tanto están sujetos a las normativas

reguladoras establecidas en los respectivos Reglamentos Internos y en el Código de Ética.

9.3. Protección de la información de carácter personal

La ACDATYS no almacena datos de carácter privado de los titulares, más allá de los solicitados durante los procesos de registro y solicitud.

9.3.1. Política de protección de datos de carácter personal

La ACDATYS ni la ARDATYS divulgan ni comparten datos personales de los titulares, excepto en los casos previstos por concepto de auditorías.

9.3.2. Información considerada como privada

Se considera información privada de un suscriptor a la información personal, solicitada durante el proceso de registro y que no es incluida en los Certificados Digitales.

Se declara expresamente como información privada:

- Las solicitudes de certificados, aprobadas o denegadas, así como toda la información personal solicitada como parte del proceso de registro,
- las llaves privadas generadas y almacenadas por la ACDATYS,

9.3.3. Información considerada como no privada

Se considera información no privada a la información personal que se incluye en los Certificados Digitales y en las CRL.

Se declara expresamente como información no privada:

- Los Certificados Digitales emitidos,
- los nombres y apellidos del titular de un Certificado Digital emitido por la ACDATYS,
- la dirección de correo electrónico del titular,

- los usos y límites económicos reseñados en el Certificado Digital,
- el periodo de validez del Certificado Digital,
- la fecha de emisión del Certificado Digital,
- la fecha de caducidad del Certificado Digital,
- el número de serie del Certificado Digital,
- los diferentes estados o situaciones del Certificado Digital y la fecha del inicio de cada uno de ellos,
- las CRL, así como el resto de informaciones de estado de revocación,
- la información publicada en el sitio oficial de la ACDATYS.

La aceptación por el titular de la emisión del Certificado Digital emitido a su nombre equivale al consentimiento dado para su publicación.

9.3.4. Responsabilidad de la protección de los datos de carácter personal

La ACDATYS garantiza el cumplimiento de sus obligaciones legales en lo referido a la protección de los datos personales de los titulares y entidades.

9.3.5. Comunicación y consentimiento para usar datos de carácter personal

El consentimiento quedará refrendado con la firma del Contrato de prestación de servicios criptográficos especializados por parte del usuario.

9.3.6. Revelación de la información personal a autoridades jurídicas

La ACDATYS solo podrá compartir información considerada confidencial o datos de carácter personal, con terceros, cuando sea requerido por una Autoridad pública competente y bajo supuestos previstos legalmente.

La ACDATYS estará obligada a revelar la identidad de los titulares o sus datos de carácter personal, en caso que sean solicitados por los órganos judiciales en el ejercicio de sus funciones y que así lo requieran.

9.4. Derechos de propiedad intelectual

Todos los derechos de propiedad intelectual relacionados con el ciclo de vida de los Certificados Digitales y las CRL emitidas por la ACDATYS, sus PC y la presente DPC son propiedad exclusiva de la ACDATYS.

De acuerdo a estos derechos, no está autorizada la reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos citados anteriormente sin la autorización expresa de la ACDATYS.

9.5. Obligaciones

9.5.1. Obligaciones de la ACDATYS

La ACDATYS para cumplir con sus funciones, dispuestas en las PC y la presente DPC, contrae las siguientes obligaciones:

- Operar de acuerdo a lo establecido en la Resolución 02/2016 del Ministerio del Interior,
- emitir, mantener actualizadas y hacer públicas sus PC y su DPC,
- prestar los servicios de certificación de conformidad con la presente DPC,
- proteger la llave privada de la ACDATYS,
- tramitar las solicitudes de emisión, renovación, revocación y suspensión de Certificados Digitales, así como las solicitudes de recuperación de llave privada, en los casos que el par de llaves criptográficas haya sido generado por la ACDATYS,

- emitir los Certificados Digitales de conformidad con lo establecido en las PC,
- proceder a la suspensión de los Certificados Digitales al término de su periodo de validez,
- proveer mecanismos de comprobación del estado de un Certificado Digital,
- proteger, no divulgar ni compartir, los datos privados de titulares y entidades,
- registrar los eventos relacionados con el ciclo de vida de los Certificados Digitales,
- colaborar con las comisiones de auditoría internas y externas,
- comunicar el cese de la ACDATYS conforme a lo establecido en esta DPC.

9.5.2. Garantías de la ACDATYS a titulares y terceras partes que confían

La ACDATYS al constituirse como una autoridad segura y confiable para la emisión, renovación y revocación de Certificados Digitales de Llave Pública garantiza:

- Brindar a los titulares un adecuado conocimiento y preparación, para que puedan conocer, dominar y hacer un uso correcto de sus Certificados Digitales de Llave Pública, así como asumir sus responsabilidades,
- un ambiente confiable y seguro de operación durante todo el ciclo de vida de los Certificados Digitales,
- prestar servicios de certificación de manera profesional y responsable, en correspondencia con las PC y la presente DPC,
- la transparencia de información en todos los procedimientos aplicables,

- la aplicación de rigurosas y adecuadas medidas, para comprobar la veracidad y autenticidad de la acreditación de los solicitantes,
- una relación contractual con los solicitantes (persona natural o jurídica),
- hacer un uso correcto del material criptográfico entregado por la ACSCC o desarrollado por la ACDATYS.
- disponer de una página web oficial y mantener actualizados todos los documentos y procedimientos públicos de interés de las entidades y titulares de Certificados Digitales de Llave Pública, así como las CRL y el servicio OCSP,
- comunicar de manera oficial y oportuna, a entidades y titulares, la extinción o suspensión de la vigencia de su Certificado Digital de Llave Pública, brindándole la información requerida,
- asumir las pertinentes responsabilidades y obligaciones frente a las entidades y los titulares en cuanto a la calidad del servicio que presta,
- la recepción y tramitación de los cuestionamientos, quejas y reclamaciones de las entidades y titulares, así como el otorgamiento de respuestas oportunas y profesionales,
- disponer de un personal altamente preparado en materias relacionadas con los servicios de certificación prestados, de experiencia, y certificados por la ACSCC.

9.5.3. Obligaciones de la ARDATYS

La ARDATYS para cumplir con sus funciones, dispuestas en las PC y la presente DPC, contrae las siguientes obligaciones:

- Operar de acuerdo a lo establecido en la Resolución 02/2016 del Ministro del Interior,
- realizar sus funciones y gestiones de acuerdo con lo establecido en la presente DPC,
- garantizar un ambiente de control interno confiable y seguro,
- comprobar y certificar la veracidad y validez de la información que se presenta en la solicitud por la entidad, el representante acreditado o el titular de un Certificado Digital de Llave Pública, de acuerdo con lo expuesto en la presente DPC,
- mantener actualizada la documentación inherente a los servicios que brinda en los repositorios públicos de su responsabilidad,
- responder ante los titulares de Certificados Digitales de Llave Pública por las operaciones realizadas en nombre de la ACDATYS,
- comunicar oficial y oportunamente a todo el que corresponda el cese de las funciones de la ARDATYS, conforme a lo establecido en esta DPC, a fin de determinar el destino que se dará a sus registros y archivos y cancelar temporalmente la recepción de nuevas solicitudes,
- notificar a la entidad, representante o al titular cuando se haya aprobado la solicitud y si este debe hacer algún trámite adicional,

- almacenar de forma protegida y por un periodo razonable la documentación relacionada con los procesos de emisión, suspensión y revocación de un Certificado Digital,

- solicitar a la ACDATYS la revocación de un Certificado Digital cuando tenga conocimiento o sospecha demostrada del comprometimiento de la llave privada asociada,

- a partir de la recepción de la solicitud de un Certificado Digital de Llave Pública, la ARDATYS tiene un período de quince (15) días para la ejecución de todo el proceso de identificación y autenticación de los datos identificativos de la entidad, representante o titular, y para aprobar o denegar la solicitud. Una vez validados los datos y aprobada la solicitud, la ARDATYS registra los datos del solicitante en el sistema, y crea y publica, vía FTP, la Orden de trabajo de emisión a la ACDATYS. La ACDATYS emitirá el Certificado Digital en un tiempo no superior a las cuarenta y ocho (48) horas, desde la recepción de la Orden de trabajo de la ARDATYS, hasta la publicación del Certificado Digital en el repositorio público de la ACDATYS.

9.5.4. Obligaciones de los titulares

Es obligación de los titulares de Certificados Digitales emitidos por la ACDATYS:

- Aceptar las condiciones, normas y regulaciones de uso, funcionamiento y seguridad de los Certificados Digitales, en particular las establecidas en las PC y en la presente DPC,

- proveer información exacta, completa y veraz con relación a los datos requeridos en los procesos de solicitud,

- informar a la ARDATYS de cualquier cambio en las informaciones contenidas en su Certificado Digital o en los datos de origen de la solicitud de este, requiriendo su renovación si corresponde,
- solicitar de inmediato la revocación o suspensión de su Certificado Digital, ante sospecha o conocimiento del comprometimiento de su llave privada,
- no transferir ni delegar a terceros sus responsabilidades sobre un Certificado Digital que le haya sido emitido,
- dejar de utilizar su llave privada, transcurrida el tiempo de validez del Certificado Digital asociado.

9.6. Responsabilidades

9.6.1. Responsabilidad de la ACDATYS

La ACDATYS solo responderá en caso de incumplimiento de las obligaciones establecidas en la Resolución 02/2016 del Ministro del Interior, en la presente DPC y en las PC.

La ACDATYS no representa en forma alguna a los titulares de Certificados Digitales emitidos por ella, ni a las terceras partes que confían en los Certificados Digitales.

9.6.2. Exención y limitaciones de responsabilidad de la ACDATYS

La ACDATYS no asume ninguna responsabilidad ante la ocurrencia de las siguientes situaciones:

- Por la no ejecución, ejecución defectuosa o negligencia demostrada, de las obligaciones a cargo de las entidades, representantes y titulares de

Certificados Digitales de Llave Pública, que ocasionen daños a sí mismos o a terceros,

- por el uso no autorizado, indebido o fraudulento de los Certificados Digitales de Llave Pública y las llaves criptográficas, por entidades, representantes o titulares, que ocasione un daño directo o indirecto, a sí mismos o a terceros,
- por posibles errores existentes en el Certificado Digital, derivados de la información facilitada por la entidad, representante o el titular, y que no sean consecuencia de errores operacionales o funcionales de la ARDATYS o la ACDATYS,
- por la no ejecución o retraso en la ejecución de las obligaciones establecidas en esta DPC, si esto fuera consecuencia de un supuesto de fuerza mayor, desastre natural o tecnológico; o de manera general, por cualquier situación sobre la que la ACDATYS no pueda tener un control razonable,
- por el contenido de documentos o archivos firmados digitalmente por titulares de Certificados Digitales de Llave Pública emitidos por la ACDATYS,
- por el contenido de sitios web protegidos por un Certificado Digital de Llave Pública emitido por la ACDATYS,
- por hechos ocurridos entre la solicitud de un Certificado Digital de Llave Pública y su emisión, publicación y entrega al titular,
- por hechos ocurridos entre el momento de revocación de un Certificado Digital de Llave Pública y la siguiente publicación de la correspondiente CRL,
- por la difusión no autorizada de información personal de un titular que esté incluida en su Certificado Digital de Llave Pública o en la CRL de la ACDATYS,

- por litigios entre titulares y terceras partes que confían, relativos con la reparación, daños y perjuicios u otras reclamaciones u obligaciones de cualquier tipo, penales o contractuales, relacionados con el uso o confianza de un Certificado Digital de Llave Pública emitido por la ACDATYS.

9.6.3. Responsabilidades de los titulares

Es responsabilidad de los titulares de Certificados Digitales emitidos por la ACDATYS:

- Conocer las condiciones, normas y regulaciones de uso, funcionamiento y seguridad de los Certificados Digitales, en particular las establecidas en las PC y en la presente DPC,
- garantizar la protección y resguardo de su archivo contenedor de llave privada, evitando su pérdida o uso no autorizado,
- no compartir con terceros la contraseña de protección de su llave privada, evitando su divulgación o modificación,
- asumir los riesgos derivados de la fiabilidad y seguridad del puesto de trabajo, equipo y/o dispositivo informático o medio desde el cual emplee su Certificado Digital,
- asumir los riesgos derivados de aceptar una conexión de infocomunicaciones, segura o no, sin haber realizado previamente la verificación de la validez de los Certificados Digitales empleados en la conexión,
- asumir los daños causados por incumplimiento del deber de proteger su llave privada.

9.6.4. Responsabilidades de las terceras partes que confían en los Certificados Digitales emitidos por la ACDATYS

Es responsabilidad de las terceras partes que confían en los Certificados Digitales emitidos por la ACDATYS:

- Circunscribir la confianza en los Certificados Digitales de Llave Pública emitidos por la ACDATYS, a los usos permitidos, en conformidad con la presente DPC, las PC y las propias extensiones de los Certificados,
- verificar la validez y el estado de los Certificados Digitales emitidos por la ACDATYS,
- verificar la disponibilidad de descarga de las CRL y del servicio OCSP,
- verificar la firma digital del titular de un Certificado Digital, antes de aceptar como válidos documentos o archivos firmados digitalmente por este.

9.7. Período de validez

9.7.1. Plazo

La presente DPC entra en vigor a partir del momento de su publicación en el sitio web oficial de la ACDATYS, y será válida mientras no se derogue expresamente por la emisión de una nueva versión.

9.7.2. Sustitución y derogación de la DPC

Al ser sustituida o derogada una versión de la DPC, se mantendrá publicada en el sitio web oficial de la ACDATYS por un periodo de treinta (30) días, antes de ser retirada. Todas las versiones de DPC serán conservadas por un período de quince (15) años.

9.7.3. Efectos de la finalización

Los elementos que se establecen en la presente DPC, relacionados con los temas de obligaciones y responsabilidades, auditorías, tratamiento de la información confidencial, mantendrán su validez, tras su sustitución o derogación por una nueva versión, siempre que no existan conflictos conceptuales o de contenido.

9.8. Notificaciones individuales y comunicaciones a los participantes

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las prácticas descritas en la presente DPC, se realizará mediante documento o mensaje electrónico de conformidad con esta última o por escrito mediante correo certificado dirigido a cualquiera de las direcciones referidas en la sección 1.5 de este documento.

9.9. Modificaciones a la DPC

La presente DPC será revisada íntegramente cada dos (2) años.

Cualquier insuficiencia o deficiencia detectadas en la presente DPC, así como sugerencias de cambios, podrán ser comunicadas por las entidades, representantes o titulares, a la ARDATYS.

9.9.1. Procedimiento para los cambios

La entidad con atribuciones para realizar y proponer cambios a la DPC de la ACDATYS es la dirección de la propia ACDATYS.

Para el versionado de la DPC de la ACDATYS se empleará el formato estándar X.Y.Z.

La ACDATYS determinará cuáles de los cambios o modificaciones propuestos podrán ser consultados a las entidades, representantes y titulares de Certificados Digitales.

En caso de que algún cambio o modificación a la DPC vigente, limite o afecte el uso de un Certificado Digital, se comunicará a las entidades, representantes y titulares de Certificados Digitales con al menos treinta (30) días antes de la publicación oficial de la nueva versión.

Los Certificados Digitales emitidos, sujetos a la versión vigente de la DPC, continuarán siendo válidos para los propósitos en ella establecidos, pero no para los nuevos propósitos referidos en la nueva versión de la DPC.

En caso necesario, se procederá a la renovación de los Certificados Digitales.

9.9.2. Procedimiento de notificación

Todos los cambios o modificaciones a que estén sujetas la presente DPC o las PC de la ACDATYS, serán notificados en su sitio web oficial.

9.9.3. Aprobación de la DPC

La DC del MININT es la autoridad competente responsabilizada de la aprobación de la presente DPC y de sus futuras versiones.

9.10. Reclamaciones y jurisdicción

Todo litigio relacionado con la gestión de Certificados Digitales de Llave Pública y llaves criptográficas, entre la ACDATYS o la ARDATYS y una entidad jurídica o persona natural, se resolverán a través de los mecanismos apropiados de resolución de litigios establecidos y vigentes en el país. Siempre que sea posible, el conflicto se resolverá mediante negociación. Todo litigio no resuelto mediante negociación se deberá resolver mediante los procedimientos de arbitraje vigentes.

9.11. Legislación aplicable

La estructura y contenido de la presente DPC está basada en 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 Autoridad Raíz ACSCC,

así como de las principales normas y estándares internacionales sobre la materia y de una selección de las mejores prácticas de experimentadas Autoridades de Certificación externas.

Firmado digitalmente por Autoridad de Certificación DATYS
Fecha: 2023.06.05 15:03:25 -04'00'