EMPRESA DE INFORMÁTICA AUTOMÁTICA Y COMUNICACIONES

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

ENTIDAD PRESTADORA DE SERVICIOS CRIPTOGRÁFICOS DE CERTIFICACIÓN (PSCC)

ACTECNOMATICA

(Versión 1.0)

ENERO 2022

"AÑO 64 DE LA REVOLUCIÓN"

RELACIÓN DE REVISIONES

Rev. 01	Nombres y Apellidos	Cargo	Firma	Fecha
Elaborado por:	Soraya del C. López Galbán.	Esp Princ. B Seguridad Informática		30/01/2022
	Yesneiler Matos Quintero	EP Tecn Com, Elect, Autom y S.Tecn		30/01/2022
	Zenia Ivis Meneses Santiesteban	Esp. B Ciencias Inf.		30/01/2022
Revisado por:	Idanelys Tirado Rubio	Dir. UEB Infocomunicaciones		30/01/2022
	Betty Iznaga Alarcón	Esp. Gestión de la Calidad		30/01/2022
	Lourdes Ramos López	Esp. Gestión de la Calidad		30/01/2022
Aprobado por:	Armando Estévez Alonso	Director General		30/01/2022

Contenido

1 INTRODUCCIÓN

Tecnomática, Empresa de Informática Automática y Comunicaciones de la Unión Cuba Petróleo - Cupet, como parte del proceso de transformación digital, incluido en la política de Informatización y Automatización que lleva adelante, fortalece la seguridad y protección de la Información e incrementa la seguridad de sitios, aplicaciones web y canales de Infocomunicaciones utilizados por sus usuarios al Certificarse, mediante la Instrucción No.7 del Jefe de la Dirección de Criptografía del Ministerio del Interior (RS: 0001215), con el acrónimo ACTECNOMATICA, como PRESTADOR CORPORATIVO DE SERVICIOS DE CONFIANZA que le autoriza la emisión de certificados digitales de los clientes de sus servicios y aplicaciones informáticas, en particular la Unión Cuba-Petróleo a la que pertenece la empresa, lo que asegura la autenticidad del firmante, ahorra tiempo, papel, agiliza los trámites entre entidades, incrementa la seguridad de sus conexiones electrónicas y la seguridad de las transacciones de información digital que lo utilicen, garantizando la identidad, autenticidad, integridad, confidencialidad y no repudio, de los archivos digitales que se intercambian en la red.

El presente documento Declaración de Prácticas de Certificación (en lo adelante DPC) muestra las principales pautas que regulan el funcionamiento de la Infraestructura de Llave Pública de Tecnomática.

1.1 PRESENTACIÓN

En cumplimiento del Decreto de Ley 199/99, la Resolución No. 2/2016 emitida por el Ministro del Interior y su Declaración de Prácticas de Certificación (DPC) en este documento se describen las políticas, prácticas y procedimientos implementados por Tecnomática para el funcionamiento y operación de la Infraestructura de Llave Pública (PKI), se detallan las normas y condiciones generales de los servicios de certificación que presta la Autoridad de Certificación ACTECNOMATICA, en relación con la gestión de los datos de creación y verificación de los certificados digitales, las condiciones aplicables a la solicitud, expedición, uso y extinción de la vigencia de estos, las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados.

Su estructura y contenido está basada en los siguientes documentos regulatorios oficiales de la República de Cuba:

- Decreto Ley 199/1999
- Resolución 2/2016 del Ministerio del Interior

- Declaración de Prácticas de Certificación de la Autoridad Raíz ACSCC
- Buenas prácticas de experimentadas Autoridades de Certificación externas

1.2 NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

Este documento se titula "Declaración de Prácticas de Certificación" (versión 1.0) de la Autoridad de Certificación (ACTECNOMATICA), Certificado digital emitido el 1 de febrero del 2021, vigente hasta el 1 de febrero del 2029 disponible en sitio web de la entidad https://actecnomatica.cupet.cu.

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 Tecnomática, se subordina a la Autoridad Raíz constituida por la Autoridad de Certificación Servicio Central Cifrado, genera y firma certificados con tipos de nombres conformes al estándar X.509.

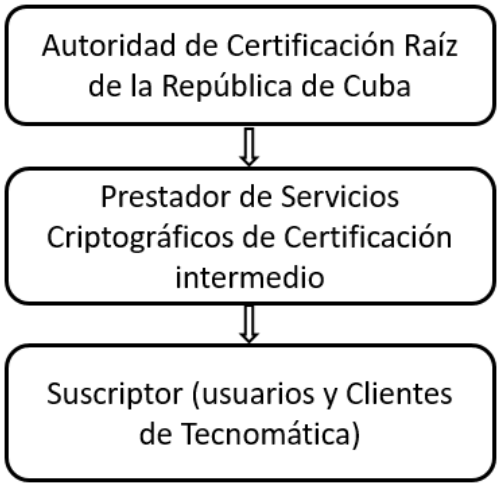

Figura 1 Jerarquía de ACTECNOMATICA

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

A través de esta Infraestructura de Llave Pública se puede establecer y mantener un entorno de red seguro para la Empresa Tecnomática y sus clientes, posibilitando el uso de certificados para la firma digital, la autenticación de usuarios y aplicaciones, y la protección de canales de comunicación con una amplia gama de aplicaciones.

Las entidades y personas participantes en la ACTECNOMATICA:

- Empresa Tecnomática como titular de la ACTECNOMATICA
- Autoridad de Certificación (CA)
- Autoridades de Registro (RA)
- Autoridad de Validación (VA)
- Autoridad de Sellado de Tiempo
- Repositorio de Certificados
- Solicitantes
- Suscriptores
- Terceros de buena fe

1.3.2 Autoridad de Certificación (AC)

La Autoridad de Certificación Raíz de la República de Cuba 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. El certificado digital de esta autoridad raíz es auto firmado 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 del Servicio Central Cifrado (ACSCC).

A continuación, se presentan los datos más relevantes del certificado de la ACTECNOMATICA:

Campo	Contenido	I	C	T
Versión	X.509 V.3	S		F
Número de serie	008bb2c97001	S		F
Algoritmo de firma	SHA512RSA	S		F
DN del emisor	E=admonpki@mail.mn.co.cu, CN=Autoridad de Certificación Servicio Central Cifrado, OU=Autoridad Raíz, O=Infraestructura de Llave Pública de la República de Cuba, L=Boyeros, ST=La Habana, C=CU	S		F
Validez	8 años	S		F
DN del sujeto	CN=Autoridad de Certificación Tecnomática, OU=Cupet, O=Ministerio de Energía y Minas, L=Centro Habana, ST=La Habana, C=CU	S		F
Limitaciones básicas	CA, Sin restricción de longitud de ruta	S	X	F
Usos de la llave	Firma digital, Firma de certificados, Firma CRL sin conexión, Firma de revocación de certificados (CRL) (86)	S	X	F
Huella digital	5a64a805b153e9899425f1295c6bf85bfb0e0084	S		F
Llave pública	RSA (4096 bits)	S		F

Leyenda de la tabla:

I = Incluida. Posibles valores: S=Siempre, O=Opcionalmente, C=Condicionalmente

C = Crítica. Si se marca la casilla, indica que es crítica.

T = Tipo. Posibles valores: D = Dinámica, F = Fijada. Fijada quiere decir que el valor es el mismo para todos los certificados de este tipo.

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

La Autoridad de Certificación Intermedia ACTECNOMATICA, subordinada a la Autoridad de Certificación Raíz, se encarga de emitir, revocar y renovar los certificados digitales. De igual forma firma cada uno de los certificados que emite, mantiene actualizado su estado mediante la publicación de Listas de Revocación de Certificados en los repositorios de certificados, mediante el servicio de validación, también proporciona el servicio estampado de tiempo de la firma digital.

1.3.3 Autoridades de Registro (RA o AR)

La Autoridad de Registro es la entidad delegada por la Autoridad de Certificación para atender y registrar las peticiones, comprobando la identificación y autenticación de los solicitantes de los certificados, con el fin de garantizar que las solicitudes contienen información veraz y completa de los Solicitantes, y que la misma se ajuste a los requisitos exigidos en la correspondiente Política de Certificado.

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 ACTECNOMATICA, 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 ACTECNOMATICA.

Funciones de la Autoridades de Registro subordinadas a la ACTECNOMATICA:

- 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 los Representantes de las entidades 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.
- Emitir la certificación oficial de aprobación de la identificación y autenticación realizada a la información del solicitante
- Gestionar con la CA la emisión del Certificado Digital de Llave Pública solicitado

- Alertar a las entidades y titulares de Certificados Digitales de Llave Pública bajo su control, la proximidad de la fecha de caducidad del mismo y el procedimiento a seguir para la renovación de este

1.3.4 Autoridad de Validación (AV)

La Autoridad de validación de la ACTECNOMATICA, 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. Este mecanismo de validación es complementario a la emisión y publicación de las CRL.

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 ACTECNOMATICA.

1.3.5 Autoridad de Sellado de Tiempo

La Autoridad de Sellado de Tiempo de la ACTECNOMATICA, 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 (Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)) y en la RFC 3628 (Policy Requirements for time-Stamping Authorities (TSA)).

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

1.3.6 Repositorio de Certificados

El repositorio de certificados es un almacén público desde donde los usuarios pueden obtener las llaves públicas de los certificados emitidos por la ACTECNOMATICA. Este repositorio será un servidor de almacenamiento en la nube donde se publican los certificados de los clientes, con acceso a través de un link en la página web, que permite la visualización, búsqueda y descarga de los Certificados, que pudiera servir además como soporte para el empleo del certificado en el cifrado de los datos entre una o varias entidades.

1.3.7 Solicitante

Es la persona jurídica que solicita, mediante un Representante legal, definido previamente mediante un contrato o previa identificación, la emisión de un certificado digital.

1.3.8 Suscriptores

Son los usuarios 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 titular 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 titulares finales son los mismos definidos como suscriptores, exceptuando a los Prestadores de Servicios Criptográficos de Certificación.

1.3.9 Terceros de buena fe

Son las personas o entidades (diferentes al titular del certificado digital) que de forma voluntaria deciden aceptar y confiar en los certificados digitales emitidos por la ACTECNOMATICA. La parte que confía debe asegurarse que el Certificado es apropiado para el uso al que ha sido destinado, que se encuentra vigente y conocer sus características expresadas en la PC y la presente DPC, según las cuales se emitió el Certificado Digital de Llave Pública.

1.4 USO DE LOS CERTIFICADOS

En la Infraestructura de Llave Pública de Tecnomática, los certificados digitales pueden utilizarse para garantizar la protección de la información oficial que se procese, se trasmita o almacene con la utilización de las tecnologías de la información y otros medios electrónicos. Los Certificados 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:

- **Certificados de personas o entidades**. Son los certificados digitales que se expiden a personas naturales o jurídicas, para la firma digital de mensajería y documentos electrónicos
- **Certificados de Autoridades de Certificación.** Son los certificados digitales que se expiden a las Autoridades de Certificación, que se determine subordinar a la ACTECNOMATICA

- **Certificados tecnológicos**. Son los certificados digitales SSL/TLS y VPN que se expiden para equipamientos tecnológicos, servidores, clientes, aplicaciones informáticas, etc., para la protección de canales y servicios de comunicaciones

1.4.1 Uso apropiado de los certificados

Atendiendo al 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/TLS o CD -VPN

Los diferentes tipos de certificados emitidos por la ACTECNOMATICA, 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 Uso prohibido de los certificados

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

a) 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

b) Los Certificados Digitales no pueden utilizarse para actuar ni como Autoridad de Registro ni como Autoridad de Certificación, firmando certificados de llave pública de ningún tipo, ni CRL

c) No están permitidas alteraciones sobre los certificados emitidos por la ACTECNOMATICA

d) Se considera prohibida toda acción que contravenga las disposiciones, obligaciones y políticas estipuladas en la presente DPC

e) 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

f) ACTECNOMATICA no está autorizada para recuperar los datos cifrados en caso de pérdida de la llave privada del Suscriptor porque la AC por seguridad no guarda la llave privada de los suscriptores, por tanto, es responsabilidad del suscriptor la protección de los datos de su llave privada

1.5 DETALLES DEL CONTACTO

1.5.1 Organización de la Administración de la DPC

Esta Declaración de Prácticas de Certificación fue redactada y revisada por un equipo de trabajo multidisciplinario, compuesto por el personal que integró el equipo de proyecto PKI–Tecnomática, creado con el objetivo de implementar la Infraestructura de Llave pública en la empresa, especialistas de calidad, además de especialistas de la UEB de Infocomunicaciones que participaron, 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 que determina la coherencia entre la DPC y las Políticas

Todo comentario o sugerencia relativa a esta Declaración de Prácticas de Certificación, puede ser dirigido al buzón de la PKI de la empresa Tecnomática pkitm@tm.cupet.cu, o al teléfono 78767115, donde será atendido por el personal especializado responsable de la elaboración, registro, mantenimiento y actualización de la DPC, las políticas(PC) y demás documentación asociada al Prestador de Servicio de Certificación Criptográfico ACTECNOMATICA.

1.5.3 Procedimiento de aprobación de las Declaraciones de Prácticas de Certificación

La organización y sistema documental de la ACTECNOMATICA, garantiza la existencia y la aplicación de los procedimientos, el correcto mantenimiento de la Declaración de Prácticas de Certificación (DPC) y de las especificaciones de servicio aquí relacionadas, elaborados según lo establecido en el numeral 1.5.4 de la DPC de la Autoridad Raíz de la República de Cuba.

Una vez elaborado la propuesta de políticas y de Declaración de Prácticas de Certificación, son aprobadas por la Dirección de Criptografía del Ministerio del Interior, luego de comprobar el cumplimiento de los requisitos establecidos.

1.6 DEFINICIONES Y ACRÓNIMOS

1.6.1 Definiciones

Se incluyen todas las definiciones establecidas en el Artículo 4 del "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". **Anexo 1** Definiciones de conceptos establecidas en el Artículo 4 de la Resolución 02/2016.

1.6.2 Acrónimos

ACSCC	Autoridad de Certificación Servicio Central Cifrado
ACTECNOMATICA	Autoridad de Certificación Intermedia TECNOMÁTICA
ACTECNOMATICA-EC	Entidad Certificadora de la Autoridad de Certificación Intermedia TECNOMÁTICA
ACTECNOMATICA-ER	Entidad Registradora de la Autoridad de Certificación Intermedia TECNOMÁTICA
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 certificado
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 o AR	Autoridad de Registro

RFC	Petición de Comentario
Sub CA	Autoridad Certificadora Subordinada
NCR	Nodo Central de la Red

2 RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIOS

2.1 REPOSITORIOS

La ACTECNOMATICA dispone de repositorios, accesibles desde Internet desde el sitio https://actecnomatica.cupet.cu , donde se publica su certificado, los certificados que esta ha emitido, las CRL (Lista de certificados revocados, la que puede ser descargada desde http://crl.cupet.cu), la DPC y otras informaciones relativas a la ACTECNOMATICA y un servicio de validación en línea del estado de los Certificados Digitales de Llave Pública, que implementa el protocolo OCSP, con acceso libre a través de Internet http://ocsp.cupet.cu

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.

ACTECNOMATICA se reserva hasta un máximo de 1 hora los sábados y domingos alternos y en el horario nocturno de lunes a viernes para efectuar tareas de mantenimiento, salvas del sistema, etc.

Si existiera 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 la 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 durara más de 48 horas.

El repositorio de ACTECNOMATICA no contiene ninguna información de naturaleza confidencial. ACTECNOMATICA no utiliza ningún otro repositorio operado por ninguna organización distinta a ella.

2.2 PUBLICACIÓN DE INFORMACIÓN SOBRE CERTIFICACIÓN

Es responsabilidad de ACTECNOMATICA publicar la información actualizada de su Declaración de Práctica de Certificación, sus Políticas de Certificación, los Contratos de Prestador de Servicio, su Tarifa de Precio, así como la información referente a su certificado y el estado actualizado de las listas certificados que emite y revoca (CRL), la llave pública de su certificado

digital firmado por la Autoridad Raíz en formato X509 y las bases de datos actualizadas del servicio de validación en línea que implementa el protocolo OCSP, todos enlazados desde la dirección: https://pkitm.cupet.cu/.

Además en los certificados digitales emitidos, se especifica en el campo Punto de distribución CRL, la dirección url de las listas de los certificados revocados (CRL), para ser descargada por los usuarios http://crl.cupet.cu y en el campo Acceso a la información de Autoridad, la url (http://ocsp.cupet.cu) de las bases de datos del servicio de validación en línea que implementa el protocolo OCSP.

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

El Certificado Digital de Llave Pública de la ACSCC y la ACTECNOMATICA son públicos y se encuentran disponibles en el sitio web oficial (https://actecnomatica.cupet.cu/).

2.3 FRECUENCIA DE PUBLICACIÓN

2.3.1 Certificado digital de la Autoridad Intermedia de TECNOMÁTICA

El certificado generado por la ACSCC se publica con anterioridad al comienzo de la prestación del servicio en el sitio oficial de ACTECNOMATICA. 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 ocho años.

2.3.2 Certificados digitales emitidos por ACTECNOMATICA

Los certificados digitales emitidos por ACTECNOMATICA, se publicarán automáticamente, una vez realizada la salva de los certificados generados por esta, en un plazo no mayor a las 24 horas.

2.3.3 Lista de los certificados revocados (CRL)

Las CRL correspondientes a la ACTECNOMATICA 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 automáticamente y se publicaran una vez realizada la salva, en un plazo 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 de forma automática una vez producida la emisión, suspensión o revocación de un certificado y podrán ser consultados mediante el servicio de validación en línea siempre disponible, a través de la autoridad de validación en **http://ocsp.cupet.cu** .

ACTECNOMATICA 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.

2.3.5 Controles de acceso a los repositorios

El acceso a la información que publica ACTECNOMATICA sólo permitirá su lectura y/o descarga. La modificación o actualización de la información, queda restringida a los funcionarios de ACTECNOMATICA 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 ACTECNOMATICA 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, que incluye como campos obligatorios el nombre y apellidos (**CN**), el número del carnet de identidad (**NIF**), la organización o entidad a la que pertenece (**O**), el OSDE-Ministerio del organismo al cual pertenece (**OU**), y el País (**C**).

El atributo “C” (countryName) se codificará de acuerdo a “ISO 3166-1-alpha-2code elements”, en PrintableString, en el caso de Cuba (CU) en mayúscula, el resto de atributos se codificarán en UTF8.

3.1.2 Necesidad de que los nombres sean significativos

El certificado emitido por la ACTECNOMATICA garantiza que los nombres distinguidos (**DN**) sean únicos y significativos, lo que permite establecer la identificación unívoca del suscriptor o titular del certificado y vincular su identidad con la clave o llave 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 (Infraestructura de llave Pública) de TECNOMÁTICA.

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 de identidad permanente o de pasaporte.

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

3.1.4 Reglas para la interpretación de los diferentes formatos de nombres

Para la interpretación de los nombres distinguidos (**DN**) en los certificados emitidos por la ACTECNOMATICA, se utilizan las reglas descritas en la ISO/IEC 9595 (X.500) Distinguished Name (DN). Para todos los atributos se utiliza la codificación UTF8. Y las reglas definidas en el Artículo 12 de la Resolución 2/2016 del MININT.

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.

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

3.1.6 Solución de conflictos relativos a nombres

La ACTECNOMATICA 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 Métodos de prueba de la posesión de la llave privada Generación y construcción de un PKCS#12 descargable

La Autoridad de Registro (RA), previa comprobación de la identidad del solicitante, confirmada a través de los Representantes que la solicitan, una vez que el suscriptor siguiendo las

instrucciones facilitadas en el sitio para la solicitud del servicio, seleccionó el tipo de certificado y registró correctamente los datos de la entidad final que corresponda, la RA emite una notificación de aprobación, dándole la posibilidad al solicitante con la misma contraseña con que se auto registró , realizar la solicitud del tipo de certificado registrado, debiendo esperar 30 minutos para obtener el criptomaterial en formato PKCS#12 .

EL criptomaterial con la llave privada es accesible sólo a través de medios que conoce exclusivamente el suscriptor y permanece bajo su custodia.

3.2.2 Autenticación de identidad de Autoridades de Registro

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

La RA cuenta con la infraestructura tecnológica requerida para realizar las funciones delegadas por ACTECNOMATICA.

Existe un contrato en vigor entre ACTECNOMATICA y la RA subordinada en caso de existir, donde se concretan los aspectos de la delegación y las responsabilidades.

La identidad de los operadores de la RA está comprobada y validada.

Los operadores de la RA han recibido la capacitación e información necesaria para el correcto desempeño en sus funciones.

La RA asume todas las obligaciones y responsabilidades relativas al desempeño de sus funciones.

La comunicación entre la RA y ACTECNOMATICA se realiza de forma segura mediante el uso de certificados digitales.

3.2.3 Autenticación de la identidad de una entidad

En la solicitud de un certificado digital para una entidad, el jefe de órgano, organismo o entidad interesado durante el proceso se contratación nombrará un Representante, el cual entregará, además de sus datos generales identificativos, toda la información que avale la existencia legal de la entidad, del Director de la entidad, y su objeto social.

El grupo comercial que integra la Autoridad de Registro comprobará en los registros legales correspondientes, establecidos por el estado cubano, la veracidad de la información entregada.

3.2.4 Autenticación de la identidad de una persona jurídica

Las solicitudes de certificados para las personas jurídicas se realizan por parte del Representante del suscriptor, quien avala la identidad y veracidad de los datos de las solicitudes realizadas.

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

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

3.2.5 Información no verificada del suscriptor

No se aceptará por parte de la ACTECNOMATICA-ER información del suscriptor a ser incluida en el certificado digital, que no pueda ser objeto de verificación. La gestión comercial de la Autoridad de Registro realizará la verificación de los datos que se solicitan al suscriptor, conforme a lo establecido en los numerales 3.2.3 y 3.2.4 de esta DPC.

3.2.6 Validación de Autoridad

La veracidad de los cargos incluidos en los certificados, está avalada por la firma en la solicitud realizada por el Representante aprobado por la máxima dirección de la empresa.

La ACTECNOMATICA 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, previo proceso de contratación.

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

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITUDES DE REVOCACIÓN

Serán reconocidas como válidas sólo aquellas solicitudes de revocación que sean solicitadas por los representantes de los suscriptores designados por los diferentes Órganos, Organismos o Entidades nacionales.

De igual forma la ACTECNOMATICA 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 numeral 4.9 Suspensión y revocación de certificados.

4 REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS

Las especificaciones contenidas no varían las estipulaciones previstas en las Políticas de Certificados definidas para los distintos tipos de certificados emitidos por la ACTECNOMATICA.

4.1 SOLICITUD DE CERTIFICADOS

4.1.1 Habilitados para solicitar certificados

La solicitud de los Servicios de Certificados Digitales (CD) Criptográficos sólo puede realizarla los Representantes nombrados por los Directores Generales de las organizaciones superiores de dirección empresarial (OSDE) y Organismos de la Administración Central del Estado (OACE) que contratan el servicio de la ACTECNOMATICA presentado como parte del contrato, en documento legal firmado (Anexo 1 del contrato) por la máxima autoridad de la entidad, nombrando el personal que los representará en las solicitudes de los servicios de Certificados Digitales (CD).

4.1.2 Proceso de solicitud y responsabilidades

La empresa interesada en el servicio de CD, deberá llenar el correspondiente Contrato de Prestación de Servicio de Certificación Digital con la información requerida en el mismo.

La ACTECNOMATICA garantizará la conservación, protección y privacidad de los datos que nos faciliten, a través de los mecanismos de seguridad dispuestos para tal fin.

La persona designada como Representante de los suscriptores de su ámbito, es responsable de garantizar la veracidad de los datos que suministra en los formularios (vía web) o planillas (entrega presencial) y de los documentos acreditativos requeridos, enviados o entregados a la Sección de contratación. La misma podrá entregarse:

- En las oficinas comerciales de Tecnomática impreso, firmado y acuñado, acompañada del contrato en formato digital
- Vía web, completando y firmando en formato electrónico mediante la interfaz pública en la sección de contratación en la página web de la PKI
- Vía correo electrónico, podrá enviar el contrato Escaneado a la sección de contratación por el buzón pkitm@tm.cupet.cu

En los contratos con **solicitudes de certificados tecnológicos (SSL y VPN)**, el Representante del suscriptor del organismo o entidad interesada, dentro de los datos solicitados en la planilla informará los datos generales identificativos de los candidatos a responsables de la custodia de ese certificado (la persona responsable de su activación), acompañado de la titularidad del dominio a proteger, además de la información sobre las características del equipamiento técnico donde funcionará.

La protección de la información de los solicitantes está dada por:

- La información de los titulares de certificados viaja por canal seguro HTTPS
- Los permisos para el envío por la interfaz pública de la PKI, se le asignan a los Representantes, aprobados por el Director General de la entidad solicitante
- La solicitud de certificados solo es visible para el Jefe de la ACTECNOMATICA-ER (AR)

4.2 Procesamiento de la solicitud del certificado

4.2.1 Realización de las funciones de identificación y autenticación

Compete al grupo comercial que integra la Autoridad de Registro la comprobación de la identidad del solicitante, la verificación de la documentación 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 y la constatación de que la empresa solicitante ha firmado y pagado el Contrato de Prestación de Servicio de Certificación Digital. También durante el proceso de acreditación de los suscriptores en el sitio se realiza la verificación de que sean válidas las direcciones de correo referenciadas.

De existir objeciones con los datos identificativos presentados, la Autoridad de Registro devuelve la solicitud para que los datos sean rectificados.

El rechazo de la solicitud no impide que pueda iniciarse el proceso nuevamente.

Las funciones de autenticación de los datos en la RA externa la realizan los propios suscriptores durante el proceso de auto registro referenciado en el instructivo **Generación de una solicitud de Certificado Digital en la ACTECNOMATICA** publicado el sitio web de la PKI, el Representante debe orientar a todos los suscriptores de su ámbito, la dirección del sitio (https://actecnomatica.cupet.cu) donde deberán crearse una cuenta.

De existir contradicciones con los datos identificativos presentados de los futuros titulares de certificados, el grupo comercial devuelve la solicitud al Representante de la entidad que realizó la solicitud para que sean rectificados.

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

4.2.2 Aprobación o denegación de la solicitud

La ACTECNOMATICA-ER (RA) 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, el grupo comercial notificará al titular la denegación de la solicitud y sus causas.

En el caso de aprobación de la solicitud por el grupo comercial, el Representante le hace saber a los aspirantes a certificado, la necesidad de crearse una cuenta en el Sitio de la PKI, desde donde recibirá las instrucciones para Solicitar en el sitio el tipo de certificado aprobado. El Administrador de la ACTECNOMATICA-ER (RA), luego de verificar los datos introducidos por el aspirante, autoriza la creación de la nueva entidad final, una vez que el usuario, seleccionó el tipo de certificado y registró correctamente los datos que se reflejan en el certificado, dándole la posibilidad al solicitante con la misma contraseña con que se auto registró, generar la creación del tipo de certificado registrado, debiendo esperar 30 minutos el suscriptor para ejecutar el paso de obtener para su descarga el criptomaterial en formato PKCS#12 .

4.2.3 Plazo para el procesamiento de la solicitud de un certificado

A partir de la recepción del Modelo solicitud entregado por el Representante una vez registrados los usuarios en el sitio de la PKI la ACTECNOMATICA-ER (RA) tiene un plazo máximo de diez (10) 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 ACTECNOMATICA-ER genera y envía, en un término no superior a los 3 (tres) días hábiles, (ya incluido en el plazo anterior) el permiso al usuario para que proceda a crearse y posteriormente descargarse desde el Sitio de la PKI el certificado Digital emitido.

4.3 EMISIÓN DEL CERTIFICADO

La emisión del certificado tendrá lugar una vez que la RA (ACTECNOMATICA-ER) y los suscriptores hayan realizado el proceso descrito en el numeral 4.2 para el Procesamiento de las solicitudes, siguiendo las instrucciones que para ello se le notifica por correo y que además están públicas en el sitio de la PKI.

4.3.1 Acciones de la Autoridad Intermedia durante la emisión del certificado

Cada vez que la ACTECNOMATICA-ER (RA) detecte la entrada de un nuevo usuario en el sitio de la PKI, revisa en cuáles de las solicitudes de las entidades está incluido, asignándole el roll que le corresponde el cual le permite tener acceso a la Autoridad de Registro para auto gestionarse el tipo de certificado aprobado en el Modelo de solicitud entregado por el Representante, siguiendo los pasos referenciados en el instructivo facilitado para la Generación de una solicitud.

Siempre que la ACTECNOMATICA-EC (CA) emite un certificado digital almacenará el mismo en su repositorio de certificados el cual publica en el sitio web oficial de la PKI. La entrega a los usuarios de los materiales criptográficos, dependerá fundamentalmente que estos no olviden el usuario y contraseña con que se acreditaron en la Autoridad de Registro, siguiendo las instrucciones que una vez acreditados se les orienta desde el Sitio de la PKI.

De igual forma la ACTECNOMATICA-EC (RA) mantiene informado al Representante a través del sitio oficial del estado de completamiento de los usuarios incluidos en las solicitudes que han finalizado el proceso y han descargado sus criptomaterial desde la Autoridad de Registro.

Simultáneamente la ACTECNOMATICA-ER notifica al suscriptor cuando es aceptada su solicitud y puede crearse el certificado probado; garantizando de esta manera que solamente este último tenga acceso al criptomaterial donde está contenida la llave privada de su certificado digital.

Un solicitante podrá tener varios certificados digitales emitidos bajo diferentes Políticas de Certificación, para lo cual estará sujeto a lo estipulado en cada una de ellas.

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

4.4 ACEPTACIÓN DEL CERTIFICADO POR EL SOLICITANTE

La aceptación de las responsabilidades, obligaciones y usos relacionada con los diferentes tipos de certificados por parte de los Representantes se produce en el momento de la firma del "Contrato de Prestación de Servicios de Certificación Digital Criptográficos" asociado a cada Política de Certificado. El contrato será firmado, en forma manuscrita o digital, por la máxima Dirección de la entidad solicitante o el Representante por el nombrado.

La aceptación del contrato implica el conocimiento y aceptación por parte del solicitante de lo estipulado en la Declaración de Prácticas de Certificación (DPC) y Política de Certificado asociada.

4.4.1 Certificados para Firma Digital (PFirma)

En el caso de los certificados para firma digital, el usuario aprobado en la solicitud realizada por el Representante, después de acreditarse en el sitio, deberá seguir las orientaciones que recibirá por correo, para auto generarse su Certificado. El titular sólo podrá utilizar su llave privada y su Certificado Digital de Llave Pública para los usos autorizados en la PC

correspondiente y en la presente DPC, de acuerdo con lo establecido en los campos KeyUsage y ExtendedKeyUsage del Certificado.

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

Las terceras partes que confían, antes de aceptar y confiar en un Certificado Digital de Llave Pública emitido por la ACTECNOMATICA, la parte que confía debe asegurarse que, el Certificado Digital es apropiado para el uso al que ha sido destinado, que se encuentra vigente y conoce sus características expresadas en la PC correspondiente y en la presente DPC.

4.4.2 Certificados para SSL y VPN

En el caso de estos certificados tecnológicos, la solicitud de emisión irá acompañada de la información personal del candidato responsable de la custodia e implementación de los certificados, quien se desempeña como suscriptor al hacer uso del certificado.

El Grupo Comercial valida la autenticidad y veracidad de la información adicional facilitada por el Represente, quien informa al Administrador de la AR (Admin. ACTECNOMATICA-ER) para aprobar la solicitud, debiendo seguir los mismos pasos descritos en el numeral anterior.

El contrato firmado por la ACTECNOMATICA y el Representante o Director, 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 la presente DPC**, así como el adecuado empleo de la PC de los certificados digitales de llave pública y de los criptomateriales.

Un suscriptor 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 el mismo.

4.4.3 Publicación del certificado

Una vez generado y firmado el certificado, este será publicado, de forma automática por el servicio OCSP. Los certificados publicados siempre podrán ser descargados desde el sitio oficial de la ACTECNOMATICA.

4.5 USO DEL CERTIFICADO Y EL PAR DE LLAVES

4.5.1 Uso de la llave privada por parte del suscriptor

El suscriptor posee una llave pública y una llave privada legalmente válidas durante el periodo de vigencia del certificado y solo podrá utilizar el par de llaves y el certificado tras aceptar las condiciones de uso establecidas en la DPC y en la Política de Certificado (PC)

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 y resguardarla en lugar seguro

c) Solicitar inmediatamente, a la ACTECNOMATICA, la revocación o suspensión del certificado, en caso de tener conocimiento o sospecha del comprometimiento de la seguridad de la llave privada 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 ACTECNOMATICA, 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 ACTECNOMATICA, 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 ACTECNOMATICA 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 y está interesado en continuar utilizando el certificado digital. También cuando han existido cambios en los datos contenidos en el Certificado Digital y cuando las llaves estén comprometidas o han perdido fiabilidad.

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

En cualquier caso, la renovación de un Certificado Digital de Llave Pública está supeditada a que se realice atendiendo al Modelo de Solicitud de Renovación establecido y que la solicitud de renovación se refiera al mismo tipo de Certificado Digital emitido inicialmente.

La RA, deberá notificar al titular o representante acreditado, con la debida antelación, la proximidad de la fecha de expiración del Certificado Digital de Llave Pública.

4.6.2 Personas habilitadas para solicitar la renovación

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

4.6.3 Procesamiento de la solicitud del certificado

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

4.6.4 Notificación al suscriptor de la emisión del nuevo certificado

Según se establece en el numeral 4.3.1 de esta DPC.

4.6.5 Conducta constitutiva de la aceptación del certificado

Según se establece en el numeral 4.1.1 de esta DPC.

4.6.6 Publicación del certificado renovado

El certificado renovado será publicado, de inmediato en el sitio oficial de la ACTECNOMATICA para el acceso de los terceros de buena fe y del suscriptor, siempre que éste no prohíba por solicitud expresa su publicación.

4.6.7 Notificación de la emisión del certificado renovado a otras entidades

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

4.7 CAMBIO DE LLAVE DEL CERTIFICADO

En la ACTECNOMATICA no se permite el cambio de llave de un certificado. Cuando se requiera realizar un cambio de llaves, es necesario solicitar de revocación revocar y realizar la solicitud de un nuevo certificado.

4.8 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 ACTECNOMATICA 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 revocación y la emisión de un nuevo certificado.

4.9 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.

4.9.1 Circunstancias para la revocación

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

- Solicitud formulada por el suscriptor del certificado
- 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
- Resolución judicial o administrativa que lo disponga
- Fallecimiento del suscriptor, acreditada legalmente la defunción por su representante ante la Autoridad de Registro
- 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
- Extinción o disolución de la persona jurídica bajo la cual el suscriptor posee y emplea el certificado digital
- Alteración de las condiciones de custodia o uso de los datos de creación de la firma digital, que estén reflejadas en los certificados expedidos
- Cese en la actividad del prestador de servicios criptográficos de certificación salvo que, previo consentimiento expreso del suscriptor, a través de su representante, la gestión de los certificados digitales expedidos por aquél se transfiera a otro prestador de servicios de la Infraestructura
- Alteración de los datos aportados para la obtención del certificado digital
- Modificación de las circunstancias verificadas para la expedición del mismo, como las relativas al cargo o a las facultades de representación, de manera que este ya no sea conforme a la realidad
- Incumplimiento en el pago de los servicios criptográficos de certificación contratados

4.9.2 Procedimiento de solicitud de la revocación

El titular de un certificado, el representante o la máxima Dirección puede notificar al Comercial la solicitud de revocación del certificado en el modelo establecido, utilizando cualquiera de las vías disponible, documento firmado digitalmente por el sitio web o por correo electrónico, o presencial en las oficinas Quienes luego de evaluarla notifican al administrador de la ACTECNOMATICA-ER, los datos para proceder a ejecutar la revocación en

la plataforma, la cual procederá a hacerla efectiva en un plazo no mayor a las veinticuatro (24) horas hábiles después de haber sido solicitada.

La ACTECNOMATICA puede revocar los certificados por decisión propia, cuando las circunstancias de seguridad de la Infraestructura, o de la información o por funciones del suscriptor así lo requieran, informando sobre la revocación en un término no mayor a las veinticuatro (24) horas al Órgano, Organismo o Entidad que ampara al suscriptor afectado.

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

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

4.9.3 Tiempo dentro del cual la Autoridad Intermedia debe procesar la solicitud de revocación

La ACTECNOMATICA procesará de forma inmediata cualquier pedido de revocación, una vez que sea de su conocimiento.

4.9.4 Requerimientos para la verificación de la revocación por los terceros de confianza

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

4.9.5 Frecuencia de emisión de la CRL

La ACTECNOMATICA mantiene publicada las CRL permanentemente en la URL http://ocsp.cupet.cu

La ACTECNOMATICA genera y actualiza automáticamente la CRL luego de una revocación de certificado; y se hace pública inmediatamente. Con frecuencia diaria, en días laborables, la ACTECNOMATICA publicará una CRL de tipo delta, siempre y cuando se produzcan suspensiones o revocaciones de Certificados. (http://deltacrl.cupet.cu)

Con frecuencia semanal, todos los miércoles, en el horario comprendido entre las 23:30 y las 24:00 horas, la ACTECNOMATICA publicará una CRL acumulativa. (http://crl.cupet.cu)

4.9.6 Disponibilidad de la verificación en línea de la revocación

La ACTECNOMATICA posee un servidor OCSP para la verificación en línea del estado de los certificados según se define en la RFC 2560. Toda la información sobre la revocación de los certificados estará disponible desde un vínculo de su página oficial (https://pkitm.cupet.cu) y directamente en la URL http://ocsp.cupet.cu.

Para garantizar la vitalidad del servicio OCSP, se implementó un clúster mediante nginx de respondedores OCSP y se garantizó que las máquinas virtuales siempre estén en servidores físicos distintos para el caso de que falle alguno.

4.9.7 Requerimientos especiales para el caso del comprometimiento de la llave privada

En caso de comprometimiento de la llave privada de la ACTECNOMATICA, 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 todos los suscriptores que tenían certificados vigentes en el momento de producirse el comprometimiento.

4.10 SERVICIOS DE COMPROBACIÓN DEL ESTADO DE LOS CERTIFICADOS

4.10.1 Características operativas

Para la validación de los certificados la ACTECNOMATICA 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 listas de certificados revocados (CRL).

Para hacer uso del servicio de validación en línea estará disponible la url http://crl.cupet.cu aunque es responsabilidad de los Terceros que confían y del suscriptor disponer de un cliente que implemente el protocolo OCSP.

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

4.10.2 Disponibilidad del servicio

Los servicios de comprobación del estado de los certificados emitidos por la ACTECNOMATICA 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 ACTECNOMATICA se reserva hasta un máximo de 1 hora los sábados y domingos alternos y en el horario nocturno de lunes a viernes, para efectuar tareas de mantenimiento, salvas del sistema, etc. (numeral 2.1).

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

4.11 FINALIZACIÓN DE LA SUSCRIPCIÓN

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

a) Caducidad de la vigencia del certificado digital

b) Revocación del certificado, por cualquiera de las circunstancias señaladas en el numeral 4.5.1c del presente documento

4.12 CUSTODIA Y RECUPERACIÓN DE LLAVES

4.12.1 Políticas y prácticas de recuperación de llaves

En el marco de la ILP (Infraestructura de Llave Pública) de la República de Cuba, ni la ACTECNOMATICA, ni cualquier otro PSCC, almacenarán la llave privada de ningún certificado digital de suscriptor emitido para firma digital.

5 CONTROLES FÍSICOS Y OPERACIONALES

5.1 CONTROLES FÍSICOS

El perímetro físico de seguridad de la ACTECNOMATICA comprende el área donde se generan los certificados digitales y se encuentran en operación en servidores del Nodo Central de la Red requeridos para prestar el servicio de certificación digital, donde se tienen 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 incendio.
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 ACTECNOMATICA se ubican en el Nodo Central de la Red con niveles de protección y solidez del local donde está ubicada y vigilancia tecnológica durante las 24 horas al día, los 7 días de la semana.

5.1.2 Acceso físico

El acceso al Nodo central de la Red 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 y sistemas de video vigilancia y de grabación, así como sistemas detección de intrusos.

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

El Nodo Central de la Red de la ACTECNOMATICA garantiza la inexistencia de peligro por inundación. Se encuentra en el segundo nivel del edificio del Ministerio de Energía y Minas, a la misma altura que el Despacho Nacional de la Electricidad.

5.1.5 Protección y prevención contra incendios

El Nodo Central de la Red de la ACTECNOMATICA dispone de sistemas automatizados para la detección y extinción 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 ACTECNOMATICA 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 conservará durante un período mínimo de quince (15) años, gestionados con el control de acceso implícito en el Sistema Papyrus implementado en la empresa. Se realizan salvas de las máquinas virtuales, en caso de que ocurra algún incidente se recupera la maquina en cuestión con la última salva y si es necesario se restaura la salva de la base de datos que se hace diaria. Este proceso de restaura no lleva mucho tiempo ya que las máquinas virtuales no deben crecer mucho en volumen. Esto es válido para el firewall de borde de la zona PKI, y máquinas virtuales EJBCA, OCSP y TSA.

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

5.1.7 Mantenimiento de los equipos

Todo trabajo de reparación o mantenimiento a un equipo de la ACTECNOMATICA solamente podrá ser realizado previa coordinación con administrador del servidor y el Custodio de la llave primaria de la ACTECNOMATICA, aprobado previamente por el Director General y debe quedar registrado en el Registro de Incidencias de la Seguridad Informática.

5.1.8 Seguridad en la reutilización o eliminación de los equipos

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

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

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

5.1.9 Protección de los activos

El acceso a los activos dentro de la PKI de la ACTECNOMATICA está dado por:

- Controles de acceso
- Acceso al software EJBCA solo de los usuarios conectados a una VPN implementada exclusivamente para este servicio
- Los roles definidos dentro de la ACTECNOMATICA solo tienen acceso a los recursos que le permita realizar sus funciones en el software EJBCA

5.1.10 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 Tecnomática, y resguardarán en los servidores de salva del Nodo Central de la Red (NCR) 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 ACTECNOMATICA para continuar brindando el servicio en caso de incidencia grave o caída del NCR. Para mayor seguridad se establecer un mecanismo de publicación de estas salvas a través de un ftp con SSL que facilite quemarlas en disco para puedan ser guardado en la Norma de control. El acceso a estos soportes está restringido a personal autorizado. También se realizan las salvas de las máquinas virtuales según se describe en el numeral 5.1.6.

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 Criptográfica ACTECNOMATICA, se dividieron las funciones en diferentes roles. Facilitando así el desempeño por separado para su mejor gestión. Estos roles o grupos administrativos se dividen en 5:

- Administrador general de la ACTECNOMATICA
- Administrador de AC
  Generador, publicador de CD
- Administrador de AR
  Verificador
  Atención al público y contratación de los servicios
- Supervisor
- Administrador de infraestructura

5.2.2 Funciones de los Roles

1. **Administrador general de la ACTECNOMATICA:** Encargado de la configuración de los perfiles de certificado, perfiles de entidad final, publicadores y servicios. Responde por la custodia compartida de la llave privada de la Autoridad de Certificación, la administración de los roles y de los aspectos generales del sistema.

- Garantiza el cumplimiento estricto de las funciones definidas en el Reglamento de la PKI en Cuba, en la Declaración de Prácticas de Certificación, así como la actuación de sus funcionarios acorde al Código de Ética de la misma
- 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
- 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
- Dirige y responde por el cumplimiento de todas las medidas físicas, técnicas y organizativas de la Autoridad de Certificación
- Organiza y dirige la realización, según corresponda del 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
- Funciona de enlace entre la Autoridad de Certificación y la Autoridad Raíz de la PKI en Cuba

- Vela que estén públicos los certificados digitales emitidos por la Autoridad de Certificación en la web de validación, para la consulta en línea de los usuarios y las aplicaciones a través del protocolo OCSP
- Mantiene actualizada en la web pública de la AC, la Declaración de Prácticas de Certificación, así como las informaciones y documentos que emita la Autoridad de Certificación para conocimiento de sus usuarios
- Brinda asesoría técnica y organizativa a los prestadores de servicios criptográficos de certificación subordinados

2. **Administrador de AC (ACTECNOMATICA–EC):** Encargado de aprobar la emisión, revocación y renovación de los certificados digitales, así como de la actualización de las Listas de Revocación de Certificados (CRL).
    - Brinda asesoría técnica y organizativa a los prestadores de servicios criptográficos de certificación subordinados
    - Almacena de manera segura los criptomateriales hasta su entrega al propietario del certificado
    - **Generador de CD:** Genera los criptomateriales asociados a los certificados digitales que emite la ACTECNOMATICA
    - Genera los criptomateriales específicos que requieran las Autoridades de Certificación aprobadas y subordinadas
    - Revoca los certificados digitales solicitados
    - Genera las listas de certificados emitidos y revocados (CRL)
3. **Administrador de AR (ACTECNOMATICA–ER):** Encargado de verificar, registrar y firmar digitalmente los datos suministrados por los representantes de los solicitantes.
    - Procesa las peticiones de revocación y renovación de los certificados
    - Comprueba la veracidad y corrección de los datos que aportan los solicitantes en las peticiones
    - 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
    - Atención al público: Recepciona y registra los contratos con 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

- Concierta el contrato de servicios para la emisión de certificados digitales y para la creación de un prestador de servicios criptográficos de certificación subordinado
- Informa al suscriptor o a su representante de manera previa o simultánea a la extinción de la vigencia de su certificado digital

- **Verificador:** Comprueba la veracidad y corrección de los datos que aportan los solicitantes en las peticiones
  - 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
  - Comprueba la veracidad de la titularidad de los nombres de dominios, datos de conectividad y servicios de Infocomunicaciones, que el solicitante requiere proteger
  - Realiza para certificado digital SSL, la verificación de la posesión de la licencia correspondiente para la operación en el ámbito de las telecomunicaciones, a través de los sistemas estatales establecidos al efecto

4. **Supervisor:** Encargo de auditar los eventos generados en el ámbito de operación del Prestador de Servicios Criptográficos, está presente en la realización de los análisis de situaciones y hechos extraordinarios.
   - Inspecciona y controla el cumplimiento de las medidas de seguridad, física y lógicas
   - Inspecciona y controla 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
   - Inspecciona los sistemas técnicos y/u organizativos de control, de bloqueo, de aviso y seguimiento de acceso y proximidad a los medios de trabajo especializados

- Supervisa 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
- Participa en las investigaciones de incidentes que atenten contra la seguridad y fiabilidad de la Autoridad de Certificación
- Controla que se mantengan actualizados y publicados en la web de validación, para la consulta en línea de los usuarios y las aplicaciones a través del protocolo OCSP, los certificados digitales emitidos por la Autoridad de Certificación
- Supervisa la seguridad de la Infraestructura de Llave Pública, de forma permanente identificando posibles debilidades

5. **Administrador de infraestructura:** Encargado del monitoreo y control de todos los sistemas informáticos que emplea el **P**ortador de **S**ervicios **C**riptográficos ACTECNOMATICA, responde por la custodia compartida de la llave privada de la Autoridad de Certificación, por la seguridad de la infraestructura y los servicios que publica.
    - Garantiza la implementación y cumplimiento de medidas de seguridad en el local tecnológico de los servidores, así como la salva y restauración segura de la información de interés
    - 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

5.2.3 Número de personas requeridas por tareas

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

a) Para la generación de certificados

En la generación de los certificados digitales estarán involucradas al menos tres personas que cumplan con los roles de Administrador de AR, Administrador de AC y Administrador general de la ACTECNOMATICA

b) Para la activación de la AC

Para ejecutar las tareas de activación/desactivación de las llaves de la ACTECNOMATICA se requiere una comisión formada por tres personas donde dos de ellas esté en posesión de un fragmento de la llave que garantiza la administración total de la Autoridad de Certificación y una para supervisar y garantizar el proceso y entrega del sobre sellado en la OCIC

5.2.4 Identificación y autenticación para cada rol

Los funcionarios de la ACTECNOMÄTICA fueron aprobados por la máxima Dirección de la Empresa. Para los procesos de autenticación y autorización en el sistema cada funcionario posee su propio certificado digital emitido por la ACTECNOMATICA. Las acciones permitidas para cada rol en el software EJBCA son asignadas de acuerdo las funciones que estos realicen.

5.2.5 Roles que requieren separación de funciones

Los roles de la **ACTECNOMATICA-ER** son incompatibles con los roles de la **ACTECNOMATICA-EC** y viceversa. Los roles Supervisor y Administrador de Sistema son incompatibles con el resto de los roles definidos.

5.3 CONTROLES DEL PERSONAL

5.3.1 Requerimientos de calificación y experiencia

Todo el personal que labora en la ACTECNOMATICA ha sido debidamente preparado para las funciones que realiza.

5.3.2 Requerimientos de formación y capacitación

El personal de la Autoridad de Certificación está sujeto a un plan de formación específico para el desarrollo de su función dentro de la organización, entre los que se incluyen:

- Formación y actualización de los aspectos legales (leyes y resoluciones) relativos a la prestación de servicios de Certificación criptográficos
- Conocimientos básicos de la criptografía Asimétrica y sus aplicaciones
- Formación en seguridad y políticas de confidencialidad de los sistemas de información requeridos en virtud de su roll
- Políticas de certificación digital y la DPC
- Conocimiento y aceptación del código de ética

- Capacitación en los procedimientos de operación y uso de las Aplicaciones informáticas requeridas para los diferentes roll a desempeñar

5.3.3 Requerimientos y frecuencia de la recalificación

La ACTECNOMATICA llevará a cabo la capacitación del personal ante cambios tecnológicos del entorno, cambio de personal, introducción de nuevas herramientas, modificación de procedimientos operativos, actualización de la Declaración de Prácticas de Certificación, Políticas de Certificado u otros documentos relacionados con la base reglamentaria vigente.

5.3.4 Sanciones por acciones no autorizadas

Las actuaciones y acciones no autorizadas, por parte de los funcionarios de las autoridades y prestadores de servicios de certificación en la PKI de TECNOMÁTICA, y en particular la ACTECNOMATICA, 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.

5.3.5 Documentación suministrada al personal

La ACTECNOMATICA proporciona durante su formación al personal para su conocimiento y aplicación toda la documentación necesaria para el correcto desempeño de sus responsabilidades. Entre la documentación facilitada se encuentra:

- Resolución 2.2016 del MININT
- Decreto ley 199.99
- Código de Ética PKI-Tecnomática
- Declaración de Prácticas de Certificación
- Plan de Seguridad Informática de TECNOMÁTICA
- Documentación relativa a las funciones y procedimientos de cada rol
- Manuales de usuarios para el uso de las herramientas a utilizar

5.4 PROCEDIMIENTO DE CONTROL DE SEGURIDAD

Entre las medidas de seguridad implementadas, la infraestructura PKI cuenta con un firewall pfSense que controla el acceso a dicha zona, solo se permite el acceso al servidor EJBCA a los usuarios conectados a una VPN implementada para este servicio, a la vez cada máquina virtual de la solución lleva implementado un firewall iptables para garantizar mayor seguridad, solo se

permite el acceso del bloque ip de la VPN y los servidores de monitoreo por los protocolos establecidos. El aviso de cualquier falla de la infraestructura PKI lo garantizan los sistemas de monitoreo CHMK y PRTG, los mismos testean con ping, snmp y test port la disponibilidad de la plataforma.

Las máquinas virtuales que conforman la solución tienen configurado el servicio syslog, los logs emitidos se almacenan en un servidor externo en el NCR. También se almacenan los logs de aplicación de forma diaria mediante un script. Estos logs estarán a disposición de la persona autorizada a auditarlos en cualquier momento.

5.4.1 Tipos de registros archivados

La ACTECNOMATICA archiva toda la información relacionada con:

- Intentos exitosos o fracasados de cambiar los parámetros de seguridad del sistema operativo
- Arranque y parada de aplicaciones
- Intentos exitosos o fracasados de solicitar, generar, firmar, emitir o revocar llaves y
- 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, equipamiento e intentos exitosos o fracasados de cambiar los parámetros de seguridad del sistema operativo
- Salvas y restauración
- Modificaciones a los procedimientos y metodologías de trabajo
- Modificaciones a las DPC
- Auditorías y controles

5.4.2 Período de conservación del archivo

La ACTECNOMATICA conservará los registros de auditoría generados por el sistema durante un período mínimo de quince (15) años, desde la fecha de su creación.

5.4.3 Protección de los registros de auditoría

Los ficheros de registro, tanto manual como electrónico, se protegen de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada usando controles de acceso lógico y físico.

5.4.4 Protección del archivo

Los registros se archivan protegidos con técnicas de criptográficas de cifrado y control de acceso, se protegen de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada, salvo los funcionarios autorizados para llevar a cabo verificaciones de integridad u otras. Se establecen además medidas de protección física y control de acceso al local donde se encuentran archivados los mismos.

5.4.5 Procedimiento para la copia de seguridad del archivo

Se generan copias de seguridad del archivo, cumpliendo con lo establecido en el procedimiento para la salva de información establecido en el Nodo Central de la Red en la empresa descritas en el numeral 5.1.10. Desde el punto de vista tecnológico el equipamiento que contiene la información es redundante.

5.4.6 Procedimiento para el sellado de tiempo de los registros

Todos los registros se archivan con información de fecha y hora. La ACTECNOMATICA posee un procedimiento para garantizar la coincidencia de la fecha y hora de los equipamientos con la oficial del país. Se cuenta con una un Servidor de Estampado de Tiempo (NTP) configurado con la hora de nuestro país (http://tsa.cupet.cu).

5.4.7 Procedimiento para obtener y verificar la información del archivo

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

5.4.8 Análisis de vulnerabilidades

Se establece la realización de, al menos, un análisis semestral de vulnerabilidades a los sistemas y servicios del PSC. De igual forma se realiza el análisis de los sistemas físicos y de control de acceso a los locales del prestador diariamente.

Los análisis de vulnerabilidades implican el inicio de las tareas precisas para corregir las debilidades detectadas y la emisión de un informe por parte del supervisor de la ACTECNOMATICA que las realiza.

5.5 CAMBIO DE LLAVE

El tiempo de validez del certificado de la ACTECNOMATICA 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 ACTECNOMATICA 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 ACTECNOMATICA, tenga en su cadena de certificación, el nuevo certificado de la Autoridad Intermedia. La ACTECNOMATICA 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 ACTECNOMATICA posee un plan contra desastres, donde se identifican todos los riesgos que pueden provocar la inutilización o degradación de los servicios que presta el NCR, 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 ACTECNOMATICA 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 ACTECNOMATICA 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 ACTECNOMATICA,

procederá a la emisión de los nuevos certificados, a los suscriptores que tenían certificados vigentes en el momento de producirse el comprometimiento.

La ACTECNOMATICA 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 ACTECNOMATICA se procederá a la ejecución del Plan de Recuperación de Desastres del NCR, 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 ACTECNOMATICA 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 TECNOMÁTICA 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 ACTECNOMATICA
- 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, ACTECNOMATICA 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 ACTECNOMATICA

- La ACTECNOMATICA 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 y el certificado digital de la ACTECNOMATICA, son generados por la Autoridad Raíz (ACSCC) cumpliendo los parámetros de seguridad establecidos por la Dirección de Criptografía para su almacenamiento.

El par de llaves de un titular es generado de acuerdo a lo establecido en las PC de la ACTECNOMATICA , previo contrato firmado por ambas partes.

6.1.2 Inclusión del Par de Llaves en EJBCA

Durante la inclusión del certificado digital y la pareja de llaves en el sistema de la ACTECNOMATICA estarán presentes al menos tres (3) personas:

1. Administrador general de la ACTECNOMATICA
2. Administrador de la infraestructura
3. Administrador de la ACTECNOMATICA-EC

6.1.3 Entrega de la llave privada al suscriptor

En el caso de los CD-PFirma, la ACTECNOMATICA facilita a través del sitio de la PKI la posibilidad de que el mismo titular declarado en las solicitudes firmadas por el Representante, solicite la generación del par de llaves según lo señalado en el numeral 4.4 y sub numerals:

6.1.4 Aceptación del certificado por el solicitante

En el contenedor que cada suscriptor puede descargar del sitio de la PKI, está implícito la llave privada, que sólo podrá ser abierto utilizando el usuario y contraseña por el mismo se creó durante la solicitud del certificado en la Autoridad de Registro.

Toda la comunicación ACTECNOMATICA- ER y ACTECNOMATICA-EC se realiza mediante el uso de un canal seguro HTTPS. El certificado usado para el canal HTTPS fue generado y firmado por la propia ACTECNOMATICA.

6.1.5 Entrega de la llave pública al emisor del certificado

Las llaves públicas de todas las AC pertenecientes a la jerarquía de confianza de la ACTECNOMATICA, se pueden descargar en su sitio oficial https://actecnomatica.cupet.cu. De igual forma pueden ser extraídas mediante herramientas o proveedores criptográficos a partir del contenedor criptográfico entregado a cada suscriptor.

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

La llave pública de la Autoridad de Certificación ACTECNOMATICA será compartida por medio del Certificado Digital de la propia AC que se hará público en el sitio Web de Tecnomática https://actecnomatica.cupet.cu para todo el que necesite hacer uso de la misma.

6.1.7 Tamaño de las llaves

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

Tipo de Certificado Digital	Longitud en bits	
	RSA	ECDSA
ACTECNOMÁTICA	4096	
OCSP	4096	384
TSA	4096	384
Sello Empresarial	4096	384
SSL/TLS	4096	384
VPN Servidor	4096	384
VPN Cliente	2048	256
Firma Digital	2048	256
Firma de Código	2048	256

6.1.8 Parámetros para la generación de llaves públicas y control de calidad

La generación de las llaves y el control de su calidad se realiza con los parámetros establecidos por la Dirección de Criptografía para los diferentes algoritmos disponibles en la generación de las llaves.

6.1.9 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) definidas por el estándar X.509 v3 para la definición y limitación de tales fines. Asimismo, pueden establecerse usos y limitaciones adicionales mediante la extensión ExtendedKeyUsage.

Tener en cuenta que la eficacia de las limitaciones basadas en extensiones de los certificados depende en ocasiones, de la implementación de aplicaciones informáticas que no han sido desarrolladas ni controladas por la ACTECNOMATICA.

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 ACTECNOMATICA, 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 ACTECNOMATICA se encuentra bajo control multipersona. Para el acceso físico a ella y la realización de operaciones sobre esta, se requiere la concurrencia de al menos dos (2) personas, cada uno en posesión de una parte o fragmento de la clave que accede a las llaves de la ACTECNOMATICA y un supervisor.

6.2.3 Custodia de la llave privada

La ACTECNOMATICA 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 serán 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

La ACTECNOMATICA no genera copias de las llaves, sino que almacena en el dispositivo de almacenamiento, entregado por la ACSCC, que contienen las llaves y el certificado de la AC. Estos se almacenan en la oficina de control de la información, su acceso está restringido al personal autorizado mientras que su empleo está limitado por el factor multipersonal.

El objetivo de mantener estos dispositivos de almacenamiento es 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 ACTECNOMATICA y su correspondiente Sobre-PIN, se almacena de manera cifrada en un dispositivo extraíble, el cual se guarda en la OCIC que tiene acceso restringido.

La llave privada de la ACTECNOMATICA 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 ACTECNOMATICA opera con su llave privada sobre el propio módulo criptográfico del EJBCA y se mantiene almacenada en él de manera cifrada. La llave privada se inserta en el momento de la activación de la AC bajo la supervisión de una comisión creada a tal efecto. 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 activa automáticamente cuando se inician los procesos de generación de certificados y de CRL por los funcionarios que cumplen ese roll. La llave solamente es descifrada y empleada en los momentos de firmar los certificados y las CRL emitidas, el resto del tiempo de operación se mantiene cifrada.

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 instalar la llave privada de la ACTECNOMÁTICA, 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 ACTECNOMATICA-AC, designa una comisión, presidida por el jefe de la ACTECNOMATICA-EC, la cual realizará, en presencia de un supervisor, 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 Cifrado 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 ACTECNOMATICA 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
ACTECNOMATICA	8 años

Suscriptores	1 o 2 años

La caducidad producirá automáticamente la invalidación de los Certificados, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de asociados.

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 ACTECNOMATICA 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 conforma 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 dos 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 de los custodios de la llave privada, la protección de los datos de activación de la llave privada.

En el caso de la ACTECNOMATICA, los datos de activación de la llave privada además de estar resguardada en la Norma de control de la OCIC, es responsabilidad de cada uno de los custodios de la llave privada de la protección de los datos, que permiten conformar el PIN con el cual se activa la llave privada de la ACTECNOMATICA.

6.5 CONTROLES DE SEGURIDAD COMPUTACIONAL

6.5.1 Requerimientos técnicos específicos de seguridad computacional

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

La ACTECNOMATICA garantiza el control de acceso a los funcionarios (operadores, administradores, supervisores y directivos) para mantener la seguridad del sistema,

incluyendo la gestión de cuentas de usuario, auditoría y modificaciones o denegaciones de acceso.

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

La ACTECNOMATICA garantiza que el acceso a los sistemas de información y aplicaciones de acuerdo a lo establecido en la política de control de acceso, así como que los sistemas proporcionan los controles de seguridad suficientes para implementar la segregación de funciones identificada en las prácticas de la Entidad, incluyendo la separación de funciones de administración de los sistemas de seguridad y de los operadores.

El personal de la Entidad está identificado y reconocido antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida de los certificados.

Los sistemas de seguridad y monitoreo permiten una rápida detección, registro y actuación ante intentos de acceso irregular o ataques informáticos a la infraestructura y los servicios.

Acceso a los depósitos públicos de la información de la ACTECNOMATICA cuenta con un control de accesos para modificaciones o borrado de datos.

El Sistema de la ACTECNOMATICA dispone de controles y protocolos de seguridad, basado en el uso de Certificados Digitales de Llave Pública que regula el acceso a sus servicios, diferenciando las facultades y obligaciones de cada uno de los roles identificados para el trabajo con la PKI.

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 ACTECNOMATICA, así como las actualizaciones de sus configuraciones, deben pasar una fase de prueba antes de ser puestos en explotación y solo pueden ser aplicados mediante la concurrencia de una comisión en la cual participa al menos 1 representante por cada uno de los roles de administración de esta.

Se utilizan procedimientos de control de cambios para las nuevas versiones y actualizaciones de los componentes son ejecutados por funcionarios facultados y autorizados, dejando evidencia oficial de estas acciones.

6.6.2 Controles de gestión de seguridad

La ACTECNOMATICA 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.

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

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 están separados lógicamente, través de los roles de los Administradores de la CA y RA, los CRL están públicos en otra instancia del EJBCA.

El sitio web oficial de la ACTECNOMATICA, así como la infraestructura PKI ubicados en la red de Tecnomática, se encuentran desplegados en su Centro de Datos, por lo que heredan los mecanismos de seguridad y de control de acceso establecidos en dicha red, protegiéndolos de dominios externos accesibles por terceras partes.

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

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 ACTECNOMATICA 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 ACTECNOMATICA, tendrán los siguientes campos:

CAMPO	VALOR
Versión	X.509 V.3
Número de Serie	Valor único (en formato hexadecimal) generado por la autoridad que emite el certificado
Algoritmo de firma	sha512RSA, SHA512WITHRSA
Algoritmo hash de firma	sha512
Emisor	CN= Autoridad Certificadora Tecnomática OU= CUPET O= MINEM L= Centro Habana ST= La Habana C= CU E=pkitm@tm.cupet.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
Sujeto	CN=Nombre del titular de acuerdo al tipo de suscripción UID=Carnet de Identidad. Title= Cargo del titular OU=Unidad Organizacional (siglas) O=Organización (siglas) ST=Provincia C=CU Dirección email.

Llave pública	Se codifica de acuerdo con la RFC 5280. La longitud mínima de la llave es 2048 bits para algoritmo RSA y 512 para algoritmos de curva elípticas ECDSA.

7.1.1 Número de versión

ACTECNOMATICA 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 ACTECNOMATICA, se utilizarán como mínimo los siguientes campos de las extensiones estándar X.509.

CAMPO	VALOR
Uso de la llave (KeyUsage)	Especifica los usos permitidos de la llave
Uso mejorado de la llave (ExtendedKeyUsage)	Se especifican otros propósitos adicionales al uso de la llave
Nombre alternativo (SubjectAlternativeName)	Especifica otros nombres que pudieran estar asociados al Certificado
Acceso a la información de la autoridad (CertificatePolicies)	Es utilizado para indicar la dirección URL donde se publica la respectiva política del certificado
Puntos de distribución CRL (CRLDistributionPoints)	Es utilizado para indicar la dirección donde se encuentra publicada la CRL y acceder al servicio OCSP
Acceso a la Información de Autoridad de Certificación (AuthorityInformationAccess)	Especifica la url de publicación de la DPC de la ACTECNOMATICA https://actecnomatica.cupet.cu

7.1.3 Identificador de objeto del algoritmo

Identificador de Objeto (OID) de los algoritmos Criptográficos:

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

7.1.4 Formato de Nombres

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 ACTECNOMATICA cumplen con la RFC 5280 y contienen los siguientes elementos básicos:

CAMPO	VALOR
Versión V2	V2
Emisor	CN= Autoridad Certificadora TECNOMATICA OU= CUPET O= MINEM L= Centro Habana ST= La Habana C= CU E=pkit@tm.cupet.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	sha512wihtRSAEncryption
Algoritmo hash de firma	sha512
Certificados revocados	Lista de certificados revocados, incluyendo el número de Serie, la fecha de revocación y causas

7.2.1 Número de versión

La ACTECNOMATICA emite las CRL en formato X.509 versión 3.

7.2.2 Extensiones de la CRL

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

CAMPO	VALOR
Número CRL	Especifica el Número consecutivo de la CRL
Uso mejorado de la clave	Se especifican otros propósitos adicionales al uso
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 para su descarga

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 Perfil del certificado del OCSP responder

Los certificados de OCSP serán emitidos por la ACTECNOMATICA y conforme a las siguientes normas:

- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate
- Revocation List (CRL) Profile
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework
- IETF RFC 2560 Online Certificate Status Protocol – OCSP
- RFC 6066: Transport Layer Security Extensions: Extension Definitions
- El periodo de validez de los mismos no será superior a los dos (2) años

- La AC emisora incluirá en el certificado de OCSP responder la extensión "*idpkix-ocsp-nocheck*", tal y como contempla la RFC 2560, para indicar que los clientes OCSP deben confiar en el prestador de servicios de validación durante el periodo de vida del certificado asociado

7.3.2 Número de versión

Los certificados de OCSP, utilizarán el estándar X.509 versión 3 (X.509 v3. Está implementada la versión 3 del protocolo OCSP según lo establecido en la RFC 2560.

7.3.3 Formato de nombres

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

7.3.4 Campos y extensiones del certificado

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

CAMPO	CONTENIDO
Versión	X509 v3
Número de serie	XXXXXXXXXXXXX
Algoritmo de firma	SHA512WithRSAEncryption o ECDSAWithSHA512
DN del Emisor	CN= Autoridad Certificadora TECNOMÁTICA OU= CUPET O= MINEM L= Centro Habana ST= La Habana C= CU E= pkitm@tm.cupet.cu
Validez	2 años
Sujeto	CN= Autoridad de validación OU= CUPET O= MINEM L= Centro Habana ST= La Habana 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
Usos extendidos de la llave	Firmador OCSP (OCSP Signer)

7.3.5 Formato de las peticiones OCSP

Se soporta la extensión Nonce (id-pkix-ocsp-nonce) tal y como contempla la norma para evitar "replay attacks". El OID es id-pkix-ocsp-nonce.

7.3.6 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 ACTECNOMATICA que se encuentren revocados
- "Good", para aquellos certificados emitidos por la ACTECNOMATICA 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 ACTECNOMATICA, 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 TECNOMÁTICA y las que disponga el Director General de Tecnomática que se reserva el derecho de exigir inspecciones de las instalaciones, procedimientos, sistema de seguridad y de control y acceso a la AC o la AR, para validar que se encuentran funcionando de acuerdo con las prácticas y procedimientos de seguridad establecidos en la presente DPC.

8.2 IDENTIFICACIÓN DEL AUDITOR

El auditor será establecido por la Dirección de Criptografía del MININT, con experiencia en auditorías a Prestadores de Servicios de Certificación, con previa presentación a los directivos de TECNOMÁTICA 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 (ACTECNOMATICA) 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 ACTECNOMATICA.

8.4 TÓPICOS CUBIERTOS POR EL CONTROL

La auditoría determinará la conformidad de los servicios de ACTECNOMATICA 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:

- Mecanismos de identificación y autenticación en la tramitación de solicitudes
- Política de Seguridad
- Seguridad física
- Evaluación tecnológica
- Administración de los servicios de la CA
- Contratos y servicios especializados
- DPC

8.5 ACCIONES A TOMAR COMO RESULTADO DE UNA DEFICIENCIA

Una vez recibido el informe de la auditoría llevada a término, la ACTECNOMATICA evalúa, con la entidad que ha ejecutado la auditoría las deficiencias encontradas, desarrolla y ejecuta un plan de medidas para solucionar dichas deficiencias, informando periódicamente al Director General de la empresa el estado de implementación de las acciones derivadas del Plan de medidas.

Si la ACTECNOMATICA 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 ACTECNOMATICA, de la forma como se describe en las secciones correspondientes de esta DPC
- Finalizar la prestación del servicio de la ACTECNOMATICA, 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 PSCC, al director (a) de TECNOMÁTICA, a los responsables de las distintas áreas en las que se detecten no conformidades y una sintesis de los resultados a la ACSCC.

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

9 REQUISITOS LEGALES Y COMERCIALES

9.1 TARIFAS

9.1.1 Tarifas de emisión de certificado o renovación

Las tarifas de emisión, y renovación de cada certificado se encuentran publicadas en el sitio oficial de Tecnomática *https://actecnomatica.cupet.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 y tiene enlace en el sitio oficial de Tecnomática *https://actecnomatica.cupet.cu/*

9.2 CAPACIDAD FINANCIERA

9.2.1 Indemnización a los terceros que confían en los certificados emitidos por la ACTECNOMATICA

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

ACTECNOMATICA 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

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

9.2.3 Procesos administrativos

ACTECNOMATICA 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 ACTECNOMATICA
- las llaves privadas de titulares que la ACTECNOMATICA haya generado y mantiene en custodia
- Toda información relativa a los parámetros de seguridad, control y procedimientos de auditoría
- Toda la información de carácter personal proporcionada a ACTECNOMATICA 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 ACTECNOMATICA 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
- Esta información no será divulgada ni compartida fuera del marco de la infraestructura de la ACTECNOMATICA, a menos que así lo exija la Ley o un documento legal

9.3.2 Información no confidencial

ACTECNOMATICA considera información de acceso público:

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

9.3.3 Deber de secreto profesional

Los funcionarios y directivos de la ACTECNOMATICA están obligados al deber de secreto profesional y por lo tanto están sujetos a las normativas reguladoras establecidas en los respectivos Reglamentos Internos y en el Código de Ética.

9.3.4 Divulgación de la información de revocación de certificados

La información relativa a la revocación de certificados es publicada en el sitio oficial de Tecnomática https://actecnomatica.cupet.cu y consultada mediante CRL u OCSP.

9.4 PROTECCIÓN DE DATOS PERSONALES

La ACTECNOMATICA 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. Dispone de un código de Etica pública en el sitio oficial.

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 ACTECNOMATICA

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 ACTECNOMATICA
- 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 (CRL), así como el resto de informaciones de estado de revocación
- La información contenida en el sitio oficial de la ACTECNOMATICA
- La aceptación por el titular de la emisión del Certificado Digital emitido a su nombre equivale al consentimiento dado para su publicación

9.4.4 Responsabilidades

La ACTECNOMATICA 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.

La ACTECNOMATICA implanta medidas de identificación y autenticación, así como el necesario control de acceso del personal a los datos personales.

9.4.5 Prestación del consentimiento del uso de datos personales

Para la prestación del servicio, la ACTECNOMATICA 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 Representante nombrado por la maxima dirección para tales efectos .

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

La ACTECNOMATICA 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 ACTECNOMATICA 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 relacionados con el ciclo de vida de los Certificados DIgitales y las CRL's emitidos por la ACTECNOMATICA, la presente DPC, así como cualquier otro documento, electrónico o de cualquier otro tipo, propiedad de ACTECNOMATICA, son propiedad exclusiva de la ACTECNOMATICA.

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

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 ACTECNOMATICA 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 ACTECNOMATICA le informa de los aspectos legales
- Emitir, mantener actualizadas y hacer públicas su Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (PC)
- Proveer mecanismos de comprobación del estado de un Certificado Digital
- 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, operar de acuerdo a lo establecido en la Resolución 02/2016 del Ministerio del Interior
- Asumir las pertinentes responsabilidades y obligaciones frente a las entidades y los titulares en cuanto a la calidad del servicio que presta
- Disponer de personal preparado en materias relacionadas con los servicios de certificación prestados
- Identificar al suscriptor del certificado, de acuerdo con el presente documento

9.6.2 Garantías ofrecidas a suscriptores

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

- El cumplimiento de sus obligaciones legales como prestador de servicios de certificación, de acuerdo con esta DPC y PC
- Un adecuado conocimiento y preparación, para que puedan conocer, dominar y hacer un uso correcto de sus Certificados Digitales de Llave Pública, así como asumir sus responsabilidades
- Un ambiente confiable y seguro de operación durante todo el ciclo de vida de los Certificados Digitales
- Que no haya errores en la información contenida en los certificados, debido a falta de diligencia en los procedimientos de emisión y renovación
- La aplicación de adecuadas medidas, para comprobar la veracidad y autenticidad de la acreditación de los solicitantes
- 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.

9.6.3 Obligaciones de las Autoridades de registro

Las personas que operan en las ARs integradas en la jerarquía de ACTECNOMATICA –operadores de Punto de Registro de Usuario– están obligadas a:

- Realizar sus operaciones en conformidad con esta DPC
- Realizar sus operaciones de acuerdo con la Política de Certificado que sea de aplicación para el tipo de certificado solicitado en cada ocasión
- Comprobar la identidad de las personas a las que se les concede el certificado digital a partir de la documentación presentada y certificada por el Representante y la revisión de los datos que al realizar la solicitud facilitan en el sitio los suscriptores
- Informar, antes de la emisión de un certificado, a la persona que solicite sus servicios, de las obligaciones que asume, la forma que debe custodiar los datos de creación de firma, el procedimiento que debe seguir para comunicar la pérdida o utilización indebida de los datos o dispositivos de creación y de verificación de firma, las limitaciones de su uso y la página web donde deberá acreditarse y podrá consultar cualquier información de la ACTECNOMATICA , la DPC y las PC vigentes, la legislación aplicable y las certificaciones obtenidas
- Validar y enviar de forma segura a la ACTECNOMATICA la solicitud de certificación debidamente cumplimentada con la información aportada por el subscriptor, y recibir los datos asociados a los certificados emitidos de acuerdo con esa solicitud
- Almacenar de forma segura y hasta el momento de su remisión a la Autoridad de Certificación, tanto la documentación aportada por el subscriptor como la generada por la propia AR, durante el proceso de registro o revocación
- Formalizar el Contrato de Certificación con el Representante del suscriptor según lo establecido por la Política de Certificado aplicable
- Solicitar la revocación de un certificado cuando tenga conocimiento o sospecha del compromiso de una llave privada
- En el caso del rechazo de una solicitud de certificación, notificar al representante dicho rechazo y el motivo del mismo

- Remitir copia firmada del contrato de certificación y de las solicitudes de revocación a la ACTECNOMATICA
- Recibir y tramitar las solicitudes de revocación presenciales que reciba de manera inmediata, después de haber llevado a cabo una identificación fiable
- Colaborar en cuantos aspectos de la operación, auditoría o control del Punto de Registro de Usuario se le soliciten por parte de la Autoridad de Certificación
- A la más general y amplia obligación de confidencialidad, durante la prestación del servicio como Autoridad de Registro, respecto de la información recibida por la ACTECNOMATICA y respecto de la información y documentación en que se haya concretado el servicio. En el mismo sentido, no transmitir a terceros dicha información, bajo ningún concepto, sin autorización expresa, escrita y con carácter previo de la ACTECNOMATICA, en cuyo caso trasladará a dichos terceros idéntica obligación de confidencialidad

9.6.4 Obligaciones de los suscriptores

La ACTECNOMATICA obliga al suscriptor a:

- Facilitar a la ACTECNOMATICA información completa, adecuada y veraz en especial por lo que respecta al procedimiento de registro
- Manifestar su consentimiento previo a la emisión de un certificado
- Cumplir las obligaciones que se establecen para el suscriptor en este documento
- No transferir ni delegar a terceros sus responsabilidades sobre un Certificado Digital que le haya sido emitido
- Utilizar el certificado de acuerdo con lo establecido en la sección de usos correspondientes
- Notificar a la ACTECNOMATICA por medio de su Representante y sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su llave privada
    - La pérdida de control sobre su llave privada, a causa del compromiso de los datos de activación (por ejemplo, el código PIN del dispositivo seguro de creación de firma) o por cualquier otra causa
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor, requiriendo su revocación si correspondiera

- Dejar de utilizar la llave privada transcurrido el tiempo de validez del certificado
- No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de la Jerarquía de la ACTECNOMATICA, sin permiso previo por escrito
- No comprometer intencionadamente la seguridad de la Jerarquía de ACTECNOMATICA
- Ser especialmente diligente en la custodia de su llave privada con el fin de evitar usos no autorizados

9.6.5 Garantías ofrecidas por el suscriptor

La ACTECNOMATICA obliga al suscriptor, mediante el correspondiente instrumento jurídico, a garantizar:

- Que todas las manifestaciones realizadas en la solicitud son correctas
- Que todas las informaciones suministradas por el suscriptor que se encuentre contenidas en el certificado son correctas
- Que el certificado se utiliza exclusivamente para usos legales y autorizados, de acuerdo con la presente DPC
- Que cada firma digital creada con la llave privada correspondiente a la llave pública listada en el certificado es la firma digital del suscriptor y que el certificado ha sido aceptado y se encuentra operativo (no ha expirado ni ha sido revocado) en el momento de creación de la firma
- Que ninguna persona no autorizada ha tenido nunca acceso a la llave privada del suscriptor

9.6.6 Protección de la llave privada

La ACTECNOMATICA obliga al suscriptor, mediante el correspondiente instrumento jurídico, a garantizar que el suscriptor es el único responsable de los daños causados por su incumplimiento del deber de proteger la llave privada.

9.6.7 Obligaciones de los terceros confiantes en los certificados emitidos por la ACTECNOMATICA

Es obligación de las partes que confíen en los certificados emitidos por ACTECNOMATICA:

- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las Políticas de Certificados pertinentes

- Verificar la validez de los certificados en el momento de realizar o verificar cualquier operación basada en los mismos
- Asumir su responsabilidad en la correcta verificación de las firmas digitales
- Asumir su responsabilidad en la comprobación de la validez, revocación o suspensión de los certificados en que confía
- Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas

9.7 RENUNCIA DE GARANTÍAS

La ACTECNOMATICA 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 ACTECNOMATICA limita su responsabilidad restringiendo el servicio a la emisión y gestión de certificados y de los pares de llaves de suscriptores suministrado por la Autoridad de Certificación. Tambíen puede limitar su responsabilidad mediante la inclusión de límites de uso del certificado.

9.8.2 Deslinde de responsabilidades

La ACTECNOMATICA 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 CRL emitidos por ACTECNOMATICA
- 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 ACTECNOMATICA 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 ACTECNOMATICA 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.

9.9.3 Supervivencia

La ACTECNOMATICA infiere, en sus instrumentos jurídicos con los suscriptores y los verificadores, regirse por lo establecido en la Resolución 2 del 2016 del MININT, en virtud de lo cual garantizará el cumplimento de las reglas que deben continuar vigentes aún después de la finalización de la relación jurídica reguladora del servicio entre las partes.

A este efecto, la ACTECNOMATICA vela porque, al menos los requisitos contenidos en las secciones Obligaciones, Responsabilidad civil, Auditoría de conformidad y Confidencialidad, continúen vigentes después de la finalización de la política de certificado y de los instrumentos jurídicos que vinculen la ACTECNOMATICA con suscriptores y verificadores.

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 MODIFICACIONES

La ACTECNOMATICA puede modificar unilateralmente este documento, sujetándose al siguiente procedimiento:

- La modificación tiene que estar justificada desde el punto de vista técnico y legal

- La modificación propuesta por la ACTECNOMATICA no puede vulnerar las disposiciones contenidas en las Políticas de Certificado ya establecidas por ella misma
- Se establece un control de modificaciones, para garantizar, en todo caso, que las especificaciones resultantes cumplan los requisitos que se intentan cumplir y que dieron pie al cambio
- Al ser sustituida o derogada una versión de la DPC, se mantendrá publicada en el sitio web oficial de la ACTECNOMATICA por un periodo de treinta (30) días, antes de ser retirada. Todas las versiones de DPC serán conservadas por un período de quince (15) años
- Se establecen las implicaciones que el cambio de especificaciones tiene sobre el suscriptor, y se prevé la necesidad de notificarle dichas modificaciones

9.11.1 Procedimiento de especificación de cambios

La entidad con atribuciones para aprobar cambios sobre la DPC de la ACTECNOMATICA es el Director General de la Empresa cuyos datos de contacto se encuentran en esta DPC.

Siempre y cuando la modificación de la DPC propuesta no reduzca materialmente la confianza que una Política de Certificado proporcionan, ni altere la aceptabilidad de los certificados que soporta la política para los propósitos para los que se han usado, se procederá al incremento del número menor de versión del documento y el último número de Identificador de Objeto (OID) que lo representa (si aplica), manteniendo el número mayor de la versión del documento, así como el resto de su OID asociado. No se considera necesario comunicar este tipo de modificaciones a los suscriptores de los certificados correspondientes a la DPC modificada.

En el supuesto de que los cambios a la especificación vigente afecten a la aceptabilidad de los certificados para propósitos específicos se procederá al incremento del número mayor de versión del documento y la puesta a cero del número menor de la misma. También se modificarán los dos últimos números del de Identificador de Objeto (OID) (si aplica) que lo representa. Este tipo de modificaciones se comunicará a los suscriptores de los certificados correspondientes a la DPC modificada mediante el envío de una notificación, con una antelación de al menos 30 días a su publicación.

El usuario puede aceptar las modificaciones o rechazarlas:

- En caso de rechazarlas, su certificado, emitido bajo las instrucciones de la anterior DPC será válido para los propósitos en ella incluidos, pero no para los propósitos

específicos que se incluyen en la nueva DPC modificada. Si transcurridos 15 días desde la notificación al usuario no se tuviera respuesta del mismo, se considerará que el usuario no ha aceptado la modificación, aunque puede aceptarla en cualquier momento posterior.

- En caso de aceptarlas, tendrá lugar un procedimiento de recertificación en el cual el nuevo certificado solamente se diferenciará del revocado en el OID de la política que le aplica, para reflejar los cambios.

9.11.2 Procedimientos de publicación y notificación

Toda modificación de esta Declaración de Prácticas de Certificación o de los Documentos de Políticas de Certificado se publicará en el sitio web de la ACTECNOMATICA.

Procedimientos de aprobación de la Declaración de Prácticas de Certificación.

La Dirección de Criptografía del MININT es la entidad competente para acordar la aprobación de la presente Declaración de Prácticas de Certificación, así como de las Políticas de Certificado asociadas a cada tipo de certificado y demás documentación del PSC.

9.12 RESOLUCIÓN DE CONFLICTOS

9.12.1 Resolución extrajudicial de conflictos

La ACTECNOMATICA 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.

9.13 LEGISLACIÓN APLICABLE

El funcionamiento y operaciones de ACTECNOMATICA, 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
- Decreto No. 370 Sobre la Informatización de la Sociedad en Cuba

- Decreto No. 360 Sobre la Seguridad de las Tecnologías de la Información la Comunicación y la defensa del ciberespacio nacional, julio 2019
- Declaración de Prácticas de Certificación de la Autoridad Raiz ACSCC
- Normas ISO y estandares internaciones incluidos en las legislaciones aplicables

ANEXO 1.

DEFINICIONES DE CONCEPTOS ESTABLECIDAS EN EL ARTÍCULO 4 DE LA RES 2 DEL 2016

- **Autoridad de Certificación (AC):** Es la entidad de confianza, responsable de emitir, renovar y revocar los certificados digitales utilizados por terceros en funciones criptográficas de protección de la información oficial mediante el empleo de criptografía de llave pública (ACTECNOMATICA-EC)
- **Autoridad de Registro (AR o RA):** Es la entidad que identifica de forma inequívoca al solicitante de un certificado y suministra a la Autoridad de Certificación los datos verificados del solicitante a fin de que se emita el correspondiente certificado. (ACTECNOMATICA-ER)
- **Cadena de confianza:** También conocida como Jerarquía de Confianza, la constituyen las autoridades de certificación relacionadas por la confiabilidad en la emisión de certificados digitales entre los diferentes niveles jerárquicos. Todos los certificados emitidos por el actual prestador de servicios de certificación, tendrán en su cadena de confianza los certificados correspondientes a la AC-Raíz y a la ACTECNOMATICA.
- **Certificado Digital de Llave Pública:** Es un archivo o documento electrónico mediante el cual, una autoridad de certificación (tercero confiable) garantiza la vinculación entre la identidad de un sujeto o entidad (nombre, dirección, número de identidad o pasaporte, y otros elementos de identificación) y una llave criptográfica pública, y es una pieza imprescindible en los protocolos que se usan para autenticar a las partes de una comunicación digital
- **Certificado raíz**: Es un certificado auto firmado y que normalmente identifica a una AC y permite comprobar la autenticidad de cualquier Certificado emitido por ella.
- **Certificado Digital de Llave Pública reconocido:** Es aquel que se expide y firma digitalmente por una autoridad de certificación, aprobada para operar en la Infraestructura, cuyo certificado digital (el de la autoridad) está firmado por la Autoridad Raíz
- **Declaración de Prácticas de Certificación**: Es el documento que establece los términos bajo los cuales será prestado el servicio de certificación digital. Estos términos establecen el marco legal sobre el cual opera ACTECNOMATICA

- **Directorio de Certificados**: Repositorio de información que sigue el estándar X.500 del ITU-T
- **Firma digital:** Es un valor numérico que se adhiere a un mensaje o documento y que se obtiene mediante un procedimiento matemático conocido, vinculado a la llave privada del suscriptor iniciador de una comunicación y al texto del mensaje para permitir determinar que este valor se ha obtenido exclusivamente con esa llave privada (secreta) del iniciador, y que el mensaje inicial no ha sido modificado después de efectuada la transformación
- **Firma electrónica avanzada**: es aquella firma electrónica que permite establecer la identidad personal del suscriptor respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al suscriptor, como a los datos a que se refiere
- **Hash:** se obtiene de la aplicación de una función matemática unidireccional que opera sobre un documento digital, secuencia digital numérica, etc., todos de gran tamaño medido en bits, y brinda como resultado un valor más pequeño y de tamaño fijo, cualquiera sea su entrada, que se utiliza en aplicaciones criptográficas que protegen la integridad de la información
- **Infraestructura de Llave Pública:** conjunto de entidades componentes del sistema jerárquico de prestadores de servicios criptográficos de certificación, que funcionan con tecnologías de seguridad, criptografía, políticas, y normas técnico-organizativas aprobadas por el Ministerio del Interior, en aras de brindar la confianza necesaria a sus suscriptores y a terceros de buena fe en el uso de los certificados digitales y criptomateriales asociados para la protección de la información oficial que se tramita por los medios de Infocomunicaciones. Una autoridad de certificación de nivel superior garantiza la confiabilidad de una o varias de nivel inferior a ella subordinada
- **Llave Privada:** Es uno de dos valores numéricos, obtenidos por métodos matemáticos complejos y criptográficamente seguros, que se asigna a una persona para su empleo en descifrar datos y la creación de la firma digital de documentos electrónicos. Este valor numérico es secreto y está asociado matemáticamente a la llave pública de la precitada persona
- **Llave Pública:** Es uno de dos valores numéricos, obtenidos por métodos matemáticos complejos y criptográficamente seguros, que se le asigna a una persona de manera pública en directorios u otro sitio accesible por terceros, para que los remitentes puedan cifrar mensajes electrónicos a enviar a ella. Se utiliza también en la

verificación por los destinatarios de un documento electrónico que tiene una firma digital hecha por la persona que actúa como remitente y es poseedora de la llave pública

- **Listas de Revocación de Certificados:** documento digital público, que expide una autoridad de validación o de certificación, donde figura exclusivamente la relación de los certificados digitales revocados o suspendidos
- **OCSP (Online Certificate Status Protocol)**: protocolo informático que permite la comprobación automática del estado de revocación de un certificado digital X.509 en el momento en que éste es utilizado
- **OID (Object Identifier)**: valor, de naturaleza jerárquica y comprensivo de una secuencia de componentes variables, aunque siempre constituidos por enteros no negativos separados por un punto, que pueden ser asignados a objetos registrados y que tienen la propiedad de ser únicos entre el resto de los OID
- **Prestador de Servicios de Certificación:** persona jurídica que presta servicios criptográficos y expide certificados digitales para su utilización en la creación y verificación de la firma digital y el establecimiento de canales de comunicaciones seguros, como por ejemplo son las autoridades de certificación, registro, sellado de tiempo, validación, tercero de confianza, custodia de documentos electrónicos, consulta de atributos, entre otros
- **Política de Certificado:** Conjunto de reglas que especifican las características de emisión, gestión, aplicabilidad y/o uso de los distintos tipos de certificados digitales en una comunidad de suscriptores y usuarios, sistemas o clase particular de aplicaciones que tengan requerimientos de seguridad comunes
- **PKCS#10 (Certification Request Syntax Standard)**: estándar desarrollado por RSA Labs, y aceptado internacionalmente como estándar, que define la sintaxis de una petición de certificado
- **Repositorio:** Sistema de información que se emplea para almacenar y recuperar certificados digitales, y otras informaciones relativas a éstos
- **Sellado de Tiempo**: Anotación firmada electrónicamente y agregada a un mensaje de datos mediante procedimientos criptográficos en la que consta como mínimo la fecha, la hora y la identidad de quien efectúa la anotación (Autoridad de Sellado de Tiempo), basándose en las especificaciones Request For Comments: 3161 – “Internet X.509 Public Key Infrastructure Time–Stamp Protocol (TSP)”

- **X.500**: estándar desarrollado por la UIT que define las recomendaciones del directorio. Se corresponde con el estándar ISO/IEC 9594-1: 1993
- **X.509:** estándar universal de la Unión Internacional de Telecomunicaciones (UIT) que establece el formato general para la confección y estructura de los certificados digitales