DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

AUTORIDAD DE CERTIFICACIÓN SERVICIO CENTRAL CIFRADO, AUTORIDAD RAÍZ DE LA INFRAESTRUCTURA DE LLAVE PÚBLICA DE LA REPÚBLICA DE CUBA

(Versión 1.0)

DICIEMBRE DE 2016
"AÑO 58 DE LA REVOLUCIÓN"

HISTORIAL DE CAMBIOS

Versión	Fecha	Descripción
1.0	25-12-2016	Documento inicial

Contenido

1. INTRODUCCIÓN

Teniendo en cuenta la necesidad de garantizar el empleo en el país de certificados digitales como medio de autenticación segura, firma digital, aseguramiento de confidencialidad y habilitación de canales de infocomunicaciones y sitios web seguros, entre otras aplicaciones, se hace necesario dejar establecidas las Prácticas de Certificación Digital que garanticen la seguridad en la implementación de una infraestructura de llave pública del país y del empleo de las aplicaciones de esta tecnología.

El presente documento muestra los principales indicadores que regulan el funcionamiento de la Infraestructura de Llave Pública en la República de Cuba y de su Autoridad Raíz.

1.1. Presentación.

El objetivo de este documento es describir las prácticas y procedimientos implementados en la Autoridad de Certificación Servicio Central Cifrado, Autoridad Raíz de la Infraestructura de Llave Pública de la República de Cuba, para brindar los Servicios Criptográficos de Certificación Digital.

El presente documento será publicado en el sitio web de la Autoridad de Certificación Servicio Central Cifrado (http://sercencif.cu) y servirá de base para la elaboración de las Declaraciones de Prácticas de Certificación del resto de las Autoridades de Certificación intermedias que se establezcan en el país.

Para la redacción del documento se utilizó el **"Reglamento sobre el funcionamiento de la Infraestructura de Llave Pública en interés de la protección criptográfica de la información oficial en la República de Cuba"** aprobado por la Resolución No. 2/2016 del Ministerio del Interior y su estructura se basa en el estándar RFC 3647 para la documentación de prácticas de certificación del grupo de trabajo IETF PKIX.

1.2. Nombre e identificación del documento.

Este documento se titula "Declaración de Prácticas de Certificación" (versión 1) de la Autoridad de Certificación Servicio Central Cifrado y fue emitido en diciembre de 2016.

1.3. Participantes de la Infraestructura de Llave Pública.

1.3.1. Estructura general de la Infraestructura de Llave Pública.

La Infraestructura de Llave Pública está representada por una topología jerárquica, en la que se interrelacionan diferentes tipos de Prestadores de Servicios Criptográficos de Certificación, definidos de acuerdo al nivel y el rol que cumplen.

Esta topología se compone de una Autoridad de Certificación Raíz en el nivel superior, los Prestadores de Servicios Criptográficos de Certificación intermedios, colocados en el nivel inmediato inferior de la Autoridad de Certificación Raíz, que se corresponden con los órganos, organismos y entidades que implementarán los mismos, para la generación, firma y gestión de los certificados digitales y otras aplicaciones. A continuación, el próximo nivel está formado por otros prestadores subordinados a los Prestadores de Servicios Criptográficos de Certificación intermedios de órganos, organismos y entidades y así hasta el nivel mínimo que se requiera.

Desde estos Prestadores de Servicios Criptográficos de Certificación Intermedios, se generarán y firmarán los certificados de identidad digital para otros prestadores subordinados y los suscriptores finales.

Los Prestadores de Servicios Criptográficos de Certificación podrán ser corporativos o comerciales.

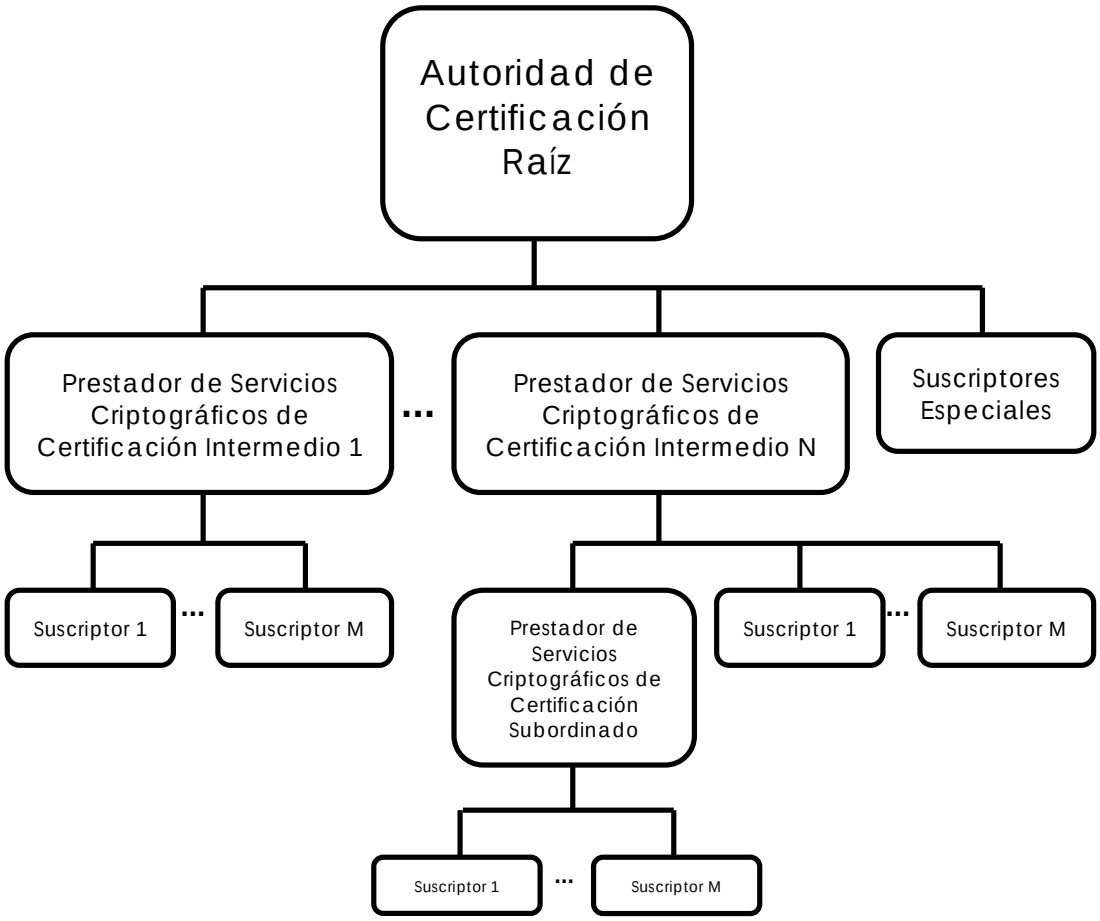

Fig. 1. Topología de la Infraestructura de Llave Pública

A través de esta Infraestructura de Llave Pública y mediante la administración de los certificados de llave pública en cada Prestador de Servicios Criptográficos de Certificación Intermedio, se puede establecer y mantener un entorno de red segura en los organismos de la Administración Central del Estado, órganos, y entidades; posibilitando el uso de la firma digital, la autenticación de usuarios y aplicaciones y la protección de canales de comunicación con una amplia gama de aplicaciones.

1.3.2. Autoridades de Certificación.

La Autoridad de Certificación Raíz es la máxima autoridad de la Infraestructura de Llave Pública y es el tope de la cadena de certificación y de confianza entre los participantes en la Infraestructura. Su certificado digital es autofirmado y se utiliza para la emisión de los certificados digitales de sus administradores, operadores, usuarios excepcionales y de los Prestadores de Servicios Criptográficos de Certificación Digital subordinados, además para la generación y producción de todo el material criptográfico necesario para generar, en las Autoridades de Certificación Intermedias, los certificados digitales para la protección de canales y servicios web. Es también la encargada de revocar los certificados bajo su firma.

El rol de Autoridad de Certificación Raíz en la Infraestructura de Llave Pública de la República de Cuba, lo cumple la Autoridad de Certificación Servicio Central Cifrado.

Las Autoridades de Certificación Intermedias están subordinadas a una Autoridad de Certificación superior. Su propósito es la emisión y revocación de certificados digitales para los Prestadores de Servicios Criptográficos de Certificación Digital y suscriptores subordinados. Utilizan el material criptográfico generado por la Autoridad de Certificación Raíz para generar los certificados digitales para la protección de canales y servicios web. Pueden funcionar como entidades mixtas para la realización de las actividades de registro y certificación.

1.3.3. Autoridades de Registro.

Son las encargadas de atender y registrar las peticiones para poseer certificados digitales. Realizan la comprobación de la veracidad de los datos del solicitante y envían la solicitud a la Autoridad de Certificación correspondiente para la generación y firma del certificado digital. Pueden funcionar de manera autónoma o formar parte de la Autoridad de Certificación.

En el caso de la Autoridad de Certificación Raíz, esta funciona como entidad mixta, realizando las funciones tanto de Autoridad de Registro (ACSCC-ER) como de Autoridad de Certificación (ACSCC-EC). Ambas funciones se encuentran perfectamente delimitadas a partir de los roles establecidos para los funcionarios de la Autoridad Raíz.

1.3.4. Suscriptores.

Son los Prestadores de Servicios Criptográficos de Certificación, las personas, los dispositivos tecnológicos, las aplicaciones informáticas, etc., que tienen asignado un certificado digital para cumplir las funciones en dependencia de su designación.

Los usuarios o suscriptores finales son los mismos definidos como suscriptores, exceptuando a los Prestadores de Servicios Criptográficos de Certificación.

1.3.5. Terceros de buena fe.

Son las personas o entidades (diferentes al titular del certificado digital) que deciden aceptar y confiar en un certificado digital de llave pública emitido por una Autoridad de Certificación de la Infraestructura de Llave Pública de la República de Cuba.

1.4. Uso de los certificados.

En la Infraestructura de Llave Pública de la República de Cuba, los certificados digitales pueden utilizarse en la garantía de la protección de la información oficial que se procesa, trasmite o almacena con la utilización de las tecnologías de la información y otros medios electrónicos. Se emitirán de acuerdo con lo normado en el "Reglamento sobre el funcionamiento de la Infraestructura de Llave Pública en interés de la protección criptográfica de la información oficial en la República de Cuba".

De acuerdo al poseedor o titular del certificado digital, estos se clasifican en:

a) Certificados de personas o entidades. Son los certificados digitales que se expiden a personas naturales o jurídicas.

b) Certificados de Autoridades de Certificación. Son los certificados digitales que se expiden a las Autoridades de Certificación.

c) Certificados tecnológicos. Son los certificados digitales que se expiden para equipamientos tecnológicos, servidores, clientes, aplicaciones informáticas, etc.

1.4.1. Uso apropiado de los certificados.

Atendiendo a su uso permitido, los certificados digitales se clasifican en las siguientes categorías:

a) Categoría 1: Certificados digitales de llave pública de carácter personal para firma digital de mensajería y ficheros electrónicos. Se les denomina CD – Pfirma.

b) Categoría 2: Certificados digitales de llave pública de carácter técnico para la protección de canales y servicios de comunicaciones. Se les denomina CD – SSL.

1.4.2. Prohibición en el uso de los certificados.

Los certificados digitales sólo podrán emplearse de acuerdo a lo establecido en el numeral 1.4.1. y su uso específico aparecerá reflejado explícitamente en el campo del certificado digital destinado al uso de la llave.

No está permitido el uso de los certificados digitales para la protección criptográfica de la confidencialidad de la información oficial clasificada. Sólo se podrán utilizar para este fin en los casos que por cuestiones técnicas y funcionales especiales así se requiera y haya sido aprobado por la Dirección de Criptografía.

1.5. Detalles del Contacto

1.5.1. Organización de la Administración de la Declaración de Prácticas de Certificación.

Esta Declaración de Prácticas de Certificación fue redactada y revisada por un grupo de trabajo multidisciplinario, compuesto por personal técnico especializado de la Dirección de Criptografía del Ministerio del Interior de la República de Cuba.

1.5.2. Colectivo técnico de contacto.

Todo comentario o sugerencia relativa a esta Declaración de Prácticas de Certificación, puede ser dirigido al Servicio Central Cifrado de la Dirección de Criptografía, teléfonos 76472156 y 78589850 ext.107, o a la dirección de correo electrónico admonpki@mail.mn.co.cu**.**

1.5.3. Colectivo técnico que determina la coherencia entre la Declaración de Prácticas de Certificación y la política.

En caso de ajustes o cambios en esta Declaración de Prácticas de Certificación, que pueda interferir lo que

está regulado en las diferentes políticas, debe contactarse con el Servicio Central Cifrado de la Dirección de Criptografía, que es el responsable de mantener actualizadas y en buen estado esta Declaración de Prácticas de Certificación y sus políticas.

Teléfonos: 76472156 y 78589850 ext.107.

Correo electrónico: admonpki@mail.mn.co.cu

1.5.4. Procedimiento de aprobación de las Declaraciones de Prácticas de Certificación.

Los Prestadores de Servicios Criptográficos de Certificación directamente subordinados a la Autoridad Raíz, elaborarán sus propuestas de políticas y de Declaración de Prácticas de Certificación y la presentarán a la aprobación de la Dirección de Criptografía del Ministerio del Interior.

En el caso de los Prestadores de Servicios Criptográficos de Certificación intermedios, no subordinados directamente a la Autoridad Raíz, presentarán su propuesta de políticas y de Declaración de Prácticas de Certificación previamente avalada por la Autoridad de Certificación superior.

1.6. Definiciones y acrónimos.

1.6.1. Definiciones.

Son las establecidas en el "Reglamento sobre el funcionamiento de la Infraestructura de Llave Pública en interés de la protección criptográfica de la información oficial en la República de Cuba"

1.6.2. Acrónimos.

AC	Autoridad de Certificación

ACI	Autoridad de Certificación Intermedia
ACSCC	Autoridad de Certificación Servicio Central Cifrado
ACSCC-EC	Entidad Certificadora de la Autoridad de Certificación Servicio Central Cifrado
ACSCC-ER	Entidad Registradora de la Autoridad de Certificación Servicio Central Cifrado
AR	Autoridad de Registro
AV	Autoridad de Validación
CD o CID	Certificado digital o certificado de identidad digital
CRL	Lista de certificados revocados
DC	Dirección de Criptografía del Ministerio del Interior
DPC	Declaración de Prácticas de Certificación
ILP	Infraestructura de LlavePública
MININT	Ministerio del Interior
OCSP	Protocolo de verificación en línea del estado de los certificados
PIN	Clave personal de acceso
PSCC	Prestador de Servicios Criptográficos de Certificación

2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIOS.

2.1. Repositorios.

La ACSCC dispone de repositorios, accesibles desde internet, donde se publican el certificado de la ACSCC, los certificados emitidos por la ACSCC, las CRL, las DPC y otras informaciones relativas a la ACSCC y a la ILP de la República de Cuba

Toda la información contenida en los repositorios es pública y está disponible las 24 horas del día y los 7 días de la semana. Cuando se produzca una interrupción por causa de fuerza mayor, el servicio se restablecerá en el menor tiempo posible.

2.2. Publicación de información sobre certificación.

Es responsabilidad de la ACSCC:

a) Publicar su certificado digital autofirmado, el cual puede ser descargado desde las direcciones http://sercencif.cu y https://va.sercencif.cu
b) Publicar y mantener actualizada las listas de los certificados emitidos, la cual puede ser revisada en la dirección https://va.sercencif.cu
c) Publicar y mantener actualizadas las listas de los certificados revocados (CRL), las cuales pueden ser descargadas desde la dirección URL
   http://crl.sercencif.cu/va/crls/search.cgi?alias=ACSCC
   Esta dirección se encuentra en los certificados digitales emitidos, especificada en el campo Punto de distribución CRL.
d) Mantener actualizadas las bases de datos del servicio de validación en línea que implementa el protocolo OCSP, al cual se accede por la dirección
   http://ocsp.sercencif.cu/va/status/ocsp

Esta dirección se encuentra en los certificados digitales emitidos, especificada en el campo Acceso a la información de autoridad.

e) Publicar y mantener actualizada la DPC (este documento), a la cual se puede acceder en el sitio http://sercencif.cu
f) Publicar y mantener actualizada la relación de los PSCC subordinados, a la cual se puede acceder en el sitio http://sercencif.cu

Todas las AC intermedias de la ILP de la República de Cuba tendrán estas mismas responsabilidades en el ámbito de su competencia.

2.3. Frecuencia de publicación.

2.3.1. Certificado digital de la Autoridad Raíz.

El certificado autofirmado de la ACSCC se publica inmediatamente después de ser generado y desplegados los sistemas que conforman la AC Raíz. El período de validez de este certificado es de quince años.

2.3.2. Certificados digitales emitidos por la Autoridad Raíz.

Los certificados digitales emitidos por la ACSCC, se publicarán en un plazo no mayor a las 24 horas, después de haber sido firmados por la ACSCC.

2.3.3. Lista de los certificados revocados.

Las CRL correspondientes a la ACSCC se publicarán trimestralmente, siempre y cuando no se produzcan suspensiones o revocaciones de certificados, en cuyo caso se actualizará en un plazo no mayor a las 24 horas de producida la suspensión o revocación. Una vez realizada la actualización, se reiniciará nuevamente el período trimestral.

2.3.4. Servicio de validación en línea del estado de un certificado.

La actualización de las bases de datos del servicio de validación en línea que implementa el protocolo OCSP, se realiza en un plazo no mayor a las 24 horas de producida la emisión, suspensión o revocación de un certificado.

2.3.5. Declaración de Prácticas de Certificación.

La ACSCC realizará cada dos años la revisión de la DPC. Las nuevas versiones de la DPC se publicarán, en forma inmediata, luego de su aprobación por la Dirección de Criptografía.

2.3.6. Relación de los PSCC subordinados.

La acreditación de un PSCC subordinado se publicará en un plazo no mayor de 24 horas, después de haber sido firmado, por la ACSCC, su correspondiente certificado.

2.4. Controles de acceso a los repositorios.

El acceso a la información que publica la ACSCC sólo permitirá su lectura y/o descarga. La modificación o actualización de la información, queda restringida a los funcionarios de la ACSCC que cumplen ese rol.

3. IDENTIFICACIÓN Y AUTENTICACIÓN.

3.1. Nombres.

3.1.1. Tipos de nombres.

La ACSCC genera y firma certificados con tipos de nombres conformes al estándar X.509.

Para el certificado autofirmado de la ACSCC, el nombre distinguido (DN), tanto del titular (subject) como del emisor (issuer), está formado por los siguientes atributos:

- CN = Autoridad de Certificación Servicio Central Cifrado
- O = Infraestructura de Llave Pública de la República de Cuba
- OU = Autoridad Raíz
- L = Boyeros
- S = La Habana
- C = CU

3.1.2. Necesidad de que los nombres sean significativos.

La ACSCC garantiza que los nombres distinguidos (DN) de los certificados emitidos por ella son significativos, lo que permite establecer la identificación unívoca del suscriptor o titular del certificado y vincular su identidad con la clave pública.

3.1.3. Anonimato o seudónimo de los suscriptores.

No se permite el uso de seudónimos o el anonimato de los suscriptores en los certificados digitales emitidos en la ILP de la República de Cuba.

3.1.4. Reglas para la interpretación de los diferentes formatos de nombres.

Para la interpretación de los nombres distinguidos en los certificados emitidos por la ACSCC, se utilizan las reglas descritas en la ITU-T X.500 DistinguishedName (DN). Para todos los atributos se utiliza la codificación UTF8.

3.1.5. Unicidad de los nombres.

Los nombres de los suscriptores o titulares son únicos para poder identificarlos plenamente. En el DN se utiliza una

combinación de valores que permite garantizar la unicidad.

3.1.6. Solución de conflictos relativos a nombres.

La ACSCC no actúa como árbitro o mediador, ni resuelve disputa alguna respecto a la titularidad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales, etc. De igual manera, se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

3.2. Validación inicial de identidad.

3.2.1. Método para probar la posesión de la llave privada.

En el caso de los CD – Pfirma las llaves son generadas directamente por el suscriptor. Este genera una solicitud de certificado en formato PKCS#10, y la firma digitalmente con la llave privada generada. Esto permite a la ACSCC comprobar que el suscriptor posee la llave privada.

3.2.2. Autenticación de la identidad de una entidad.

Para la solicitud de un certificado digital para una entidad, el jefe de órgano, organismo o entidad interesado nombrará un representante, el cual entregará, además de sus datos generales identificativos, toda la información que avale la existencia legal de la entidad y su objeto social.

La autoridad de registro comprobará en los registros legales correspondientes, establecidos por el estado cubano, la veracidad de la información entregada.

3.2.3. Autenticación de la identidad de una persona.

Las solicitudes de certificados se realizan por parte del representante del suscriptor, el cual entregará todos los datos personales necesarios para avalar su identidad.

En el caso de las solicitudes para la obtención de certificados SSL el representante del suscriptor tiene que entregar la información de titularidad de los nombres de dominios, datos de conectividad y servicios de infocomunicaciones que el solicitante requiere proteger, así como las características del equipamiento técnico donde funcionará y los datos generales identificativos de los candidatos a responsables de su custodia y activación.

En todos los casos, la Autoridad de Registro comprobará en los registros legales correspondientes, establecidos por el estado cubano, la veracidad de la información entregada.

3.2.4. Información no verificada del suscriptor.

La ACSCC-ER no se aceptará información del suscriptor a ser incluida en el certificado digital, que no pueda ser objeto de verificación.

La ACSCC-ER realizará la verificación de los datos que se solicitan al suscriptor, conforme a lo establecido en los numerales 3.2.2 y 3.2.3 de esta DPC.

3.2.5. Validación de Autoridad.

El solicitante que requiera incluir en su certificado digital un cargo determinado deberá presentar, además de los datos personales necesarios para avalar su identidad, la documentación pertinente que acredite el mismo en el órgano, organismo o entidad correspondiente.

3.2.6. Criterios para la Interoperación.

La ACSCC funge como autoridad de enlace técnico con autoridades raíces de otros países y de organizaciones internacionales, para asegurar la interoperabilidad de los certificados digitales cubanos y de la Infraestructura con sistemas similares del resto del mundo, en las transacciones electrónicas de Cuba con el extranjero, que estén aprobadas por los órganos y organismos de la Administración Central del Estado competentes.

A la puesta en vigor de las presentes DPC, no se han establecido relaciones de confianza con otro Prestador de Servicios Criptográficos de Certificación extranjero.

3.3. Identificación y Autenticación de solicitudes de renovación de claves.

La renovación de claves implica la renovación del certificado.

Los procedimientos para la renovación de un certificado se describen en el numeral 4.7 de estas DPC.

3.4. Identificación y Autenticación de solicitudes de revocación.

El jefe del órgano, organismo o entidad que ampara al PSCC firma y envía la solicitud de revocación a la ACSCC. En el caso de los suscriptores, la elabora y firma el representante del suscriptor.

En ambos casos la firma de la solicitud garantiza que la ACSCC puede comprobar la autenticidad de la solicitud.

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS.

4.1. Solicitud de certificados.

4.1.1. Habilitados para solicitar certificados.

Los jefes de los órganos, organismos y entidades están habilitados para solicitar certificados digitales para PSCC que actuarán en su ámbito.

Para el resto de las solicitudes se habilitarán los representantes de los órganos, organismos y entidades, para lo cual presentarán ante la ACSCC, un documento legal firmado por el jefe del órgano, organismo o entidad, nombrándolo como representante del mismo.

4.1.2. Proceso de solicitud y responsabilidades.

Para realizar la solicitud de certificados, el jefe del órgano, organismo o entidad correspondiente, mediante la persona designada por él como representante de los suscriptores de su ámbito, envía a la ACSCC, por escrito y acuñada, así como en el formato electrónico establecido por la Dirección de Criptografía al efecto, la relación de los datos de los candidatos a titulares de CD, necesarios para el llenado de los campos obligatorios establecidos para la emisión del certificado. En los casos de autogeneración de llaves criptográficas para la creación de la firma digital, la solicitud en formato electrónico vendrá acompañada de la llave pública producida.

Las solicitudes de certificados SSL, se realizarán por el representante del suscriptor del órgano, organismo o entidad interesada, de forma personal y presencial en las oficinas de la ACSCC-ER, acompañado de los documentos originales de identificación, entre ellos la

titularidad del dominio a proteger, para suscribir el contrato correspondiente de petición de emisión; los datos generales identificativos de los candidatos a responsables de su custodia y activación y la información sobre las características del equipamiento técnico donde funcionará.

4.2. Procesamiento de la solicitud del certificado.

4.2.1. Realización de las funciones de identificación y autenticación.

Las funciones de identificación y autenticación las realizan los funcionarios de la ACSCC-ER, los cuales han sido acreditados por la Dirección de Criptografía y poseen los medios necesarios para la realización de estas tareas.

Una vez recibida la solicitud en la ACSCC-ER, sus funcionarios realizan la comprobación de la identidad de cada candidato a suscriptor y de la posesión de las licencias correspondientes para la operación en el ámbito de las telecomunicaciones, a través de los sistemas estatales establecidos al efecto.

De existir contradicciones con los datos identificativos presentados de los futuros titulares de certificados, la ACSCC-ER devuelve la solicitud al representante de los candidatos a suscriptores para que sean rectificados.

Todo el proceso de identificación y autenticación es documentado y firmado por los funcionarios que lo ejecutan y asentado en los registros correspondientes. Finalmente, todo el proceso es validado por el Jefe de la ACSCC-ER.

4.2.2. Aprobación o denegación de la solicitud.

De acuerdo a la legislación vigente, las solicitudes de certificados digitales para los PSCC, serán aprobadas o denegadas por el Ministro del Interior, a partir del dictamen realizado por la Dirección de Criptografía.

En los casos restantes, la ACSCC tiene la función de aprobar o denegar las solicitudes de certificados.

Las solicitudes de certificación serán rechazadas, cuando estas no cumplan con los requerimientos de información establecidos, cuando no sea posible la verificación de la información brindada por la entidad, o cuando se compruebe la no veracidad de la información proporcionada.

En todos los casos, se notificará el representante de la entidad la denegación de la solicitud y sus causas.

En el caso de aprobación de la solicitud, la ACSCC-ER genera un permiso de emisión y lo envía a la ACSCC-EC, con la información necesaria para la emisión del certificado digital. Este permiso de emisión se envía en formato electrónico, firmado digitalmente por el funcionario que procesó la información y el Jefe de la ACSCC-ER como garantía de la integridad y la autenticación de origen de la misma.

4.2.3. Plazo para el procesamiento de la solicitud de un certificado.

A partir de la recepción de la solicitud de certificado digital, la ACSCC-ER tiene un período de quince (15) días para la ejecución de todo el proceso de identificación y autenticación de los datos identificativos del suscriptor y para aprobar o denegar la solicitud.

Una vez validados los datos y aprobada la solicitud, la ACSCC-ER genera y envía, en un término no superior a los siete (7) días, el permiso de emisión a la ACSCC-EC.

4.3. Emisión del certificado.

4.3.1. Acciones de la Autoridad Raíz durante la emisión del certificado.

Una vez recibido en la ACSCC-EC el permiso de emisión del certificado, la ACSCC tiene un plazo no mayor a los treinta (30) días, para producir los materiales criptográficos (para los CD-SSL) y los certificados digitales, publicar los certificados digitales y entregar el material criptográfico (para los CD-SSL) y el certificado digital al suscriptor, en los formatos convenidos con el mismo y de acuerdo a lo establecido en las presentes DPC.

4.3.1.1. Certificados PFirma.

En el caso de los certificados para firma digital, el permiso de emisión va acompañado de un fichero digital en formato PKCS#10, que contiene la llave pública del suscriptor.

La ACSCC-EC valida la autenticidad e integridad del permiso de emisión y a partir de la información contenida en el fichero PKCS#10, genera y firma el certificado digital del suscriptor, lo publica en el repositorio y lo envía además a la ACSCC-ER con la notificación de la emisión del certificado, firmada por el jefe de la ACSCC-EC.

La ACSCC-ER informa al suscriptor de la emisión y publicación del certificado y se lo entrega por la vía convenida de antemano.

4.3.1.2. Certificados SSL.

En el caso de los certificados SSL, una vez validada la autenticidad e integridad del permiso de emisión por parte de la ACSCC-EC, esta procede a la generación de las llaves pública y privada y a la generación y firma del certificado digital.

El sistema que posee la ACSCC, garantiza la generación automática de la llave privada y su cifrado a partir de una contraseña generada aleatoriamente, además, que la llave privada cifrada sólo se guarda en el dispositivo destinado al uso del suscriptor. La grabación de la llave privada cifrada en el dispositivo y la impresión del sobre pin que protege la contraseña son realizadas por operadores diferentes.

Los dispositivos contenedores de la llave privada cifrada y los sobre pin conteniendo las contraseñas, son entregados por los funcionarios encargados de la generación de cada uno, a funcionarios diferentes de la ACSCC-ER. En esta se mantienen bajo un sistema de almacenaje y custodia compartido.

El funcionario que custodia el dispositivo contenedor de la llave privada entrega éste, personalmente y mediante acta, al suscriptor y el funcionario que custodia el sobre pin, lo tramita por correo postal seguro a la oficina de control de la información clasificada o entidad equivalente, del órgano, organismo o entidad a la cual pertenece el suscriptor.

4.3.2. Notificación al suscriptor por parte de la Autoridad Raíz acerca de la emisión de su certificado.

El jefe de la ACSCC-ER envía una notificación oficial al representante del suscriptor informándole de la emisión del certificado solicitado.

4.4. Aceptación del certificado.

4.4.1. Forma en la que se acepta el certificado.

El contrato firmado por la ACSCC y el representante del suscriptor, garantiza el reconocimiento y acuerdo con los términos y condiciones contenidos en dicho documento, que rige los deberes y derechos de las partes y donde estas se obligan a cumplir con las prestaciones establecidas en las presentes DPC, así como el adecuado empleo de los certificados digitales de llave pública y de los criptomateriales. El contrato será firmado, en forma manuscrita, por el suscriptor o su representante.

4.4.2. Publicación del certificado.

Una vez generado y firmado el certificado, este será publicado, en un plazo no superior a las 24 horas, en el repositorio de la ACSCC para el acceso de los terceros de buena fe y del suscriptor, siempre que éste autorice su publicación.

4.4.3. Notificación de la emisión del certificado a otras entidades.

En el caso de los certificados emitidos a los PSCC, se publicarán en el sitio WEB de la ACSCC. Además, se informará, vía correo electrónico, al resto de los PSCC subordinados del primer nivel de jerarquía de la ILP.

4.5. Uso del certificado y el par de llaves.

4.5.1. Uso de la llave privada por parte del suscriptor.

El suscriptor, poseedor de un certificado está en la obligación de:

a) Emplear el certificado digital de llave pública y sus medios criptográficos para los usos establecidos en su emisión y para las tareas establecidas en sus funciones administrativas.
b) Resguardar en lugar seguro, el dispositivo de resguardo de la llave privada.
c) No transferir a otra persona, el dispositivo de resguardo de la llave privada y la clave personal de acceso a dicho dispositivo (PIN).
d) Solicitar inmediatamente, a la ACSCC, la revocación o suspensión del certificado, a través de su representante legal, en caso de tener conocimiento o sospecha del comprometimiento de la seguridad de la llave criptográfica privada correspondiente a la llave criptográfica pública contenida en el certificado, entre otras causas por: pérdida, robo, compromiso potencial, conocimiento por terceros de la clave personal de acceso al dispositivo de resguardo de la llave criptográfica privada y detección de inexactitudes en la información.
e) Notificar, en un plazo no mayor de las 24 horas, a su dirección superior inmediata, a los funcionarios de seguridad y protección de su órgano, organismo o entidad, así como a la ACSCC, cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo, informando cuando considere o tenga sospechas que la seguridad del sistema ha sido violada o comprometida.

f) No realizar acciones o intentos de acciones de monitoreo, manipulación o de ingeniería inversa sobre la implantación técnica – hardware y software – de los servicios de certificación.

4.5.2. Uso del certificado y la llave pública por el tercero de buena fe.

Los terceros de buena fe sólo pueden depositar su confianza en los certificados para el uso que establece esta DPC. Así mismo, deben asumir la responsabilidad de verificar el estado del certificado utilizando los medios que se establecen en esta DPC.

Además, se requiere de los terceros de buena fe:

a) No realizar acciones o intentos de acciones de monitoreo, manipulación o de ingeniería inversa sobre la implantación técnica – hardware y software – de los servicios de certificación.
b) Notificar a la ACSCC, cualquier hecho o situación anómala relativa a los certificados, así como informaciones o sospechas de comprometimiento o violación de la seguridad del sistema.

4.6. Renovación de un certificado.

En la ILP de la República de Cuba, se entiende por renovación de un certificado, el proceso de emisión de un nuevo par de llaves y su certificado correspondiente, para sustituir a uno que haya expirado.

4.6.1. Circunstancias para la renovación de un certificado.

Un certificado es renovado, cuando expira el tiempo de vigencia del mismo y el suscriptor desea continuar utilizando un certificado digital.

4.6.2. Personas habilitadas para solicitar la renovación.

Las personas habilitadas para solicitar la renovación, son las mismas que se establecen en el numeral 4.1.1 de esta DPC.

4.6.3. Procesamiento de la solicitud del certificado.

El procesamiento se realiza tal como se establece en el numeral 4.2 de esta DPC.

4.6.4. Notificación al suscriptor de la emisión del nuevo certificado.

El jefe de la ACSCC-ER envía una notificación oficial al representante del suscriptor informándole de la emisión del nuevo certificado.

4.6.5. Conducta constitutiva de la aceptación del certificado.

Es la misma que se establece en el numeral 4.4.1 de la presente DPC.

4.6.6. Publicación del certificado renovado.

El certificado renovado será publicado, en un plazo no superior a las 24 horas de haber sido emitido, en el repositorio de la ACSCC para el acceso de los terceros de buena fe y del suscriptor, siempre que éste autorice su publicación.

4.6.7. Notificación de la emisión del certificado renovado a otras entidades.

En el caso de la renovación de los certificados de los PSCC, se publicará la información en el sitio WEB de la ACSCC. Además, se informará, vía correo electrónico, al resto de los PSCC subordinados del primer nivel de jerarquía de la ICP.

4.7. Cambio de llave del certificado.

En la ILP de la República de Cuba, no se permite el cambio de llave de un certificado. Cuando se requiera realizar un cambio de llaves, es necesario realizar la solicitud de un nuevo certificado.

4.8. Modificación del certificado.

En la ILP de la República de Cuba, durante el ciclo de vida de un certificado, no está permitido efectuar modificaciones en ninguno de sus campos. Cuando se requiera realizar la modificación de algún campo, es necesario realizar la solicitud de un nuevo certificado.

4.9. Suspensión y revocación del certificado.

4.9.1. Circunstancias para la revocación.

Son circunstancias para la revocación de un certificado emitido por la ACSCC:

a) Solicitud formulada por el suscriptor del certificado a través de su representante.
b) Violación o puesta en peligro del secreto de los datos de creación de firma del suscriptor o del PSCC, o la utilización indebida de dichos datos por un tercero.
c) Resolución judicial o administrativa que lo disponga.
d) Fallecimiento del suscriptor, acreditada legalmente la defunción por su representante.
e) Extinción de alguno de los atributos legales del suscriptor para hacer uso del certificado, informado por su representante, o como resultado de investigaciones, auditorías y controles establecidos por la legislación vigente.

f) Fallecimiento, o extinción del estatus establecido por el órgano, organismo o entidad de la persona que ejerce como representante del suscriptor.
g) Incapacidad sobrevenida, total o parcial del suscriptor del certificado o de su representante.
h) Terminación o extinción de la representación del firmante del contrato.
i) Extinción o disolución de la persona jurídica bajo la cual el suscriptor posee y emplea el certificado digital.
j) Alteración de las condiciones de custodia o uso de los datos de creación de la firma digital, que estén reflejadas en los certificados expedidos.
k) Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.

4.9.2. Entidad que puede solicitar la revocación.

La solicitud de revocación del certificado de PSCC, se realizará a la ACSCC, por el jefe de órgano, organismo o entidad que lo ampara.

La ACSCC puede revocar el certificado por decisión propia, sin mediar solicitud expresa, cuando existan incumplimientos de los compromisos establecidos en la presente DPC; violaciones de las regulaciones establecidas en la legislación vigente y cuando las circunstancias de seguridad de la Infraestructura así lo requieran.

En el caso de los certificados emitidos a personas o tecnológicos, la solicitud de revocación será solicitada por el suscriptor del certificado a través de su

representante. Al igual que en el caso de los certificados emitidos para PSCC, la ACSCC puede revocar el certificado por decisión propia, sin mediar solicitud expresa, cuando concurran las circunstancias anteriormente descritas.

4.9.3. Procedimiento de solicitud de la revocación.

El jefe del órgano, organismo o entidad que ampara al PSCC firma y envía la solicitud de revocación a la ACSCC. Una vez recibida la solicitud, la Dirección de Criptografía realiza un dictamen previo, en coordinación con los organismos implicados, el cual es sometido a la aprobación del Ministro del Interior en función del acto efectivo de revocación, el cual es realizado de manera inmediata por la ACSCC.

En el caso de los suscriptores, el representante firmará la solicitud de revocación y la enviará a la ACSCC. La ACSCC-ER evalúa la solicitud de revocación, en un plazo no mayor a los tres (3) días hábiles, y en caso de proceder firma y envía la orden de revocación a la ACSCC-EC, la cual procederá a hacerla efectiva de inmediato.

En cualquiera de los casos, la solicitud de revocación enviada a la ACSCC, tendrá la siguiente información:

- Fecha de solicitud de la revocación.
- Identidad del suscriptor.
- Razón detallada para la petición de revocación.
- Nombre y título de la persona que pide la revocación.
- Datos de localización de la persona que pide la revocación.

4.9.4. Período de gracia de la solicitud de revocación.

No se establece periodo de gracia asociado a este proceso, durante el que se pueda anular la revocación de un certificado.

4.9.5. Tiempo dentro del cual la Autoridad Raíz debe procesar la solicitud de revocación.

La ACSCC procesará, en un plazo no mayor a los tres (3) días, cualquier pedido de revocación, una vez que sea de su conocimiento.

4.9.6. Requerimientos para la verificación de la revocación por los terceros de confianza.

Una vez realizada la revocación de un certificado por parte de la ACSCC, ésta publica el estado del certificado en sus repositorios de acuerdo a lo señalado en el numeral 2.3 del presente documento.

4.9.7. Frecuencia de emisión de la CRL.

La ACSCC publica las CRL trimestralmente. Siempre que se produzca una suspensión o revocación de certificado la actualización de la CRL se realizará en un plazo no mayor a las 24 horas. Una vez realizada la actualización, se reiniciará nuevamente el período de emisión trimestral.

En la CRL se indica la fecha de publicación de la siguiente lista y su punto de distribución. La CRL es generada y firmada por la ACSCC.

4.9.8. Máxima latencia para CRL.

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

4.9.9. Disponibilidad de la verificación en línea de la revocación.

La ACSCC posee un servidor OCSP para la verificación en línea del estado de los certificados. El acceso a este servicio se realiza por la dirección

http://ocsp.sercencif.cu/va/status/ocsp

Esta dirección se encuentra especificada en los certificados digitales emitidos, en el campo Acceso a la información de autoridad.

4.9.10. Requerimientos para la verificación en línea de la revocación.

No existe ningún requerimiento para el uso del servidor OCSP, excepto los derivados del propio protocolo OCSP según se define en la RFC 2560.

4.9.11. Otras formas disponibles de publicar la revocación.

Cuando la ACSCC revoca el certificado de un PSCC subordinado, informa inmediatamente al resto de los PSCC vía correo electrónico.

4.9.12. Requerimientos especiales para el caso del comprometimiento de la llave privada.

En caso de comprometimiento de la llave privada de la ACSCC, ésta revocará todos los certificados emitidos y lo notificará, vía correo electrónico, a todos los PSCC subordinados y suscriptores.

En un plazo no mayor de 24 horas la ACSCC generará un nuevo par de llaves y generará, firmará y publicará su nuevo certificado.

A partir de ese momento procederá a la emisión de los nuevos certificados, a los PSCC subordinados y suscriptores que tenían certificados vigentes en el momento de producirse el comprometimiento.

4.9.13. Circunstancias para la suspensión de un certificado.

Son circunstancias para la suspensión de un certificado, las mismas que se establecen para la revocación y que aparecen en el numeral 4.8.1 de la presente DPC.

4.9.14. Entidad que puede solicitar la suspensión.

Las entidades que pueden solicitar la suspensión, son las mismas que se establecen para el caso de la revocación y que aparecen en el numeral 4.8.2 de la presente DPC.

4.9.15. Procedimiento para solicitar la suspensión.

Los procedimientos para solicitar la suspensión de un certificado son los mismos que se establecen para la revocación, los cuales aparecen en el numeral 4.8.3 de la presente DPC.

4.9.16. Límite del periodo de suspensión.

El tiempo máximo para la suspensión de un certificado serán treinta (30) días. Si al cabo de ese tiempo la ACSCC, no ha recibido del representante, la solicitud para anular la suspensión y activar el certificado, se procederá de inmediato a su revocación, la cual será efectiva desde la fecha en que se procedió a su suspensión.

4.10. Servicios de estado del certificado.

Para la validación de los certificados, se dispone de varias formas que proporcionan información sobre el estado de los certificados emitidos por la ACSCC:

- Relación de los PSCC subordinados, a la cual se puede acceder en el sitio http://sercencif.cu
- Listas de certificados revocados (CRL), las cuales pueden ser descargadas desde la dirección URL

  http://crl.sercencif.cu/va/crls/search.cgi?alias=ACSCC

- Servicio de validación en línea que implementa el protocolo OCSP, al cual se accede por la dirección http://ocsp.sercencif.cu/va/status/ocsp

4.10.1. Características operacionales.

Cualquier información publicada por la ACSCC respecto al estado de los certificados emitidos por ella, es firmada digitalmente por la ACSCC.

4.10.2. Disponibilidad del servicio.

El servicio de comprobación del estado de los certificados emitidos por la ACSCC es accesible de forma ininterrumpida los 365 días del año.

4.10.3. Características adicionales.

Para hacer uso del servicio de validación en línea es responsabilidad del tercero de buena fe disponer de un Cliente OCSP que cumpla la RFC 2560.

4.11. Finalización de la suscripción.

Se dará por finalizada la suscripción de un certificado digital en los siguientes casos:

a) Caducidad de la vigencia del certificado digital.
b) Por revocación del certificado, por cualquiera de las circunstancias señaladas en el numeral 4.8.1 del presente documento.

4.12. Custodia y recuperación de llaves.

4.12.1. Políticas y prácticas de recuperación de llaves.

En el marco de la ILP de la República de Cuba, ni la ACSCC, ni cualquier otro PSCC, almacenarán la llave privada de ningún certificado digital de suscriptor, emitido para firma digital.

5. CONTROLES FÍSICOS Y OPERACIONALES.

5.1. Controles físicos.

La Autoridad Raíz tiene implementadas medidas de seguridad para la protección física de los locales donde realiza sus operaciones.

5.1.1. Ubicación y construcción del local.

La unidad de la Dirección de Criptografía que opera la ACSCC, está ubicada dentro de una instalación del Ministerio del Interior, que tiene guardia de seguridad y video vigilancia las 24 horas del día y los 7 días de la semana.

Los locales donde se ubica son de concreto reforzado y las ventanas están protegidas con barrotes metálicos.

5.1.2. Acceso físico.

La unidad que opera la ACSCC, posee, además, un servicio propio de guardia las 24 horas y los 7 días de la semana y además control de acceso biométrico. Todo personal ajeno a la misma necesita de autorización para entrar, es identificado y registrado y durante su estancia debe portar un pase en forma visible y estar acompañado permanentemente por un miembro de la unidad.

El local donde se realizan las operaciones críticas de la autoridad, posee tres niveles de control de acceso biométrico y cámaras de seguridad, tanto en las puertas de acceso como en el interior del local.

5.1.3. Alimentación eléctrica y aire acondicionado.

Los locales donde están ubicados los equipos cuentan con las condiciones de alimentación eléctrica y

estabilización de voltaje necesarios, para evitar fallas y otras anomalías eléctricas.

Los equipos se encuentran conectados a fuentes de alimentación ininterrumpidas (UPS) que garantizan el apagado controlado del equipamiento, durante la ausencia de fluido eléctrico, así como la protección del mismo ante fluctuaciones de voltaje.

Los sistemas de aire acondicionado garantizan las condiciones de temperatura y humedad adecuadas para el correcto funcionamiento y mantenimiento del equipamiento.

5.1.4. Prevención y protección contra incendios.

Se dispone de medios para la extinción de incendios en ubicaciones señalizadas y el personal ha sido preparado para la actuación ante este tipo de situaciones.

5.1.5. Almacenamiento de los medios.

Toda la información y documentación relativa a la gestión de los certificados, se conserva durante un período mínimo de 15 años, en archivos protegidos con técnicas criptográficas de cifrado y control de acceso.

5.1.6. Eliminación de residuos.

La depuración de los archivos de conservación de la información relativa a los certificados, se realiza en un acto con la participación de los funcionarios designados de la autoridad, y previa coordinación con los órganos, organismos y entidades usuarias involucradas.

La destrucción de los materiales y medios se realiza por una comisión designada por el Jefe de la ACSCC, la cual hace constar en acta cada medio o material destruido.

5.2. Controles de procedimientos.

5.2.1. Roles de confianza.

Los roles de confianza establecidos para el trabajo de la Autoridad Raíz son los siguientes:

- Jefe de la ACSCC
- Inspector auditor
- Administrador del Sistema (compartido por dos funcionarios)

Para el trabajo de la ACSCC-ER

- Jefe
- Atención al público
- Verificador
- Expedidor de permisos de emisión

Para el trabajo de la ACSCC-EC

- Jefe
- Custodio de llave privada (compartido por dos funcionarios)
- Receptor de permisos de emisión
- Generador de CD (compartido por dos funcionarios)
- Publicador de CD

Estos roles se describen en el documento interno "Asignación de roles"

5.2.2. Número de personas requeridas por tareas.

Se requiere un mínimo de dos personas acreditadas por cada rol, para garantizar el funcionamiento ininterrumpido de la autoridad.

Para la realización de las funciones diarias, se requiere la presencia de un funcionario acreditado para cada rol, con la excepción de los siguientes:

- Administrador del Sistema. Se requiere de dos (2) funcionarios acreditados para administrar los sistemas.
- Custodio de llave privada. Se requiere de dos (2) funcionarios acreditados para realizar la activación de la llave privada de la autoridad.
- Generador de CD. Se requiere de dos (2) funcionarios acreditados, uno para todo el trabajo de gestión de las llaves y certificados y otro para la gestión de los datos de activación de las llaves privadas.

5.2.3. Identificación y autenticación por cada rol.

Todos los funcionarios de la ACSCC poseen un carné que los acredita como tales y en él se detalla el rol que cumple.

Cada funcionario posee su propio certificado digital emitido por la ACSCC.

5.2.4. Roles que requieren separación de funciones.

Los roles de la ACSCC-ER son incompatibles con los roles de la ACSCC-EC y viceversa.

Los roles de Inspector auditor y administrador de sistema son incompatibles con todos los roles.

5.3. Controles del personal.

5.3.1. Requerimientos de calificación y experiencia.

Todo el personal que labora en la ACSCC es miembro activo del Ministerio del Interior y posee no menos de 5 años de experiencia en la actividad de Criptografía y ha sido debidamente preparado y acreditado para las funciones que realiza.

5.3.2. Requerimientos de formación y capacitación.

Para ser acreditado como funcionario de la ACSCC es necesario haber cursado y aprobado con resultados satisfactorios, el plan aprobado por la DC para la acreditación de funcionarios de una Autoridad de Certificación, el cual incluye como mínimo los siguientes elementos:

- Conocimientos básicos de la Criptografía Asimétrica y sus aplicaciones.
- Normativas vigentes en materia de Criptografía, seguridad de la información oficial y las relacionadas con la Infraestructura y el empleo de los certificados.
- Políticas de certificación digital y la DPC.
- Políticas de Seguridad.
- Aceptación del código de ética de la especialidad de Criptografía.
- Políticas establecidas para la confidencialidad sobre la información que maneja en virtud de su rol.
- Operación de los medios computacionales y/o electrónicos, así como de las aplicaciones informáticas para el puesto de trabajo específico.
- Procedimientos de seguridad en general y criptográficas en particular para cada rol especifico en la autoridad.
- Procedimientos de operación y administración de cada rol específico para la segregación de funciones de registro y certificación.
- Procedimientos relacionados con el enfrentamiento a las contingencias.

Se podrán incluir otros temas, con la finalidad de mantener un proceso de mejora continua en la formación y calificación del personal.

5.3.3. Requerimientos y frecuencia de la recalificación.

La ACSCC 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 ACSCC y que involucre los aspectos funcionales de los roles establecidos.

5.3.4. Sanciones por acciones no autorizadas.

Las actuaciones y acciones no autorizadas, por parte de los funcionarios de las autoridades y prestadores de servicios de certificación en la ILP de la República de Cuba, y en particular la ACSCC, violatorias del régimen de seguridad y de roles especificados para la operación de estas entidades, se califican como hechos sancionables administrativa y/o jurídicamente, en correspondencia con la legislación vigente en el país.

5.3.5. Documentación suministrada al personal.

La ACSCC proporciona a su personal toda la documentación necesaria para el correcto desempeño de sus responsabilidades. Entre la documentación que se entrega se encuentra:

- Código de Ética de la especialidad de Criptografía.
- Declaración de Prácticas de Certificación.
- Manuales de operación, administración e instalación de las herramientas informáticas y electrónicas de la ACSCC.

- Documentación relativa a las funciones y procedimientos de cada rol.

5.4. Archivo de registros.

5.4.1. Tipos de registros archivados.

La ACSCC archiva toda la información relacionada con:

- Ciclo de vida de las llaves de la autoridad.
- Ciclo de vida de los certificados digitales.
- Ciclo de vida de los sistemas criptográficos.
- Ciclo de vida del sistema automatizado para la gestión de los certificados digitales.
- Controles de acceso a locales y equipamiento.
- Modificaciones a los procedimientos y metodologías de trabajo.
- Modificaciones a la DPC.
- Auditorías y controles.

5.4.2. Período de conservación del archivo.

Tanto la ACSCC, como el resto de los PSCC de la ILP conservarán los registros durante un período mínimo de 15 años.

5.4.3. Protección del archivo.

Los registros se archivan protegidos con técnicas criptográficas de cifrado y control de acceso, de forma que nadie pueda acceder a ella, salvo los funcionarios autorizados para llevar a cabo verificaciones de integridad u otras.

Además, se establecen medidas de protección física y control de acceso al local donde se encuentran archivados los registros.

5.4.4. Procedimiento para la copia de seguridad del archivo.

El equipamiento que contiene las bases de datos de la Autoridad Raíz es redundante.

Diariamente se realiza una copia completa de las bases de datos.

5.4.5. Procedimiento para el sellado de tiempo de los registros.

Todos los registros se archivan con información de fecha y hora. La ACSCC posee un procedimiento para garantizar la coincidencia de la fecha y hora de los equipamientos con la oficial del país.

5.4.6. Sistema de recopilación de archivo (interno o externo).

El sistema de recopilación de la información es interno.

5.4.7. Procedimiento para obtener y verificar la información del archivo.

La obtención y verificación de la información sólo se realiza por el personal debidamente autorizado, el cual hará uso de las herramientas de verificación y control aprobadas por la Dirección de Criptografía para esos fines.

5.5. Cambio de llaves.

El tiempo de validez del certificado de la ACSCC es superior al período de validez de los certificados que emite.

Las llaves de la Autoridad Raíz expiran en el momento que su certificado deja de tener validez. Una vez expirado el certificado, la ACSCC procede a generar un nuevo par de llaves, el nuevo certificado y lo autofirma. Una vez concluido este proceso, se procede, de forma inmediata, a renovar los certificados de los PSCC subordinados, de forma tal que todo certificado que se genere en la ILP, luego del cambio de

llaves de la ACSCC, tenga en su cadena de certificación, el nuevo certificado de la Autoridad Raíz.

5.6. Recuperación ante el comprometimiento y desastres.

5.6.1. Procedimientos para la gestión de incidentes y comprometimiento.

La ACSCC posee un plan contra desastres, donde se identifican todos los riesgos que pueden provocar la inutilización o degradación de los servicios que presta, así como las acciones a realizar ante cada uno de los eventos, de forma tal que permita dar continuidad a la prestación de sus servicios esenciales.

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

Ante una sospecha o alteración de los recursos de hardware, software y/o los datos, la ACSCC detendrá su funcionamiento, informando de inmediato a todos los PSCC subordinados, y procederá a efectuar una auditoría para identificar la causa de la alteración y asegurar su eliminación.

Una vez restablecida la seguridad del entorno, se procederá a la restitución de los servicios, dando prioridad a la publicación de las CRL.

Todos los PSCC de la ILP procederán de igual forma ante eventos de este tipo.

5.6.3. Procedimiento ante el comprometimiento de la llave privada.

El plan contra desastres de la ACSCC, considera el compromiso o sospecha de comprometimiento de su clave privada como un desastre.

En ese caso se prevé la revocación inmediata de su certificado y la notificación, vía correo electrónico, a todos los PSCC subordinados y suscriptores para impedir la confianza en el mismo. Igualmente procederá a la revocación del resto de los certificados emitidos.

En un plazo no mayor de 24 horas la ACSCC generará un nuevo par de llaves y generará, firmará y publicará su nuevo certificado.

A partir de ese momento procederá a la emisión de los nuevos certificados, a los PSCC subordinados y suscriptores que tenían certificados vigentes en el momento de producirse el comprometimiento.

La ACSCC mantendrá en sus repositorios los certificados revocados, incluyendo el suyo, con el objetivo de garantizar la verificación de los certificados emitidos durante el período de funcionamiento.

5.6.4. Capacidad de la continuidad de las operaciones después de un desastre.

La ACSCC tiene previsto en su plan contra desastres, las acciones a realizar ante cualquier evento, para garantizar la continuidad de sus operaciones

5.7. Cese de las operaciones.

La ACSCC en su condición de Autoridad Raíz en la jerarquía de la ILP de la República de Cuba, no podrá cesar sus actividades de servicios de certificación.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. Generación e instalación del par de llaves.

6.1.1. Generación del par de llaves.

El par de llaves de la ACSCC se genera y almacena en el módulo criptográfico, el cual cumple los parámetros de seguridad establecidos por la Dirección de Criptografía.

6.1.2. Envío de la llave privada del suscriptor.

En el caso de los certificados PFirma, el suscriptor genera su par de llaves y es el responsable de su resguardo y custodia.

Para los certificados SSL, la llave privada se entrega al suscriptor, personalmente en la ACSCC-ER, en formato PKCS#12 protegido con una contraseña, la cual es generada aleatoriamente por el módulo criptográfico. El sobre pin que contiene la contraseña es tratado como información oficial clasificada y enviado a la OCIC de la entidad donde labora el suscritor.

Todas las Autoridades de Certificación subordinadas actuarán de igual forma en su ámbito de competencia.

6.1.3. Entrega de la llave pública al emisor del certificado.

Los suscriptores que generan su propio par de llaves, entregan a la ACSCC como parte de la solicitud de emisión del certificado PFirma, su llave pública en formato PKCS#10 firmada digitalmente con su llave privada, lo cual permite a la ACSCC validar la autenticidad del suscriptor.

6.1.4. Entrega o envío de la clave pública de la autoridad a los terceros de buena fe.

La clave pública de la ACSCC se encuentra en su certificado digital. Su certificado digital autofirmado se

encuentra publicado en la web oficial de la Autoridad Raíz (http://sercencif.cu) y además en el repositorio de certificados de la autoridad de validación de la ACSCC, que puede ser accedido en la dirección http://sercencif.cu

6.1.5. Tamaño de las llaves.

El algoritmo utilizado por la ACSCC para la firma de los certificados digitales es sha512 con RSA.

Los tamaños mínimos de llaves RSA, establecidos por la Dirección de Criptografía del MININT, para la ILP son:

	Longitud mínima de las llaves
ACSCC	8192 bits
PSCC intermedios	4096 bits
Suscriptores finales	2048 bits

6.1.6. Parámetros para la generación de llaves públicas y control de calidad.

La generación de las llaves y el control de su calidad se realiza por los parámetros establecidos por la Dirección de Criptografía para las llaves RSA.

6.1.7. Propósito de uso de la llave.

Los propósitos para el uso de la llave, se establecen en cada certificado en el campo Uso de la clave (keyusage).

6.2. Protección de la llave privada y controles del módulo criptográfico.

6.2.1. Normas y controles para el módulo criptográfico.

El módulo criptográfico se encuentra físicamente aislado y dentro de él se realiza la generación de las llaves, 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 del certificado digital, la revocación de los certificados y la generación y firma de las CRL.

Para transferir hacia el módulo criptográfico los datos para realizar sus operaciones; y desde éste la llave privada cifrada, su dato de activación, el certificado firmado y la CRL firmada, se utiliza una aplicación web, la cual sólo puede ser activada desde dos terminales específicas conectadas directamente al módulo criptográfico, aisladas físicamente de cualquier otro equipamiento y destinadas exclusivamente para esta función.

El módulo criptográfico cumple con todos los requerimientos y normas de seguridad, de control de acceso y de defensa criptológica establecidos por la Dirección de Criptografía.

6.2.2. Control multipersonal de la llave privada.

Para el acceso a la copia de seguridad de la llave privada y sus datos de activación se requiere la concurrencia de cuatro (4) funcionarios en cada caso.

Para el acceso físico al módulo criptográfico se requiere la concurrencia de tres (3) funcionarios. Si este acceso físico al módulo criptográfico, es para cargar la copia de seguridad de la llave privada, entonces se requiere la concurrencia de cinco (5) funcionarios.

6.2.3. Custodia de la llave privada.

La ACSCC no admite la realización de copia, almacenamiento o custodia de las llaves privadas para firma de los usuarios finales. Sólo realiza la custodia de una copia de su propia llave privada, tal como se

establece en los numerales 6.2.4 y 6.2.5 de las presentes DPC.

6.2.4. Copia de seguridad de la llave privada.

Al generarse, en el módulo criptográfico, el par de llaves de la Autoridad Raíz, se crea una copia de respaldo de la llave privada con el objetivo garantizar la continuidad de las operaciones ante la ocurrencia de desastres.

6.2.5. Archivo de la llave privada.

La copia de respaldo de la llave privada de la ACSCC se almacena, de manera cifrada, en un dispositivo extraíble, el cual se guarda en una caja fuerte con control de acceso multipersona. En esa caja fuerte no se guarda ningún otro material fuera de la copia de la llave privada y para acceder a la misma se necesita la activación de la combinación, de forma conjunta por dos funcionarios de la ACSCC que posean la combinación compartida y en presencia de dos custodios de llave privada.

La llave privada de la ACSCC se clasifica como SECRETO.

Los dos sobre PIN que contienen partes diferentes de la sucesión aleatoria para la activación de la copia de respaldo de la llave privada, son clasificados como documento SECRETO y se almacenan en otra caja fuerte destinada sólo a ese fin, con control de acceso multipersona.

6.2.6. Transferencia de la llave privada desde o hacia el módulo criptográfico.

La contraseña para acceder al módulo criptográfico, fue generada por mecanismos de secreto compartido que involucran a dos funcionarios que cumplen rol de

administrador, además se requiere la presencia del Jefe de la ACSCC-EC que es quien custodia la llave de acceso al gabinete donde se encuentra el módulo criptográfico.

Para transferir la llave privada desde o hacia el módulo criptográfico se requiere, además, la presencia de dos funcionarios que cumplen el rol de custodio de la llave privada.

6.2.7. Almacenamiento de la llave privada en el módulo criptográfico.

La llave privada de la ACSCC es generada por el módulo criptográfico y se mantiene almacenada en él de manera cifrada.

6.2.8. Método de activación de la llave privada.

La activación de la llave privada se produce cuando se realizan los procesos de firma de certificados y de CRL y se tiene que realizar por dos funcionarios que cumplen el rol de custodio de llave privada.

6.2.9. Método de desactivación de la llave privada.

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

6.2.10. Método de destrucción de la llave privada.

En el módulo criptográfico, antes de generar el par de llaves de la Autoridad Raíz, se realiza un borrado seguro de la zona de almacenamiento de la llave privada, lo que garantiza que la llave privada anterior sea irrecuperable.

Para la destrucción de la copia de respaldo de la llave privada, el Jefe de la ACSCC, designa una comisión,

presidida por el Jefe de la ACSCC-EC, la cual realizará, en presencia de un inspector auditor, el borrado seguro del medio de almacenamiento donde se encuentra la copia y posteriormente destruirá físicamente el mismo.

Igualmente, el Jefe de la ACSCC designa una comisión, presidida por el Jefe de la ACSCC-ER, la cual procederá, en presencia de un inspector auditor, a la incineración del sobre PIN donde se encuentra el dato de activación de la llave privada.

Ambas comisiones harán constar en acta las acciones realizadas.

La destrucción de los materiales y medios se realiza por una comisión designada por el Jefe de la ACSCC, la cual hace constar cada medio o material destruido.

6.2.11. Clasificación del módulo criptográfico.

El módulo criptográfico se clasifica como una Técnica Especial de Cifras secreta y cumple con todos los requerimientos establecidos por la Dirección de Criptografía para este tipo de dispositivo.

6.3. Otros aspectos de la gestión de llaves.

6.3.1. Archivo de llave pública.

La ACSCC mantiene en el repositorio de su Autoridad de Validación todos los certificados emitidos para que puedan ser consultados en cualquier momento y validada la cadena de confianza.

Igualmente los mantiene archivados en sus bases de datos internas y en los respaldos que se realizan de las mismas.

6.3.2. Períodos operacionales del certificado y períodos de uso de las llaves.

Los períodos de uso de las llaves están determinados por el tiempo de vigencia del certificado, una vez transcurrido éste no se pueden utilizar las llaves. La Dirección de Criptografía del MININT ha establecido los siguientes períodos para el uso de los certificados:

	Tiempo máximo de vigencia del certificado digital
ACSCC	15 años
PSCC intermedios	10 años
Suscriptores finales	2 años

6.4. Datos de activación.

6.4.1. Generación e instalación de los datos de activación.

Para la generación de los datos de activación de la llave privada de la ACSCC se procede de la siguiente forma:

Dos (2) funcionarios acreditados como custodio de llave privada, generan cada uno, de manera independiente y a partir de procesos físicos, una sucesión aleatoria que es protegida en un sobre PIN. La combinación de ambas sucesiones conforma el dato de activación de la llave privada de la autoridad. Por tanto, para la realización de cualquier proceso que necesite utilizar la llave privada, se necesita la concurrencia de ambos funcionarios para su activación, la cual siempre se realiza en presencia de al menos otro funcionario de la autoridad de acuerdo al proceso a realizar.

Para los certificados Pfirma, el dato de activación consiste en el PIN o clave de acceso que introduce el titular del certificado en el momento de la generación

de las llaves, siendo por tanto el único que tiene conocimiento del mismo y es el responsable de que permanezca bajo su exclusivo control.

En el caso de los certificados SSL, el dato de activación consiste igualmente en la clave personal de acceso –PIN- del dispositivo que contiene la llave privada. Este PIN es generado de forma aleatoria por el sistema y es impreso en un sobre especial que lo resguarda, sin que los operadores del sistema tengan acceso a la clave personal. Este sobre es entregado al funcionario, el cual es el único que llega a tener conocimiento del PIN.

6.4.2. Protección de los datos de activación.

Es responsabilidad del suscriptor la protección de los datos de activación de la llave privada.

En el caso de la Autoridad Raíz, es responsabilidad de los custodios de la llave privada la protección de los datos que posee cada uno, que permiten conformar el PIN con el cual se activa la llave privada de la ACSCC.

6.4.3. Otros aspectos de los datos de activación.

La clave personal de acceso (PIN) es confidencial, personal e intransferible y es el parámetro que protege la llave privada, por lo tanto, el suscriptor debe tener en cuenta normas de seguridad para su custodia y uso como son:

- Memorizar el PIN y procurar no anotarlo en ningún documento físico ni electrónico que el titular conserve o transporte junto con el dispositivo contenedor de la llave privada.
- No enviar ni comunicar a nadie su PIN.
- Notificar de inmediato la pérdida de control sobre su llave privada, a causa del compromiso del PIN.
- Cambiar periódicamente el PIN.

- Utilizar un PIN con no menos de 16 caracteres, donde se combinen letras en mayúsculas, minúsculas y números.
- No utilizar como PIN códigos relacionados con sus datos personales, así como cualquier otro que pueda resultar fácilmente predecible por terceras personas (nombres de familiares, fecha de nacimiento, número de identidad, teléfono, series de caracteres consecutivos, repeticiones de un mismo carácter, etc.).

6.5. Controles de seguridad computacional.

6.5.1. Requerimientos técnicos específicos de seguridad computacional.

La ACSCC tiene aprobado su Reglamento de Seguridad Informática, el cual es de estricto cumplimiento para todos sus funcionarios.

Todo el equipamiento posee protección contra virus y malware, la cual se actualiza diariamente. Además, existen controles de accesos físicos y lógicos a los mismos.

A todos los dispositivos de almacenamiento extraíble que se utilizan para el intercambio de información con el módulo criptográfico y con el sistema de registro se les realiza un control antivirus, antes de su uso, en una computadora, fuera de línea, destinada a ese fin. Al concluir las operaciones, se realiza un borrado seguro del dispositivo extraíble.

Todo movimiento de medios es registrado y controlado y se les da tratamiento como medios de almacenamiento de información oficial clasificada.

6.6. Controles técnicos del ciclo de vida.

6.6.1. Controles del desarrollo de los sistemas.

Todo el hardware y software que se utiliza en la ACSCC, así como sus configuraciones, pasaron una fase de prueba antes de ser puestos en explotación.

Se utilizan procedimientos de control de cambios para las nuevas versiones y actualizaciones de los componentes.

Todo el software que se utiliza está firmado digitalmente para garantizar su integridad y autenticidad.

6.6.2. Controles de gestión de seguridad.

La ACSCC mantiene un inventario de todos los activos que se utilizan en los procesos de registro y gestión de certificados digitales, y realiza una clasificación de los mismos de acuerdo con sus necesidades de protección, de forma coherente con los análisis de riesgos efectuados.

6.6.3. Controles de seguridad del ciclo de vida.

Existen controles de seguridad a lo largo de todo el ciclo de vida de los sistemas de la Autoridad Raíz, que permiten instrumentar y auditar cada fase de los mismos.

6.7. Controles de seguridad de redes.

El trabajo de la ACSCC se realiza fuera de línea, por lo tanto, el equipamiento que realiza el registro y la generación de llaves, certificados y CRL no se encuentra conectado a red alguna.

El intercambio de información entre la ACSCC-EC y la ACSCC-ER y entre esta última y los usuarios se realiza exclusivamente mediante dispositivos de almacenamiento removibles.

7. PERFILES DE CERTIFICADOS, LISTAS DE REVOCACIÓN (CRL) Y SERVICIO DE VERIFICACIÓN EN LÍNEA DEL ESTADO DEL CERTIFICADO (OCSP).

7.1. Perfil del certificado.

Los certificados emitidos por la Infraestructura de Llave Pública de la República de Cuba se ajustan a las siguientes normas:

- ITU-T Recommendation X.509: Information Technology – Open Systems Interconnection - The Directory: Authentication Framework.
- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile.

Como mínimo, los certificados emitidos por la ACSCC, tendrán los siguientes campos:

Campo	**Valor**
Versión	V3
Número de Serie	Valor único (en formato hexadecimal) generado por la autoridad que emite el certificado
Algoritmo de firma	sha512RSA
Algoritmo hash de firma	sha512
Emisor	CN = Autoridad de Certificación Servicio Central Cifrado OU = Autoridad Raíz O = Infraestructura de Llave Pública de la República de Cuba L = Boyeros S = La Habana C = CU E = admonpki@mail.mn.co.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
Clave pública	Se codifica de acuerdo con la RFC 5280. La longitud mínima de la llave es 2048 bits y algoritmo RSA.

- Para personas

Sujeto	CN = Nombre y apellidos OU = Dependencia O = Organismo L = Municipio S = Provincia C = CU T = Cargo SERIALNUMBER = Número de identidad permanente

- Para entidades

Sujeto	CN = Denominación de la entidad OU = Dependencia O = Organismo L = Municipio S = Provincia C = CU

- Para autoridades de certificación intermedias

Sujeto	CN = Denominación de la Autoridad OU = Dependencia O = Infraestructura de Llave Pública de la República de Cuba L = Municipio S = Provincia C = CU

- Para servidores

Sujeto	CN = Denominación del servidor OU = Dependencia O = Organismo L = Municipio S = Provincia C = CU

El certificado de la Autoridad Raíz ACSCC es:

Campo	**Valor**
Versión	V3
Número de Serie	02 54 0b e4 01
Algoritmo de firma	sha512RSA
Algoritmo hash de firma	sha512
Emisor	CN = Autoridad de Certificación Servicio Central Cifrado OU = Autoridad Raíz O = Infraestructura de Llave Pública de la República de Cuba L = Boyeros S = La Habana C = CU E = admonpki@mail.mn.co.cu
Válido desde	lunes, 14 de diciembre de 2015 16:26:33
Válido hasta	martes, 10 de diciembre de 2030 16:26:33
Sujeto	CN = Autoridad de Certificación Servicio Central Cifrado OU = Autoridad Raíz O = Infraestructura de Llave Pública de la República de Cuba L = Boyeros S = La Habana

	C = CU E = admonpki@mail.mn.co.cu
Clave pública	RSA (8192 Bits) 62 e1 4e 1b 91 6f 2b 8d bc 90 3e e7 85 96 e1 bf 50 84 be e9 ab cb cc e4 1e a3 82 c0 8a 04 15 2a c9 b5 9d 64 d0 88 06 2c 9d 99 b1 1b 91 41 51 8f dbcb 7b 95 40 d0 60 7f a6 48 5e d2 c1 57 d2 98 51 7c 9b 70 55 5a e7 7f ff 8c 24 f6 4e 99 4e 83 f0 ec d0 31 e7 28 b7 70 55 01 27 4f 52 c4 4c 60 25 b7 60 a6 36 4d d5 73 20 a6 8f f3 db 26 64 c7 e5 3d 56 4c 7b 1b 45 dd 3d 6c 2d 9e 9f fc 0c 1f 7d 1d 25 f3 b9 e7 64 ee cc a1 d0 11 49 09 14 25 cf 29 a0 a2 44 c9 84 59 84 2d b2 38 e4 34 3e e4 ac e1 a7 84 1d 0e 13 eb 7c 78 02 55 96 65 7d 63 6b 7a 9c dd 68 f7 67 65 81 d0 90 c9 e0 47 e5 ce 1a 1e 69 ba 66 ae 36 95 a8 5f 84 f9 64 29 82 f4 02 92 09 a6 a8 3c 8d 8a b7 84 f9 6f a1 72 fc 50 c6 78 14 83 8b fc 95 d2 90 7c 55 29 e1 42 66 7f 97 0c c3 51 c3 22 d0 f0 ae 97 63 78 45 13 83 a4 e9 e1 46 72 8e 2b b9 28 6f a4 ddddba 12 18 2d 7b 3c ed e7 c4 8a 8e f4 55 25 eb 6e 02 34 6b 5c 42 79 f4 f0 35 5e 06 35 5b 4c b1 3f ebaf 09 90 92 50 0a 2c cd 7f 4f f5 53 52 41 6b 00 3d cb 62 51 ed 69 fe f2 2b 24 f2 d3 49 68 47 1c d6 92 20 b0 4b 31 76 6e d4 20 3b 8e d1 52 7b 17 b7 2b dd d7 5b b8 c4 2d 2f cd 51 81 ab 03 c5 a1 ee 24 83 ea 4f fd 62 a0 dd 74 f0 75 b5 58 1d 41 c3 23 b4 cf 09 f6 58 3d 73 53 13 ad 1b 40 d7 53 ca 9d fb 81 ca b2 bfdf 8b 35 de fa cf 00 19 98 38 53 b3 90 3a 7b c4 e9 d8 11 67 73 b5 f1 e1 0d 57 77 42 37 f3 9a 13 b9 37 bdaa 22 4f db 22 1a 2b 1f 01 89 02 f8 69 7e 2a ea 3c 05 cd 8d f5 55 72 36 9f 72 64 cf 6a 83 8e c5 bd f0 04 8f 8d 1a 2d 04 d9 97 7a 63 cb 8c f7 1f 95 93 6d 4a 70 94 6d 3f 53 f9 b9 da 5f 29 20 8f 83 dd 1f 79 29 77 1d 55 c1 bf 6d b8 9f 32 e5 4d 6c 3b 36 62 9f 30 b0 07 9e 4b 4e 04 ed ab db 13 5f 38 b5 1f baae 90 51 1c 01 63 09 a8 36 77 65 f5 5c 97 0d 81 73 e1 70 18 49 90 76 ce fb 06 bc 70 7a 00 d0 dd 49 c2 30 e0 2b 41 11 f7 64 a2 f2 9a e1 f4 ca 8d e8 d9 ae 93 7c 7b 75 0d 82 7e 26 81 9b 87 04 7d 62 c6 c7 e4 21 63 c1 f0 be 64 cafb 79 11 bb d9 ff 95 a4 58 5f 3d 78 99 93 37 00 bf 99 9a 5c a7 74 d0 a9 dd c3 17 bdbf 19 98 bc 77 6c 42 26 dc 8d 5b 90 7a cd 0d 1b a9 e6 f2 eb 65 ac 97 05 f3 2e 76 d8 9e d4 3d

	bcdf 4e 02 93 b0 6a 57 b7 bb f9 60 71 71 c4 16 18 3b 9c 49 d4 69 93 9a 22 3c 2c fc d8 f5 e0 92 f5 84 a2 a4 5f 39 54 78 21 bf d5 a8 c0 12 05 97 e8 6b 41 97 94 1a cffcfc e8 d5 70 a9 25 73 98 e1 c4 55 6d 1c 53 4d c6 3b 3c 48 b7 4e e7 08 19 6f 88 c8 67 44 be a1 60 8a 44 f0 1a 64 b8 a7 ad f1 f0 10 35 5d 75 d4 f1 3c 97 77 55 af 4b 76 78 e2 d4 56 6f 96 8d 49 1d 8c 94 03 f8 56 b1 36 fa dd a1 48 de 65 fe 8a 1c 96 fb 2a dc 4f be be a6 5f cb 98 c8 5c 5f 96 52 ad b5 b9 22 fe 8b c4 c7 24 c9 70 4a a6 72 99 e3 6b 9a 01 8e 38 d9 f9 84 93 b5 e2 b7 cf 28 72 34 d4 b7 0f fe d2 0e 51 18 34 35 b1 ce 90 a2 ec 93 df b0 6e fc 7f 04 d9 d3 5c 28 c9 6d 33 c1 01 c5 2e 4b f2 02 ef 14 d6 99 f0 ca 4d 63 76 a4 11 fa 0a 6c 91 88 69 95 39 9a 66 b0 dfac b0 61 82 74 97 31 5e c3 fe 2d be 6e 1d f8 94 87 a1 4c 6e 55 02 ea 7f 23 62 5c 6f 87 f8 f9 1c 02 9a 81 91 95 96 be e3 73 0d 6e 47 7e 21 af 64 6c d6 aa 88 30 28 4e c0 32 88 01 12 bd 6e 43 fcdf c5 0f ff e7 0f 56 3c c1 07 51 f3 a8 90 f1 16 84 11 7d be cbdb 05 2b 02 03 01 00 01
Restricciones básicas	Tipo de asunto=Entidad de certificación (CA) Restricción de longitud de ruta=Ninguno
Identificador de clave del titular	0a 99 a2 e6 71 66 dd e9 d2 61 01 c3 cd 17 e9 3c 87 63 1e 91
Identificador de clave de entidad emisora	Id. de clave=0a 99 a2 e6 71 66 dd e9 d2 61 01 c3 cd 17 e9 3c 87 63 1e 91 Emisor de certificado: Dirección del directorio: CN=Autoridad de Certificación Servicio Central Cifrado OU=Autoridad Raíz O=Infraestructura de Llave Pública de la República de Cuba L=Boyeros S=La Habana
Acceso a la información de entidad emisora	[1]Acceso a información de autoridad Método de acceso = Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL =

	http://ocsp.sercencif.cu/va/status/ocsp
Puntos de distribución CRL	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://crl.sercencif.cu/va/crls/search.cgi?alias=ACSCC
Comentario de Netscape	Certificado de la Autoridad Raíz de la Infraestructura de Llave Pública de la República de Cuba
Algoritmo de identificación	sha 1
Huella digital	45 3d 7a 01 04 95 fa c8 cd 10 0b 30 99 5b 45 1a 2d ac d5 2d

7.1.1. Número de la versión.

Todos los certificados emitidos por la ACSCC y demás PSCC son X.509 versión 3.

7.1.2. Extensiones de los certificados.

Las extensiones de los certificados permiten codificar información adicional en los mismos.

En los certificados emitidos por la ACSCC, se utilizarán como mínimo los siguientes campos de las extensiones estándar X.509.

Campo	**Valor**
Uso de la clave	Especifica los usos permitidos de la llave.
Uso mejorado de la clave	Se especifican otros propósitos adicionales al uso de la llave.
Acceso a la información de la autoridad	Es utilizado para indicar la dirección URL para acceder al servicio OCSP.
Puntos de distribución CRL	Es utilizado para indicar la dirección donde se encuentra publicada la CRL.

7.1.3. Identificador de objeto del algoritmo.

El algoritmo criptográfico utilizado por la ACSCC es *SHA512 with RSA Encription*.

7.1.4. Formato de Nombres.

Es el definido en el numeral 3.1 de la presente DPC.

7.2. Perfil de la CRL.

Las listas de certificados revocados, emitidas por la ACSCC cumplen con la RFC 5280 y contienen los siguientes elementos básicos:

Campo	**Valor**
Versión	V2
Emisor	CN = Autoridad de Certificación Servicio Central Cifrado OU = Autoridad Raíz O = Infraestructura de Llave Pública de la República de Cuba L = Boyeros S = La Habana C = CU E = admonpki@mail.mn.co.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	sha512RSA
Algoritmo hash de firma	sha512
Certificados revocados	Lista de certificados revocados, incluyendo el número de serie y la fecha de revocación.

7.2.1. Número de versión.

La ACSCC emite las CRL en formato X.509 versión 2.

7.2.2. Extensiones de la CRL.

La extensión de la CRL emitida por la ACSCC es la siguiente:

Campo	**Valor**
Número CRL	Número consecutivo.

7.3. Perfil del OCSP.

La ACSCC permite también comprobar la validez de un certificado, mediante el uso del protocolo en línea del estado del certificado (OCSP)

7.3.1. Número de versión.

Está implementada la versión 1 del protocolo OCSP según lo establecido en la RFC 2560.