Prácticas de Certificación de la Unidad de Certificación Electrónica del Tribunal Electoral del Poder Judicial de la Federación

Acuerdo General número 2/2015

Anexo 1

ÍNDICE

Página

1. Introducción

La Unidad de Certificación Electrónica del Tribunal Electoral del Poder Judicial de la Federación (UCE) es la instancia encargada de la gestión de certificados de firma electrónica avanzada de uso institucional, está integrada por la infraestructura tecnológica, con la que se llevan a cabo los procesos informáticos relativos a la emisión, revocación, y renovación de certificados, a la cual brinda soporte la Dirección General de Sistemas y los agentes certificadores que operan estos servicios en cada uno de los módulos de la Sala Superior y Salas Regionales.

Este documento establece el conjunto de reglas, definiciones técnicas y procedimientos de operación de la Unidad de Certificación Electrónica del Tribunal Electoral del Poder Judicial de la Federación y es de acceso público para ser consultado por los interesados en hacer uso de los certificados emitidos y conocer las condiciones técnicas de operación.

Con base en las mejores prácticas, este documento se basa en el **RFC 3647: "Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Framework".**

La **Unidad de Certificación Electrónica del Tribunal Electoral** es subordinada de la Autoridad Certificadora Raíz del Poder Judicial de la Federación de conformidad con el Acuerdo General Conjunto número 1/2013 de la Suprema Corte de Justicia de la Nación, del Tribunal Electoral del Poder Judicial de la Federación y del Consejo de la Judicatura Federal, relativo a la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL) y al expediente electrónico.

1.1. Marco legal

Las presentes **Prácticas de Certificación** se encuentran fundamentadas bajo el siguiente marco normativo:

I. Ley General del Sistema de Medios de Impugnación en Materia Electoral;
II. Acuerdo General Conjunto número 1/2013 de la Suprema Corte de Justicia de la Nación, del Tribunal Electoral del Poder Judicial de la Federación y del Consejo de la Judicatura Federal, relativo a la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL) y al expediente electrónico.
III. Reglamento Interno del Tribunal Electoral del Poder Judicial de la Federación;
IV. Acuerdo de la Comisión de Administración del Tribunal Electoral del Poder Judicial de la Federación número 075/S3(12-III-2008), por el que se establece la Firma Digital para la Suscripción de Documentos Generados por la Secretaría Administrativa y el Procedimiento de certificación de la Clave Digital

de los Servidores Públicos del Tribunal Electoral del Poder Judicial de la Federación, y

V. Acuerdo General número 2/2015, por el que se aprobaron las Prácticas de Certificación de la Unidad de Certificación Electrónica y el Manual de Operación de las Notificaciones por Correo Electrónico.

1.2. Definiciones y acrónimos.

Para efectos de las presentes Prácticas de Certificación se entenderá por:

I. **AGC 1/2013**: El Acuerdo General Conjunto número 1/2013 de la Suprema Corte de Justicia de la Nación, del Tribunal Electoral del Poder Judicial de la Federación y del Consejo de la Judicatura Federal, relativo a la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL) y al expediente electrónico.

II. **Agente Certificador**: Servidor público del Tribunal Electoral del Poder Judicial de la Federación designado por la Secretaría General de Acuerdos, por conducto del cual actuará la Unidad de Certificación correspondiente para tramitar la emisión, renovación y revocación de Certificados Digitales;

III. **Autoridades del Tribunal Electoral**: Los Presidentes y Secretarios Generales de Acuerdos de las Salas del Tribunal Electoral;

IV. **Autoridad Certificadora del Tribunal Electoral**: La infraestructura tecnológica de la Dirección General de Sistemas del TE, con la que se llevan a cabo los procesos informáticos relativos a la emisión, revocación, y renovación de certificados, para proporcionar Servicios Relacionados con la FIREL;

V. **CN** *Common Name*: El nombre de la entidad final, en el caso de las personas, se refiere a su nombre completo;

VI. **CRL**: La lista de revocación de certificados;

VII. **CSR** *Certificate signing request*: El mensaje electrónico que contiene la información formateada y requerida para procesar un certificado;

VIII. **DGS**: La Dirección General de Sistemas del Tribunal Electoral;

IX. **FQDN** *full qualified domain name*: El Nombre identificador completo de dominio, el cual incluye el nombre del equipo de cómputo, así como el nombre de dominio asociado al sistema;

X. **NTP** *Network Time Protocol*: El protocolo de internet para sincronizar los relojes de los sistemas informáticos a través de ruteo de paquetes de redes con latencia variable;

XI. **OCSP** *Online Certificate Status Protocol*: El servicio en línea que permite evaluar el estado y validez de un certificado;

XII. **PKI** *Public Key Infrastructure:* El conjunto de hardware, software, personas, políticas, procedimientos necesarios para crear, manejar, distribuir, usar, almacenar y revocar certificados digitales.

XIII. **Renovar*:*** El Restablecimiento de nuevas fechas de vigencia del certificado;
XIV. **Revocar*:*** El procedimiento mediante el cual se deja sin efecto el certificado electrónico;
XV. **RFC** *Request for comments***:** Es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo o infraestructura tecnológica, que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.
XVI. **Servidor Público:** Los servidores públicos del Tribunal Electoral del Poder Judicial de la Federación.
XVII. **SEPJF:** El Sistema Electrónico del PJF
XVIII. **Firmante**: La persona concreta que utiliza su Certificado Digital de la FIREL para suscribir documentos electrónicos y, en su caso, mensajes de datos;
XIX. **Token:** El dispositivo criptográfico que almacena llaves privadas de manera segura, a manera de llavero electrónico;
XX. **Tribunal Electoral**: El Tribunal Electoral del Poder Judicial de la Federación.
XXI. **UCE**: La Unidad de Certificación Electrónica del Tribunal Electoral del Poder Judicial de la Federación;
XXII. **UPS** *uninterruptible power supply*: La fuente ininterrumpida de energía eléctrica es un banco de baterías que provee energía eléctrica de manera ininterrumpida, puede proporcionar energía eléctrica tras una falla en el sistema de energía eléctrica convencional, y
XXIII. **UR:** La Unidad Registradora, que es el módulo de enrolamiento en el cual los solicitantes tramitan el certificado digital FIREL.

1.3. Nombre de documento e identificación

Título: Prácticas de Certificación de la Unidad de Certificación Electrónica del Tribunal Electoral del Poder Judicial de la Federación.

Versión: 2.0 autorizada el 10 de febrero de 2015.

1.3.1. Unidad de Certificación Electrónica

La **UCE** no emite certificados a través autoridades certificadoras subordinadas.

1.3.2. Unidades Registradoras

La **UCE** dispondrá de Unidades Registradoras **(UR)** en las Sala del Tribunal Electoral, las cuales procesan, administrativamente, las solicitudes y validarán, con las unidades administrativas del Tribunal Electoral, la información proporcionada en las solicitudes.

Las **UR** serán operadas por los agentes certificadores, designados por las Secretarias Generales de Acuerdo de cada una de las Sala del Tribunal Electoral, quienes deberán ser auxiliados en los aspectos técnicos por personal del área de Sistemas.

1.3.3. Usuarios o Firmantes

La **UCE** emitirá certificados digitales FIREL a fin de dar cumplimiento a lo dispuesto en el Acuerdo General Conjunto 1/2013 de la Suprema Corte de Justicia de la Nación, del Tribunal Electoral del Poder Judicial de la Federación y del Consejo de la Judicatura Federal, relativo a la firma electrónica certificada del Poder Judicial de la Federación (FIREL) y al expediente electrónico.

1.4. Uso valido de certificados digitales

El certificado intermedio de la **UCE** únicamente será utilizado para la firma de certificados, validación de certificados y firma de listas de revocación de certificados **CRL.**

Los agentes certificadores utilizarán el certificado personal autorizado para autenticarse en los sistemas de la **UCE** y llevar a cabo las actividades relativas a su perfil de operación.

Los certificados emitidos por la **UCE**, podrán ser utilizados en cualquier aplicación compatible con el estándar **X.509**, en particular para:

I. Autenticar la identidad de usuarios, sistemas o servicios;
II. Autenticación de documentos y mensajes de datos firmados digitalmente; y
III. Proteger documentos y comunicaciones electrónicos mediante el cifrado de datos.

Los firmantes no deberán compartir las llaves privadas de sus certificados.

1.5. Lineamientos de administración

1.5.1. Publicación y actualización de este documento

La **UCE** es responsable del registro y mantenimiento de este documento, por lo que cualquier solicitud adicional de información sobre el mismo, deberá dirigir a esta instancia en el domicilio siguiente:

Tribunal Electoral del Poder Judicial de la Federación
Carlota Armero # 5000, Col CTM Culhuacán C.P. 04480. México D.F.
Teléfono de Contacto: 52+ (55) 5728-2300 ext. 2856

Para la elaboración de propuestas de modificación de este documento, será necesaria la actuación colegida de la DGS y de las Secretaría Generales de Acuerdos, quienes las someterán a la aprobación del pleno de la Sala Superior.

1.5.2. Contactos técnicos

La DGS es responsable de la operación y administración de la infraestructura de la **UCE,** por lo que ésta responderá cualquier duda o comentario de carácter técnico que se formule sobre las presentes Prácticas de Certificación, a las direcciones de correo electrónico siguientes:

admin-ac@te.gob.mx

1.5.3. Procedimiento de aprobación de Prácticas de Certificación

Mediante actuación colegiada de la **DGS** y de las Secretaría Generales de Acuerdos se elaborarán las propuestas de modificación a las presentes **Prácticas de Certificación** y las someterán a la aprobación del pleno de la Sala Superior.

2. Publicación y repositorio de certificados

2.1. Repositorios

Los repositorios en línea de certificados e información sobre la **UCE** se encuentran accesibles en la **URL** siguiente:

http://uce.te.gob.mx/

La **UCE** proporcionará los servicios de consulta en línea de la lista de revocación de certificados **CRL** y **OCSP,** respectivamente, en las direcciones electrónicas siguientes:

Servicio	Servidor	Observaciones
CRL	http://uce.te.gob.mx/firel/crl/acite.crl	Lista de revocación de certificados
OCSP	http://uce.te.gob.mx:1350/OCSPFIREL	Servicio de verificación, en tiempo real, del estado de los certificados.

2.2. Publicación de información de la UCE

Los certificados y la información relativa a la **UCE**, se encuentra en línea en la dirección electrónica citada en el **punto 2.1**, donde podrá obtenerse:

I. El Certificado Raíz del PJF
II. El certificado de la **UCE,** disponible para su descarga;
III. Certificados emitidos por la **UCE**;
IV. La lista de revocación de certificados **CRL**;
V. La versión actualizada de las **Practicas de Certificación,**
VI. La demás información relacionada con las unidades de certificación intermedia respecto de los certificados digitales de la FIREL y
VII. La Información sobre los servicios relacionados con el uso de los certificados.

2.3. Frecuencia de publicación

Los certificados emitidos por la **UCE** serán publicados de manera permanente.

Por las características propias del servicio de **OCSP**, la comprobación del estado de los certificados se realizará directamente en línea sobre los repositorios de la **UCE.**

La **UCE** administrará y mantendrá actualizada la **CRL** con una periodicidad de 7 días, en caso de procesar la revocación de certificados también emitirá una nueva **CRL.**

Las **Prácticas de Certificación** podrán modificarse con base en las necesidades del Tribunal Electoral, por lo que las modificaciones de este documento serán publicadas una vez que éstas sean aprobadas.

2.4. Control de acceso a repositorios

El repositorio se mantendrá en línea y disponible las 24 hrs. del día, los 7 días de la semana, salvo que por actividades de mantenimiento tenga que interrumpirse su acceso a los sistemas informáticos y redes que soportan a la **UCE.** En ese supuesto, se emitirá el aviso correspondiente en el que se indicará el horario del período de mantenimiento.

3. Identificación y Autenticación

3.1. Nombres

3.1.1. Tipos de Nombres

Las cadenas de caracteres válidas asociadas a los campos del **Subject Name** de los certificados emitidos por la **UCE** estarán basadas en el prototipo de datos de intercambio **X.500**, por lo que las cadenas asociadas al campo de identificación **Common Name** (**CN)** tendrán una longitud máxima de 128 caracteres imprimibles.

El nombre distintivo de los certificados digitales de la FIREL contempla los siguientes valores:

I. Para usuarios finales de la FIREL:
   a. CN = <NOMBRES><APELLIDOS>
   b. E = Dirección de correo electrónico del titular del certificado
   c. SN = CURP del titular del certificado.

II. Para servicios informáticos del TEPJF:
   a. CN = <NOMBRE DEL SERVICIO>
   b. E = Dirección de correo electrónico de Administración del Servicio
   c. C = MX

El conjunto de caracteres válidos para el campo de identificación **Common Name** (**CN**) de los certificados emitidos por la **UCE** son:

Conjunto de caracteres	Descripción
‘0’ al ‘9’	Numéricos
‘a’ a la ‘z’	Alfabéticos minúsculas
‘A’ a la ‘Z’	Alfabéticos mayúsculas
‘.’, ‘-‘ ‘ ‘	Espacio en blanco para generar nombres completos de usuarios, así como punto y guiones
‘á’ a la ‘ú’	Vocales acentuadas
Ñ o ñ	Ñ mayúscula y minúscula

3.1.2. Nombres válidos

El **Subject Name** de cada certificado emitido por la **UCE** debe tener una asociación razonable que permita identificar al firmante, por lo que éste deberá proporcionar información distintiva de identificación única.

3.1.3. Nombres únicos y no ambiguos

La información proporcionada para el campo **Distinguished Name** (**DN**) debe ser única y no ambigua para cada certificado emitido por la **UCE**.

En este sentido, se entiende como nombre idéntico al que sólo es diferente por la presentación de mayúsculas o minúsculas, esto es, cuando la presentación en mayúsculas o minúsculas del nombre no es un diferenciador de nombre.

3.2. Validación inicial de identidad

3.2.1. Método de validación de posesión de llave privada

La **UCE** determinará la posesión de la llave privada relacionada con la solicitud de un certificado digital, a través de la autofirma del formato **CSR** mediante el cual se envía la solicitud de certificado.

3.2.2. Autenticación de pertenencia

3.2.2.1. Validación inicial de la identidad del Servidor Público del PJF que solicita un certificado intermedio para el TEPJF

En la ceremonia de generación del certificado Intermedio respectivo, el servidor público se deberá identificar ante el notario público con la credencial oficial vigente que acredite su identidad.

3.2.2.2. Validación inicial de identidad de un Agente Certificador del TEPJF

Al momento de solicitar su certificado, el Servidor Público del PJF deberá acreditar su identidad ante la UCE conforme a lo previsto al artículo 4, inciso d) del AGC 1/2013 y mediante copia digital del oficio de designación correspondiente.

Los agentes certificadores serán designados por los titulares de las Secretarías Generales de Acuerdos de la Sala Superior y de las Salas Regionales, por lo que, para el registro de los mismos en los sistemas de la **UR,** las Secretarías Generales de Acuerdos, deberán notificar por oficio a la **DGS**, el nombre, así como el curp de los servidores públicos que fungirán como tales.

3.2.3. Autenticación de individuos

El Agente Certificador recibirá los documentos y recabará los registros biométricos para validar la identidad de los Justiciables, previo consentimiento expreso de éste conforme a lo señalado en el artículo 4 del AGC 1/2013.

3.3. Identificación y autenticación de solicitudes de revocación

En caso de pérdida o encontrarse en riesgo la seguridad de la llave privada del certificado, el firmante deberá iniciar el proceso de revocación de manera electrónica a través del sistema electrónico de la FIREL o personalmente ante la UR, conforme a lo establecido en el punto 6.4 de las Políticas para la obtención y uso de la firma electrónica certificada del Poder Judicial de la Federación (FIREL), así como para la operación de su infraestructura tecnológica.

4. Requerimientos de operación y ciclo de vida del certificado

4.1. Solicitud de Certificado

4.1.1. Quién puede solicitar un certificado

De conformidad con el artículo 4 del AGC 1/2013, toda persona física, incluyendo a los servidores públicos, que pretenda tener acceso a la FIREL podrán tramitar en la UCE del TEPJF Certificado de Firma FIREL.

Los servidores públicos del Tribunal Electoral a fin de dar cumplimiento a los acuerdos emitidos por este órgano jurisdiccional en el uso de firma electrónica avanzada.

Para efectos de notificaciones vía correo electrónico, únicamente los Secretarios Generales de Acuerdos, el Subsecretario General de Acuerdos y los Actuarios de este Tribunal Electoral, tendrán certificado de firma electrónica avanzada.

4.1.2. Proceso de inscripción y responsabilidades

El interesado en obtener un Certificado Digital deberá ingresar al SEPJF en la dirección http://www.pjf.gob.mx/firel y dirigirse a la sección “Solicitud de un Certificado digital de Firma Electrónica “FIREL”, leer y aceptar los términos y condiciones de uso que se presentan en dicho portal.

El proceso de solicitud comprende:

1. Generación de su Llave Privada y Requerimiento de certificación: El interesado deberá descargar el software generador de requerimiento, proporcionar la información solicitada para generar el requerimiento de certificación, generar sus claves de acceso y revocación, y finalmente resguardar de manera segura la llave privada de su certificado.
   En el caso de los funcionarios públicos del PJF, el resguardo de dicha llave se deberá realizar en un dispositivo criptográfico Token, mientras que en los demás casos el resguardo se realizará en el repositorio seguro de certificados del equipo en el que se procesó la solicitud.
2. Formulación de la solicitud de Certificado Digital: Una vez generado el requerimiento de certificación, el interesado adjuntará dicho requerimiento dentro del SEPJF y formulará la solicitud de su certificado. Para esto deberá proporcionar la información requerida, anexar la documentación solicitada en archivos digitales PDF menores a 1 MB y registrar su solicitud dentro del sistema.
3. Programación de Cita: El interesado agendará una cita para la revisión de la documentación enviada, la captura de su información biométrica y la emisión de su certificado digital en el módulo de atención del organismo del PJF de su conveniencia. Seleccionará alguna de las fechas y horarios dispuestos para ello dentro del SEPJF y recibirá un acuse de recibo que deberá presentar impreso por duplicado junto con la documentación registrada en su solicitud en el lugar, fecha y hora que haya seleccionado.

El interesado asume las siguientes responsabilidades:

I. Leer y aceptar los términos y condiciones de uso de los certificados emitidos por la **UCE**, así como los procedimientos establecidos en este documento;
II. Hacer uso de los certificados únicamente para los fines autorizados;
III. Tomar las precauciones para evitar la pérdida, divulgación o acceso no autorizado a la llave privada asociada al certificado, y
IV. Realizar la revocación de su certificado digital ante cualquier circunstancia que pueda poner en riesgo la confidencialidad de la llave privada.

4.2. Procesamiento de la solicitud

4.2.1. Validación de identidad y pertenencia

El servidor público autorizado que desempeñe las actividades de Agente Certificador de la UCE, se autenticará en el módulo de enrolamiento de la **UCE** e identificará todas las citas agendadas. El operador deberá de proceder a verificar el

cumplimiento de lo establecido para la emisión de certificados, así como para la revocación de certificados.

En este sentido el Agente Certificador deberá:

I. Verificar que el interesado presenta la documentación establecida para sustentar pertenencia e identidad;
II. Autenticar la información que se incorpora a la solicitud de certificado que corresponda a la identidad del solicitante;
III. Verificar que el solicitante está en posesión de la llave privada correspondiente a la solicitud en cuestión,
IV. Recabar los registros biométricos del solicitante y
V. Continuar con el proceso de emisión del certificado cuando las solicitudes del certificado procedan a fin de liberarlo o, en caso contrario, informar, vía correo electrónico, al interesado la razón por la que no fue posible emitir el certificado.

4.2.2. Aprobación o rechazo de solicitudes

Si la validación de la información contenida en la solicitud de certificado **CSR,** la comprobación de documentación, así como el registro de la información biométrica son exitosos, se tramitará mediante transacción segura firmada por el Agente Certificador de la **UCE,** la solicitud a fin que ésta proceda con la firma y liberación del certificado.

En caso contrario, se informará al solicitante, vía correo electrónico, la razón por la cual no fue posible emitir el certificado.

El solicitante podrá solventar la información o documentación indicada por la **UCE** y solicitar nuevamente el certificado, conforme a lo señalado en la **sección 4.1**.

4.2.3. Duración del proceso de la solicitud

Se estima un tiempo máximo de 20 minutos para el trámite de la solicitud de un certificado dependerá del proceso de validación de la información proporcionada, el registro de la información biométrica y la aprobación por parte del Agente Certificador para la emisión del certificado.

4.3. Emisión de certificados

4.3.1. Acciones durante la emisión de certificado

El solicitante a través del SEPJF, ingresa el archivo de requerimiento de certificado (**CSR),** el cual será transferido por medio seguro al módulo de certificación de la **UCE**. En este sistema, una vez generado y firmado el certificado, será publicado en línea.

4.3.2. Notificación al firmante de la emisión del certificado emitido

Por conducto del Sistema Electrónico del PJF se enviará un correo electrónico a la cuenta registrada por el solicitante, en el que se indicará que su Certificado Digital de la FIREL ha sido emitido, así como el procedimiento a seguir por el propio solicitante para la descarga

4.4. Aceptación del certificado

4.4.1. Conducta constitutiva de aceptación de certificado

Una vez recibido el correo electrónico indicando la ruta **URL** de descarga del certificado, el solicitante deberá realizar la descarga e instalación de dicho Certificado Digital en el Dispositivo de Seguridad Token – tratándose de los Servidores Públicos de PJF- o la generación de un archivo PFX con el Certificado Digital de la FIREL respectivo –tratándose de los justiciables-.

.

4.4.2. Publicación del certificado por la UCE

De acuerdo con lo establecido en el numeral 2.1 de estas prácticas de certificación, La **UCE** publicará los certificados emitidos en la URL:

http://uce.te.gob.mx/

4.4.3. Notificación de emisión de certificado a otras entidades

El SEPJF emitirá la notificar que correspondan a las demás autoridades certificadoras del PJF de la emisión de un certificado digital.

4.5. Uso del certificado y par de llaves

4.5.1. Uso del certificado de firmantes y llaves privadas de firmantes

Los certificados digitales FIREL emitidos por la **UCE** y sus llaves privadas asociadas deben ser usados únicamente para los fines establecidos en la **sección**

1.4 de este documento. Cuando un certificado sea revocado, la llave privada no podrá ser utilizada posteriormente para ningún propósito adicional.

4.6. Renovación de certificados

4.6.1. Circunstancias para renovación de certificados

La renovación de un Certificado Digital de la FIREL deberá efectuarse dentro de los treinta días anteriores a la conclusión de su vigencia, en la inteligencia de que si en ese lapso no se renueva el Certificado Digital de la FIREL correspondiente, éste caducará y el interesado deberá formular una nueva solicitud conforme a la sección 4.1 de este documento.

4.6.2. Quién puede solicitar la renovación de certificado

Todos los funcionarios públicos del PJF y los justiciables que cuenten ya con un certificado digital podrán solicitar la renovación del mismo cuando éste se encuentre próximo a expirar, de acuerdo con lo establecido en el apartado 6.1 de estas prácticas de certificación**.**

4.6.3. Procedimiento para solicitar una renovación de certificado

El titular del Certificado Digital de la FIREL deberá ingresar al Sistema Electrónico del PJF en la dirección http://www.pjf.gob.mx/firel/ acceder al vínculo denominado FIREL y seleccionar la opción “Renovación de un certificado digital de firma electrónica (FIREL)”, así como aceptar los términos y condiciones de uso.

El procedimiento de renovación contempla:

1. Generación del Requerimiento de Renovación: Haciendo uso de la aplicación institucional para la generación de un requerimiento (que en caso necesario deberá volver a descargar del sitio anteriormente mencionado), el interesado usará su dispositivo de seguridad – tratándose de un funcionario del PJF – o su archivo PFX – tratándose de cualquier otro justiciable – en conjunto con la clave de acceso a la Llave Privada de su certificado actual para generar un requerimiento de renovación. Actualizará la información correspondiente y resguardará de manera segura la llave privada de su certificado. En el caso de los funcionarios públicos del PJF, el resguardo de dicha llave se deberá realizar en un dispositivo criptográfico Token, mientras que en los demás casos el resguardo se realizará en el repositorio seguro de certificados del equipo en el que se llevó a cabo este procedimiento.
2. Envío de la solicitud de renovación: A través del SEPJF, el interesado deberá enviar el archivo de requerimiento de renovación para que el propio sistema

valide que éste se encuentra firmado por el Certificado Digital de la FIREL vigente del solicitante, y de esta forma se realice la renovación de manera inmediata.

4.6.4. Notificación de emisión de renovación de certificado

Una vez que el SEPJF realizó la validación de la firma de la solicitud de renovación y ha emitido el nuevo Certificado Digital de la FIREL, el interesado recibirá en su cuenta de correo electrónico la dirección URL para realizar la descarga de su nuevo certificado digital.

4.6.5. Conducta constitutiva de aceptación de certificado renovado

Una vez recibido el correo electrónico indicando la ruta **URL** de descarga del certificado, el interesado deberá realizar la descarga e instalación de dicho Certificado Digital en el Dispositivo de Seguridad Token – tratándose de los Servidores Públicos de PJF- o la generación de un archivo PFX con el Certificado Digital de la FIREL respectivo –tratándose de los justiciables.

4.6.6. Publicación de certificados renovados por la UCE

De acuerdo con lo establecido en el numeral 2.1 de estas prácticas de certificación, la **UCE** publicará los certificados emitidos en la URL:
http://uce.te.gob.mx/PracticasCertificacion.

4.6.7. Notificación de emisión de certificado renovado a otras entidades

El SEPJF será el encargado de notificar a las demás autoridades certificadoras del PJF la emisión de un certificado digital.

4.7. Cambio de llaves del certificado

4.7.1. Circunstancias para cambiar llaves a un certificado

Por razones de seguridad, la **UCE** no dispone de mecanismos de cambio de llave a certificados emitidos, por lo que el firmante interesado en cambiar algún parámetro del certificado deberá revocar el certificado actual y solicitar un nuevo certificado.

4.8. Modificación de certificados

4.8.1. Circunstancias para modificación de certificado

Los certificados emitidos por la **UCE** no pueden ser modificados, por lo que, los firmantes que por alguna circunstancia requieran alguna modificación a su certificado, deberán proceder a revocarlo y solicitar un nuevo certificado.

4.9. Revocación y suspensión de certificado

4.9.1. Circunstancias de revocación

Un certificado puede ser revocado durante su período de vigencia por causa de muerte de su titular o por diversa que encuentre sustento en una disposición general, cuando la Unidad de Certificación del TEPJF cuente con la documentación que acredite fehacientemente la existencia de dicha causa.

Tratándose de un servidor público del TEPJF por motivo de baja, el titular del órgano respectivo dentro de los treinta días hábiles siguientes, deberá comunicar tal situación mediante oficio a la Unidad de Certificación de este órgano jurisdiccional.

4.9.2. Quién puede solicitar la revocación

La revocación de un certificado únicamente puede ser solicitada por:

I. El firmante (titular) propietario del certificado y
II. Las autoridades del Tribunal Electoral, por causa que encuentre sustento en una disposición general.

4.9.3. Procedimiento de solicitud de revocación

El firmante podrá solicitar la revocación de su certificado digital a través de alguna de las siguientes opciones:

1. Revocación en línea: A través del SEPJF, el interesado podrá revocar su certificado digital proporcionando su CURP y la clave de revocación de su certificado actual vigente.
2. A través de los módulos de atención del TE: Si el interesado no cuenta con su clave de revocación, deberá presentar de manera personal en alguno de los módulos de atención del PJF una carta donde manifieste la voluntad de revocar su certificado digital. Adicionalmente deberá acreditar su identidad proporcionando su nombre, su CURP y acreditando su identidad ante los dispositivos biométricos.

Para el caso de la muerte del titular la solicitud de revocación podrá ser realizada por un tercero, el cual deberá presentar en los módulos de atención del TEPJF el acta de defunción correspondiente.

Una vez revocado un Certificado Digital éste ya no podrá ser utilizado, por lo que si el interesado requiere de otro, tendrá que solicitarlo de nueva cuenta conforme al procedimiento establecido en estas prácticas de certificación.

4.9.4. Periodo de gracia de solicitud de revocación

La solicitud de revocación únicamente podrá realizarse durante el período de vigencia del certificado digital; por tanto, no existe un período de gracia para esta solicitud.

4.9.5. Tiempo de respuesta en el cual la UCE procesará la solicitud de revocación

Para el caso de la revocación en línea, la revocación del certificado procederá de forma inmediata.

En caso de no contar con la clave de revocación, deberá acudir personalmente a las instalaciones de la UCE, donde fue emitido el certificado, con el objeto de que presente un escrito en el que manifieste su voluntad de revocar su certificado digital de la FIREL indicando su nombre y su CURP, a efecto de que el Agente Certificador habilitado para tal fin verifique a través del Sistema AFIS la identidad del solicitante y realice el trámite necesario para la revocación solicitada.

4.9.6. Requerimientos de verificación por relación de confianza

Antes de usar un certificado emitido por la **UCE,** se deberá validar vía **OCSP** o en la **CRL** si éste no está revocado.

4.9.7. Frecuencia de emisión de CRL

La **CRL** será actualizada y emitida después de que se revoque un certificado o al menos cada 7 días antes que expire la última lista de revocación.

4.9.8. Máxima latencia de CRL

La **CRL** firmada por la **UCE** deberá ser transferida de manera inmediata y segura al repositorio en línea donde podrán ser consultadas.

4.9.9. Verificación en línea de revocación

Los certificados revocados podrán verificarse, preferentemente, vía el protocolo **OCSP** o a través de la **CRL** que se encontrará disponible en línea en el repositorio de la **UCE** en las rutas comentadas en la **sección 2.1**. No existe ningún otro lugar de descarga autorizado.

4.9.10. Requerimientos para verificar en línea la revocación

Los interesados deberán verificar vía el protocolo **OCSP** o a través de la **CRL**, antes de usar el certificado, si éste es vigente, para lo cual la **UCE** no limitará el acceso a los servicios de validación de revocación **OCSP** o **CRL**.

4.10. Servicios de validación de certificados

4.10.1. Características de operación

La **UCE** mantendrá respaldos de los repositorios en línea y disponibles a través del sitio oficial que se indica en la **sección 2.1**, donde podrá obtenerse:

I. Certificado intermedio de la **UCE**;
II. Todos los certificados emitidos, y
III. Acceso a los servicios de verificación de revocación en línea vía **OCSP** o última **CRL.**

4.10.2. Disponibilidad de servicios.

En los mismos términos definidos en la **secciones 2.3 y 2.4**

4.11. Terminación de suscripción

La suscripción termina al expirar la vigencia del certificado o al revocarse.

4.11.1. Depósito y recuperación de llaves

La **UCE** no almacena llaves privadas de los firmantes, el propietario de las llaves es responsable de prever cualquier contingencia con la misma.

5. Instalaciones, controles y operación

5.1. Controles de acceso

La **UCE** se encuentra protegida al interior de las instalaciones de la Sala Superior del Tribunal Electoral y cuenta con controles de acceso restringido.

5.1.1. Ubicación

Domicilio proporcionado en la **sección 1.5.1**

5.1.2. Acceso físico

La **UCE** se encuentra resguardada en un entorno de acceso controlado, donde el acceso es restringido sólo al personal autorizado y se mantiene registro de los ingresos al sitio.

5.1.3. Energía ininterrumpida y entorno ambiental controlado

Los equipos de cómputo y telecomunicaciones que soportan la operación de la **UCE** se encuentran bajo un entorno controlado de temperatura y humedad, así también, los equipos están protegidos por la operación de un sistema redundante de **UPS** de **30 KVA/ 27 KW** de **doble conversión**, para evitar la interrupción de los servicios y fallas de los sistemas por alteración en los suministros de energía eléctrica.

5.1.4. Exposición a inundaciones

Los sistemas de cómputo en los cuales reside la **UCE** se encuentran alojados en un primer piso de las instalaciones de la Sala Superior del Tribunal Electoral, a una altura por arriba de 4.50 metros, sobre el nivel de la calle, reduciendo de manera significativa los riesgo de una inundación.

5.1.5. Control contra incendios

El sitio donde residen los equipos de cómputo donde se alojan la **UCE** cuenta con sistema de extintores para incendios

5.1.6. Medios removibles

El uso de los medios de almacenamiento removibles se encuentra restringido de manera que sólo los dispositivos autorizados (**dispositivos Token USB de autenticación de usuarios)** pueden ser utilizados en el equipo donde reside el certificado de la **UCE**.

5.1.7. Respaldos fuera de línea

Se mantendrán respaldos para garantizar la continuidad de las operaciones de los siguientes repositorios:

I. Certificado intermedio de la **UCE**;
II. Certificados emitidos, y
III. **CRL.**

5.2. Procedimientos de control

5.2.1. Responsabilidades y roles de operación

A continuación se enumeran las responsabilidades y roles de la operación técnica de la **UCE**:

I. Administrador de la **UCE.** Este rol será asumido por personal de la Dirección de Seguridad Informática de la **DGS**;
II. Agentes certificadores. Este rol será asumido por personal de las Secretarías Generales de Acuerdos, con el apoyo de la **DGS.**

5.2.2. Número de personas requeridas por tarea

A fin de ejecutar las tareas de gestión de certificados se requiere de un agente certificador y del apoyo, en su caso, de la **DGS**.

5.2.3. Identificación y autenticación para cada rol de operación

El acceso a los sistemas de administración y operación de la **UCE** se realizará mediante el uso de certificados de firma electrónica emitidos para este fin y que se encuentran bajo resguardo del administrador u operadores de la **UCE.**

5.2.4. Separación de funciones

A excepción de las tareas de gestión del **HSM**, las tareas adicionales de la **UCE** no requieren de separación de funciones.

5.3. Controles del personal

5.3.1. Calificaciones, experiencia y cumplimiento de requerimientos

El personal que administra la **UCE** deberá tener experiencia y habilidades en tecnología **de PKI** y **administración de sistemas.**

5.3.2. Procedimiento de verificación

El personal que opera y administra la infraestructura tecnológica de la **UCE** serán servidores públicos que para este efecto han sido autorizados por la Dirección de Seguridad Informática de la Dirección General de Sistemas.

5.3.3. Capacitación

El personal que realice actividades de administración y operación de la **UCE** estará capacitado para realizar dichas tareas.

5.3.4. Actualización y capacitación

El personal que opera los sistemas y equipos de la **UCE** deberá cumplir un programa de actualización y capacitación que refleje la integración de nuevas características en los sistemas o procedimientos de operación de la **UCE**.

5.3.5. Sanciones de acciones no autorizadas

Se aplicará la normatividad interna vigente.

5.3.6. Documentación proporcionada al personal

Se proporcionará los manuales de operación y administración de sistemas requeridos para dar cumplimiento a las actividades encomendadas de administración y operación de la **UCE.**

5.4. Procedimientos de auditorías

5.4.1. Tipos de eventos registrados

Serán registrados eventos de los sistemas informático **UCE** siguientes:

I. Accesos y salidas de usuarios al sistema;
II. Reinicios del Sistemas;

III. Solicitudes de certificados;
IV. Firma de certificados;
V. Emisión de **CRL,** y

Cada registro de los eventos contiene campos que indican la fecha y hora del momento en que ocurrieron, de manera que puede darse un seguimiento puntual a las actividades en los sistemas.

Los sistemas que soportan la operación de la **UCE** están sincronizados a través del servicio de **NTP** con el tiempo oficial del centro de la República Mexicana.

5.4.2. Frecuencia de procesamiento de registros

El personal de la Dirección de Seguridad Informática de la **DGS** administrador de la **UCE** procesará los registros semanalmente o en caso de observarse algún tipo de incidente en los sistemas que lo requiera, como pueden ser algún problema de operación de los sistemas informáticos.

5.4.3. Retención de registros de eventos

El periodo mínimo de retención de los archivos de registros de eventos es de 5 años.

5.4.4. Protección de los registros de auditoría

Los registros de auditoría deben ser accesibles solo para los operadores, administradores y auditores de la **UCE.** Esta información se considera como reservada, por lo que se mantendrá bajo mecanismos de protección correspondientes.

5.4.5. Procedimiento para el respaldo de registros de auditoría

Los registros de auditoría serán respaldados en línea en tiempo real a través del sistema de administración de registros de la Dirección de Seguridad Informática de la **DGS.**

5.4.6. Sistemas de recolección de registros

El monitoreo y administración de los registros de auditoría se realizará a través de un sistema de administración de registros, a fin de identificar posibles violaciones a la infraestructura de seguridad.

5.4.7. Evaluación de vulnerabilidades

El área de Seguridad Informática de la **DGS** es la encargada de mantener un monitoreo continuo sobre la operación de la infraestructura de la **UCE**, a fin de identificar riesgos o vulnerabilidades potenciales y ejecutar los procesos de remediación adecuados y convenientes.

Al menos una vez al año, se llevará a cabo una auditoría de seguridad a los sistemas e infraestructura de telecomunicaciones de la **UCE.**

5.5. Respaldo de registros

5.5.1. Tipo de registros a respaldar

Los enumerados en la **sección 5.4.1.**

5.5.2. Retención de respaldos

Se mantendrán los respaldos de los registros por un mínimo de 5 años.

5.5.3. Protección de los respaldos

Únicamente el personal autorizado de la **UCE** tendrá acceso a los respaldos.

5.5.4. Procedimiento de respaldos de registros

Se aplicará el procedimiento de respaldo vigente en la **DGS**, haciendo uso de las unidades de respaldo y/o de almacenamiento.

5.5.5. Requerimientos de estampado de tiempo de registros

Todos los eventos registrados deberán contener un registro de fecha y hora de ejecución.

5.5.6. Sistema de almacenamiento de respaldos

Se mantendrán respaldos locales en la **DGS**, en cumplimiento a los procedimientos de respaldo de información vigentes.

5.5.7. Procedimiento para obtener y verificar la información en los respaldos

Se aplicarán los procedimientos de verificación y restauración de información establecidos en la **DGS** para este fin.

5.6. Manejo de incidentes y recuperación de desastres

5.6.1. Manejo de incidente de llaves comprometidas

Si la seguridad de las llaves privadas de los agentes certificadores se encuentra en riesgo, el administrador de la **UCE** deberá ser informado y los certificados relacionados al incidente deberán ser revocados.

Si la confidencialidad de la llave privada asociada al certificado intermedio se encuentra en riesgo, se deberá:

I. Informar a los agentes certificadores, firmantes y terceros involucrados en relaciones de confianza;
II. Dar por terminado la generación de certificados y firma de **CRL** con la llave relacionada al incidente;
III. Revocar el certificado comprometido;
IV. Generar un nuevo par de llaves cumpliendo el protocolo de inicialización, y
V. Publicar el nuevo certificado.

5.6.2. Recursos informáticos, programas y/o datos corruptos

A fin de reducir los riesgos de un incidente de seguridad en los sistemas informáticos, se dispondrán de la infraestructura de seguridad perimetral y de gestión de sistemas alineados a las mejores prácticas en la materia:

I. Sistemas actualizados;
II. Respaldos de sistemas e información;
III. Registros de actividad para la identificación en tiempo de cualquier incidencia;
IV. Operación de seguridad perimetral: Firewall y detección de intrusos, y
V. Mecanismos de recuperación de sistemas e información.

5.6.3. Procedimiento en caso de llave privada de firmante comprometida

Si la llave privada de algún firmante se extravía o es comprometida, el firmante deber informar a la **UCE** de este incidente y proceder a solicitar la revocación del certificado.

Una vez revocado, la información sobre el certificado será publicada a través del **CRL** y del **OCSP.**

5.6.4. Plan de continuidad

La **UCE** se encuentra ubicada dentro de instalaciones del Tribunal Electoral y, por formar parte de la infraestructura crítica de operación, estos sistemas serán respaldados y considerados dentro del plan de continuidad de la **DGS**

5.7. Terminación de servicios

Antes que se den por terminados los servicios de la **UCE,** ésta deberá de:

I. Informar a los agentes certificadores, firmantes y terceros relacionados sobre la baja del servicio;
II. Informar sobre las condiciones y terminación del mismo;
III. Revocar todos los certificados;
IV. Emitir y publicar el **CRL**, y
V. Destruir las llaves privadas y los respaldos.

La Dirección de Seguridad Informática de la **DGS** será la encargada de realizar las acciones necesarias para asegurar la operación y mantenimiento de la **UCE,** en consecuencia, mantendrá la operación al menos durante 12 meses posteriores al vencimiento del último certificado emitido. Esto a fin de proporcionar continuidad en el uso legal de los certificados autorizados por el Tribunal Electoral.

6. Controles de seguridad lógica

6.1. Generación e instalación del par de llaves

6.1.1. Generación de llaves

El par de llaves del certificado intermedio de la **UCE** fueron generadas por servidores públicos autorizados utilizando el hardware de seguridad **HSM** que forma parte de la infraestructura de llave pública, de manera que la llave privada reside exclusivamente en este dispositivo de seguridad.

El par de llaves generadas de los certificados de los usuarios, incluidos agentes certificadores, serán generadas utilizando el programa informático de solicitud de certificado FIREL, y la llave privada en el caso de los servidores públicos del Tribunal Electoral deberán residir preferentemente en un dispositivo criptográfico **Token** autorizado.

6.1.2. Entrega de llaves privadas a firmantes.

Cada firmante debe generar su propio par de llaves haciendo uso del equipo de cómputo institucional y a través de los sistemas informáticos dispuestos para estos fines. La **UCE** no hace entrega de llaves privadas a firmantes, ya que éstas son generadas en el equipo utilizado por el solicitante.

6.1.3. Entrega de llaves públicas de certificados emitidos

Las llaves públicas de los firmantes se encontrarán disponibles como parte de los certificados digitales FIREL, a través del sitio web de la **UCE**.

6.1.4. Entrega de llave pública de la UCE

El certificado intermedio de la **UCE** se encuentra disponible en línea en los repositorios como se indica en la **sección 2.2.**

6.1.5. Tamaño de las llaves

Las llaves del certificado intermedio de la **UCE** tendrán una longitud de **4096 bits**, mientras que las llaves de los certificados emitidos por la **UCE** tendrán una longitud de **2048 bits** como mínimo.

6.1.6. Uso del par de llaves

Las llaves deberán ser utilizadas de acuerdo al tipo de certificado.

I. Certificado de usuario para:

a. Autenticación;
b. No repudiación;
c. Cifrado de información;
d. Integridad de mensajes, y
e. Firmado de objetos.

II. Los certificados de agentes certificadores de las **UR** para:

a. Actividades relacionadas a la operación de acreditación y operación de registro.

III. El certificado intermedio de la **UCE**:

a. Firmar certificados, y
b. Firmar **CRL.**

6.2. Protección de la llave privada de certificado intermedio y controles del modelo criptográfico

6.2.1. Controles y estándares criptográficos

Los solicitantes deberán hacer uso de los sistemas informáticos de la **UCE** para solicitar la generación de certificados, ya que éste sistema genera el documento electrónico de solicitud **CSR** que permite validar la posesión de la llave privada asociada.

La llave privada del certificado intermedio de la **UCE** fue generada y se encuentra almacenada en el módulo criptográfico **HSM**, no hay copias o respaldo en claro de la llave privada intermedio de la **UCE**.

Cada operador de la **UCE** tendrá un certificado de usuario y la llave privada asociada estará almacenada en dispositivo criptográfico tipo **Token**, cuya operación que estará protegido por contraseña.

6.2.2. Control multi-personas (m de n)

Para inicializar la operación de la **UCE** se requiere de la intervención de dos operadores de los cuatro definidos.

6.2.3. Almacenamiento de llave privada

La llave privada asociada al certificado intermedio de la **UCE** se encuentra almacenado en el **HSM** como se establece en la **sección 6.2.1**.

6.2.4. Respaldo de llave privada

Se dispone de un respaldo de la llave privada del certificado de la **UCE** que deberá permanecer protegido en dispositivo criptográfico seguro, como parte del esquema de continuidad de operaciones y recuperación en caso de desastres.

El respaldo de esta llave privada se encontrará en resguardo en la Dirección de Seguridad Informática de la **DGS.**

6.2.5. Transferencia de llave privada hacia y desde modulo criptográfico

La llave privada asociada al certificado intermedio de la **UCE** será generada en el dispositivo **HSM** y permanecerá en éste para su operación.

El respaldo de la llave privada será ejecutado a través de procedimiento protocolizado y formalizado en un acta circunstanciada de hechos.

6.2.6. Seguridad de almacenamiento de llave privada

La llave privada del certificado intermedio de la **UCE** se encuentra alojada en un módulo de protección del sistema de hardware de seguridad **HSM**.

6.2.7. Método de activación de llave privada

El uso y operaciones de la llave privada de la **UCE** se encuentran protegidas en el **HSM** y se requiere cumplir con una autenticación de doble factor para iniciar las operaciones con la llave privada.

6.2.8. Método para desactivar la llave privada

La llave privada de la **UCE** no se instala en dispositivos de memoria **RAM** accesible por aplicaciones de terceros, ya que las operaciones de firma de certificados y **CRL** se realizan a través de la interfaz del **HSM**, por lo que sólo los aplicativos autenticados con el **HSM** pueden tener acceso a estas aplicaciones.

A través de autenticación de doble factor del **HSM,** se controla la operación y acceso a la llave privada almacenada en el dispositivo criptográfico

6.2.9. Método para destruir llaves privadas

Será a través de la interfaz de administración del módulo **HSM,** como se realizará un proceso de borrado seguro de la llave privada asociados al certificado intermedio, una vez que la misma cumpla el ciclo de operación de la misma.

6.3. Otros aspectos de administración del par de llaves

6.3.1. Histórico de llaves públicas

La **UCE** dispondrá de un respaldo histórico fuera de línea de todos los certificados que emita.

6.3.2. Periodo de vigencia de certificados y par de llaves

Los certificados emitidos por la **UCE** tendrán las siguientes vigencias:

I. El certificado intermedio de la **UCE** tendrá un periodo de vigencia de diez años, y

II. Los certificados emitidos para los usuarios tendrán un periodo de vigencia de tres años o menor en caso que así lo determinen las instancias que correspondan del Tribunal Electoral.

6.4. Activación de sistemas y datos

Adicionalmente a las contraseña de administración y operación de la **UCE**, se disponen de controles a través de roles y perfiles para la administración y operación de la **UR** y del módulo de certificación. El uso de la llave privada del certificado intermedio de la **UCE** solamente está habilitado para lo establecido en **la sección 6.1.6**

6.4.1. Activación para la Instalación y generación de certificados

Con base en las definiciones generales establecidas en la **sección 6.4.**

6.4.2. Mecanismos de protección de la activación

Con base en las definiciones generales establecidas en la **sección 6.4.**

6.5. Controles de seguridad informática

6.5.1. Requerimientos de seguridad informática

La infraestructura de servidores sobre la cual reside la **UCE** son sistemas que deben cumplir con mecanismos razonables de rastreabilidad de actividades, así como manejo de actualizaciones de seguridad en los equipos y un robustecimiento de la seguridad específico para cada sistema que forma parte de esta infraestructura.

6.5.2. Controles de administración de la seguridad

Los sistemas y equipos se contarán con los controles de administración de seguridad siguientes:

I. Se realizarán auditorias de cumplimiento de configuración de seguridad al menos una vez al año en los sistemas informáticos en base a lo establecido en la sección 6.5.1;
II. Se evaluará mensualmente la aplicación de actualizaciones de seguridad autorizadas en aplicativos y sistema operativo;
III. Revisión de usuarios, perfiles y permisos al menos una vez cada 6 meses, y
IV. Revisión de registros en base a lo establecido en la sección 5.4.

6.5.3. Controles de ciclo de vida de seguridad

Se mantendrán las siguientes reglas de ciclo de vida en los sistemas y equipos de la **UCE**:

I. El hardware sobre el que operan los sistemas informáticos deberán tener garantía y soporte de mantenimiento vigente;
II. Los sistemas operativos sobre los que residen los sistemas de la **UCE** deberán tener mantenimiento y soporte del fabricante. Una vez que éste informe sobre la obsolescencia del sistema operativo, el mismo será migrado a un sistema con mantenimiento vigente, y
III. Los aplicativos que forman parte de la **UCE** deberán tener una póliza de mantenimiento y soporte vigente.

6.6. Control de seguridad de red.

El módulo de certificación de la **UCE** se encuentra aislado a través de un **firewall** de propósito específico, que controla el acceso exclusivamente de los módulos de la **UR**.

El sistema informático de la **UR** se comunican con los sistemas de la FIREL a través de la red de datos del Poder Judicial de la Federación, ya que estos servidores no se publican en internet.

6.7. Time-stamping.

Todos los sistemas en línea de la **UCE** se encuentran sincronizados a través del protocolo **NTP** con la hora oficial de la Ciudad de México emitida por el **Centro Nacional de Metrología.**

7. Perfil de certificado, CRL y OSCP.

7.1. Perfil de certificado

Los certificados emitidos por la **UCE** cumplen con las especificaciones establecidas para la operación de Certificados **X.509** en el **RFC 3280**: "**Internet X.509 Public Key Infraestructure: Certificate and CRL Profile".**

Adicionalmente para la liberación de certificados se requiere la participación de un agente acreditador y el administrador de la **UCE.**

7.1.1. Versión de certificados

La **UCE** emite certificados **X.509 versión 3.**

7.1.2. Extensiones validas en certificados

El Certificado intermedio de la **UCE** presentará las siguientes extensiones:

Extensión	Definición/Característica
Basic Constraints:	Subject Type=CA ,Path Length Constraint=0
Subject Key Identifier:	Hash
Key Usage:	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Subject alternative name:	RFC822 Name=EMAIL=admin-ac@te.gob.mx

Los certificados para usuarios, se extenderán certificados con al menos las siguientes extensiones:

Extensión	Definición/Característica
Basic Constraints:	Critical, Subject type: End Entity, Path length constraint= None
Subject Key Identifier:	Hash
Authority Key Identifier:	Keyid
Key Usage:	Digital Signature, Non Repudiation, Key Encipherment
Extended Key Usage:	Client Authentication, Secure Email
X509v3 CRL Distribution Points:	URI
Subject alternative name:	RFC822 Name= e-mail
Issuer alternative name:	RFC822 Name =admin-ac@te.gob.mx
Certificate Policies:	OID

7.1.3. Identificadores de objetos algoritmos

I. **Encryption:** rsaEncryption 1.2.840.113549.1.1.1, y
II. **Signature**: sha256WithRSA Encryption 1.2.840.113549.1.1.11

7.1.4. Formato de nombre

Cada certificado emitido por la **UCE** debe contener un **Nombre Distintivo Distinguished Name DN**, basado en las recomendaciones del **estándar técnico ITU-T X.501**.

Para el campo **Issuer**, los certificados de la **UCE** tendrán la estructura siguiente:

> **C=**MX, **O**=Tribunal Electoral del Poder Judicial de la Federación, **OU**=Dirección General de Sistemas, CN=Unidad de Certificación Electrónica - PJF.

El componente **CN** del campo **subject** de los certificados emitidos por la **UCE** para personas, deberá contener una cadena basada en el nombre del interesado.

CN=Nombre Apellidos, **E**=correo electrónico, **SERIALNUMBER**=CURP.

En caso de certificados emitidos para identificar equipos o sistemas informáticos, el **CN** deberá contener el nombre completo de dominio **FQDN** del sistema donde será instalado el certificado digital, de manera que pueda ser identificable de manera única.

7.1.5. Limitaciones en formato de nombres

No hay limitaciones adicionales a las establecidas en las **secciones 3.1.1, 3.1.2 y 7.1.4.**

7.1.6. Identificador de objeto de lineamientos del certificado

Cada certificado emitido por la UCE contendrá un identificador único asociado a la definición de **Prácticas de Certificación** sobre las cuales se liberó dicho certificado, este **OID**, identificará la versión de documento y estará asociado a lo establecido en la **sección 1.3**.

7.2. Perfil de CRL

7.2.1. Versión de CRL

La **UCE** publicará la **CRL** en el formato **X.509 v2.**

7.2.2. Extensiones y campos CRL

La **UCE** emitirá la **CRL** que contendrá todos los certificados revocados independientemente de la motivación. La **CRL** podrá contener información adicional sobre la razón de la revocación.

La **CRL** deberá incluir obligatoriamente la fecha de la siguiente emisión de la **CRL.** En caso de presentarse una revocación de certificado previamente a esta fecha, se emitirá una nueva **CRL** que actualice dicha información.

Las extensiones de la **CRL** incluirán el Identificador clave de autoridad **Authority Key Identifier,** y el número de **CRL.**

Por cada entrada de certificado revocado, la **CRL** deberá incluir la fecha de revocación.

7.3. Perfil de OCSP

La versión del **OCSP** emitido por la **UCE** corresponde a la **versión 1** definida en el **RFC 2560.**

8. Auditorias de cumplimiento técnicos

8.1. Frecuencia o circunstancias de evaluación.

La **DGS** deberá al menos una vez al año evaluar que la **UCE** cumpla con las definiciones de operación establecidas en este documento.

La **UCE** deberá, al menos una vez al año, evaluar que los operadores de las **UR** cumplan las definiciones y procedimientos de operación establecidos para éstos.

8.2. Entidades evaluadoras calificadas

Las evaluaciones de cumplimiento interno serán realizadas por personal de la Dirección de Seguridad Informática de la **DGS** con conocimientos en la operación de Infraestructura de llave pública.

En caso de requerirse de una auditoría externa, será una institución especializada en investigación y desarrollo de infraestructura de llave pública quien deberá ser considerada para este proceso.

Así también, lo disponga la Unidad para el control de Certificación de Firmas del Poder Judicial de la Federación en termino de los alcances y condiciones de este tipo de auditoría.

8.3. Temas a cubrirse en evaluación

La auditoría deberá verificar que los servicios proporcionados por la **UCE** cumplan con las definiciones establecidas en la última versión de este documento.

8.4. Acciones a tomar en caso de resultados deficientes

En caso de encontrarse desviaciones en la operación, la **DGS** deberá informar a las autoridades del Tribunal Electoral el plan de acciones que se llevarán a cabo para remediar las deficiencias.

Si las desviaciones están relacionadas con el proceso de liberación de certificados, el certificado en cuestión deberá ser revocado inmediatamente.

8.5. Comunicación de resultados

Las **autoridades del Tribunal Electoral** determinarán, con base en los resultados de la auditoría de operación, los mecanismos de comunicación de los resultados a terceras entidades involucrados, si fuera el caso.

9. Cumplimientos legales

9.1. Tarifas

Los servicios que la **DGS** ofrece, a través de la **UCE**, no tienen costo directo a los firmantes.

9.1.1. Tarifas de otros servicios

No se establece costo alguno para servicio que el Tribunal Electoral ofrezca a través de la **UCE.**

9.2. Confidencialidad de la información

El Tratamiento y protección de la información proporcionada por los funcionarios públicos a la **UCE,** para el trámite de generación de certificados será resguardada con base en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y el Acuerdo General de Transparencia, Acceso a la Información y Protección de Datos Personales del Tribunal Electoral del Poder Judicial de la Federación.

9.2.1. Divulgación de información de conformidad con procedimientos administrativos o judiciales

La **DGS**, en cumplimiento a sus obligaciones, pondrá a disposición de las **autoridades del Tribunal Electoral**, la información que sea requerida de la **UCE** conforme a los acuerdos que emita el Tribunal Electoral.

9.3. Propiedad intelectual

La **UCE** no reclama ninguna propiedad intelectual sobre los certificados emitidos.

9.4. Representaciones y garantías

9.4.1. Representaciones y garantías de la UCE

La **UCE**, garantiza la verificación de la identidad de los firmantes de acuerdo a los procedimientos integrados en este documento.

9.4.2. Representaciones y garantías del firmante

El firmante debe garantizar a la **UCE** que hará un uso responsable del certificado y las llaves asociadas al mismo, así como proteger la llave privada de acuerdo a lo estipulado en este documento.

El firmante debe:

I. Leer y adherirse a los lineamientos publicados en el uso de los certificados emitidos por la **UCE**;
II. Hacer uso sólo de los certificados para los fines autorizados, y
III. Tomar las previsiones para evitar pérdida, divulgación o acceso no permitido a la llave privada asociada al certificado.

9.5. Declaración de garantías

La **UCE** sólo garantiza el uso de programas informáticos y procedimientos para autenticar la identidad de los firmantes, apegadas a las mejores prácticas existentes en la materia, ejecutándose los procedimientos conforme a lo estipulado en este documento.

9.6. Terminación de prácticas

En los mismos términos definidos en la **sección 5.7**.

9.6.1. Expiración de prácticas

No se establece fecha de expiración de este documento, el cual tiene vigencia hasta que se libere una nueva versión.

9.6.2. Sobre modificaciones

Las modificaciones a este documento deberán ser publicadas al menos 2 semanas antes de entrar en vigencia el procedimiento, para aplicar estas modificaciones estará alineado a lo establecido en la **sección 1.5.1.**

9.6.3. Circunstancia validas de cambio en OID

El **OID** debe reflejar la versión de este documento, por lo que debe reflejar los cambios de versiones en el mismo.

9.7. Marco legal

La operación de la **UCE** se encuentra sujeta a las leyes vigentes en los Estado Unidos Mexicanos, por lo que toda disputa legal sobre el contenido de este documento, así como los procedimientos de operación y acreditación, incluyendo los servicios de emisión y revocación de certificados serán resueltos conforme a las mismas.

De conformidad con lo establecido en la fracción III, del Punto Quinto del Acuerdo General 1/2015 del Pleno de la Sala Superior, se validan los aspectos técnicos del contenido del presente documento por el personal de la Dirección General de Sistemas del TEPJF.

Elaboró y Validó	*Vo. Bo.*
Lic. José Rivelino Salinas Parrilla	***Mtro. David Amézquita Pérez***
Dirección de Seguridad Informática	*Director General*
	Dirección General de Sistemas