# *DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN*

**AUTORIDAD DE CERTIFICACIÓN INTERMEDIA DE LA INFRAESTRUCTURA DE LLAVE PÚBLICA DE SEGURMÁTICA (ACSEGURMATICA)**
**(Versión 1.0)**

# INDICE

# 1. INTRODUCCIÓN

La Empresa de Consultoría y Seguridad Informática, Segurmática, integrada al Grupo Empresarial de la Informática y las Comunicaciones (GEIC), tiene como objeto social "Comercializar licencias de uso y tecnología de seguridad informática, así como brindar servicios asociados a ella."

A partir de la aprobación de la Política para el perfeccionamiento de la Informatización de la sociedad en febrero de 2018, así como la publicación de un grupo de normas jurídicas que potencian el uso de certificados digitales, se identifica por la empresa la oportunidad de convertirse en Prestador de Servicios Criptográficos de Certificación Digital (PSCCD). Lo anterior tributa a la necesidad de garantizar el empleo en el país de los 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.

El presente documento muestra las principales pautas que regulan el funcionamiento de la Infraestructura de Llave Pública de Segurmática.

## 1.1. PRESENTACIÓN.

Este documento presenta la **Declaración de Prácticas de Certificación (DPC)** que rige el funcionamiento y operación de la **Infraestructura de Llave Pública (PKI)** de Segurmática. Expone las normas y prácticas de la Autoridad de Certificación para prestar el servicio, relaciona las medidas técnicas y organizativas para garantizar los niveles de seguridad necesarios, así como establece los requisitos técnicos y legales para aprobar, emitir, administrar, usar y revocar certificados dentro de la jerarquía de certificación.

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.

El presente documento estará publicado en el sitio web de la empresa *https://pki.segurmatica.cu/*.

## 1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO.

| | |
|---|---|
| **Nombre del documento** | Declaración de Prácticas de Certificación de la ACSEGURMATICA. |
| **Versión del documento** | 1.0 |
| **Fecha de emisión** | 30/09/2020 |
| **Localización** | *https://pki.segurmatica.cu/* |

***Tabla 1: Nombre e identificación del documento.***

## 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 de Segurmática, se subordina a la Autoridad Raíz constituida por la Autoridad de Certificación Servicio Central Cifrado.

La Autoridad de Certificación de Segurmática implementará lo pautado en esta Declaración de Prácticas de Certificación hacia lo interno y a sus clientes.

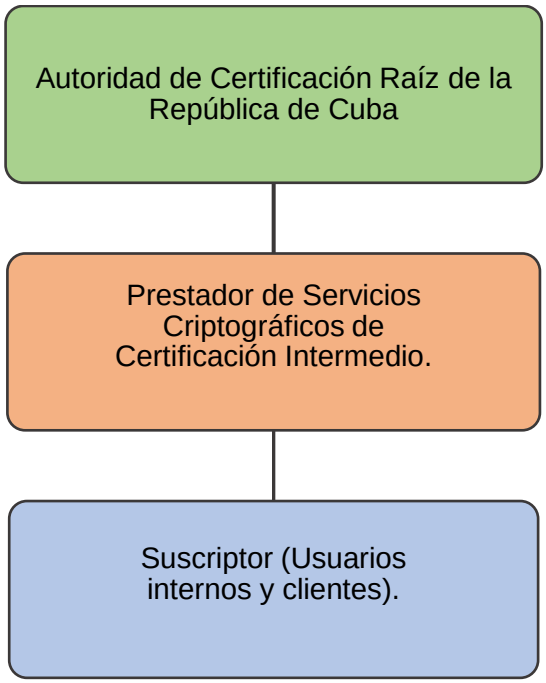


***Figura 1: Jerarquía de ACSEGURMATICA***

A través de esta Infraestructura de Llave Pública se puede establecer y mantener un entorno de red seguro para la empresa Segurmática y sus clientes, 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. Autoridad de certificación (CA).

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.

La **ACSEGURMATICA**, es una Autoridad de Certificación Intermedia y está subordinada a la Autoridad de Certificación Raíz. Se encarga de emitir, revocar y renovar los diferentes tipos de certificados digitales. De igual forma firma cada uno de los certificados que se emiten y mantiene actualizado su estado mediante la publicación de Listas de Revocación de Certificados y de los repositorios de certificados.

### 1.3.3. Autoridades de registro (RA).

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 ACSEGURMATICA, funciona como entidad mixta, realizando las funciones tanto de Autoridad de Registro, como de Autoridad de

Certificación. Ambas funciones se encuentran perfectamente delimitadas a partir de los roles establecidos para los funcionarios de la Autoridad de Segurmática.

Las funciones de la Autoridades de Registro Segurmática, se extienden a:

- Comprobar la identidad y las circunstancias personales de los solicitantes de certificados relevantes para el fin propio de estos.
- Informar con carácter previo a la emisión del certificado a la persona que lo solicite, de las condiciones precisas para la utilización del certificado y de sus limitaciones de uso.
- Verificar que la información contenida en el certificado es exacta y que incluye toda la información prescrita para un certificado reconocido.
- Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.

### 1.3.4. Autoridad de Validación (VA)

La Autoridad de validación de la ACSEGURMATICA, proporciona el servicio para la validación de los certificados emitidos mediante el empleo del protocolo de consulta en línea del estado de los certificados (OCSP), conforme a lo descrito en la RFC 2560.

Las respuestas OCSP están firmadas con la llave privada correspondiente al certificado de firma de respuestas OCSP de la Autoridad de Validación emitido por la ACSEGURMATICA.

### 1.3.5. Autoridad de Sellado de Tiempo.

La Autoridad de Sellado de Tiempo de la ACSEGURMÁTICA, proporciona el servicio de tokens de sellado de tiempo (TST), que indica que una firma o dato ha existido y no ha sido alterado desde un instante específico en el tiempo, a través del protocolo de estampado de tiempo (TSP), conforme a lo establecido en la RFC 3161.

La sincronización de la hora de los equipos de la Autoridad de Sellado de Tiempo de SEGURMATICA, se realizará mediante el protocolo de sincronización de tiempo en red (NTP).

### 1.3.6. Solicitante

Solicitante es la persona natural o jurídica que solicita, directamente o mediante un representante legal, la emisión de un certificado digital mediante un contrato y previa identificación.

### 1.3.7. 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. El Suscriptor asume la responsabilidad de custodia de los datos de creación de firma, sin que pueda ceder su uso a cualquier otra persona bajo ningún concepto.

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

### 1.3.8. Terceros que confían.

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 la Autoridad de Certificación de la Infraestructura de Llave Pública Intermedia de SEGURMÁTICA.

## 1.4. USO DE LOS CERTIFICADOS

En la Infraestructura de Llave Pública de SEGURMÁTICA, los certificados digitales pueden utilizarse para garantizar 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.

Los certificados de diferentes tipos emitidos por la ACSEGURMÁTICA, serán utilizados solamente durante su período de vigencia para dar cumplimiento a las funciones que le son propias y legítimas, de acuerdo a los fines y especificaciones definidos en las respectivas Políticas de Certificación (PC), sin que puedan utilizarse para otros propósitos no contemplados en aquella.

### 1.4.2. Prohibición en el uso de los certificados.

La realización de operaciones no autorizadas según esta DPC, por parte de terceros o titulares del servicio, eximirá a la ACSEGURMATICA de cualquier responsabilidad por este uso prohibido, en consecuencia:

- 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 están permitidas alteraciones sobre los certificados emitidos por la ACSEGURMATICA.

- Se considera prohibida toda acción que contravenga las disposiciones, obligaciones y políticas estipuladas en la presente DPC.
- 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 de Segurmática, bajo la supervisión de la Dirección General de la Empresa y el 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 a la Dirección Comercial de la empresa Segurmática, teléfonos 78781987 y 78703536 ext.136, o a la dirección de correo electrónico comercial@segurmatica.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 en la siguiente dirección con el colectivo técnico, responsable de mantener actualizadas y en buen estado esta Declaración de Prácticas de Certificación y sus políticas.

UEB Técnico Comercial. Grupo Soporte

teléfono: 7 8703536 ext. 135, dirección de correo soporte@segurmatica.cu.

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

A partir de la aplicación de los correspondientes procedimientos, la ACSEGURMÁTICA, garantiza el correcto mantenimiento de la Declaración de Prácticas de Certificación y de las especificaciones de servicio relacionadas con ella.

Una vez se han elaborado la propuesta de políticas y de Declaración de Prácticas de Certificación, se presentan a la aprobación de la Dirección de Criptografía del Ministerio del Interior.

## 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

| | |
|---|---|
| **ACSCC** | Autoridad de Certificación Servicio Central Cifrado |
| **ACSEGURMATICA** | Autoridad de Certificación Intermedia SEGURMÁTICA |
| **ACSEGURMATICA -EC** | Entidad Certificadora de la Autoridad de Certificación Intermedia SEGURMÁTICA |
| **ACSEGURMATICA-ER** | Entidad Registradora de la Autoridad de Certificación Intermedia SEGURMÁTICA |
| **CA** | Autoridad de Certificación |
| **CD o CID** | Certificado digital o certificado de identidad digital |
| **CRL** | Lista de Revocación de Certificados |
| **DC** | Dirección de Criptografía del Ministerio del Interior |
| **DPC** | Declaración de Prácticas de Certificación |

| | |
|---|---|
| **ILP** | Infraestructura de Llave Pública |
| **MININT** | Ministerio del Interior |
| **OCSP** | Protocolo de verificación en línea del estado de los certificados |
| **PC** | Política de certificado |
| **PIN** | Clave personal de acceso |
| **PKI** | Infraestructura de Llave pública |
| **PKCS** | Estándares de criptografía de llaves públicas |
| **PSCC** | Prestador de Servicios Criptográficos de Certificación |
| **RA** | Autoridad de Registro |

# 2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIOS.

## 2.1. Repositorios

La ACSEGURMATICA dispone de repositorios, accesibles desde Internet, donde se publican su certificado, los certificados que esta ha emitido, las CRL, las DPC y otras informaciones relativas a la ACSEGURMATICA y a la ILP de SEGURMÁTICA.

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.

ACSEGURMATICA se reserva hasta un máximo de 3 horas los sábados y domingos alternos y en el horario nocturno de lunes a viernes, para efectuar tareas de mantenimiento, salvas del sistema, etc.

Si existe un mal funcionamiento de los sistemas que operan los servicios, se informará a los representantes de los suscriptores sobre el problema y el tiempo previsto para normalización. En caso de desastres, se mantendrá un plan completo de recuperación del desastre y se notificará a los clientes si la interrupción del servicio dura más de 48 horas.

El repositorio de ACSEGURMATICA no contiene ninguna información de naturaleza confidencial.

## 2.2. Publicación

Es responsabilidad de la ACSEGURMATICA:

a) Publicar su certificado digital firmado por la ACSCC, el cual puede ser descargado desde la dirección: *https://pki.segurmatica.cu/*

b) Publicar y mantener actualizada las listas de los certificados emitidos, la cual puede ser revisada en la dirección *https://pki.segurmatica.cu/*

c) Publicar y mantener actualizadas las listas de los certificados revocados (CRL), las cuales pueden ser descargadas desde la dirección *https://pki.segurmatica.cu/*

   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 *https://pki.segurmatica.cu/*

   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 *https://pki.segurmatica.cu/*

## 2.3. Frecuencia de publicación.

### 2.3.1. Certificado digital de la Autoridad Intermedia de SEGURMÁTICA.

El certificado generado por la ACSCC se publica con anterioridad al comienzo de la prestación del servicio en el sitio oficial de la ACSEGURMATICA. De igual forma se procederá cada vez que el certificado de la Autoridad de Certificación sea renovado. El período de validez de este certificado es de diez años.

### 2.3.2. Certificados digitales emitidos por la ACSEGURMATICA.

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

### 2.3.3. Lista de los certificados revocados.

Las CRL correspondientes a la ACSEGURMATICA se publicarán en la ubicación referida en el punto 2.2 (c).

Cuando se realice un cambio de estado en los certificados emitidos que modifique la anterior CRL, esta se actualizará en un término no mayor a las 24 horas. En caso de no existir un cambio en los estados de los certificados emitidos, se actualizará esta CRL antes de su fecha de caducidad.

### 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 ACSEGURMATICA 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. Controles de acceso a los repositorios.

El acceso a la información que publica la ACSEGURMATICA sólo permitirá su lectura y/o descarga. La modificación o actualización de la información, queda restringida a los funcionarios de la ACSEGURMATICA que cumplen ese rol. Para ello se establecerán medidas y controles de seguridad que impidan a personas no autorizadas manipular la información publicada en los repositorios.

# 3. IDENTIFICACIÓN Y AUTENTICACIÓN.

## 3.1. Nombres.

### 3.1.1. Tipos de nombres.

La ACSEGURMATICA genera y firma certificados con tipos de nombres conformes al estándar X.509. El nombre distinguido será conformado de acuerdo a lo estipulado en el artículo 12 de la Resolución 2/2016 del MININT.

Para el certificado que se genera, el nombre distinguido (DN), tanto del titular (subject) como del emisor (issuer), está formado por los siguientes atributos:

- CN = Nombre y apellidos
- NIF= Número de identidad
- O = Órgano al cual pertenece
- OU = Organismo u Entidad
- C = País

### 3.1.2. Necesidad de que los nombres sean significativos.

La ACSEGURMATICA 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 SEGURMATICA.

En el caso de una entidad o persona jurídica el nombre debe ser exactamente igual a la razón social, no se admiten nombres abreviados.

En el caso de una persona natural el nombre debe estar conformado por nombres y apellidos tal como figura en el documento identidad permanente o de pasaporte.

### 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 ACSEGURMATICA, 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 ACSEGURMATICA no actúa como árbitro o mediador, ni resuelve disputa alguna respecto a la titularidad de nombres de personas u organizaciones, nombres de dominio, etc. con previa verificación de los datos necesarios para avalar su identidad. 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. Autenticación de identidad de Autoridades de Registro

Las RA vinculadas al modelo de confianza ACSEGURMATICA cumplen el siguiente protocolo:

1. La RA cuenta con la infraestructura tecnológica requerida para realizar las funciones delegadas por ACSEGURMATICA.
2. Existe un contrato en vigor entre ACSEGURMATICA y la RA donde se concretan los aspectos de la delegación y las responsabilidades.
3. La identidad de los operadores de la RA está comprobada y validada.
4. Los operadores de la RA han recibido la información necesaria para el correcto desempeño en sus funciones.

5. La RA asume todas las obligaciones y responsabilidades relativas al desempeño de sus funciones
6. La comunicación entre la RA y ACSEGURMATICA se realiza de forma segura mediante el uso de certificados digitales.

### 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, en las entidades jurídicas, y en el caso de las personas naturales, por el propio suscriptor. Quien entregará todos los datos necesarios para avalar la identidad.

En el caso de las solicitudes para la obtención de certificados SSL el representante del suscriptor, en las entidades jurídicas, y en el caso de las personas naturales, por el propio suscriptor, tiene que entregar la información de titularidad de los nombres de dominios, datos de conectividad y servicios de info-comunicaciones 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 ACSEGURMATICA-ER no aceptará información del suscriptor a ser incluida en el certificado digital, que no pueda ser objeto de verificación.

La ACSEGURMATICA-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 ACSEGURMATICA funge como autoridad de enlace técnico con la ACSCC y esta a su vez 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.

## 3.3. Identificación y Autenticación de solicitudes de renovación de llaves.

La renovación de llaves implica la renovación del certificado. Solamente serán reconocidas como válidas aquellas solicitudes de renovación que sean solicitadas por los representantes de los suscriptores designados por los diferentes Órganos, Organismos o Entidades nacionales, y en el caso de las personas naturales, por el propio suscriptor.

Los procedimientos para la renovación de un certificado se describen en el numeral 4.6 de estas DPC.

## 3.4. Identificación y Autenticación de solicitudes de revocación.

Solamente serán reconocidas como válidas aquellas solicitudes de revocación que sean solicitadas por los representantes de los suscriptores designados por los diferentes Órganos, Organismos o Entidades nacionales, y en el caso de las personas naturales, por el propio suscriptor.

. En los casos de los clientes contratados para que SEGURMÁTICA les brinde el servicio de PKI, el personal designado por el cliente como Administrador de la Autoridad de Registro gestiona las solicitudes de revocación.

De igual forma la ACSEGURMATICA podrá solicitar la revocación de un certificado si tuviera el conocimiento o sospecha del compromiso de la llave privada del suscriptor, o cualquier otro hecho de los dispuestos en el acápite 4.9 Suspensión y revocación de certificados.

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

## 4.1. Solicitud de certificados.

### 4.1.1. Habilitados para solicitar certificados.

La solicitud de un CD puede realizarla cualquier persona, mayor de edad, en plena capacidad de asumir las obligaciones y responsabilidades inherentes a la posesión y uso del certificado.

En el caso de las personas jurídicas, se habilitarán los representantes de los órganos, organismos y entidades, para lo cual presentarán ante la ACSEGURMATICA, un documento legal firmado por máxima autoridad de estos, nombrándolo como representante del mismo.

### 4.1.2. Proceso de solicitud y responsabilidades.

El solicitante de un certificado digital debe suscribir el correspondiente Contrato de Prestación de Servicio de Certificación Digital con la información requerida en el mismo. La ACSEGURMATICA garantizará la protección de los datos de carácter personal, a través de los mecanismos de seguridad dispuestos para tal fin.

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 ACSEGURMATICA, 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. La misma podrá entregarse en los siguientes formatos:

- Escrito y acuñada, acompañada del documento en formato electrónico establecido al efecto.
- Por correo electrónico, firmada digitalmente por el **Representante** del organismo o entidad, a la dirección comercial@segurmatica.cu.

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 ACSEGURMATICA-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 ACSEGURMATICA-ER, los cuales han sido acreditados por la Dirección de SEGURMÁTICA y poseen los medios necesarios para la realización de estas tareas.

Una vez recibida la solicitud en la ACSEGURMATICA-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 ACSEGURMATICA-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 ACSEGURMATICA -ER.

#### 4.2.2. Aprobación o denegación de la solicitud.

La ACSEGURMATICA-ER 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 el titular, o cuando se compruebe la no veracidad de la información proporcionada. El rechazo de la solicitud no impide que se pueda nuevamente iniciar el proceso.

En todos los casos, se notificará al titular la denegación de la solicitud y sus causas.

En el caso de aprobación de la solicitud, la ACSEGURMATICA-ER genera un permiso de emisión firmado digitalmente por el Jefe de esta y lo envía a la ACSEGURMATICA-EC, con la información necesaria para la emisión del certificado digital.

#### 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 ACSEGURMATICA-ER tiene un plazo máximo de diez (7) días hábiles para la ejecución de todo el proceso de aprobación o denegación de la solicitud.

Una vez validados los datos y aprobada la solicitud, la ACSEGURMATICA-ER genera y envía, en un término no superior a los siete (5) días, el permiso de emisión a la ACSEGURMATICA-EC.

### 4.3. Emisión del certificado.

#### 4.3.1. Acciones de la Autoridad Intermedia durante la emisión del certificado.

Una vez recibido en la ACSEGURMATICA-EC la solicitud de emisión del certificado, existirá un plazo no mayor a los dos (2) días, para emitir el CD correspondiente. Una vez generado el CD este se encontrará publicado y disponible para su entrega al titular por parte de la ACSEGURMATICA-ER.

#### 4.3.1.1. Certificados para Firma Digital

En el caso de los certificados para firma digital, el usuario tanto jurídico como natural, después de validar su identidad, presentará la solicitud de emisión del certificado que irá acompañada de la información personal del titular y de un fichero digital .CSR en formato PKCS #10, que contiene parte de la información de solicitud y la llave pública del titular. La ACSEGURMATICA-EC valida la autenticidad e integridad de la solicitud de emisión y a partir de la información contenida en el fichero PKCS #10, se genera el correspondiente certificado digital del titular en la ACSEGURMATICA.

#### 4.3.1.2. Certificados para SSL.

En el caso de los certificados para SSL, la solicitud de emisión irá acompañada de la información personal del titular o entidad que solicita, y la información del sitio o servidor que hará uso del certificado. A partir de dicho momento, se hará uso de los criptomateriales proporcionados por la Dirección de Criptografía del MININT, para la generación del correspondiente fichero digital .CSR en formato PKCS #10, que contiene parte de la información de solicitud y la llave pública del sitio o servidor. La ACSEGURMATICA-EC valida la autenticidad e integridad de la solicitud de emisión y a partir de la información contenida en el fichero PKCS #10, se genera el correspondiente certificado digital del titular en la ACSEGURMATICA.

## 4.4. Aceptación del certificado

### 4.4.1. Forma en que se acepta el certificado

El contrato firmado por la ACSEGURMATICA y el 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. Un solicitante podrá tener varios certificados digitales emitidos bajo diferentes Políticas de Certificación, donde, en todo lo demás relativo a la emisión del certificado, se sujetará a lo estipulado en la misma.

#### 4.4.2. Publicación del certificado.

Una vez generado el certificado, la ACSEGURMATICA–ER notificará al titular que el certificado solicitado ha sido publicado y que podrá ser descargado desde el sitio oficial de la ACSEGURMATICA.

### 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) No transferir a otra persona la llave privada.
c) Solicitar inmediatamente, a la ACSEGURMATICA, la revocación o suspensión del certificado, 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 y detección de inexactitudes en la información.
d) 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 ACSEGURMATICA, cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de renovación del mismo, informando cuando considere o tenga sospechas que la seguridad del sistema ha sido violada o comprometida.

### 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.

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 ACSEGURMATICA, 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 certificado.

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.

La ACSEGURMATICA procesa solicitudes de renovación de certificados que estén en un período de tres (3) meses previos a su expiración. Si el suscriptor desea obtener un nuevo certificado debe solicitar la emisión del mismo, cuando el anterior haya caducado o durante el período de tres (3) meses previos a su expiración.

Una vez presentada la solicitud de renovación se realiza el mismo proceso utilizado para solicitar un certificado.

### 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 necesita 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. Conducta constitutiva de la aceptación del certificado.

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

#### 4.6.5. Publicación del certificado renovado.

El certificado renovado será publicado, de inmediato en el sitio oficial de la ACSEGURMATICA para el acceso de los terceros de buena fe y del suscriptor, siempre que éste autorice su publicación.

#### 4.6.6. Cambio de llave del certificado.

En la ACSEGURMATICA 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.

### 4.7. Modificación del certificado.

Todas las circunstancias que obligarían a efectuar modificaciones en los certificados emitidos a un suscriptor por variación de los datos contenidos en el mismo, también obligarían al cambio del contenedor criptográfico. En la ACSEGURMATICA 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.

### 4.8. Revocación de certificados.

La revocación del certificado ocasiona el cese de la operatividad e impide su uso legítimo. Esto implica su publicación en la Lista de Certificados Revocados (CRL) de acceso público.

Los certificados revocados no podrán bajo ningún criterio volver al estado activo.

### 4.8.1. Circunstancias para la revocación.

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

a) Solicitud formulada por el suscriptor del certificado.

b) Violación o puesta en peligro del secreto de los datos de creación de firma del suscriptor (poseedor del certificado digital), o del prestador de servicios criptográficos de certificación, 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 ante la Autoridad de Registro.

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) Extinción o disolución de la persona jurídica bajo la cual el suscriptor posee y emplea el certificado digital.

g) Alteración de las condiciones de custodia o uso de los datos de creación de la firma digital, que estén reflejadas en los certificados expedidos.

### 4.8.2. Procedimiento de solicitud de la revocación.

El suscriptor o el directivo facultado notifica a la ACSEGURMATICA- ER la revocación del certificado. El jefe de la ACSEGURMATICA-ER evalúa la solicitud de revocación en un plazo no mayor a los tres (3) días hábiles, y en caso de proceder envía la orden de revocación a la ACSEGURMATICA -EC, la cual procederá a hacerla efectiva en un plazo no mayor a las veinticuatro (24) horas.

### 4.8.3. Tiempo dentro del cual la Autoridad Intermedia debe procesar la solicitud de revocación.

La ACSEGURMATICA procesará de manera inmediata cualquier pedido de revocación, una vez que sea de su conocimiento.

#### 4.8.4. Requerimientos para la verificación de la revocación por los terceros de confianza.

Una vez realizada la revocación de un certificado por parte de la ACSEGURMATICA, se publica el estado del mismo en los repositorios de acuerdo a lo señalado en el acápite 2.3 del presente documento.

#### 4.8.5. Frecuencia de emisión de la CRL.

La ACSEGURMATICA mantiene publicada las CRL permanentemente en la URL *https://pki.segurmatica.cu/*

La ACSEGURMATICA genera y actualiza automáticamente la CRL cada veinticuatro (24) horas y luego de una revocación de certificado; y se hace pública diariamente de manera manual en los días laborales.

#### 4.8.6. Disponibilidad de la verificación en línea de la revocación.

Toda la información sobre la revocación de los certificados estará disponible en URL *https://pki.segurmatica.cu/*. Para este propósito se utiliza el protocolo OSCP.

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

En caso de comprometimiento de la llave privada de la ACSEGURMATICA, ésta revocará todos los certificados emitidos y lo notificará a los suscriptores de CD y gestionará con la ACSCC la emisión de un nuevo par de llaves. Obtenidas las nuevas llaves criptográficas se procederá a la emisión de los nuevos certificados a suscriptores que tenían certificados vigentes en el momento de producirse el comprometimiento.

## 4.9. Servicios de comprobación del estado de los certificados.

### 4.9.1. Características operativas.

Para la validación de los certificados la ACSEGURMATICA proporciona el servicio de consulta en línea mediante la Autoridad de Validación, brindando información, en tiempo real, acerca del estado de los certificados digitales; además, publica en su página oficial las CRL.

Para hacer uso del servicio de validación en línea es responsabilidad de los Terceros que confían y del suscriptor disponer de un cliente que implemente el protocolo OCSP.

### 4.9.2. Disponibilidad del servicio.

Los servicios de comprobación del estado de los certificados emitidos por la ACSEGURMATICA están disponibles durante las 24 horas los 7 días de la semana, así como la disponibilidad de descarga de los ficheros CRL.

Entendiendo por disponibilidad, la capacidad de acceder al servicio por parte de quien lo demanda, con independencia de la rapidez o ritmo al que posteriormente éste sea prestado.

La ACSEGURMATICA se reserva hasta un máximo de 3 horas los sábados y domingos alternos y en el horario nocturno de lunes a viernes, para efectuar tareas de mantenimiento, salvas del sistema, etc.

En caso que se produzca una interrupción por causa de fuerza mayor, el servicio se restablecerá en el menor tiempo posible.

## 4.10. 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) Revocación del certificado, por cualquiera de las circunstancias señaladas en el numeral 4.9.1 del presente documento.

### 4.11. Custodia y recuperación de llaves.

#### 4.11.1. Políticas y prácticas de recuperación de llaves.

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

## 5. CONTROLES FÍSICOS Y OPERACIONALES.

### 5.1. Controles físicos.

La ACSEGURMATICA tiene implementadas medidas para controlar la seguridad física y ambiental de las instalaciones, así como los sistemas que garantizan el correcto funcionamiento del prestador de Servicio de Certificación, mediante:

a) Controles de acceso físico.
b) Protección ante desastres naturales.
c) Medidas de protección contra incendios.
d) Fallo de los sistemas de soporte (energía eléctrica, telecomunicaciones, etc.).
e) Inundaciones.
f) Protección antirrobo.
g) Conformidad y entrada no autorizada.
h) Recuperación del desastre.

#### 5.1.1. Ubicación y construcción del local.

Los sistemas de información de la ACSEGURMATICA se ubican en Centro de datos con niveles de protección y solidez de la construcción adecuada y vigilancia durante las 24 horas al día, los 7 días de la semana.

#### 5.1.2. Acceso físico.

El acceso al centro de datos de la ACSEGURMATICA dispone de diversos perímetros de seguridad, con diferentes requerimientos de seguridad y autorizaciones. Entre los equipos que protegen los perímetros de seguridad se encuentran sistemas de control de acceso físico mediante sensor biométrico.

El acceso físico a las instalaciones de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales. Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo.

Las instalaciones cuentan con sistemas de alarma para detección de intrusos.

El acceso a los elementos más críticos del sistema se realiza a través de puntos de control con acceso limitado incrementalmente.

### 5.1.3. Alimentación eléctrica y aire acondicionado

Las instalaciones disponen de sistemas de alimentación ininterrumpida con un nivel de respaldo eléctrico suficiente para mantener autónomamente la red eléctrica durante los períodos de apagado controlado del sistema y para proteger a los equipos frente a fluctuaciones eléctricas que los pudieran dañar.

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

### 5.1.4. Exposición al agua

La ubicación actual y el diseño del Centro de Datos de la ACSEGURMATICA garantizan la inexistencia de peligro por inundación.

### 5.1.5. Protección y prevención contra incendios

El Centro de Datos de la ACSEGURMATICA dispone de sistemas automatizados para la detección de incendios. De igual forma existen medios de extinción alternativos como extintores y formación del personal para actuar ante incendios.

### 5.1.6. Almacenamiento de los medios

La ACSEGURMATICA ha establecido los procedimientos necesarios para disponer de copias de respaldo de toda la información y documentación relativa a la gestión de los certificados, se realizará y resguardará en copias tanto en un disco de almacenamiento externo como en el espacio de almacenamiento del servidor replica o de respaldo del sistema

de la PKI. La copia en el disco de almacenamiento externo se resguardará en la bóveda de la empresa o en el local de la OCIC. El acceso a estos soportes está restringido a personal autorizado.

#### 5.1.7. Seguridad en la reutilización o eliminación de los equipos.

Antes de autorizar la salida de cualquier elemento del equipo que contenga dispositivos de almacenamiento de la ACSEGURMATICA que contengan datos para realizar operaciones de mantenimiento, se procederá a su borrado físico.

#### 5.1.8. Salvas

Periódicamente se realizarán salvas de la información, tanto de la configuración, de los logs o trazas, como de la base de datos; así como copias de las máquinas virtuales que constituyen la PKI de Segurmática, y resguardarán en copias tanto en un disco de almacenamiento externo como en el espacio de almacenamiento del servidor replica o de respaldo del sistema de la PKI, desde donde se restaurarán los datos de las operaciones de la ACSEGURMATICA para continuar brindando el servicio en caso de incidencia grave o caída del Centro de Datos principal. La copia en el disco de almacenamiento externo se resguardará en la bóveda de la empresa o en el local de la OCIC. El acceso a estos soportes está restringido a personal autorizado.

### 5.2. Controles de procedimientos

#### 5.2.1. Roles de confianza

Para el buen desempeño de las actividades dentro del prestador de servicios de certificación, se dividieron las funciones en diferentes roles. Facilitando así el desempeño por separado para su mejor gestión. Estos roles de confianza establecidos para el trabajo son los siguientes:

**Para el trabajo de las ACSEGURMATICA –ER**

**Jefe de Autoridad de Registro:** Director(a) de la UEB Técnico Comercial

a) Garantiza el cumplimiento estricto de la Declaración de Prácticas de Certificación, del reglamento sobre el empleo de los certificados digitales de llave pública para la protección de la información oficial en la República de Cuba, así como la actuación de sus funcionarios acorde al Código de Ética de la misma.
b) Garantiza el cumplimiento de las medidas de seguridad, físicas y lógicas, así como las trazas auditables de los eventos. Responde por la implementación y cumplimiento de medidas para evitar y/o extinguir incendios, inundaciones, excesos de humedad y otros desastres tecnológicos, así como para la salva y restauración segura de la información de interés.
c) Responde por la implementación y cumplimiento de medidas para evitar y/o extinguir incendios, inundaciones, excesos de humedad y otros desastres tecnológicos, así como para la salva y restauración segura de la información de interés.
d) Garantiza la conservación de toda la información relevante sobre las operaciones realizadas en el proceso de registro de solicitudes de emisión, revocación y renovación de los certificados digitales, y la actualización permanente del registro de estos eventos.
e) Garantiza la seguridad de la parte de la Infraestructura de Llave Pública bajo su jurisdicción de forma permanente para identificar posibles debilidades.
f) Atiende y da respuestas a las peticiones, quejas y reclamos hechos por los suscriptores y terceros de buena fe, de conformidad con lo que se establezca en la Declaración de Prácticas de Certificación.

**Custodio de Llave Privada de la Autoridad:** Funcionarios de la PKI designados

a) Responde por la custodia compartida de la llave privada de la Autoridad de Registro. Conoce una parte de las contraseñas de protección para el acceso a la misma.
b) Manipula la llave privada y la contraseña de acceso a la Autoridad de Registro de forma compartida, ante la necesidad de restaurar el sistema informático.

**Atención al público:** Especialistas de la UEB Técnico Comercial

a) Recepciona y registra las solicitudes de: emisión, revocación y renovación de certificados digitales de llave pública y de los documentos, informaciones y ficheros digitales que se requieren para cada tipo de servicio que se solicite.
b) Concerta y firma el contrato de servicios para la emisión de certificados digitales.
c) Informa al suscriptor o a su representante de manera previa o simultánea a la extinción de la vigencia de su certificado digital.

**Verificador:** Especialistas de la UEB Técnico Comercial

a) Comprueba la veracidad y corrección de los datos que aportan los solicitantes en las peticiones.
b) Realiza la verificación de la identidad de cada candidato a suscriptor de un certificado digital para firma digital o de cada responsable de un certificado digital SSL.
c) Realiza para certificado digital SSL, la verificación de la posesión de la licencia correspondientes para la operación en el ámbito de las telecomunicaciones, a través de los sistemas estatales establecidos al efecto. Comprueba la veracidad de la titularidad de los nombres de dominios, datos de conectividad y servicios de infocomunicaciones, que el solicitante requiere proteger.

**Expedidor de permisos de emisión:** Especialistas de la UEB Técnico Comercial

a) Registra y firma digitalmente las solicitudes de emisión, renovación, o revocación que hagan las personas naturales y jurídicas, expidiendo el registro con el correspondiente permiso de emisión para su entrega a la Autoridad de Certificación correspondiente.
b) Realiza la salva de los registros de emisión, renovación, o revocación de un certificado digital.

**Para el trabajo de las ACSEGURMATICA –EC**

**Jefe de Autoridad de Certificación:** Director(a) de la UEB Técnico Comercial

a) Hace cumplir y asume todas las funciones definidas en el Reglamento de la PKI en Cuba y en la Declaración de Prácticas de Certificación para una de Autoridad de Certificación.

b) Verifica y firma digitalmente las solicitudes de emisión y renovación enviadas desde la Autoridad de Registro correspondiente.
c) Aprueba y firma digitalmente las solicitudes de revocación de un certificado digital.
d) Concerta y firma el contrato de servicios para la creación de un prestador de servicios criptográficos de certificación subordinado.
e) Dirige y responde por el cumplimiento de todas las medidas físicas, técnicas y organizativas de la Autoridad de Certificación.
f) Organiza y dirige la realización, según corresponda el sistema de preparación especializada de los funcionarios de los prestadores de servicios criptográficos de certificación subordinados, así como el proceso de evaluación y acreditación de los niveles de profesionalidad alcanzados por cada uno, como condición necesaria de idoneidad para ejercer la actividad.
g) Brinda asesoría técnica y organizativa a los prestadores de servicios criptográficos de certificación subordinados.
h) Funciona de enlace entre la Autoridad de Certificación y la Autoridad Raíz de la PKI en Cuba.
i) Inspecciona y controla el cumplimiento de las medidas de seguridad, física y lógicas, las trazas auditables de los eventos para el aseguramiento del dispositivo de confidencialidad de su llave criptográfica privada, y otros datos y medios requeridos por los suscriptores, así como sistemas técnicos y/u organizativos de control, bloqueo, aviso y seguimiento de acceso y proximidad a los medios de trabajo especializados.
j) Inspecciona y controla el cumplimiento de las medidas para evitar y/o extinguir incendios, inundaciones, excesos de humedad y otros desastres tecnológicos, así como para la salva y restauración segura de la información de interés.
k) Participa en las investigaciones de incidentes que atenten contra la seguridad y fiabilidad de la Autoridad de Certificación.

**Custodios de Llave Privada de la Autoridad:** funcionarios de la PKI designados

a) Responde por la custodia compartida de la llave privada de la Autoridad de Certificación. Conoce una parte de las contraseñas de protección para el acceso a la misma.
b) Manipula la llave privada y la contraseña de acceso a la Autoridad de Certificación de forma compartida, ante la necesidad de restaurar el sistema informático.

**Receptor de datos de permisos de emisión**: funcionarios de la Autoridad de Certificación designados (Administradores de Red designados)

a) Recepciona y verifica los datos definidos en las solicitudes de servicios criptográficos de certificación: emisión, renovación y revocación de certificados digitales y de criptomateriales asociados, aprobadas por la Autoridad de Registro y los registros con los permisos de emisión correspondientes.
b) Firma digitalmente la entrada de permisos de emisión a la Autoridad de Certificación.

**Generador:** Funcionarios de la Autoridad de Registro y Autoridad de Certificación designados

a) Comprueba la veracidad y corrección de los datos que aportan los solicitantes en las peticiones.
b) Genera los criptomateriales asociados a los certificados digitales que emite.
c) Genera los criptomateriales específicos que requieran las Autoridades de Certificación aprobadas y subordinadas.
d) Revoca los certificados digitales solicitados.
e) Genera las listas de certificados revocados (CRL)
f) Descarga el certificado digital y la correspondiente llave privada.
g) Almacena de manera segura las llaves privadas hasta su entrega al propietario del certificado.

**Publicador:** Funcionarios de la Autoridad de Certificación designados (Administradores de Red designados)

a) Publica los certificados digitales emitidos por la Autoridad de Certificación en la web de validación, siempre que los titulares de los mismos hayan autorizado su publicación.
b) Publica la lista de los certificados revocados (CRL) en la web de validación.
c) Define el estado de los certificados digitales publicados en la web de validación, para la consulta en línea de los usuarios y las aplicaciones a través del protocolo OCSP.
d) Publica en la web pública de la Autoridad de Certificación la Declaración de Practicas de Certificación y sus respectivas actualizaciones, así como todas las informaciones y documentos que emita la Autoridad de Certificación para conocimiento de sus usuarios.

**Inspector auditor:**

a) Audita los eventos generados en el ámbito de operación del PSC
b) Está presente en la realización de análisis de situaciones y hechos extraordinarios.

### 5.2.2. Número de personas requeridas por tareas

En la generación de los certificados digitales estarán involucradas las siguientes personas por Rol:

**Para el trabajo de las ACSEGURMATICA-ER**

a) Jefe de Autoridad de Registro: Una Persona
b) Custodio de Llave Privada de la Autoridad: Tres Personas
c) Atención al público: Tres Personas
d) Verificador: Tres Personas
e) Expedidor de permisos de emisión: Tres Personas

**Para el trabajo de las ACSEGURMATICA –EC**

a) Jefe de Autoridad de Certificación: Una Persona
c) Custodios de Llave Privada de la Autoridad: Tres Personas
d) Receptor de datos de permisos de emisión: Tres Personas
e) Generador: Tres Personas

f) Publicador: Tres Personas
g) Inspector auditor: Una Persona

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

Los procesos de autenticación y autorización en el sistema se llevarán a cabo mediante el uso de certificados digitales generados y asociados a las personas que desempeñan los diferentes roles.

### 5.3. Controles del personal

#### 5.3.1. 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 SEGURMATICA, y en particular la ACSEGURMATICA, violatorias del régimen de seguridad y de roles especificados para la operación de estas entidades, se califican como hechos sancionables administrativamente, en correspondencia con la legislación vigente, de acuerdo a la magnitud, fines y daños ocasionados por la violación.

#### 5.3.2. Documentación suministrada al personal

La ACSEGURMATICA 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 para las TIC.
- Declaración de Prácticas de Certificación.
- Plan de Seguridad Informática de SEGURMATICA.
- Documentación relativa a las funciones y procedimientos de cada rol.

### 5.4. Archivo de registros

#### 5.4.1. Tipos de registros archivados

La ACSEGURMATICA 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 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 las DPC.
- Auditorias y controles.

Los controles, modificaciones y auditorías procederán y serán registrados como es debido de acuerdo al Plan de Seguridad Informática de SEGURMATICA.

#### 5.4.2. Período de conservación del archivo.

La ACSEGURMATICA conservará los registros durante un período mínimo de quince (15) años.

#### 5.4.3. Protección del archivo

Los registros se protegen de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada usando controles de acceso lógico y físico.

#### 5.4.4. Procedimiento para la copia de seguridad del archivo

Se generan copias de seguridad del archivo, cumpliendo con lo establecido en la empresa para las salvas de respaldo. Desde el punto de vista tecnológico el equipamiento que contiene la información es redundante.

#### 5.4.5. 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 SEGURMATICA para esos fines.

### 5.5. Cambio de llave

El tiempo de validez del certificado de la ACSEGURMATICA es superior al período de validez de los certificados que emite. Las llaves de la Autoridad Intermedia expiran en el momento que su certificado deja de tener validez. Tres meses antes de la fecha de expiración del certificado, el representante legal de la ACSEGURMATICA solicita a la ACSCC la generación de un nuevo par de llaves y el nuevo certificado digital firmado por ella.

Una vez concluido este proceso, se procede, de forma inmediata, a renovar los certificados de los suscriptores, de forma tal que todo certificado que se genere, luego del cambio de llaves de la ACSEGURMATICA, tenga en su cadena de certificación, el nuevo certificado de la Autoridad Intermedia. La ACSEGURMATICA continúa emitiendo CRL firmadas con la llave privada original, hasta la fecha de vencimiento del último certificado emitido usando el par de llaves original.

## 5.6. Recuperación ante el comprometimiento y desastres

### 5.6.1. Procedimientos para la gestión de incidentes y comprometimiento.

La ACSEGURMATICA 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 ACSEGURMATICA detendrá su funcionamiento, informando de inmediato a todos los suscriptores, 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.

### 5.6.3. Procedimiento ante el comprometimiento de la llave privada

En el supuesto de compromiso o sospecha de comprometimiento de su llave privada la ACSEGURMATICA notificará a los representantes de los suscriptores, revocará los

certificados que se encuentren operativos y publicará la correspondiente CRL. Posterior a la generación del nuevo par de llaves y el nuevo certificado por parte de la ACSCC, la ACSEGURMATICA, procederá a la emisión de los nuevos certificados, a los suscriptores que tenían certificados vigentes en el momento de producirse el comprometimiento.

La ACSEGURMATICA 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 continuidad del negocio ante un desastre

En caso de que se produjese un incidente que implique la no disponibilidad de los servicios de certificación de la ACSEGURMATICA se procederá a la ejecución del Plan de Recuperación de Desastres, garantizando, en la medida de lo posible, que los servicios críticos estén disponibles en menos de setenta y dos (72) horas.

## 5.7. Cese de las operaciones

La ACSEGURMATICA en su condición de Autoridad Intermedia en la jerarquía de la ILP de la República de Cuba, podrá cesar sus actividades de servicios de certificación por decisión de la Dirección de SEGURMATICA debido a condiciones que lo justifiquen.

Las causas que pueden producir el cese de la actividad de la Autoridad de Certificación son:

- Compromiso de la llave privada de la AC.
- Por ley o resolución normativa que así lo designe.
- Ocurrencia de acciones que pongan en duda la integridad operacional de la infraestructura.

En caso de cese de su actividad como Prestador de Servicios de Certificación, ACSEGURMATICA realizará, con una antelación mínima de dos meses, las siguientes acciones:

- Informar a todos los suscriptores de sus certificados y extinguir la vigencia de los mismos revocándolos.

- Informar a todas las terceras partes con las que haya firmado un convenio de certificación.
- Comunicar a la ACSCC del cese de su actividad y del destino que va a dar a los certificados, así como cualquier otra circunstancia relevante relacionada con el cese de actividad.
- Destrucción de las llaves privadas de la ACSEGURMATICA.
- La ACSEGURMATICA no contempla la transferencia de la gestión de los certificados que todavía pudieran estar vigentes en el momento del cese de su operación, por lo que procederá a su revocación.

# 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 ACSEGURMATICA, por ser una PKI autofirmada, se genera en el propio módulo criptográfico del EJBCA como solución implementada de la PKI; el cual cumple los parámetros y requisitos establecidos por la Dirección de Criptografía.

En el diseño y modelo de la PKI ACSEGURMATICA no se genera ningún criptomaterial de ningún cliente, usuario o suscriptor. En el caso de las solicitudes de certificados para firma digital se hará disponible para los usuarios una herramienta para que los mismos generen su propio par de llaves (privada y pública) y sean responsables de su uso; así como de la guarda y custodia de las mismas. Dicha herramienta estará disponible en el sitio web de Segurmática *https://pki.segurmatica.cu/* para su descarga y su empleo en la generación de los correspondientes criptomateriales, y del correspondiente fichero de solicitud de generación de certificados en formato PKCS#10.

En el caso de las solicitudes de certificados SSL, los criptomateriales serán generados y proporcionados por la Dirección de Criptografía de la Republica de Cuba, las cuales se emplearán en el proceso de generación de los correspondientes certificados SSL, y se entregarán a los correspondientes usuarios o suscritores, de conjunto con el correspondiente Sobre-PIN. Los criptomateriales se los entrega al cliente el Funcionario

de la Autoridad de Certificado designado; y el correspondiente Sobre-PIN se lo entrega el Funcionario de la Autoridad de Registro designado. El proceso de entrega tanto de los criptomateriales como del correspondiente Sobre-PIN será adecuadamente documentado.

### 6.1.2. Entrega de la llave privada del suscriptor.

En lo referente a la entrega de la llave privada del suscriptor, la ACSEGURMATICA, reperesentada por alguno de los funcionarios de la Autoridad de Certificados (AC), hará entrega de los correspondientes criptomariales de manera personal a la correspondiente persona natural o a la persona jurídica designada y autorizada. A la vez, también se hará la entrega del correspondiente Sobre-PIN de manera de manera personal a la correspondiente persona natural o a la persona jurídica designada y autorizada, por alguno de los funcionarios de la autoridad de Registro (AR). En el caso de las personas jurídica, la entrega tambien se puediera realizar a traves del sistema de las OCIC de los diferentes Organismos del Estado.

Estos procedimientos solo se aplican en el caso de los criptomateriales relacionados con los certificados SSL; los cuales son generados y suministrados por la Dirección de Criptografía de la Republica de Cuba y a partir de los cuales se generan los correspondientes CSR y Cetificados Digitales.

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

La entrega de la llave pública del suscriptor a la ACSEGURMATICA para la generación del correspondiente Certificados Digital para Firma se hará por medio de un fichero CSR en formato PKCS#10 de conjunto con sus datos personales; el cual será generado por la propia persona jurídica o natural. La engrega de dicho fichero podrá realizarse de manera personal a los funcionarios de la autoridad de Registro (AR) o por medio del correo electrónico comercial@segurmatica.cu.

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

La llave pública de la Autoridad de Certificados ACSEGURMATICA será compartida por medio del Certificado Digital de la propia Autoridad de Certificados que se hará publico en el sitio Web de Segurmatica *https://pki.segurmatica.cu/* para todo el que necesite hacer uso de la mismo.

### 6.1.5. Tamaño de las llaves.

El algoritmo utilizado por la ACSEGURMATICA 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 |
| ACSEGURMATICA (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.

Los módulos utilizados para la generación de las llaves emitidas por la ACSEGURMATICA, cumplen los requerimientos y normas de seguridad establecidos por la Dirección de Criptografía.

### 6.2.2. Control multipersona de la llave privada

La llave privada de la ACSEGURMATICA se encuentra bajo control multipersona. Para el acceso a la copia de seguridad de la llave privada y sus datos de activación se requiere la concurrencia de los funcionarios designados en cada caso; cada uno en posesión de una parte o fragmento de la clave que accede a las llaves de la ACSEGURMATICA.

### 6.2.3. Custodia de la llave privada

La ACSEGURMATICA no admite la realización de copia, almacenamiento o custodia de las llaves privadas de los suscriptores. Sólo mantendrá la custodia de una copia de su propia llave privada. Los criptomateriales generados y proporcionados por la Dirección de Criptografía de la República de Cuba será destruidos de forma segura después de haber sido empleados en la generación de los correspondientes certificados SSL.

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

Al generarse, en el módulo criptográfico, el par de llaves de la ACSEGURMATICA, 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 ACSEGURMATICA y su correspondiente Sobre-PIN, se almacena de manera cifrada en un dispositivo extraíble, el cual se guarda en la OCIC que tiene acceso restrigido.

La llave privada de la ACSEGURMATICA se clasifica como SECRETO.

Los 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 la OCIC.

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

La ACSEGURMATICA opera con su llave privada sobre el propio módulo criptográfico del EJBCA y se mantiene almacenada en él de manera cifrada. Para transferir la llave privada desde o hacia el módulo criptográfico se requiere, además, la presencia de los funcionarios designados que cumplen con el rol de custodio de la llave privada. Una vez instalada la llave esta no puede ser removida hasta tanto no se proceda con su destrucción.

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

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

### 6.2.8. 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.

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

En el módulo criptográfico, antes de generar el par de llaves de la ACSEGURMATICA, 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 ACSEGURMATICA-AC, designa una comisión, presidida por el Jefe de la ACSEGURMATICA-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. Además de la incineración del sobre PIN donde se encuentra el dato de activación de la llave privada.

Todas las operaciones realizadas serán documentadas en actas, haciendo constar cada medio o material destruido.

### 6.2.10. 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 ACSEGURMATICA 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 este 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 |
|---|---|
| ACSCC | 15 años |
| ACSEGURMATICA | 10 años |
| Suscriptores | 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 ACSEGURMATICA se procede de la siguiente forma:

Los funcionarios designados y acreditados como custodios de llave privada, generan cada uno, de manera independiente, una sucesión aleatoria de caracteres Alfa-numérico que es protegida en un Sobre-PIN. La combinación de dichas sucesiones en el orden correspondiente conforman el dato de activación de la llave privada de la autoridad. Por tanto, para la realización de cualquier proceso que necesite de utilizar la llave privada, se necesitará la concurrencia de los funcionarios designados y acreditados para su activación, la cual siempre se realiza en presencia de al menos otro funcionario de la autoridad de acuerdo al proceso a realizar.

### 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 ACSEGURMATICA, los datos de activación de la llave privada además de estar resguardad en la OCIC, es responsabilidad de cada uno de los custodios de la llave privada de la protección de los datos que posee cada uno y que permiten conformar el PIN con el cual se activa la llave privada de la ACSEGURMATICA.

## 6.5. Controles de seguridad computacional.

### 6.5.1. Requerimientos técnicos específicos de seguridad computacional

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

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

Todo movimiento de medios es registrado y controlado. Además, 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 ACSEGURMATICA, 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.

### 6.6.2. Controles de gestión de seguridad

La ACSEGURMATICA 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 Intermedia, que permiten instrumentar y auditar cada fase de los mismos.

### 6.6.4. Controles de seguridad de redes

El trabajo del registro de datos y de generación de certificados y CRL de la PKI ACSEGURMATICA se realiza fuera de línea, por lo tanto, el equipamiento que intervienen en dichos procesos no se encuentra conectado a red alguna; constituyen una red aislada del mundo exterior.

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

# 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 el sistema de la ACSEGURMATICA serán conformes con las siguientes normas:

- Resolución 2/2016 del MININT.
- 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 ACSEGURMATICA, 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 Certificadora SEGURMATICA<br>OU= GEIC<br>O= MINCOM<br>L= Centro Habana<br>ST= La Habana<br>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 2048 bits y algoritmo RSA. |

### 7.1.1. Número de versión

ACSEGURMATICA opera mediante el empleo de certificados digitales X.509 en su versión 3; estándar desarrollado por la Unión Internacional de Telecomunicaciones (Organización Internacional de las Naciones Unidas para coordinación de servicios de redes de telecomunicaciones entre Gobiernos y empresas) para las Infraestructuras de Llave Pública y los Certificados digitales.

### 7.1.2. Extensiones del certificado

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

| **CAMPO** | **VALOR** |
|---|---|
| Uso de la llave | Especifica los usos permitidos de la llave. |
| Uso mejorado de la llave | 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 ACSEGURMATICA 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 ACSEGURMATICA cumplen con la RFC 5280 y contienen los siguientes elementos básicos:

| **CAMPO** | **VALOR** |
|---|---|
| Versión V2 | V2 |
| Emisor | CN= Autoridad Certificadora SEGURMATICA<br>OU= GEIC<br>O= MINCOM<br>L= Centro Habana<br>ST= La Habana<br>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 | 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 ACSEGURMATICA emite las CRL en formato X.509 versión 2.

#### 7.2.2. Extensiones de la CRL.

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

| CAMPO | VALOR |
|---|---|
| Número CRL | Número consecutivo. |
| 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. |

### 7.3. 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.

#### 7.3.2. Formato de nombres

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

#### 7.3.3. Campos y extensiones del certificado

El perfil del certificado del OCSP responder que emite la ACSEGURMATICA es:

| CAMPO | CONTENIDO |
|---|---|
| Versión | X509 v3 |
| Número de serie | XXXXXXXXXXXXX |
| Algoritmo de firma | sha512RSA |
| DN del Emisor | CN= Autoridad Certificadora SEGURMATICA<br>OU= GEIC |

| | |
|---|---|
| | O= MINCOM<br>L= Centro Habana<br>ST= La Habana<br>C= CU |
| Validez | 10 años |
| Sujeto | CN= Autoridad de validación<br>OU= GEIC<br>O= MINCOM<br>L= Centro Habana<br>ST= La Habana<br>C= CU |
| Información de la llave pública del sujeto | RSA (4096 bits) |
| Identificador de llave del sujeto | Derivada de utilizar la función de hash SHA-1 sobre la llave pública del sujeto. |
| Identificador de llave de la Autoridad | Derivada de utilizar la función de hash SHA-1 sobre la llave pública de la AC emisora. |
| Usos de la llave | Firma digital o SSL |
| Usos extendido de la llave | Firmador OCSP |

### 7.3.4. Formato de las peticiones OCSP

Se soporta la extensión Nonce (id-pkix-ocsp-nonce) tal y como contempla la norma para evitar “replay attacks”.

### 7.3.5. Formato de las respuestas

El OCSP responder del servicio de validación es capaz, al menos, de generar respuestas de tipo id-pkix-ocsp-basic.

**Respecto al estado de los certificados**:

- “Revoked”, para aquellos certificados emitidos por la ACSEGURMATICA que se encuentren revocados.
- “Good”, para aquellos certificados emitidos por la ACSEGURMATICA y que no estén revocados. El estado “good” es simplemente una respuesta “positiva” a la petición OCSP, indica que el certificado no está revocado, pero no implica necesariamente que el certificado se encuentra dentro del período de validez.
- “unknown” si la petición corresponde a una AC emisora desconocida.

**Respecto a la semántica de los campos:**

- “producedAt” contiene el instante de tiempo en el que el OCSP responder genera y firma la respuesta.
- “thisUpdate”, indica el momento en el que se establece que el estado definido en la respuesta es correcto.
- “thisUpdate” de la CRL que se haya utilizado. En el resto de casos se utilizará la fecha local.
- “nextUpdate”, indica el instante de tiempo en el que se dispondrá de nueva información de revocación. En el caso de certificados revocados deberá contener el campo “nextUpdate” de la CRL que se ha utilizado, salvo cuando la fecha de “nextUpdate” sea anterior a la fecha local. En el resto de casos no se establecerá el campo nextUpdate, lo que es equivalente según la RFC 2560 a indicar que se puede disponer de nueva información de revocación en cualquier momento, con lo que es responsabilidad del cliente volver a consultar cuando lo estime oportuno.

## 8. Auditoría de conformidad

### 8.1. Frecuencia de los controles para cada entidad

Se llevará a cabo una auditoría sobre ACSEGURMATICA, al menos una vez al año, para garantizar la adecuación de su funcionamiento con las disposiciones incluidas en esta DPC. El MININT se reserva el derecho de realizar controles al prestador en el momento que considere necesario.

Se llevarán a cabo otras auditorías técnicas y de seguridad recogidas en el plan de seguridad informática de SEGURMATICA.

### 8.2. Identificación del auditor

El auditor será establecido por la Dirección del Servicio Central Cifrado del MININT, con experiencia en auditorías a Prestadores de Servicios de Certificación, con previa presentación a los directivos de SEGURMATICA que garantizan y responden por el servicio.

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

Al margen de la función de auditoría, el auditor y la parte auditada (ACSEGURMATICA) no deberán tener ninguna relación, actual o planificada, financiera, legal, o de cualquier otra clase que pueda derivar en un conflicto de intereses. En cumplimiento de lo establecido en la normativa vigente en nuestro ordenamiento sobre protección de datos de carácter personal, y habiendo tenido en cuenta de que, para el cumplimiento, por parte del auditor, de los servicios regulados en el contrato será preciso acceder a los datos de carácter personal de los ficheros titularidad de la ACSEGURMATICA.

### 8.4. Tópicos cubiertos por el control

La auditoría determinará la conformidad de los servicios de ACSEGURMATICA con esta DPC. También determinará los riesgos del no cumplimiento de la adecuación con la operativa definida por esos documentos. Los aspectos cubiertos por una auditoría incluirán, pero no estarán limitados a:

- Política de seguridad.
- Seguridad física.
- Evaluación tecnológica.
- Administración de los servicios de la CA.
- DPC

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

Una vez recibido el informe de la auditoría llevada a término, la ACSEGURMATICA discute, con la entidad que ha ejecutado la auditoría las deficiencias encontradas, desarrolla y ejecuta un plan de medidas para solucionar dichas deficiencias.

Si la ACSEGURMATICA es incapaz de desarrollar y/o ejecutar dicho plan, o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema se realizará una de las siguientes acciones:

- Revocar la llave de la ACSEGURMATICA, de la forma como se describe en las secciones correspondientes de esta DPC.
- Finalizar la prestación del servicio de la ACSEGURMATICA, de la forma como se describe en la sección correspondiente de esta DPC.

### 8.6. Comunicación de los resultados

El auditor comunicará los resultados de la auditoría al funcionario responsable por el funcionamiento del PSC, al director (a) de SEGURMATICA, así como a los responsables de las distintas áreas en las que se detecten no conformidades.

## 9. Requisitos legales y comerciales

### 9.1. Tarifas

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

Las tarifas de emisión, revocación y renovación de cada certificado se encuentran publicadas en el sitio oficial de SEGURMATICA *https://pki.segurmatica.cu/*

#### 9.1.2. Tarifa de acceso a los certificados

El acceso a los certificados emitidos, dada su naturaleza pública, es libre y gratuito y por tanto no es de aplicación ninguna tarifa sobre los mismos.

### 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 basado en CRLs y 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 aplicará ninguna tarifa por el servicio de información sobre esta. El acceso a esta información está público en el sitio oficial de SEGURMATICA *https://pki.segurmatica.cu/*

### 9.1.5. Política de reintegros

Sin estipulación adicional.

## 9.2. Capacidad financiera

### 9.2.1. Indemnización a los terceros que confían en los certificados emitidos por la ACSEGURMATICA.

Ante la materialización de hechos extraordinarios referentes al proceso de certificación o protección de los datos de los implicados en los distintos procesos, y en los cuales la ACSEGURMATICA sea encontrada responsable del mismo por las entidades dispuestas para ello, se realizará el pago por concepto de indemnización a los suscriptores empleando los recursos económicos a su disposición para afrontar el riesgo de la responsabilidad por daños y perjuicios ante los usuarios y terceros.

### 9.2.2. Relaciones fiduciarias

ACSEGURMATICA no se desempeña como agente fiduciario ni representante en forma alguna de suscriptores ni de terceros que confían en los certificados emitidos por la ACSEGURMATICA

### 9.2.3. Procesos administrativos

ACSEGURMATICA garantiza la realización de auditorías de los procesos y procedimientos establecidos de manera regular. Estas auditorías se llevarán a cabo tanto de manera interna como externa.

## 9.3. Política de confidencialidad

### 9.3.1. Información confidencial

Se declara expresamente como información confidencial, que no podrá ser divulgada a terceros, excepto en aquellos supuestos previstos legalmente:

- La llave privada de la ACSEGURMATICA.
- Toda información relativa a los parámetros de seguridad, control y procedimientos de auditoría.
- Toda la información de carácter personal proporcionada a ACSEGURMATICA durante el proceso de registro de los suscriptores de certificados, con la salvedad de lo especificado por el contrato de certificación.
- La información de negocio suministrada por sus proveedores y otras personas con las que la ACSEGURMATICA tiene el deber de guardar secreto establecida legal o convencionalmente.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.

### 9.3.2. Información no confidencial

ACSEGURMATICA considera información de acceso público:

- La contenida en la Declaración de Prácticas de Certificación aprobada por la ACSEGURMATICA.
- Los certificados emitidos, así como las informaciones contenidas en éstos.
- La lista de certificados revocados (CRL).

### 9.3.3. Divulgación de la información de revocación de certificados

La información relativa a la revocación de certificados es publicada en el sitio de Segurmática *https://pki.segurmatica.cu/* y consultada mediante CRL u OCSP.

## 9.4. Protección de datos personales

La ACSEGURMATICA no almacena datos de carácter privado de los suscriptores más allá de aquellos que se recogen en las planillas de solicitud y que se añaden al certificado digital reconocido de la identidad del propietario.

### 9.4.1. Plan de protección de datos personales

La Entidad de Certificación no divulga ni cede datos personales, excepto en los casos previstos por concepto de auditorías.

### 9.4.2. Información considerada privada

Se consideran datos de carácter privado la información personal que no haya de ser incluida en los certificados. En cualquier caso, los siguientes datos son considerados como información privada:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados.
- Llaves privadas generadas y/o almacenadas de la ACSEGURMATICA.

Los datos captados por el Prestador de Servicios de Certificación tienen la consideración legal de datos de nivel básico.

### 9.4.3. Información no considerada privada

Esta información hace referencia a la información personal que se incluye en los certificados y en el referido mecanismo de comprobación del estado de los certificados, de acuerdo con la sección 3.1 de este documento. La información no tiene carácter privado, por imperativo legal (“datos públicos”), pero solo se publica en el depósito si lo consiente el suscriptor.

En todo caso, es considerada no confidencial la siguiente información:

- Los certificados emitidos.
- La vinculación del suscriptor a un certificado emitido por la ACSEGURMATICA.
- El nombre y los apellidos del suscriptor del certificado, así como cualesquiera otras circunstancias o datos personales del titular, en el supuesto que sean significativas en función de la finalidad del certificado, de acuerdo con este documento.
- La dirección electrónica del suscriptor del certificado.
- Los usos y límites económicos reseñados en el certificado.
- El período de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (CRLs), así como el resto de informaciones de estado de revocación.
- La información contenida en el sitio oficial de la ACSEGURMATICA.

### 9.4.4. Responsabilidades

La ACSEGURMATICA garantiza el cumplimento de sus obligaciones legales como prestador de servicios de certificación, de conformidad con lo expuesto en este documento, y en virtud de esto, responderá por los daños y perjuicios que cause en el ejercicio de la actividad por el incumplimiento de las prescripciones relativas a la protección de datos personales.

### 9.4.5. Prestación del consentimiento del uso de datos personales

Para la prestación del servicio, la ACSEGURMATICA habrá de obtener el consentimiento de los titulares de los datos necesarios para prestación los servicios de certificación. Se entenderá obtenido el consentimiento con la firma del contrato de certificación por parte del usuario.

### 9.4.6. Comunicación de la información a autoridades administrativas y/o judiciales

La ACSEGURMATICA sólo podrá comunicar informaciones calificadas como confidenciales o que contengan datos de carácter personal en aquellos supuestos en los que así se le requiera por la autoridad pública competente y en los supuestos previstos legalmente.

En concreto, la ACSEGURMATICA está obligada a revelar la identidad de los suscriptores cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tengan atribuidas y que así se lo requiera.

## 9.5. Derechos de propiedad de intelectual

Todos los derechos de propiedad intelectual incluyendo los referidos a certificados y CRL's emitidos por la ACSEGURMATICA, la presente DPC, así como cualquier otro documento, electrónico o de cualquier otro tipo, propiedad de ACSEGURMATICA, pertenecen a la ACSEGURMATICA.

Las llaves privada y pública son propiedad del suscriptor, independientemente del medio físico que se emplee para su almacenamiento.

## 9.6. Obligaciones y responsabilidad civil

### 9.6.1. Obligaciones de la Entidad de certificación

La ACSEGURMATICA se obliga a cumplir lo siguiente:

- Garantizar bajo su plena responsabilidad, que se cumpla con todos los requisitos establecidos en este documento.
- Prestar los servicios de certificación de acuerdo con este documento, en el que se detallan al menos los contenidos previstos legalmente.
- Antes de la emisión y entrega del certificado al suscriptor, la ACSEGURMATICA lo informa de los aspectos legales.
- Cumplir con su Declaración de Prácticas de Certificación.

- Publicar su certificado digital y garantizar su acceso por terceros.
- Manifestar que la información contenida en el certificado es correcta.
- Cumplir la ley aplicable y jurisdicción competente.
- Identificar al suscriptor del certificado, de acuerdo con el presente documento.

### 9.6.2. Garantías ofrecidas a suscriptores

La ACSEGURMATICA, como mínimo, garantiza al suscriptor:

- El cumplimiento de sus obligaciones legales como prestador de servicios de certificación, de acuerdo con esta DPC.
- Que no haya errores en la información contenida en los certificados, debido a falta de diligencia en los procedimientos de emisión y renovación.
- Que los certificados cumplan todos los requisitos materiales establecidos en la correspondiente DPC.
- Cumplir con los límites que se establezcan en el contrato de servicio.

Adicionalmente, la Entidad de Certificación garantiza que el certificado contiene la información suficiente que lo acredita como un certificado reconocido.

## 9.7. Renuncia de garantías

La ACSEGURMATICA puede rechazar todas las garantías del servicio que no se encuentren vinculadas a las obligaciones establecidas por la presente DPC.

## 9.8. Limitaciones de responsabilidad

### 9.8.1. Garantías y limitaciones de garantías

La ACSEGURMATICA puede limitar su responsabilidad mediante la inclusión de límites de uso del certificado.

### 9.8.2. Deslinde de responsabilidades

La ACSEGURMATICA no asume ninguna responsabilidad en caso de pérdida o perjuicio:

- De los servicios que prestan, en caso de guerra, desastres naturales o cualquier otro caso de fuerza mayor.
- Ocasionados por el uso de certificados que exceda los límites establecidos.
- Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por ACSEGURMATICA.
- Ocasionados al firmante o terceros de buena fe si el destinatario de los documentos firmados electrónicamente no comprueba ni tiene en cuenta las restricciones que figuren en el certificado en cuanto a sus posibles usos, o cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado publicada en la CRL, o cuando no verifique la firma electrónica.

## 9.9. Plazo y finalización

### 9.9.1. Plazo

La ACSEGURMATICA establece, en sus instrumentos jurídicos con los suscriptores, una cláusula que determina el período de vigencia de la relación jurídica en virtud de la que suministran certificados a los suscriptores.

### 9.9.2. Finalización

La ACSEGURMATICA establece, en sus instrumentos jurídicos con los suscriptores, una cláusula que determina las consecuencias de la finalización de la relación jurídica en virtud de la que suministran certificados a los suscriptores.

## 9.10. Notificaciones

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las prácticas descritas en esta 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 contenidas en el punto 1.5 de esta DCP.

Las comunicaciones electrónicas se harán efectivas una vez que las reciba el destinatario al que van dirigidas.

### 9.11. Resolución de conflictos

#### 9.11.1. Resolución extrajudicial de conflictos

La ACSEGURMATICA podrá establecer, a través de los instrumentos jurídicos mediante los que se articule su relación con suscriptores y auditores, los procedimientos de mediación, arbitraje y resolución de conflictos que se consideren oportunos, todo ello sin perjuicio de la legislación de procedimiento administrativo.

### 9.12. Legislación aplicable

El funcionamiento y operaciones de ACSEGURMATICA, así como la presente DPC están regidos por la legislación comunitaria y estatal vigente en cada momento. Explícitamente se asumen como de aplicación las siguientes normas:

• Decreto Ley 199 Sobre la Seguridad y Protección de la Información Oficial diciembre 1999.

• Resolución No. 2 del Ministro del Interior. Julio 2002.

• Resolución No. 2 del Ministro del Interior. Septiembre 2016.