	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

Control de Versiones

Versión	Sustituye Versión	Entra en Vigor	Elaboró	Fecha Revisión	Revisó	Autorización	Próxima Revisión	Observaciones
2.0		27/08/2008	CSI-DGNM	01/07/2008	CSI-DGNM	CSI-DGNM	14/07/2009	
1.0		24/09/2007	CSI-DGNM	24/09/2007	CSI-DGNM	CSI-DGNM	26/02/2008	Primera Versión

Declaración de Intención

En este documento se describe la Declaración de Prácticas de Certificación (DPC) para las Autoridades Certificadoras del SIGER (AC-SIGER) y de la DGNM (AC-DGNM), que son parte de la Infraestructura de Clave Pública de la Secretaría de Economía.

Audiencia y Alcances


Agentes certificadores, auxiliares de agente, administradores y usuarios de la AC-SIGER y la AC-DGNM.

Objetivos

Definir los procedimientos aplicables a la solicitud, validación, emisión, aceptación y revocación de certificados digitales emitidos por la AC-SIGER y la AC-DGNM.

Definiciones y Abreviaturas

AC: Autoridad Certificadora
Agente certificador: Personal de la DGNM designada para realizar el procedimiento de generación y revocación de certificados digitales.
Auxiliar de agente: Personal autorizado, que apoya al agente certificador en el proceso de generación de certificados digitales, a excepción de la generación del certificado digital.
DPC: Declaración de Prácticas de Certificación de la AC-DGNM y AC-SIGER.
AC-SIGER: Autoridad Certificadora del SIGER.
AC-DGNM Autoridad Certificadora de la DGNM.
CD: Certificado Digital.
Centro de Datos del SIGER: Centro encargado de la operación y servicios del SIGER.
Claves: Clave Pública y Clave Privada.
Comunidad de la AC-SIGER: Aquella integrada por agentes certificadores, responsables de oficina, fedatarios públicos, sistemas o equipos a quienes se les ha emitido un certificado digital de la AC-SIGER.
Comunidad de la AC-DGNM: Aquella integrada por agentes certificadores y personal de Unidades Administrativas y organismos descentralizados y desconcentrados de la SE, a quienes se les ha emitido un certificado digital de la AC-DGNM.
CRL: Lista de Certificados Revocados, por sus siglas en inglés (Certificate Revocation List.)
DSA: Digital Signature Algorithm. Algoritmo de Firma Digital
DGNM: Dirección General de Normatividad Mercantil
DSIGER: Dirección del Sistema Integral de Gestión Registral.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

Definiciones y Abreviaturas

e-mail: Dirección de correo electrónico.

FEA (Firma Electrónica Avanzada): Firma Electrónica que cumple con los requisitos contemplados en el artículo 97 del Código de Comercio.

Firmante: La persona que posee los datos de creación de la firma electrónica y que actúa en nombre propio o de la persona a la que representa.

FIPS 140-1: Acrónimo de **Federal Information Processing Standard** (Estándares Federales de Procesamiento de la Información), publicación 140-1, es un estándar de seguridad de ordenadores del gobierno de Estados Unidos para la acreditación de módulos criptográficos.

HSM: Dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y suele aportar aceleración hardware para operaciones criptográficas

OCSP: Protocolo de Estatus de Certificados en Línea (por sus siglas en inglés). Online Certificate Status Protocol.)

PC (Política de Certificación): Conjunto de reglas establecidas y difundidas por la DGNM, para garantizar un nivel alto de operación y seguridad en la emisión y en la revocación de los certificados de la AC-SIGER y AC-DGNM.

PKI (Public Key Infrastructure): Infraestructura de Clave Pública.

PSC: Prestadores de Servicios de Certificación.

SE: Secretaría de Economía.

SIGER: Sistema Integral de Gestión Registral.

RPC: Registro Público de Comercio.

RSA: Algoritmo criptográfico de clave pública que adopta su nombre de las iniciales de sus creadores: Rivest, Shamir y Adleman.

SSH: Secure Shell, protocolo y programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

SSL: Secure Socket Layer, protocolo que proporciona autenticación y privacidad de la información a través de Internet mediante el uso de criptografía

Titular: Persona a cuyo favor fue expedido el certificado digital.

Página del SIGER: <http://www.siger.gob.mx>

UPS: Sistema de Alimentación Ininterrumpida (Uninterruptible Power Supply), es un dispositivo que, gracias a su batería, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos existentes en la red eléctrica.

Introducción

Este documento se desarrolló tomando como base el ETSI 102 042 y el RFC 3647 [1].

Las Autoridades Certificadoras de la DGNM y del SIGER (AC-DGNM y AC-SIGER), emiten certificados digitales del tipo que se especifican en el punto 5.1 del presente documento.

IDENTIFICACIÓN

A este documento se le denomina “Declaración de Prácticas de Certificación de las Autoridades Certificadoras de la DGNM y del SIGER” (DPC). La versión actual está

Introducción

disponible en la página del SIGER (<http://www.siger.gob.mx>)

El Object Identifier, identificador de objeto (OID) ASN.1 de esta DPC es el siguiente:
2.16.484.101.10.316.1.10.2

Se compone de las siguientes partes:

JOINT - ISO - ITU-T	2
PAÍS	16
MÉXICO	484
GOBIERNO FEDERAL	101
SECRETARÍA DE ECONOMÍA	10
DGNM	316
AUTORIDAD CERTIFICADORA DE LA SECRETARÍA DE ECONOMÍA	1
AUTORIDAD CERTIFICADORA DEL SIGER	10
DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM y AC-SIGER	2

DECLARACIÓN DE PRACTICAS DE CERTICACIÓN

1. INTERPRETACIÓN Y APLICACIÓN

1.1 ÁMBITO LEGAL

Esta DPC se desarrolla considerando la Política de Certificación de la AC-DGNM y AC-SIGER, Código de Comercio, Reglamento del RPC, Lineamientos para la Operación del RPC y Acuerdo Interinstitucional por el que se establecen los lineamientos para la homologación, implantación y uso de la Firma Electrónica Avanzada en la Administración Pública Federal, publicado en el Diario Oficial de la Federación el 24 de agosto de 2006.

1.2 VIGENCIA Y NOTIFICACIÓN

La DGNM garantiza la continuidad de las actividades de las AC por un periodo de 1 año tras el vencimiento del último certificado firmado por las AC.

Si por alguna razón, la entidad responsable de la operación de las AC cambiara, la DGNM se compromete a publicar en la página del SIGER, si es posible, como mínimo 2 meses antes de que se produzca dicho cambio.

La organización que a partir de ese momento se haga cargo de las AC debe apegarse al presente documento.

Una vez terminada la operación de los servicios proporcionados por las AC, éstas no firman CRL ni certificado digital alguno.

Cualquier certificado digital firmado antes de la terminación de los servicios, y una vez

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

DECLARACIÓN DE PRACTICAS DE CERTICACIÓN

anunciada ésta, no puede tener un periodo de validez superior a la fecha fijada como cese de actividad. Una semana después del cese de la actividad, son revocados los certificados que continúen siendo válidos.

1.3 RESOLUCIÓN DE DISCREPANCIAS

En caso de existir dudas o discrepancias en la interpretación de esta DPC, el personal del Comité de Seguridad de la Información de la DGNM es quien las resuelve, emitiendo criterios definitivos para su aplicación.

2. PUBLICACIÓN

2.1 ACTUALIZACIÓN DE LA DPC

La última versión autorizada de este documento de DPC de las AC está en todo momento disponible al público en la página del SIGER.

2.2 REPOSITARIOS

La DGNM, a través de la DSIGER, es responsable de administrar el repositorio de certificados digitales y CRL de las AC.

Las AC no mantienen copias de las claves privadas asociadas con los certificados digitales emitidos por ellas.

2.2.1 FRECUENCIA DE FIRMADO DE CRL Y OCSP

Cada AC debe generar una CRL cada 24 horas, y tienen el compromiso de mantenerla actualizada, incluyendo todos los certificados digitales revocados desde la última actualización.

El servicio de OCSP es en línea, por lo que comprueba directamente del repositorio de claves públicas.

2.2.2 COMPROBACIÓN DE CRL Y OCSP.

Cualquier parte involucrada en una transacción electrónica que haga uso de certificados digitales emitidos por alguna AC, debe verificar el estado de los mismos contra la última CRL publicada por las AC en el camino de certificación ó contra el OCSP, desde el certificado digital en sí hasta la raíz de la jerarquía.

2.2.3 DISPONIBILIDAD DEL CRL Y OCSP.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

DECLARACIÓN DE PRACTICAS DE CERTICACIÓN

Las AC ofrecen un servicio de consulta en línea de CRL disponible en:

- AC-DGNM: <https://ac.siger.gob.mx/crls/dgnm>
- AC-SIGER: <https://ac.siger.gob.mx/crls/siger>

Las AC ofrecen el servicio de OCSP en la siguiente URL:

- <https://ac.siger.gob.mx/ocsp>

2.3 CONTROL DE ACCESO

La información publicada sobre DPC, PC, OCSP y CRL es de dominio público. Este acceso es de sólo lectura.

3. POLÍTICA DE CONFIDENCIALIDAD

3.1 TIPO DE INFORMACIÓN CONSIDERADA CONFIDENCIAL Y RESERVADA

Las AC, de acuerdo con la Política de Identificación y Clasificación de la Información de la DGNM, considera como información confidencial la siguiente:

- Toda información de los usuarios que no aparezca en el certificado digital emitido a favor de los mismos.

Y como reservada:

- Material criptográfico privado asociado con las AC.
- Información técnica de la infraestructura de las AC.

La información de carácter confidencial y reservada es tratada de acuerdo a lo dispuesto en la Política de Identificación y Clasificación de la Información de la DGNM, basada en la Ley Federal de Transparencia y Acceso a la Información Gubernamental, Criterios específicos para la administración de documentos, organización de archivos y clasificación de información, Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal; Lineamientos Generales para la organización y conservación de los archivos de las dependencias y entidades de la Administración Pública Federal; Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental; Lineamientos de Protección de Datos Personales; Ley Federal de Responsabilidades Administrativas de los Servidores Públicos; Lineamientos para la Elaboración de Versiones Públicas, por parte de las Dependencias y Entidades de la Administración Pública; Ley Federal de Procedimiento Administrativo.

4. REGISTRO INICIAL

4.1 TIPOS DE NOMBRES

Cada entidad perteneciente a esta infraestructura debe tener un DN (Distinguished Name

DECLARACIÓN DE PRACTICAS DE CERTICACIÓN

o Nombre Distinguido) único y claro.

El campo "Subject" o "Asunto" del certificado digital de identificación personal, firmado por las AC, debe proporcionar los siguientes atributos.

ATRIBUTO	DESCRIPCIÓN	ETIQUETA DEL REQUERIMIENTO
O	OrganizationName	Razón Social
OU	OrganizationalUnitName	Área
CN	CommonName	Nombre
T	Title	Cargo
STREET	StreetAddress	Dirección
PostalCode	PostalCode	Código Postal
L	LocalityName	Ciudad
S	State	Entidad Federativa
C	CountryName	País
E	EmailAddress	Correo Electrónico
Phone	Phone	Teléfono
2.5.4.23	Fax	Fax

Adicionalmente se puede incorporar los siguientes atributos:

ATRIBUTO	DESCRIPCIÓN	ETIQUETA EN EL REQUERIMIENTO
SN	SerialNumber	CURP Titular del Certificado Digital
2.5.4.45	X500uniqueididentifier	RFC del Titular del Certificado

El DN de los certificados digitales para equipo de cómputo a firmar por las AC deben proporcionar los siguientes atributos:

ATRIBUTO	DESCRIPCIÓN	ETIQUETA EN EL REQUERIMIENTO
O	OrganizationName	Razón Social
OU	OrganizationalUnitName	Área
CN	CommonName	Nombre
STREET	StreetAddress	Dirección
PostalCode	PostalCode	Código Postal
L	LocalityName	Ciudad
S	State	Entidad Federativa
C	CountryName	País
E	EmailAddress	Correo Electrónico

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

4.2 PROCEDIMIENTOS DE GENERACIÓN DE CLAVES DE LAS AC

Los únicos casos en los que se realiza generación de claves para Autoridad Certificadora son:

1. Fin de vida de la AC (Al cubrir el 80%).
2. Claves privadas comprometidas.
3. Avance tecnológico.

En cualquiera de los casos anteriores, se generará un nuevo par de claves de la longitud y tecnología adecuada.

5. EMISIÓN DE CERTIFICADOS

5.1 TIPOS DE CERTIFICADOS.

La AC-SIGER emite exclusivamente:

1. Certificados Digitales para Agentes Certificadores del SIGER (CD-AGS);
2. Certificados Digitales para Responsables de Oficina (CD-RO);
3. Certificados Digitales para Fedatarios Públicos (notarios y corredores públicos) (CD-FP);
4. Certificados Digitales para Identidad de equipo de cómputo y telecomunicaciones del SIGER (CD-SSL)
5. Certificados Digitales para Código de Programas Fuente y Objeto de los Sistemas y Subsistemas del SIGER (CD-CSSS)
6. Certificados de Dispositivos de Firma Electrónica (CD-DFE)

La AC-DGNM emite exclusivamente:

7. Certificados Digitales para Agentes Certificadores de la DGNM (CD-AGNM);
8. Certificados Digitales para personas de Unidades Administrativas y organismos descentralizados y desconcentrados de la SE (CD-SE);
9. Personas de Organismos del Sector Público autorizados por la DGNM.(CD-SP)

Para fines de los procedimientos descritos en esta DPC, los certificados de Identidad personal (CD-IP) serán los siguientes:

- CD-AGS
- CD-RO
- CD-FP
- CD-AGNM
- CD-SE
- CD-SP

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Los certificados que emiten las AC-SIGER y AC-DGNM almacenan la llave privada en un token o tarjeta biométrica.

Los únicos certificados con almacenamiento de llave privada en archivo son los que se emitirán para los Agentes Certificadores, para personas de Unidades Administrativas y organismos descentralizados y desconcentrados de la SE (CD-SE) y Personas de Organismos del Sector Público autorizados por la DGNM.(CD-SP).

5.2 PERÍODO DE VALIDEZ DE LOS CERTIFICADOS DIGITALES

- Para la Autoridad Certificadora es de veinte años, a partir de su fecha de emisión.
- Para los Agentes Certificadores es de dos años, a partir de su fecha de emisión.
- Para servidor y código fuente y objeto de los sistemas y subsistemas del SIGER, es de cinco años a partir de su fecha de emisión.
- Para el resto de la **comunidad** es máximo de dos años, a partir de su fecha de emisión.
- Se puede emitir certificados de menor duración, siempre y cuando así lo exprese el solicitante en el formato de solicitud firmado, o bien en el caso establecido en el punto 5.3.1. de esta DPC.

5.3 PROCEDIMIENTO DE IDENTIFICACION Y PERSONALIDAD JURÍDICA

5.3.1 Documentos de Identificación y Personalidad Jurídica para certificados de identidad personal:

La identificación del solicitante de un certificado digital se hace tomando en cuenta los documentos de identidad señalados en el formato de solicitud DGNM-IT-5-CG-SOL

Asimismo, debe acreditar su personalidad jurídica:

- Notarios Públicos: con su patente, FIAT, nombramiento o credencial de notario.
- Corredores Públicos: con su credencial o habilitación de corredor.
- Responsables de oficina: Habilitación expedida por la SE o Nombramiento de Gobierno del Estado, cédula profesional o título profesional de licenciado en Derecho o carta de pasante y carta compromiso del titular del RPC en la entidad para la entrega del título en un plazo no mayor a un año, por una sola vez.
- Personal de Unidades Administrativas y organismos descentralizados y desconcentrados de la SE y Personal de organismos del Sector Público autorizados por la DGNM: Credencial del IFE y credencial de empleado de la unidad administrativa, en caso de no contar con esta última, deberán presentar el talón de pago de la última quincena, así mismo, deberá aparecer su nombre en la lista de Solicitud de Certificado Digital para Servidor Público autorizado por la DGNM.

5.3.2 El procedimiento de identificación comprende los siguientes pasos:

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

DECLARACIÓN DE PRACTICAS DE CERTICACIÓN

- 1 El solicitante de un certificado digital se presenta personalmente ante el Agente Certificador o Auxiliar de Agente, con el original y copia de cualquiera de los documentos de identidad, así como de personalidad jurídica, establecidas en el punto 5.3.1, para cotejar la información con la copia simple de éste, la cual se integra a su expediente.
- 2 Para el caso de certificados CD-SE y CD-SP el Agente o Auxiliar de Agente deberá cotejar de que su nombre aparezca en la lista de Solicitud de Certificado Digital para Servidor Público autorizado por la DGNM, de la cual pedirá copia simple al solicitante o confirmará con el archivo del Departamento de Control de Certificados Digitales de la DGNM.
- 3 Confirmada la validez de las identificaciones, el agente certificador o el auxiliar del agente, verifica la coincidencia entre la fotografía contenida en aquellas y la filiación del solicitante.
- 4 El solicitante debe llenar el formato de solicitud correspondiente.
- 5 Realizado lo anterior, el agente certificador o el auxiliar, procede a solicitar que firme de forma autógrafa la solicitud del certificado y coteja la firma autógrafa de la solicitud contra el documento de identidad .

5.4 PROCEDIMIENTO DE EMISIÓN DE CERTIFICADOS DE IDENTIDAD PERSONAL:

- 1 El agente certificador o el auxiliar del agente, verifica si el solicitante cuenta con un certificado anterior, conectándose a:

<https://ac.siger.gob.mx> para certificados de la AC-SIGER.

<https://ac.siger.gob.mx/DGNM> para certificados de la AC-DGNM

En el módulo de consulta, introduce el nombre o apellido del solicitante, para buscar si tiene certificados a su nombre y si están vigentes.

De ser así, si la actividad la hizo el auxiliar de agente, procede a notificar al agente certificador para que realice el procedimiento de revocación señalado en el punto 6.2.3 de esta DPC. Si el agente certificador no puede realizar la revocación del certificado existente, deberá realizar la petición al Administrador de la AC correspondiente.

- 2 El agente certificador o el auxiliar del agente, prepara la tarjeta o *token* biométrico del solicitante y captura la huella dactilar en la misma.
- 3 En caso de que, el solicitante presente ilegibilidad en sus huellas dactilares, el

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

DECLARACIÓN DE PRACTICAS DE CERTICACIÓN


agente certificador o auxiliar de agente deberá llenar la Constancia de Ilegibilidad de Huellas Dactilares, en donde certifica que se realizaron varios intentos con sus diferentes dedos y no se encontraron huellas dactilares, y se procederá a preparar el *token* para que utilice contraseña. Es responsabilidad del Auxiliar de Agente comunicarle al Agente que se trata de un certificado de esta naturaleza y asentar la leyenda que se señala en los criterios de llenado del punto 5.4.1. de este documento

- 4 Solo la AC-DGNM podrá emitir certificados de identidad personal con protección de las claves en archivos y para lo cual se seguirá el procedimiento descrito en el punto 5.6 de esta DPC
- 5 A continuación el agente certificador o el auxiliar del agente, de acuerdo a la comunidad a la que pertenezca el solicitante, se conecta a una de las siguientes páginas:

<https://ac.siger.gob.mx> para solicitudes de certificados de la AC-SIGER.

<https://ac.siger.gob.mx/DGNM> para solicitudes de certificados de la AC-DGNM

- 6 Se procede a llenar el requerimiento, sujetándose a los criterios de llenado, que se detallan en el numeral 5.4.1. de este documento. El agente certificador o auxiliar del agente, así como el solicitante, deben cerciorarse que se haya capturado correctamente la información y que esté conforme a la solicitud. A continuación, el solicitante genera el requerimiento y graba la clave privada en la tarjeta o *token*, autenticándose con su huella dactilar o con su contraseña para los casos señalados en el punto 3 de este procedimiento. El requerimiento se envía a la autoridad certificadora.
- 7 En caso de que todos los pasos anteriores los haya realizado un auxiliar de agente, éste se debe comunicar con el agente certificador, para notificar que se envió el requerimiento. El agente certificador se conecta a la AC, según corresponda la comunidad del solicitante, revisa el requerimiento, y emite el certificado con la vigencia autorizada.
- 8 Si el requerimiento no cumple con los criterios señalados en el punto 5.4.1, se debe repetir el proceso para generar otro requerimiento.
- 9 Si el auxiliar de agente ha realizado correctamente las actividades señaladas del punto 1 al 4 de este procedimiento, el agente certificador se comunica con el auxiliar y le proporciona el número de serie del certificado generado.
- 10 El agente certificador ó el auxiliar del agente entra a la página de la AC correspondiente, y apoya al usuario en la instalación del certificado en la tarjeta o *token*. Para el caso de las tarjetas, comprueba que realmente se haya grabado, para lo cual quita y agrega el certificado del Contenedor de Windows. Y para el

 SECRETARÍA DE ECONOMÍA	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

DECLARACIÓN DE PRACTICAS DE CERTICACIÓN

token se elimina el certificado del contenedor de Windows, se expulsa el token, se vuelve a conectar y se observa que se agregue automáticamente al contenedor de Windows.

- 11 El titular del certificado debe firmar la carta de confidencialidad de acuerdo a la comunidad que pertenezca, así como el comprobante de emisión de certificado digital de FEA.
- 12 El agente certificador y el auxiliar del agente debe recopilar la documentación establecida en el formato de Solicitud de Certificado Digital DGNM-IT-5-CG-SOL, Carta de Confidencialidad y Comprobante de Emisión del Certificado.
- 13 El agente certificador y el auxiliar del agente son responsables de enviar la documentación derivada del procedimiento de generación al Departamento de Control de Certificados Digitales de la DGNM.

5.4.1 CRITERIOS DE LLENADO DEL REQUERIMIENTO DE CD DE IDENTIDAD PERSONAL:

- 1 Se utilizan mayúsculas y minúsculas.
- 2 No se utilizan acentos.
- 3 Sólo se utilizan abreviaturas en los campos de Razón Social y Dirección cuando la información exceda el límite, conforme a las reglas ortográficas.
- 4 Razón Social:
 - Para AC-DGNM: se captura "Secretaria de Economía".
 - Para Responsables de Oficina: se captura "Registro Publico de la Propiedad y de Comercio", seguido del municipio y estado al que pertenezca.
 - Para el Registro Inmediato de Empresas (RIE) es "Registro Publico de la Propiedad y del Comercio del Estado de" seguido del nombre del estado correspondiente.
 - Para Fedatarios Públicos: se captura "Correduria" o "Notaria Publica" seguido del número, municipio o delegación política (en el caso del Distrito Federal) y entidad correspondiente.
 - En caso de que el titular del certicado tenga la personalidad jurídica de Corredor y Notario se asentará "Correduria No. nn y Notaria Publica No. nn" seguido de municipio o delegación política y entidad correspondiente. (En donde nn es el número de correduría o notaría correspondiente).
- 5 Área:
 - Para AC-DGNM: Dirección de Área, Delegación o Subdelegación Federal de la SE a la que pertenezcan: ejemplo "Delegación Federal en Guanajuato".
 - Para AC-SIGER: se deja en blanco, excepto para el RIE que se coloca la leyenda "Registro Inmediato de Empresas" y para el caso de los certificado

 SECRETARÍA DE ECONOMÍA	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

DECLARACIÓN DE PRACTICAS DE CERTICACIÓN

- que se emiten por ilegibilidad de huellas dactilares, se pondrá "Clave Privada en Token"
- 6 Tanto el RFC y CURP son necesarios cuando el titular del certificado desee que su certificado sea aceptado por las dependencias integrantes de la Subcomisión de la FEA. En cuyo caso se debe aplicar el **"Procedimiento para la Validación de CURP y RFC"** que se encuentra en la dirección electrónica <http://www.cidge.gob.mx>.
 - 7 Nombre, se captura primero el nombre de pila y en seguida los apellidos del solicitante.
 - 8 Profesión:
 - Para AC-DGNM: cargo o puesto correspondiente.
 - Para fedatario público se anota "Notario Publico" Titular, Suplente, Adscrito o como señale su patente o FIAT y "Corredor Publico".
 - Para Responsable de Oficina: se anota "Responsable de Oficina" o "Registrador Publico".
 - 9 Dirección: Se anota el domicilio en que se ubique la oficina del solicitante; utilizando el signo #, en lugar de cualquier otra forma de abreviatura para el número del inmueble en el que se ubiquen.
 - 10 Código postal: (5 dígitos),
 - 11 Ciudad y entidad federativa: los que corresponden al domicilio.
 - 12 Nivel de seguridad: al menos de *High Grade* (1024 bits).
 - 13 País: México.
 - 14 Correo electrónico: se captura el *e-mail* del solicitante, todo en minúsculas.
 - 15 Teléfono y fax: se anota la clave lada entre paréntesis y después el número de teléfono correspondiente si tiene extensión, especificar. Ejemplo: (33)51433121 Ext. 33544
 - 16 Clave de anulación: se anota en letras mayúsculas o minúsculas, o números, o las combinaciones de ambos con un máximo de 20 caracteres.
 - 17 Confirmación, se repite la clave de anulación, con el mismo formato.
 - 18 CryptProvider (Proveedor criptográfico): el que corresponda a la tecnología utilizada en los dispositivos biométricos, ejemplos:
 - Para tarjetas criptográficas Cyberflex y Miotec: SeguriCSP-Cryptographic Service Provider v 1.0
 - Para lector Biotoken: SafeSign Standard Cryptographic Service Provider

5.5 EMISIÓN DE CERTIFICADOS DIGITALES PARA EQUIPOS DE CÓMPUTO.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

DECLARACIÓN DE PRACTICAS DE CERTICACIÓN

Se emiten certificados para equipo de los siguientes tipos:

- Certificados Digitales para Identidad de Equipo de Cómputo y Telecomunicaciones del SIGER (CD-SSL), se activa el atributo de SSL.
- Certificados Digitales para Código de Programas Fuente y Objeto de los Sistemas y Subsistemas del SIGER (CD-CSSS), se activa el atributo de firma de código.
- Certificados de Dispositivos para Servicios de Firma Electrónica (CD-DSFE), se activa el atributo de firma.

La emisión de dichos certificados se realiza de la siguiente manera:

1. El solicitante debe llenar y firmar formato de Solicitud de Certificado para Equipo de Cómputo, el cual debe entregar para su autorización a la DGNM.
2. Una vez autorizado, la solicitud se debe hacer llegar al agente certificador.
3. El solicitante debe llenar el requerimiento de acuerdo a lo señalado en el apartado 5.5.1.
4. El archivo del requerimiento se debe enviar por medios electrónicos al agente certificador autorizado por la DGNM para su emisión.
5. El agente certificador recibe el formato de solicitud y el requerimiento, debe comprobar que estén debidamente llenados según lo descrito en esta DPC y que todos los datos que aparecen en los mismos son correctos, con lo que procede a la generación del certificado activando el atributo de acuerdo al tipo de certificado que se autorizó.
6. El agente certificador debe cerciorarse de recibir debidamente firmada la carta de confidencialidad y uso del certificado de equipo antes de hacer entrega del certificado al solicitante.
7. Si la solicitud o el requerimiento no cumplen con lo establecido, se debe hacer del conocimiento del solicitante, para que haga las correcciones correspondientes.

5.5.1 CRITERIOS DE LLENADO DEL REQUERIMIENTO PARA CERTIFICADOS DE EQUIPO.

1. Se utilizan mayúsculas y minúsculas.
2. No se utilizan acentos.
3. Sólo se utilizan abreviaturas en los campos de Razón Social y Dirección cuando la información exceda el límite, conforme a las reglas ortográficas.
4. Razón Social: Se captura el nombre de la organización correspondiente, por ejemplo: "Secretaría de Economía".
5. Área: Se captura el área a la que pertenezca.
6. Nombre: Nombre del equipo, dominio o IP pública del servidor o equipo

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

correspondiente

7. Dirección: Se anota el domicilio en donde se ubique el equipo; utilizando el signo #, en lugar de cualquier otra forma de abreviatura para el número del inmueble en el que se ubiquen.
8. Código postal: (5 dígitos)
9. Ciudad y entidad federativa, los que corresponden al domicilio.
10. Nivel de seguridad: es al menos *High Grade* (1024 bits).
11. País: México.
12. Correo electrónico: se captura el *e-mail* del solicitante, todo en minúsculas.
13. Clave de Acceso: Capturar una contraseña de al menos 8 caracteres, con combinación de letras y números (opcional).
14. CryptProvider (Proveedor criptográfico): el que corresponda al dispositivo o mecanismo de protección de la clave privada (opcional).

5.6 EMISIÓN DE CERTIFICADOS DIGITALES CON PROTECCIÓN DE CLAVES EN ARCHIVOS.

1. Solo se emitirán en los casos señalados en esta DPC.
2. Se utilizará una herramienta informática para la generación del archivo .req y .key.
3. El Archivo .req se generará utilizando los criterios de llenado de requerimiento.
4. El Archivo .key solo debe quedar en posesión del titular y no se guardarán copias.
5. El archivo .req se enviará al agente certificador para la generación del certificado digital y se enviará el archivo .cer al titular.
6. El titular o responsable del certificado deberá firmar los documentos señalados en los apartados correspondientes para el tipo de certificado digital que se le emitió.

6. REVOCACIÓN DE CERTIFICADOS DIGITALES

6.1 CAUSAS ADMISIBLES DE REVOCACIÓN

Cuando la clave privada de las AC estuviera comprometida, se revocan todos los certificados digitales de la comunidad correspondiente. No se puede solicitar ni generar certificados digitales hasta que no se restaure la identidad de la AC.

Cualquier certificado digital puede ser revocado si:

- Por extinción del periodo de validez del propio certificado digital
- Ha existido pérdida, robo, modificación, divulgación no autorizada u otro compromiso de la clave privada asociada al certificado digital.

 SE <small>SECRETARÍA DE ECONOMÍA</small>	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

DECLARACIÓN DE PRACTICAS DE CERTIFICACIÓN

- Por incumplimiento del titular en alguna de las obligaciones descritas en la Política de Certificación y en esta DPC.
- Falsedad, inexactitud o errores en los datos presentados en el certificado digital.
- Cuando alguno de los requisitos de emisión del certificado digital no se cumplió.
- El sistema de certificación se vio comprometido de modo tal que afecta a la fiabilidad del certificado digital.
- Fallecimiento del titular o incapacidad jurídica declarada por una autoridad competente.
- Cambio de información relativa al titular.
- Resolución administrativa o judicial que lo ordene.
- A solicitud del titular del certificado.
- Imposibilidad de lectura de la tarjeta o *token* en que se resguardó la clave privada.
- Conclusión de las funciones para las que le fue otorgado el certificado.

6.2 PROCEDIMIENTO DE REVOCACIÓN DE CERTIFICADOS

6.2.1 Por petición del titular del certificado:

- El titular del certificado, deberá acudir a las oficinas de la Dirección General de Normatividad Mercantil o a las Delegaciones Federales de la Secretaría de Economía
- Presentar un escrito libre con firma autógrafa del titular.
- Presentar algún documento de identidad de los señalados en el formato de solicitud DGNM-IT-5-CG-SOL.
- Si el procedimiento se realiza ante el Auxiliar de Agente, deberá ponerse en contacto con el Agente Certificador que emitió el certificado ó con el Administrador de la AC y esperar la confirmación de revocación.
- Se deberá emitir el comprobante de revocación del certificado y entregarlo al solicitante, de acuerdo con los Lineamientos para la homologación, implantación y uso de la FEA en la Administración Pública Federal, capítulo VI párrafo noveno.



6.2.2 Revocación en Línea:

Se brinda el servicio de revocación en línea para que el titular revoque su certificado digital, proporcionando para ello únicamente su clave de revocación que indicó en el requerimiento de certificación:

- Para la AC-SIGER : <https://ac.siger.gob.mx>
- Para la AC-DGNM : <https://ac.siger.gob.mx/DGNM>

6.2.3 Otras Revocaciones:

Si se produjo algún error durante la emisión de un certificado y es necesario generar otro, el agente certificador, debe revocar de inmediato el anterior, para poder generar otro al mismo titular.

 SECRETARÍA DE ECONOMÍA	 DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

DECLARACIÓN DE PRACTICAS DE CERTICACIÓN

Si el titular, cuenta con certificado previamente y no puede usarlo, se le revocará previo a la generación de un nuevo certificado.

7. AUDITORÍA DE SEGURIDAD INFORMÁTICA

Se recomienda la auditoría del Programa para Autoridades Certificadoras WebTrust.

7.1 TIPOS DE EVENTOS REGISTRADOS

- Los registros de accesos al servidor que contiene al sistema de las AC.
- Los registros que genera el sistema de las AC.
- Las solicitudes de emisión de certificados y de revocación (documental).
- La generación de los CD y las CRL.

7.2 PROCEDIMIENTOS DE RESPALDO DE REGISTROS DE AUDITORÍA

Para los registros electrónicos, se aplica la Política de Respaldos de la Información de la DGNM y sus procedimientos.

7.3 NOTIFICACIÓN DE VULNERABILIDADES

El administrador de la AC notifica cualquier vulnerabilidad en el sistema de AC al personal del área de Seguridad. El área de Seguridad deberá revisar el análisis de riesgos del sistema de AC al menos una vez al año.

8. ARCHIVOS

8.1 ARCHIVO DOCUMENTAL

El Departamento de Control de Certificados Digitales de la DGNM. almacena los siguientes registros en papel:

Para los Certificados de Identidad Personal:

- Formato de solicitud DGNM-IT-5-CG-SOL
- Copia simple de los documentos de identidad señalados en el formato DGNM-IT-5-CG-SOL.
- Copia simple de los documentos de personalidad jurídica señalados en el formato DGNM-IT-5-CG-SOL.
- Carta de Confidencialidad
- Comprobante de Emisión del Certificado.
- Copia de la Solicitud de Certificado Digital para Servidor Público

Para los Certificados de Equipo:

- Formato de solicitud DGNM-IT-5-CG-SOL.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

DECLARACIÓN DE PRACTICAS DE CERTICACIÓN

- Carta de Confidencialidad y Uso
- Copia de la Identificación del Responsable del Equipo.

En caso de Revocaciones a petición del titular:

- Comprobante de Solicitud y Revocación de Certificado de FEA de Identidad Personal.

Otros:

- Copia de Nombramiento de Agentes.
- Copia de Nombramiento de Auxiliar de Agentes

8.2 PROTECCION DE ARCHIVOS

Los archivos electrónicos de auditoría son almacenados digitalmente de forma segura para evitar lectura, modificación o destrucción no autorizada. Para hacer esto, las copias de seguridad están protegidas criptográficamente y almacenadas en lugares de acceso sólo a personal autorizado.

La contraseña utilizada en las copias, sigue la Política de Contraseñas para el SIGER, y es sólo conocida por el personal que administra las AC.

La información almacenada en papel está bajo llave. Esta llave está bajo la responsabilidad del personal autorizado.

8.3 PERIODO DE ALMACENAMIENTO

Los archivos de auditoría y documental, se almacenan por un tiempo máximo de doce años.

9. RESPALDO Y RECUPERACIÓN

9.1 RESPALDOS

Se respalda la información del servidor que opere la AC-DGNM y AC-SIGER de acuerdo a la Política de Respaldo de la Información de la DGNM.

En cuanto a la clave privada de las AC está en todo momento cifrada cuando se almacene de modo permanente (FIPS 140-1 nivel 3). Este almacenaje se realiza en un lugar seguro que permita su recuperación si se produce algún tipo de contingencia.

9.2 RECUPERACION

9.2.1 POR COMPROMISO DE LA CLAVE PRIVADA

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

DECLARACIÓN DE PRACTICAS DE CERTICACIÓN

Si la clave privada de la AC-DGNM o AC-SIGER estuviera comprometida, se procedería a la revocación de la misma, siendo solamente válidos aquellos certificados digitales emitidos por la AC-DGNM o AC-SIGER cuya fecha de emisión fuera anterior a la fecha de revocación de la misma. El Comité de Seguridad de la Información de la DGNM decidirá si se toman medidas adicionales.

La generación de CRL se suspende hasta que se restaure la identidad de la AC comprometida.

El mismo procedimiento se lleva a cabo en las organizaciones con las que se hayan establecido reconocimiento de certificados digitales.

9.2.2 POR CONTINGENCIAS

En caso de contingencia, el personal a cargo de las AC-SIGER seguirá el procedimiento establecido en Plan de Contingencias del SIGER y PKI-SE.

10. SEGURIDAD

10.1 SEGURIDAD FÍSICA

El servidor que contiene las AC debe estar ubicado en la bóveda de seguridad del Centro de Datos de la DGNM.

El área está protegida por esclusas y un mecanismo de seguridad que evita la captación externa de las emanaciones de ondas electromagnéticas de los equipos.

10.1.1 ACCESO FÍSICO

El acceso a la bóveda de seguridad del centro de datos, está restringido a personal del SIGER autorizado, mediante un sistema de control de accesos, quedando registrado y grabado en CCTV (Circuito Cerrado de Televisión) cualquier acceso a la misma.

10.1.2 CONDICIONES FÍSICAS DE LA BÓVEDA DE SEGURIDAD.

La bóveda de seguridad del centro de datos tiene unidades de aire acondicionado de precisión. Tanto la humedad como la temperatura se controlan automáticamente.

Tiene módulos UPS instalados, una planta de emergencia generadora de energía eléctrica, supresores de transitorios que garantizan un fluido eléctrico constante sin interrupciones ni picos, y tierra física.

El centro de datos tiene medidas de seguridad contra inundaciones. Así mismo, tiene

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

DECLARACIÓN DE PRACTICAS DE CERTICACIÓN

sistemas de detección temprana de humo y extinción de incendios.

10.1.3 MEDIOS DE ALMACENAMIENTO

Los sistemas del SIGER cuentan con *software* para respaldos (en el equipo HP). Se realizan copias de seguridad de acuerdo a la Política de Respaldos de la Información de la DGNM. Las copias de seguridad se resguardan en sitios determinados.

10.1.4 RESPALDO DE INFORMACIÓN FUERA DEL CENTRO DE DATOS DE LA DGNM

El respaldo de información se localiza en un sitio alternativo.

10.2 SEGURIDAD EN LOS PROCEDIMIENTOS DE OPERACIÓN

10.2.1 ACTORES DE CONFIANZA INVOLUCRADOS

Se puede distinguir los siguientes actores en la operación de las AC:

- La DSIGER.
- Administrador del sistema de AC.
- Personal de seguridad del SIGER.
- Los agentes certificadores .
- Auxiliares de agente.

Las responsabilidades de estos actores, se delimitan en la sección de Responsabilidades de este documento.

10.2.2 NÚMERO DE PERSONAS REQUERIDO POR TAREA

- Un administrador del servidor de AC, del servidor de publicación de certificados digitales, CRL y del servicio OCSP.
- Un administrador de la infraestructura de emisión de Sellos de Tiempo.
- Agentes certificadores.
- Al menos un auxiliar de agente en cada representación federal.

10.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE CADA ACTOR

No existe ningún tipo de identificación y autenticación para los actores. Los actores de confianza involucrados se conocen unos a otros y forman parte del personal de la DGNM, a excepción de los auxiliares de agente de las delegaciones estatales, quienes se autenticarán previamente a la emisión de cada certificado, con el envío de su nombramiento firmado por el titular de la dependencia y se podrá consultar en el archivo del Departamento de Control de Certificados Digitales de la DGNM.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

DECLARACIÓN DE PRACTICAS DE CERTICACIÓN

10.3 SEGURIDAD EN EL PERSONAL

10.3.1 REQUERIMIENTOS DE FORMACIÓN DEL PERSONAL DE SEGURIDAD

El personal debe ser licenciado o ingeniero en Informática o área afin. Comprobar al menos dos años de experiencia en el campo de seguridad informática y acreditar conocimientos en seguridad informática.

Cumplir con el requisito de no haber sido condenado por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo haya sido inhabilitado para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

10.3.1.1 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL QUE OPERA LAS AC

Al personal que se encarga de la operación de las AC se le entrega la siguiente documentación:

- 1) Política de Certificación de las AC-DGNM y AC-SIGER.
- 2) Declaración de Prácticas de Certificación de las AC-DGNM y AC-SIGER.
- 3) Manuales de Operación de las AC-DGNM y AC-SIGER.
- 4) Plan de Administración de Claves de las AC-DGNM y AC-SIGER.
- 5) Política General de Seguridad de la Información de la DGNM.
- 6) Política de Seguridad Física del SIGER.
- 7) Plan de Contingencias del SIGER y PKI-SE.

10.3.2 DESIGNACIÓN DE UN AGENTE CERTIFICADOR

1. El candidato a agente certificador, debe ajustarse al Procedimiento de Nombramiento de Agente Certificador, procedimiento interno de la DGNM.
2. Una vez concluído el mismo, recibe un oficio de Nombramiento de Agente Certificador, emitido por el Director General de Normatividad Mercantil, con copia para el Director del SIGER para que se le genere su certificado de agente.
3. Con la recepción de su certificado de agente, debe firmar su carta de Confidencialidad y de Reconocimiento de la Política de Certificación.

10.3.3 DESIGNACIÓN DE UN AUXILIAR DE AGENTE CERTIFICADOR

1. El auxiliar de agente certificador, debe ser nombrado por el delegado o subdelegado federal de la entidad correspondiente mediante el oficio de Nombramiento de

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

DECLARACIÓN DE PRACTICAS DE CERTICACIÓN

- Auxiliar de Agente, con copia al Director General de Normatividad Mercantil.
2. Por la naturaleza de sus funciones, se recomienda que cuente con licenciatura o carrera técnica en el área de informática.
 3. Debe obtener los conocimientos sobre las actividades que realiza el auxiliar de agente, auto-capacitándose con los manuales que le proporcionará la DGNM.
 4. Debe firmar su carta de Confidencialidad y de Reconocimiento de la Política de Certificación y enviarla a la Dirección General de Normatividad Mercantil.

10.4 SEGURIDAD LÓGICA

10.4.1 INSTALACIÓN Y GENERACIÓN DEL PAR DE CLAVES

El par de claves de cada AC, son generadas utilizando el módulo criptográfico de almacenamiento seguro de claves (HSM).

La contraseña para la protección de la clave privada, almacenada en el módulo criptográfico (HSM), debe cumplir con lo estipulado en la Política de Contraseñas del SIGER y PSC. La clave privada, una vez que se almacene en el módulo criptográfico, debe estar cifrada.

10.4.2 SISTEMA DE CUSTODIOS PARA LA OPERACIÓN DE LA AC.

El arranque de la operación de la AC está protegido por el módulo criptográfico, el cual está configurado con un sistema de operadores o custodios en el que se requieren n de m tarjetas presentes, que están bajo resguardo de personal de la DGNM.

Las contraseñas utilizadas para el arranque de las AC debe cumplir con la Política de Contraseñas del SIGER. La contraseña de cada persona que gestiona la actividad de las AC es conocida sólo por ésta. Cualquier cambio de dicho personal implica la modificación de dicha contraseña.

Mantenimiento

Todos los cambios realizados sobre estas Prácticas de Certificación son anunciados en la página WEB del SIGER.

Si los cambios son de envergadura se deja abierto un periodo de quince días para la recepción de comentarios. Si no es posible conseguir una aprobación de los cambios estos no son realizados.

Responsabilidades

RESPONSABILIDADES DE LA DSIGER



1. Ofrecer y mantener la infraestructura necesaria para el establecimiento de una PKI, según lo descrito en este documento.
2. Implantar y mantener los requerimientos de seguridad impuestos a las claves criptográficas de la AC-SIGER y AC-DGNM, según lo descrito en este documento.
3. Poner a disposición de quien desee verificar una FEA, las copias de los certificados digitales y de cualquier información de revocación con referencia a dichos certificados digitales. Para ello cumplirá con lo establecido en el apartado de Disponibilidad de CRL y OCSP.
4. Proteger los datos de carácter personal que sean suministrados por la **comunidad**, de acuerdo con la Ley Federal de Transparencia y de Acceso a la Información Pública Gubernamental.
5. Comunicar inmediatamente a la comunidad, el compromiso, pérdida, divulgación, modificación o uso no autorizado de la clave privada de las AC, con el fin de restaurar la PKI lo antes posible según lo establecido en este documento.
6. Cualquier anomalía o incidente producidos entre el momento de la revocación del certificado digital y de la clave privada de las AC y el momento de la notificación a la **comunidad** y posterior revocación de los certificados digitales emitidos, es responsabilidad única y exclusiva de la DSIGER.
7. Cualquier incidente o responsabilidad generada de la clave privada de las AC que se encuentre comprometida, es responsabilidad única y exclusiva de la DSIGER.

RESPONSABILIDADES DEL ADMINISTRADOR DEL SISTEMA DE AC:

1. Dar mantenimiento y manejar los servidores que opera la AC.
2. Respalidar información (*software*, base de datos, etc.)
3. Seguir los procedimientos y dictámenes de esta DPC para la generación y revocación de certificados digitales.
4. Monitorear los registros generados por el sistema de AC, del S.O. del servidor y de los accesos a la bóveda de seguridad del centro de datos que alberga el servidor dedicado a la operación de la AC.

RESPONSABILIDADES DEL PERSONAL DE SEGURIDAD DEL SIGER:

1. Mantener la seguridad física de la PKI.
2. Revisar los registros generados por el sistema de AC, del S.O. del servidor de AC y de los accesos a la bóveda de seguridad del centro de datos donde se localiza el servidor de AC.

DE LOS AGENTES CERTIFICADORES.

1. Conocer la Política de Certificación y la Declaración de Prácticas de Certificación y seguir todas las reglas en ellas descritas.
2. Vigilar la vigencia de su certificado de Agente Certificador y gestionar su renovación

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

- previo a su vencimiento.
3. Llevar a cabo el procedimiento para la emisión de CD, establecido en esta DPC.
 4. Emitir certificados digitales de la duración y tipo establecidos en esta DPC.
 5. No emitirán certificados de prueba.
 6. Cuando el CD es solicitado ante un Auxiliar de Agente, es responsabilidad del agente certificador cerciorarse de que el titular de un CD haya acreditado su personalidad jurídica y comprobado su identidad.
 7. Cuando el CD es solicitado ante un agente, debe llevar a cabo la identificación y acreditación jurídica del titular, conforme a lo establecido en la DPC.
 8. Realizarán la revocación de certificados digitales, de acuerdo a lo establecido en esta DPC.
 9. Cuando el CD es solicitado ante el Agente, deberá recabar la documentación que se indica en la presente DPC y hacerla llegar al Departamento de Control de Certificados Digitales de la DGNM para su archivo.
 10. Cualquier incidente o responsabilidad generada por el compromiso de la clave privada de los agentes certificadores será responsabilidad única y exclusiva de ellos

DE LOS AUXILIARES DE AGENTES CERTIFICADORES

1. Conocer la Política de Certificación y la Declaración de Prácticas de Certificación y seguir todas las reglas en ellas descritas
2. Llevar a cabo la identificación y acreditación jurídica del titular, de acuerdo con los procedimientos establecidos en esta DPC.
3. Realizar los pasos que los involucran y que están descritos en los Procedimientos de Emisión de Certificados Digitales de la presente DPC
4. Recabar la documentación que se indica en la presente DPC y hacerla llegar al Departamento de Control de Certificados Digitales de la DGNM para su archivo.

RESPONSABILIDADES DE LOS USUARIOS

1. En el caso de compromiso de la clave privada (o de sospecha de compromiso) del certificado digital de un usuario, éste se compromete a notificarlo a AC-DGNM o AC-SIGER y a las partes implicadas.
2. Cualquier anomalía o incidente producidos entre el momento de la revocación de un certificado digital emitido por la AC-DGNM y AC-SIGER, y el momento de la notificación de tal evento a la Autoridad Certificadora, es responsabilidad única y exclusiva del usuario propietario de dicho certificado digital.
3. Cualquier incidente o responsabilidad originados del compromiso de la clave privada de un usuario será responsabilidad única y exclusiva de éste.
4. El titular del CD es el responsable único y final de mantener la confidencialidad de la clave privada de FEA, por tanto la información que firme utilizando su CD le será atribuible exclusivamente a él.

SANCIONES

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

Los agentes certificadores y sus auxiliares, para salvaguardar la legalidad, honradez, lealtad, imparcialidad y eficiencia que deben ser observadas en el desempeño de su función y cuyo incumplimiento dará lugar al procedimiento y a las sanciones que correspondan, en términos de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, y tendrán las siguientes obligaciones:

- I. Cumplir con la máxima diligencia el servicio que le sea encomendado y abstenerse de cualquier acto u omisión que cause la suspensión o deficiencia del servicio que implique abuso o ejercicio indebido de su cargo o comisión;
- II. Utilizar los recursos que tengan asignados para el desempeño de su cargo o comisión, las facultades que le sean atribuidas o la información reservada a que tenga acceso por su función exclusivamente para los fines establecidos es esta política;
- III. Custodiar y cuidar la documentación e información que por razón de su cargo o comisión conserve bajo su cuidado o a la cual tenga acceso, impidiendo o evitando el uso, la sustracción, destrucción, ocultamiento o inutilización indebidas de aquéllas;
- IV. Observar buena conducta en su cargo o comisión, tratando con respeto, diligencia, imparcialidad y rectitud a las personas con las que tenga relación con motivo de éste.

Sí llegare a detectarse alguna anomalía que presuma el incumplimiento de la política de certificación, la misma será puesta a consideración del Comité de Seguridad de la Información de la DGNM a fin de evaluar la gravedad del caso y de considerarlo necesario se hará del conocimiento del Director General de Normatividad Mercantil a fin a que proceda a instrumentar las acciones necesarias para evitar reincidencias e independientemente, de hacerlo del conocimiento del órgano de control interno para los efectos correspondientes.

Registro de Cambios			
Versión Anterior	Descripción del Cambio	Fecha del Cambio	Participantes en la Revisión del Cambio
1.0	<p>Se eliminan secciones y procedimientos considerados como internos de la DGNM.</p> <p>Se modifica la redacción de la DPC, en todas sus secciones, para que quede más clara, precisa y sobre todo previendo los cambios tecnológicos.</p> <p>Se agrega el procedimiento para tipo de certificado para el Sector Público. (CD-SP).</p> <p>Se agrega el procedimiento para la Emisión de Certificados Digitales con Protección de Claves en</p>	<p>Del 01/May/2008 al 07/Ago/2008/</p>	<p>Silvia Elena Hernández Martínez</p> <p>Karina Romo Maldonado</p> <p>Ernesto del Castillo Hernández</p> <p>Mario Guerrero Barrera</p>

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

	Archivos. Se agregan especificaciones para los certificados que se emiten con motivo de huellas ilegibles. Se realizaron modificaciones a los formatos. Se agrega el cuadro de registro de cambios.		
--	--	--	--

Referencias
<p>[1] RFC 2527 " <i>Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework</i>" Marzo 1999 ftp://ftp.isi.edu/in-notes/rfc2527.txt</p> <p>[2] Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de protección de datos de carácter personal y sus normas de desarrollo https://www.agenciaprotecciondatos.org/datd1.htm</p> <p>[3] RFC 2459 " <i>Internet X.509 Public Key Infrastructure: Certificate and CRL Profile</i>" Enero 1999 ftp://ftp.isi.edu/in-notes/rfc2459.txt</p>



**DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN
DE LA AC-DGNM Y AC-SIGER**

Versión
2.0
Fecha
27/AGO/2008

Anexos

SOLICITUD DE CERTIFICADO DIGITAL DE FEA

Nombre del Solicitante: _____		
R.F.C.: _____ CURP: _____		
Razón Social: _____		Estado/plaza: _____
Area: _____		Municipio: _____
Domicilio de la oficina del Solicitante: (Incluir: calle, numero, colonia, Del. ó Mun. y codigo postal) _____ _____		
Correo electrónico: _____		Tel.(s): _____ Fax: _____
DOCUMENTO DE IDENTIDAD.	DOCUMENTO PROBATORIO DE IDENTIDAD	DOCUMENTO DE PERSONALIDAD JURÍDICA
<input type="checkbox"/> Cédula Profesional <input type="checkbox"/> Pasaporte <input type="checkbox"/> Credencial de Elector <input type="checkbox"/> Cartilla del Servicio Militar Nacional. <input type="checkbox"/> Identificación con fotografía expedida por Gobierno Federal, Estatal o Municipal	<input type="checkbox"/> Copia Certificada de Acta de Nacimiento <input type="checkbox"/> Documento Migratorio <input type="checkbox"/> Carta de Naturalización <input type="checkbox"/> Certificado de Nacionalidad Mexicana	<input type="checkbox"/> FIAT <input type="checkbox"/> Nombramiento <input type="checkbox"/> Patente <input type="checkbox"/> credencial de notario <input type="checkbox"/> Credencial de corredor <input type="checkbox"/> Habilitación de corredor. <input type="checkbox"/> Habilitación de Responsables de oficina.
Observaciones: _____ _____ _____		

Firma del Solicitante: _____	Fecha: _____
--	------------------------

Datos del Agente Certificador o Auxiliar del Agente:

Nombre: _____	
Cargo: _____	Firma: _____



DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER

Versión
2.0
Fecha
27/AGO/2008


TERMINOS:

- El suscrito, cuyos datos generales aparecen al anverso de la presente solicitud, y a quien en lo sucesivo se le denominará como "El Solicitante" para todos los efectos legales que deriven del presente documento a que haya lugar, manifiesta ante **La Secretaría de Economía** a quien en lo sucesivo se le denominará como "La Agencia o Autoridad Certificadora" (AC), que es su libre voluntad contar con un Certificado Digital de Firma Electrónica Avanzada en el que conste la clave pública que se encuentra asociada a la clave privada y frase de seguridad de revocación que manifiesta haber generado previamente y en absoluto secreto, sin que persona alguna lo haya asistido durante dicho proceso.
- Asimismo, "El Solicitante", manifiesta su conformidad en que "La AC" utilice el procedimiento de certificación de identidad que estime conveniente.
- "El Solicitante" reconoce que para la emisión del referido Certificado Digital de Firma Electrónica Avanzada, "La AC" revisó la documentación que se indica en el anverso de esta solicitud, con la cual el propio usuario se identificó, constatando a simple vista que los documentos corresponden a "El Solicitante", por lo que este último asume la responsabilidad exclusiva respecto de la autenticidad de los datos y documentación por él proporcionada a "La AC". De la misma forma "El Solicitante" asume la responsabilidad exclusiva del debido uso del Certificado Digital de Firma Electrónica Avanzada.
- "El Solicitante" en este acto acepta el certificado digital mencionado, sirviendo este documento como el acuse de recibo más amplio que en derecho proceda.
- Adicionalmente, "El Solicitante", acepta que el uso de la clave privada y frase de seguridad de revocación, con base en las cuales dicho certificado fue elaborado, quedarán bajo su estricta y absoluta responsabilidad, la cual incluye en forma enunciativa, los daños y perjuicios, incluso aquéllos de carácter financiero, que pudieran causarse por su uso indebido, no pudiendo alegar que tal uso se realizó por persona no autorizada.
- "El Solicitante" conoce y acepta que la clave pública proporcionada por él y contenida en el Certificado Digital de Firma Electrónica Avanzada, así como en cualquier otro certificado digital que con posterioridad se obtenga, será de carácter público y podrá ser consultada libremente por cualquier interesado a través de los medios y formas que disponga "La AC".
- Por lo anterior, "El Solicitante" se obliga a mantener absoluta confidencialidad de la clave privada y frase de seguridad de revocación, así como a realizar los trámites necesarios para la revocación de dicho certificado ante "La AC", mediante los mecanismos y procedimientos que el mismo establezca, en el caso de que por cualquier causa dicha información sea divulgada o se realice cualquier supuesto por el que "El Solicitante" deba solicitar su revocación en los términos de las disposiciones legales vigentes.
- Por otra parte "El Solicitante" manifiesta conocer el contenido y alcance de las disposiciones legales y reglamentarias relativas a la celebración de actos jurídicos mediante el uso de medios electrónicos, digitales o de cualquier otra tecnología, por lo que asume plena responsabilidad respecto de la información y contenido de todo documento electrónico o digital elaborado y enviado en el que se haga uso de la citada clave privada, toda vez que por ese solo hecho se considerara que el documento electrónico o digital le es atribuible.
- "El Solicitante" reconoce y acepta que "La AC" únicamente es responsable de los errores que, en su caso, llegaren a cometer con motivo de culpa grave en el proceso de generación, registro, entrega y revocación del certificado digital, según corresponda, así como que no será responsable por los daños y perjuicios que se pudieran causar a "El Solicitante" o a terceros, cuando por caso fortuito o fuerza mayor no puedan realizarse registros, verificaciones, revocaciones o tramitar documentos electrónicos cifrados con las claves públicas y privadas relacionadas con dicho certificado. Por caso fortuito o fuerza mayor se entenderá todo acontecimiento o circunstancia inevitable, más allá del control razonable de "La AC", que le impida el cumplimiento de sus funciones con el carácter que le corresponde y reconoce a través de su firma autógrafa asentada en el espacio designado para ello en el anverso y reverso de este formato, como prueba fehaciente de la aceptación de todo lo especificado en el mismo.

CONDICIONES:

- El Certificado Digital que se genera, derivado de la realización de este trámite, estará disponible en <https://ac.siger.gob.mx>; para que "El Solicitante" realice la descarga del mismo.
- La Firma Electrónica Avanzada asignada es personal e intransferible y el uso de la misma es responsabilidad de la persona que la solicite.
- La Firma Electrónica Avanzada tendrá los mismos alcances y efectos que la firma autógrafa.
- Con esta firma podrá hacer uso de servicios y trámites electrónicos disponibles en las Dependencias, Entidades, Organizaciones e Instituciones.
- "El Solicitante" será responsable de las obligaciones derivadas del uso no autorizado de su firma.
- "El Solicitante" acepta que deberá notificar oportunamente a "La AC", la invalidación, pérdida o cualquier otra situación que pudiera implicar la reproducción o uso indebido de su clave privada.
- "El Solicitante" acepta las condiciones de operación y límites de responsabilidad de la **Secretaría de Economía** en su calidad de "La AC".

Firma del Solicitante:

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

COMPROBANTE DE EMISION DE CERTIFICADO DE IDENTIDAD PERSONAL DE FIRMA ELECTRONICA AVANZADA

<Lugar y fecha aquí>

La Autoridad Certificadora <del Sistema Integral de Gestión Registral ó de la Dirección General de Normatividad Mercantil> de la Secretaría de Economía, certifica que el Solicitante: <poner aquí nombre del Solicitante>, entregó un requerimiento de certificación que contiene la solicitud para la generación de su Certificado Digital de Firma Electrónica Avanzada.

Estando presente el Solicitante se llevó a cabo el procedimiento de emisión y registro de certificados digitales de conformidad con lo establecido en el "Acuerdo Interinstitucional por el que se establecen los lineamientos para la homologación, implantación y uso de la Firma Electrónica Avanzada en la Administración Pública Federal" publicado en el Diario Oficial de la Federación el 24 de agosto de 2006.

Asimismo, que como resultado del proceso se generó su Certificado Digital con número de serie: <poner aquí número de serie> y clave pública: <poner clave pública en cadena de caracteres>

Previo a la emisión del presente certificado, el titular reconoce haber leído y aceptado los términos y condiciones de uso establecidos en el anverso del formato "Solicitud de Certificado Digital de Firma Electrónica Avanzada".


El resguardo de la clave privada relacionada con el certificado amparado por el presente Acuse, así como su medio de almacenamiento, es responsabilidad del titular del Certificado Digital.

Titular: <poner nombre del Solicitante aquí>

CURP: <poner CURP aquí>

RFC: <poner RFC aquí>

Firma de conformidad

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

**COMPROBANTE DE SOLICITUD Y REVOCACION DE CERTIFICADO
DIGITAL DE FIRMA ELECTRONICA AVANZADA DE IDENTIDAD
PERSONAL.**

La Autoridad Certificadora <del Sistema Integral de Gestión Registral ó de la Dirección General de Normatividad Mercantil> de la Secretaría de Economía, certifica que el Titular: <poner aquí nombre del Titular>, solicitó la revocación de su Certificado Digital con número de serie: <poner aquí número de serie> y clave pública: <poner clave pública en cadena de caracteres>, en virtud de <poner el motivo de la revocación>, de conformidad con lo establecido en el Acuerdo Interinstitucional por el que se establecen los lineamientos para la homologación, implantación y uso de la Firma Electrónica Avanzada en la Administración Pública Federal" publicado en el Diario Oficial de la Federación el 24 de agosto del 2006.

Por consiguiente, se llevó a cabo la revocación del referido Certificado Digital, siendo las <poner hora aquí> del <poner fecha aquí>.

Nombre y Firma del solicitante:	Nombre y Firma del Agente:
_____	_____

 SE <small>SECRETARÍA DE ECONOMÍA</small>	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008


CARTA DE CONFIDENCIALIDAD Y RESPONSABILIDAD DE FEDATARIO PÚBLICO

Secretaría de Economía
Presente.

El que suscribe (nombre del fedatario público), titular de la (señalar: 1) si se trata de notaría o correduría, 2) el número que le corresponde, 3) estado o plaza y 4) en caso de notarios el municipio o distrito) cuyos datos de certificado se anexan a la presente carta, advertido por (el agente certificador o auxiliar de agente)(nombre del agente certificador ó del auxiliar de agente que actúa) de la (Dirección General de Normatividad Mercantil ó Delegación Federal de la Secretaría de Economía del Estado de) de los delitos en que incurren los que se conducen con falsedad ante una autoridad distinta a la judicial, manifiesto que:

- I. Reconozco desde el día de hoy como propia y auténtica la información que en lo sucesivo envíe por medios electrónicos, que sea distinguida a través de la firma electrónica que se produzca a partir de la utilización de mis datos de creación de firma y del certificado que me ha generado la Secretaría de Economía por conducto de la Dirección General de Normatividad Mercantil, con número de serie _____ y la vigencia del _____ al _____.
- II. Que el agente certificador de la Secretaría de Economía puso a mi disposición los elementos técnicos necesarios para elaborar mi requerimiento, y posteriormente generar mis datos de creación de firma, estos últimos han sido de mi exclusivo conocimiento en todo momento.
- III. Acepto que el uso de mis datos de creación de firma quedará bajo mi exclusiva responsabilidad y que no debo de revelar mis datos de creación de firma. le corresponda.
- IV. Notificaré a la Secretaría de Economía, para su invalidación, la pérdida o cualquier otra situación que pudiera implicar el uso indebido de mis datos de creación de firma en los términos a que se refiere el artículo 14 del Reglamento del Registro Público de Comercio.
- V. Estoy de acuerdo en proporcionar a la Dirección General de Normatividad Mercantil de la Secretaría de Economía, la información adicional que respecto del proceso de generación de mi certificado me sea requerida.
- VI. Manifiesto que el agente certificador de la Secretaría de Economía dio lectura y explicó el alcance de los artículos 11 y 12 del Reglamento del Registro Público de Comercio.
- VII. Que el certificado y mis datos de creación de firma los utilizaré para los efectos que marcan los artículos 30 Bis y 30 Bis 1 del Código de Comercio los cuales me fueron leídos y explicados en su alcance por el agente certificador de la Secretaría de Economía.
- VIII. En caso de incumplir con lo estipulado en la presente carta acepto que la Secretaría de Economía revoque en cualquier momento mi certificado, sin perjuicio de las demás responsabilidades en las que pueda incurrir o que me correspondan.

(Nombre y firma del fedatario público al calce y al margen)

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

CONSTANCIA DE ILEGIBILIDAD DE HUELLAS DACTILARES

<Lugar y fecha aquí>

El Agente Certificador o Auxiliar del Agente Certificador <poner aquí nombre del Agente o Auxiliar > adscrito a la <poner aquí nombre de la unidad a la que pertenece> de la Secretaría de Economía, **HACE CONSTAR** que el fedatario <poner aquí nombre del Solicitante y número de la Notaria o Correduría Pública> se presentó de forma personal para solicitar la generación de su Certificado de Digital de Firma Electrónica Avanzada y se hace constar lo siguiente:

Se llevó a cabo el procedimiento de captura de su huella dactilar, para el procedimiento de generación de Certificado Digital con el uso de dispositivo biométrico, y una vez que se probó el procedimiento con todos sus dedos sin que se haya conseguido capturar su huella dactilar por ser ilegible, por lo que se procede, dada esta circunstancia, a generar un certificado digital con uso de contraseña, almacenando en el dispositivo biométrico sus llaves pública y privada.

Nombre y Firma del Agente Certificador o Auxiliar del Agente Certificador.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

**CARTA DE CONFIDENCIALIDAD Y RESPONSABILIDAD DE FEDATARIO PÚBLICO
(Para huellas ilegibles)**

**Secretaría de Economía
P r e s e n t e.**

El que suscribe (nombre del fedatario), titular de la (señalar: 1) si se trata de notaría o correduría, 2) el número que le corresponde, 3) estado o plaza y 4) en caso de notarios el municipio o distrito) cuyos datos de certificado se anexan a la presente carta, advertido por (el agente certificador o auxiliar de agente)(nombre del agente certificador ó del auxiliar de agente que actúa) de la (Dirección General de Normatividad Mercantil ó Delegación Federal de la Secretaría de Economía del Estado de) de los delitos en que incurrir los que se conducen con falsedad ante una autoridad distinta a la judicial, manifiesto que:

Debido a que durante el procedimiento de captura de la huella dactilar en el dispositivo biométrico, no fue posible realizarlo para ninguno de mis dedos por ser ilegibles los rasgos, ante esta imposibilidad y a mi solicitud, la Dirección General de Normatividad Mercantil por conducto del Agente Certificados antes señalado, procedió a generar mi certificado digital con el uso de contraseña que solo yo conozco, asimismo, que en el dispositivo biométrico queda almacenada mi llave pública y privada, por lo que a partir de este momento me hago responsable único del uso que se le de a mi llave privada, adicionalmente:

- I. Reconozco desde el día de hoy como propia y auténtica la información que en lo sucesivo envíe por medios electrónicos, y que sea distinguida a través de la firma electrónica que se produzca a partir de la utilización de mis datos de creación de firma y del certificado que me ha generado la Secretaría de Economía por conducto de la Dirección General de Normatividad Mercantil, con número de serie _____ y la vigencia del _____ al _____.
- II. Que el agente certificador de la Secretaría de Economía puso a mi disposición los elementos técnicos necesarios para elaborar mi requerimiento, y posteriormente generar mis datos de creación de firma, estos últimos han sido de mi exclusivo conocimiento en todo momento.
- III. Acepto que el uso de mis datos de creación de firma quedará bajo mi exclusiva responsabilidad y que no debo de revelar mi contraseña ni mis datos de creación de firma a ningún tercero, ya que son de mi exclusivo uso y responsabilidad.
- IV. Notificaré a la Secretaría de Economía, la pérdida o cualquier otra situación que pudiera implicar el uso indebido de mi contraseña, así como de mis datos de creación de firma en los términos a que se refiere el artículo 14 del Reglamento del Registro Público de Comercio, para su invalidación.
- V. Estoy de acuerdo en proporcionar a la Dirección General de Normatividad Mercantil de la Secretaría de Economía, la información adicional que respecto del proceso de generación de mi certificado me sea requerida.
- VI. Manifiesto que el agente certificador de la Secretaría de Economía dio lectura y explicó el alcance de los artículos 11 y 12 del Reglamento del Registro Público de Comercio.
- VII. Que el certificado, mi contraseña y mis datos de creación de firma los utilizaré para los efectos que marcan los artículos 30 Bis y 30 Bis 1 del Código de Comercio los cuales me fueron leídos y explicados en su alcance por el agente certificador de la Secretaría de Economía.
- VIII. En caso de incumplir con lo estipulado en la presente carta acepto que la Secretaría de Economía revoque en cualquier momento mi certificado, sin perjuicio de las demás responsabilidades de carácter civil y/o penal en las que pueda incurrir o que me correspondan.

(Nombre y firma del fedatario público)

 SE <small>SECRETARÍA DE ECONOMÍA</small>	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

CARTA DE CONFIDENCIALIDAD Y RESPONSABILIDAD DE RESPONSABLE DE OFICINA

Secretaría de Economía P r e s e n t e.

El que suscribe (nombre del responsable de oficina), habilitado por la Secretaría de Economía como Responsable de la Oficina en (señalar la oficina según su habilitación) cuyos datos de certificado se anexan a la presente carta, advertido por (el agente certificador o auxiliar de agente) (nombre del agente certificador ó del auxiliar de agente que actúa) de la (Dirección General de Normatividad Mercantil ó Delegación Federal de la Secretaría de Economía del Estado de) de los delitos en que incurren los que se conducen con falsedad ante una autoridad distinta a la judicial, manifiesto que:

- I. Reconozco desde el día de hoy como propia y auténtica la información que en lo sucesivo envíe por medios electrónicos, que sea distinguida a través de la firma electrónica que se produzca a partir de mis datos de creación de firma y de la utilización del certificado que me ha generado la Secretaría de Economía por conducto de la Dirección General de Normatividad Mercantil, con número de serie _____ y la vigencia del _____ al _____.
- II. Que el agente certificador de la Secretaría de Economía puso a mi disposición los elementos técnicos necesarios para elaborar mi requerimiento, y posteriormente generar mis datos de creación de firma, estos últimos han sido de mi exclusivo conocimiento en todo momento.
- III. Acepto que el uso de mis datos de creación de firma quedará bajo mi exclusiva responsabilidad y que no debo de revelar mis datos de creación de firma.
- IV. Notificaré a la Secretaría de Economía, para su invalidación, la pérdida o cualquier otra situación que pudiera implicar el uso indebido de mis datos de creación de firma en los términos a que se refiere el artículo 11 del Reglamento del Registro Público de Comercio.
- V. Estoy de acuerdo en proporcionar a la Dirección General de Normatividad Mercantil de la Secretaría de Economía, la información adicional que respecto del proceso de generación de mi certificado me sea requerida.
- VI. Manifiesto que el agente certificador de la Secretaría de Economía dio lectura y explicó el alcance del artículo 11 del Reglamento del Registro Público de Comercio.
- VII. Que el certificado y mis datos de creación de firma sólo los utilizaré para los efectos que marcan los artículos 20 Bis y 21 Bis inciso c) del Código de Comercio y 11 del Reglamento del Registro Público de Comercio, los cuales me fueron leídos y explicados en su alcance por el agente certificador de la Secretaría de Economía.
- VIII. En caso de incumplir con lo estipulado en la presente carta acepto que la Secretaría de Economía revoque en cualquier momento mi certificado y habilitación, sin perjuicio de las demás responsabilidades en las que pueda incurrir o que me correspondan.

(Nombre y firma del responsable de oficina al calce y al margen)

 SE SECRETARÍA DE ECONOMÍA	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008


CARTA DE CONFIDENCIALIDAD Y RESPONSABILIDAD DE RESPONSABLE DE OFICINA (PARA EL REGISTRO INMEDIATO DE EMPRESAS)

Secretaría de Economía
P r e s e n t e.

El que suscribe (Nombre del Res. de Oficina), habilitado por la Secretaría de Economía como Responsable de la Oficina del Registro Público de Comercio en el Estado de _____, cuyos datos de identificación se anexan a la presente carta, advertido por (el agente certificador o auxiliar de agente)(Nombre del agente autorizado por la DGNM), de los delitos en que incurrir los que se conducen con falsedad ante una autoridad distinta a la autoridad judicial, manifiesto que:

- I. Reconozco a partir del día de hoy como propia y auténtica la información que en lo sucesivo certifique o firme, a través de la firma electrónica, utilizando el Certificado Digital que me fue expedido por la Secretaría de Economía, por conducto de la Dirección General de Normatividad Mercantil, con número de serie _____ y la vigencia del _____ al _____.
- II. Asimismo, que el agente certificador de la DGNM, puso a mi disposición los elementos técnicos necesarios para elaborar mi requerimiento, y posteriormente generar mi Certificado Digital, datos de creación que han sido de mi exclusivo conocimiento.
- III. Acepto que el uso de mis datos de creación de firma quedan bajo mi exclusiva responsabilidad y que no debo de revelar mi contraseña ni mis datos de creación de firma.
- IV. Debo notificar a la DGNM, para que invalide mi certificado en caso de presentarse alguna situación que pudiera implicar el uso indebido de mis datos de creación de firma en los términos a que se refiere el artículo 11 del Reglamento del Registro Público de Comercio.
- V. Estoy de acuerdo en proporcionar a la DGNM de la Secretaría de Economía, la información adicional que respecto del proceso de generación de mi certificado me sea requerida.
- VI. Manifiesto que el agente certificador de la DGNM, una vez concluido el procedimiento de generación de mi certificado digital dio lectura y explicó el alcance del artículo 11 del Reglamento del Registro Público de Comercio.
- VII. Que el certificado digital y mis datos de creación de firma electrónica se utilizarán para los efectos de inscribir en el Registro Público de Comercio de esta entidad federativa los actos a constitución de Sociedades Mercantiles y Sociedades Microindustriales utilizando las Formas Precodificadas M-4 y M-5 y siempre y cuando sean enviadas por Fedatarios Públicos autorizados utilizando el SIGER-Fed@net.
- VIII. En caso de incumplir con lo estipulado en la presente carta acepto que la DGNM revoque en cualquier momento mi certificado y habilitación, sin perjuicio de las demás responsabilidades en las que pueda incurrir o que me correspondan.

Nombre y firma del Responsable de Oficina

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

CARTA DE CONFIDENCIALIDAD Y RESPONSABILIDAD DEL SERVIDOR PÚBLICO

Secretaría de Economía
Presente

El que suscribe <nombre del servidor público>, en mi carácter de titular de < señalar puesto y unidad administrativa, estado, > en términos del acuerdo <poner términos> mediante el cual < poner términos >, manifiesto, bajo protesta de decir verdad lo siguiente:

- I. Reconozco desde el día de hoy como propia y auténtica la información que en lo sucesivo envíe por medios electrónicos, que sea distinguida a través de la firma electrónica que se produzca a partir de mis datos de creación de firma y de la utilización del certificado que me ha generado la Secretaría de Economía por conducto de la Dirección General de Normatividad Mercantil, con número de serie _____ y la vigencia del _____ al _____.
- II. Notificaré a la Dirección General de Normatividad Mercantil, como Unidad Certificadora de la Secretaría de Economía para la revocación del certificado a que se refiere la presente carta; la pérdida o cualquier otra situación que pudiera implicar la reproducción o uso indebido de mis datos de creación de firma electrónica y del certificado en un plazo que no mayor a 12 horas por medios electrónicos con acuse de recibo o por escrito al día hábil siguiente.
- III. Acepto que el uso de datos de creación de mi firma electrónica y de mi certificado por persona distinta quedará bajo mi exclusiva responsabilidad, que por lo tanto soy responsable de su resguardo, asimismo, que en el caso de revelarlos en cualquier forma acepto como propia la información que sea enviada.
- IV. Asumo cualquier tipo de responsabilidad derivada del mal uso que haga de mi certificado digital.
- V. Que mi certificado y mis datos de creación de firma sólo los utilizaré para los efectos que marca el capítulo VI del Reglamento Interior de la Secretaría de Economía, publicado en el Diario Oficial de la Federación el 22 de noviembre de 2002.
- VI. Estoy de acuerdo en ser requerido para el envío de cualquier información adicional respecto de mi certificado.
- VII. Acepto que en caso de incumplir con lo estipulado en la presente carta la Unidad Certificadora de la Secretaría Economía podrá revocar en cualquier momento mi certificado, sin perjuicio de las demás responsabilidades en las que puedan incurrir o que correspondan.

<Nombre, cargo y firma del servidor público>.

**DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN
DE LA AC-DGNM Y AC-SIGER**

SOLICITUD DE CERTIFICADO DIGITAL PARA SERVIDOR PÚBLICO

TITULAR DE LA UNIDAD SOLICITANTE	
Nombre:	
Cargo:	
Organización:	
Correo Electrónico:	Tel/Fax.
Firma:	Fecha.

Por este conducto solicito la generación de certificado digital para las siguientes personas:

Nombre:	Cargo

AUTORIZACIÓN DGNM		
Nombre:		
Cargo:		
Firma:	Fecha.	Tipo de Certificado Autorizado

AGENTE CERTIFICADOR	
Nombre:	
Cargo:	
Firma:	Fecha.



DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER

Versión
2.0
Fecha
27/AGO/2008

TERMINOS:

- Los suscritos, cuyos datos generales aparecen al anverso de la presente solicitud, y a quienes en lo sucesivo se le denominará como “El Solicitante” para todos los efectos legales que deriven del presente documento a que haya lugar, manifiestan ante **La Secretaría de Economía** a quien en lo sucesivo se le denominará “La Autoridad Certificadora” (AC), que es su voluntad contar con un Certificado Digital para Firma del Equipo de cómputo descrito en el anverso de la presente.
- “El Solicitante”, manifiesta su conformidad en que “La AC” para que utilice el procedimiento de certificación de identidad que estime conveniente.
- “El Solicitante” reconoce que para la emisión del referido Certificado Digital, “La AC” acreditó la personalidad de los solicitantes, por lo que el responsable del equipo aquí descrito, asume la responsabilidad exclusiva respecto de la autenticación de los datos y documentación por él proporcionada a “La AC”. De la misma forma el titular de la unidad solicitante, asume la responsabilidad de supervisar el correcto uso del Certificado Digital del equipo de cómputo.
- “El Solicitante” en este acto acepta el certificado digital mencionado, sirviendo este documento como el acuse de recibo más amplio que en derecho proceda.
- Adicionalmente, “El solicitante”, acepta que el uso de la clave privada y frase de seguridad de revocación, con base en las cuales dicho certificado fue elaborado, quedarán bajo su estricta y absoluta responsabilidad, la cual incluye en forma enunciativa, los daños y perjuicios, incluso aquéllos de carácter financiero, que pudieran causarse por su uso indebido, no pudiendo alegar que tal uso se realizó por persona no autorizada.
- “El Solicitante” conoce y acepta que la clave pública proporcionada y contenida en el Certificado Digital para firma de equipo, así como en cualquier otro certificado digital que con posterioridad se obtenga, será de carácter público y podrá ser consultado libremente por cualquier interesado a través de los medios y formas que disponga “La AC”.
- Por lo anterior, “El Solicitante” se obliga a mantener absoluta confidencialidad de la clave privada y frase de seguridad de revocación, así como a realizar los trámites necesarios para la revocación de dicho certificado ante “La AC”, mediante los mecanismos y procedimientos que el mismo establezca, en el caso de que por cualquier causa dicha información sea divulgada o se realice cualquier supuesto por el que “El Solicitante” deba solicitar su revocación en los términos de las disposiciones legales vigentes.
- Por otra parte “El Solicitante” manifiesta conocer el contenido y alcance de las disposiciones legales y reglamentarias relativas a la celebración de actos jurídicos mediante el uso de medios electrónicos, digitales o de cualquier otra tecnología, por lo que asume plena responsabilidad respecto de la información y contenido de todo documento electrónico o digital elaborado y enviado en el que se haga uso de la citada clave privada, toda vez que por ese solo hecho se considerara que el documento electrónico o digital le es atribuible.
- “EL Solicitante” reconoce y acepta que “La AC” únicamente es responsable de los errores que, en su caso, llegaren a cometer con motivo de culpa grave en el proceso de generación, registro, entrega y revocación del certificado digital, según corresponda, así como que no será responsable por los daños y perjuicios que se pudieran causar a “El Solicitante” o a terceros, cuando por caso fortuito o fuerza mayor no puedan realizarse registros, verificaciones, revocaciones o tramitar documentos electrónicos cifrados con las claves públicas y privadas relacionadas con dicho certificado. Por caso fortuito o fuerza mayor se entenderá todo acontecimiento o circunstancia inevitable, más allá del control razonable de “La AC”, que le impida el cumplimiento de sus funciones con el carácter que le corresponde y reconocen a través de sus firmas autógrafas asentada en el espacio designado para ello en el anverso y reverso de este formato, como prueba fehaciente de la aceptación de todo lo especificado en la presente Solicitud.

CONDICIONES:

- El Certificado Digital para Servidor Público que se genera, derivado de la realización de este trámite, estará disponible en <https://ac.siger.gob.m/DGNMx>; para que “La Unidad Solicitante” realice la descarga del mismo.
- El Certificado Digital para Firma de Servidor Público asignada es exclusiva para el Servidor Público especificado en la presente e intransferible y el uso de la misma es responsabilidad de la persona señalada y que tiene a su cargo el Servidor Público.
- Con este certificado podrá realizar las actividades asignadas estrictamente al Servidor Público dentro de la organización.
- “El Solicitante” será responsable de las obligaciones derivadas del uso no autorizado del Servidor Público.
- “El Solicitante” y el Servidor Público aceptan que deberán notificar oportunamente a “La AC”, la invalidación, pérdida o cualquier otra situación que pudiera implicar la reproducción o uso indebido del certificado Digital para Firma de Servidor Público y aceptan las condiciones de operación y límites de responsabilidad de la **Secretaría de Economía** en su calidad de “La AC”.

Firma el titular de la Unidad solicitante:



SOLICITUD DE CERTIFICADO DIGITAL PARA EQUIPO DE CÓMPUTO

DATOS DEL EQUIPO		
No. de serie:	IP:	
No. Inventario:	MAC Address:	
Nombre y dominio:		
Ubicación:		
Del. o Mpio.:	Estado:	C.P.
Breve descripción del uso que se le dará al certificado		

TITULAR DE LA UNIDAD SOLICITANTE	
Nombre:	
Cargo:	
Organización:	
Correo Electrónico:	Tel/Fax.
Firma:	Fecha.

RESPONSABLE TÉCNICO DEL EQUIPO	
Nombre:	
Quien se identificó con:	
Cargo:	
Organización:	
Correo Electrónico:	Tel/Fax.
Firma:	Fecha.

AUTORIZACIÓN DGNM		
Nombre:		
Cargo:		
Firma:	Fecha.	Tipo de Certificado Autorizado

AGENTE CERTIFICADOR	
Nombre:	
Cargo:	
Firma:	Fecha.

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER

Versión
2.0
Fecha
27/AGO/2008


TERMINOS:

- Los suscritos, cuyos datos generales aparecen al anverso de la presente solicitud, y a quienes en lo sucesivo se le denominará como “El Solicitante” para todos los efectos legales que deriven del presente documento a que haya lugar, manifiestan ante **La Secretaría de Economía** a quien en lo sucesivo se le denominará “La Autoridad Certificadora” (AC), que es su voluntad contar con un Certificado Digital para Firma del Equipo de cómputo descrito en el anverso de la presente.
- “El Solicitante”, manifiesta su conformidad en que “La AC” para que utilice el procedimiento de certificación de identidad que estime conveniente.
- “El Solicitante” reconoce que para la emisión del referido Certificado Digital, “La AC” acredita la personalidad de los solicitantes, por lo que el responsable del equipo aquí descrito, asume la responsabilidad exclusiva respecto de la autenticidad de los datos y documentación por él proporcionada a “La AC”. De la misma forma el titular de la unidad solicitante, asume la responsabilidad de supervisar el correcto uso del Certificado Digital del equipo de cómputo.
- “El Solicitante” en este acto acepta el certificado digital mencionado, sirviendo este documento como el acuse de recibo más amplio que en derecho proceda.
- Adicionalmente, “El solicitante”, acepta que el uso de la clave privada y frase de seguridad de revocación, con base en las cuales dicho certificado fue elaborado, quedarán bajo su estricta y absoluta responsabilidad, la cual incluye en forma enunciativa, los daños y perjuicios, incluso aquéllos de carácter financiero, que pudieran causarse por su uso indebido, no pudiendo alegar que tal uso se realizó por persona no autorizada.
- “El Solicitante” conoce y acepta que la clave pública proporcionada y contenida en el Certificado Digital para firma de equipo, así como en cualquier otro certificado digital que con posterioridad se obtenga, será de carácter público y podrá ser consultado libremente por cualquier interesado a través de los medios y formas que disponga “La AC”.
- Por lo anterior, “El Solicitante” se obliga a mantener absoluta confidencialidad de la clave privada y frase de seguridad de revocación, así como a realizar los trámites necesarios para la revocación de dicho certificado ante “La AC”, mediante los mecanismos y procedimientos que el mismo establezca, en el caso de que por cualquier causa dicha información sea divulgada o se realice cualquier supuesto por el que “El Solicitante” deba solicitar su revocación en los términos de las disposiciones legales vigentes.
- Por otra parte “El Solicitante” manifiesta conocer el contenido y alcance de las disposiciones legales y reglamentarias relativas a la celebración de actos jurídicos mediante el uso de medios electrónicos, digitales o de cualquier otra tecnología, por lo que asume plena responsabilidad respecto de la información y contenido de todo documento electrónico o digital elaborado y enviado en el que se haga uso de la citada clave privada, toda vez que por ese solo hecho se considerara que el documento electrónico o digital le es atribuible.
- “El Solicitante” reconoce y acepta que “La AC” únicamente es responsable de los errores que, en su caso, llegaren a cometer con motivo de culpa grave en el proceso de generación, registro, entrega y revocación del certificado digital, según corresponda, así como que no será responsable por los daños y perjuicios que se pudieran causar a “El Solicitante” o a terceros, cuando por caso fortuito o fuerza mayor no puedan realizarse registros, verificaciones, revocaciones o tramitar documentos electrónicos cifrados con las claves públicas y privadas relacionadas con dicho certificado. Por caso fortuito o fuerza mayor se entenderá todo acontecimiento o circunstancia inevitable, más allá del control razonable de “La AC”, que le impida el cumplimiento de sus funciones con el carácter que le corresponde y reconocen a través de sus firmas autógrafas asentada en el espacio designado para ello en el anverso y reverso de este formato, como prueba fehaciente de la aceptación de todo lo especificado en la presente Solicitud.

CONDICIONES:

- El Certificado Digital para Firma de Equipo que se genera, derivado de la realización de este trámite, estará disponible en <https://ac.siger.gob.mx>; para que “La Unidad Solicitante” realice la descarga del mismo.
- El Certificado Digital para Firma de Equipo asignada es exclusiva para el equipo especificado en la presente e intransferible y el uso de la misma es responsabilidad de la persona señalada y que tiene a su cargo el equipo.
- Con este certificado podrá realizar las actividades asignadas estrictamente al equipo de cómputo dentro de la organización.
- “El Solicitante” será responsable de las obligaciones derivadas del uso no autorizado del equipo.
- “El Solicitante” y el responsable del equipo aceptan que deberán notificar oportunamente a “La AC”, la invalidación, pérdida o cualquier otra situación que pudiera implicar la reproducción o uso indebido del certificado Digital para Firma de Equipo y aceptan las condiciones de operación y límites de responsabilidad de la **Secretaría de Economía** en su calidad de “La AC”.

<p>Firma el titular de la Unidad solicitante:</p> <p>_____</p>	<p>Firma del Responsable del Equipo de Cómputo:</p> <p>_____</p>


	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

CARTA DE CONFIDENCIALIDAD Y USO DE CERTIFICADO DIGITAL DE EQUIPO DE CÓMPUTO

Secretaría de Economía
P r e s e n t e.

El que suscribe _____, en mi carácter de _____, adscrito a la unidad de _____, de la Secretaría de Economía, advertido por (el agente certificador o auxiliar de agente) (Nombre del Agente Certificador) de la Dirección General de Normatividad Mercantil, de los delitos en que incurrir los que se conducen con falsedad ante una autoridad distinta a la autoridad judicial, manifiesto que:

- I. Que a partir de este día, acepto bajo mi responsabilidad el uso del certificado digital con número de serie _____ y con vigencia del _____ al _____, emitido por la Dirección General de Normatividad Mercantil para el uso del equipo de cómputo con número de serie _____; modelo _____, marca _____, con número de inventario _____.
- II. Acepto que el uso de los datos de creación del certificado digital señalado con anterioridad, queda bajo mi responsabilidad, en virtud de que el agente certificador de la Dirección General de Normatividad Mercantil puso a mi disposición los elementos técnicos necesarios para elaborar el requerimiento, y generación del certificado digital, datos que han sido de mi exclusivo conocimiento en todo momento, por lo que me obligo a no revelar los datos de creación del certificado, ya que en el caso de hacerlo, me serán atribuibles las responsabilidades administrativas, civiles y penales que se pudieran derivar por el mal uso que se le pudiera dar.
- III. Que alinearé todas mis actividades y procesos para cumplir con la Política de Certificación y con la Declaratoria de Prácticas de Certificación de la DGNM y me aseguraré que sea ejecutada por las personas bajo mi supervisión, a fin de mantener la integridad, confidencialidad y disponibilidad la información del equipo de cómputo señalado en la fracción I de esta Carta.
- IV. Que me aseguraré de informar a mi superior jerárquico y al Comité de Seguridad de la Información de la DGN, sobre cualquier conducta violatoria de que tenga conocimiento que pudiera incidir en la correcta operación del equipo de cómputo antes descrito, así como de la confidencialidad o disponibilidad de la información en éste contenida.
- V. En caso de incumplir con lo estipulado en la presente carta, acepto que la DGNM revoque el certificado Digital del equipo de cómputo a mi cargo y que ha quedado descrito en la presente carta, sin perjuicio de que me puedan ser aplicables las responsabilidades administrativas, civiles o penales, por las acciones u omisión en que pudiera haber incurrido.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

Oficio No. 316.08.

Asunto: Nombramiento de Agente
Certificador.

México, D.F.

(Nombre del Agente y Cargo)

Por este conducto le comunico que a sido designado Agente Certificador de la Secretaría de Economía, para los efectos que disponen los artículos 30 bis del Código de Comercio, 20 fracción X del Reglamento Interior de la Secretaría de Economía y 11 del Reglamento del Registro Público de Comercio.

Por lo que, a partir de esta fecha está facultado para generar y revocar los Certificados Digitales de las Autoridades Certificadoras de la DGNM y del SIGER, conforme a lo establecido en la Política de Certificación y Declaración de Prácticas de Certificación emitidas por esta Dirección General.

A t e n t a m e n t e
El Director General

Oscar A. Margain Pitman

C.c.p.- Act. Gustavo de la Colina Flores, Director del SIGER.- Para la Generación del certificado de Agente correspondiente.



DELEGACIÓN O SUBDELEGACIÓN FEDERAL DE LA SECRETARÍA
DE ECONOMÍA EN EL ESTADO DE

Oficio No.

Asunto: Nombramiento de Auxiliar de
Agente Certificador.
México, D.F.

(Nombre del Auxiliar de Agente Certificador y Cargo)


Por este conducto le comunico que a sido designado Auxiliar de Agente Certificador de la Secretaría de Economía, para los efectos que disponen los artículos 30 bis del Código de Comercio, 20 fracción X del Reglamento Interior de la Secretaría de Economía y 11 del Reglamento del Registro Público de Comercio.

Por lo que, a partir de esta fecha deberá brindarle apoyo a los Agentes Certificadores nombrados por la Dirección General de Normatividad Mercantil de esta Secretaría, en la generación de los Certificados Digitales de las Autoridades Certificadoras de la DGNM y del SIGER, conforme a lo establecido en la Política de Certificación y Declaración de Prácticas de Certificación emitidas por la Dirección General de Normatividad Mercantil.

Atentamente
El Delegado o Subdelegado

Nombre y Firma

C.c.p.- Lic. Oscar A. Margain Pitman.- Director General de Normatividad Mercantil.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER	Versión
		2.0
		Fecha
		27/AGO/2008

CARTA DE CONFIDENCIALIDAD DE AUXILIAR DE AGENTE

Secretaría de Economía Presente

El que suscribe <nombre del Auxiliar de Agente>, habilitado por < Delegado o subdelegado, de la ciudad y estado > como Auxiliar de Agente Certificador, con pleno conocimiento de causa y advertido por la Dirección General de Normatividad Mercantil de los delitos en los que incurrir los que se conducen con falsedad ante una autoridad distinta ala judicial, manifiesto que:

- I. Declaro bajo protesta de decir verdad que es de mi conocimiento la Política de Certificación y Declaración de Prácticas de Certificación, misma que entiendo y en consecuencia estoy de acuerdo en aplicarlas y cumplirlas cabalmente.
- II. Que es de mi conocimiento que toda la información derivada del procedimiento de Generación de Certificados Digitales de la Secretaría de Economía es estrictamente confidencial, por lo que me obligo a respetar dicha condición de la información y abstenerme de divulgarla o distribuirla a terceras personas.
- III. Igualmente, que me abstendré de conservar copias o respaldos totales o parciales, sean físicos o electrónicos, salvo aquellos realizados en el ejerció de mis funciones laborales, y no utilizaré en provecho propio la información que obtuve en el proceso de generación de certificados digitales.
- IV. Que realizaré de manera cuidadosa, imparcial y gratuita el apoyo para la generación certificados digitales y en especial el procedimiento de identificación y personalidad jurídica de los solicitantes y el envío de la documentación recopilada en el procedimiento.
- V. Estoy de acuerdo en proporcionar a la Dirección General de Normatividad Mercantil de la Secretaría de Economía la información adicional que respecto del proceso de generación de certificados me sea requerida.

<Nombre, cargo y firma del Auxiliar de agente>

<p>SE SECRETARÍA DE ECONOMÍA</p>	<p>DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER</p>	<p>Versión</p>
		<p>2.0</p>
		<p>Fecha</p>
		<p>27/AGO/2008</p>

Director General de Normatividad Mercantil	
<p>Lic. Oscar A. Margain Pittman Director General de Normatividad Mercantil</p>	

Comité de Seguridad de la Información de la DGNM	
<p>Act. Gustavo Lázaro de la Colina Flores Dirección General Adjunta de Regulación de Servicios de Firma Electrónica y Sistemas Registrales. Presidente del Comité</p>	
<p>Lic. Edgar Dimitri Veites Palavicini Pesquera Director de Coordinación del Registro Público de Comercio Coordinador Jurídico</p>	
<p>Lic. Abraham Rodríguez Félix Director del Sistema Integral de Gestión Registral Coordinador Técnico SIGER</p>	
<p>Act. Carlos Alberto Cadena Sandoval Director de Regulación y Supervisión de los PSC Coordinador Técnico PSC</p>	
<p>Ing. Israel Becerril Sierra Subdirector de Seguridad Registral Secretario del Comité</p>	
<p>Ing. Alejandra Ángeles Poblano Subdirectora de Operación Registral Vocal Técnico</p>	
<p>Ing. Alejandro Portas Sánchez Subdirector de Desarrollo SIGER Propiedad Vocal Técnico</p>	
<p>M. en C. Luis Miguel Mitchell Arana Jefe de Departamento de Atención a Usuarios del RPC Vocal Técnico</p>	
<p>Ing. Silvia Elena Hernández Martínez Consultor Externo de Sistemas de Información y de Seguridad Informática Vocal Técnico</p>	
<p>Lic. Karina Romo Maldonado Jefe de Departamento de Capacitación Registral Vocal Técnico</p>	
<p>Lic. Mario Guerrero Barrera Subdirector de Servicios y Modernización Registral Vocal Jurídico</p>	
<p>Lic. María del Pilar Martínez Sánchez Jefe de Departamento de Técnicas de Evaluación de la Capacitación Registral Vocal Jurídico</p>	
<p>Lic. Osvaldo Hernández González Jefe de Garantías Mobiliarias. Vocal Jurídico</p>	