



# DIARIO OFICIAL DE LA FEDERACION

ORGANO DEL GOBIERNO CONSTITUCIONAL DE LOS ESTADOS UNIDOS MEXICANOS

Tomo DCLXXXVI No. 14 México, D.F., miércoles 17 de noviembre de 2010

## CONTENIDO

Secretaría de Energía

Secretaría de Salud

Secretaría de la Reforma Agraria

Comisión Nacional para el Desarrollo de los Pueblos Indígenas

Tribunal Electoral del Poder Judicial de la Federación

Banco de México

Instituto Federal Electoral

Gobierno del Distrito Federal

Avisos

Indice en página 94

---

\$31.00 EJEMPLAR

**PODER JUDICIAL**  
**TRIBUNAL ELECTORAL DEL PODER JUDICIAL DE LA**  
**FEDERACION**

**ACUERDO General de la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación número 5/2010, de veintisiete de octubre de dos mil diez, por el que se aprueban las Prácticas de Certificación de la Unidad de Certificación Electrónica y el Manual de Operación de las Notificaciones por Correo Electrónico.**

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Tribunal Electoral del Poder Judicial de la Federación.- Sala Superior.- Secretaría General de Acuerdos.

ACUERDO GENERAL DE LA SALA SUPERIOR DEL TRIBUNAL ELECTORAL DEL PODER JUDICIAL DE LA FEDERACION NUMERO 5/2010, DE VEINTISIETE DE OCTUBRE DE DOS MIL DIEZ, POR EL QUE SE APRUEBAN LAS PRACTICAS DE CERTIFICACION DE LA UNIDAD DE CERTIFICACION ELECTRONICA Y EL MANUAL DE OPERACION DE LAS NOTIFICACIONES POR CORREO ELECTRONICO.

**CONSIDERANDO:**

I. Conforme con los artículos 99, párrafos primero y décimo, de la Constitución Política de los Estados Unidos Mexicanos, 184, 186, fracción VII, y 189, fracción X, de la Ley Orgánica del Poder Judicial de la Federación, así como 3, del Reglamento Interno, el Tribunal Electoral del Poder Judicial de la Federación es, con excepción de lo dispuesto en la fracción II del artículo 105 constitucional, la máxima autoridad en la materia y órgano especializado del Poder Judicial de la Federación, y está facultado, a través de su Sala Superior, para emitir los acuerdos generales que sean necesarios para el adecuado ejercicio de sus atribuciones y su funcionamiento.

II. El seis de septiembre de dos mil diez, la Sala Superior del Tribunal Electoral aprobó el Acuerdo General número 3/2010, relativo a la Implementación de las Notificaciones por Correo Electrónico.

Dicho acuerdo fue publicado en el *Diario Oficial de la Federación la Federación* el primero de octubre del mismo año.

III. En cumplimiento con el artículo Transitorio Segundo del Acuerdo General 3/2010, la Secretaría General de Acuerdos de la Sala Superior y la Dirección General de Sistemas, sometieron a la Sala Superior, para su aprobación, las Prácticas de Certificación de la Unidad de Certificación Electrónica del Tribunal Electoral y el Manual de Operación de las Notificaciones por Correo Electrónico.

En atención a lo expuesto, la Sala Superior del Tribunal Electoral emite el siguiente:

**ACUERDO GENERAL**

**PRIMERO.** Se aprueban la Prácticas de Certificación de la Unidad de Certificación Electrónica del Tribunal Electoral contenidas en el anexo 1.

**SEGUNDO.** Se aprueba el Manual de Operación de las Notificaciones por Correo Electrónico contenido en el anexo 2.

**TRANSITORIOS**

**PRIMERO.** Este acuerdo entrará en vigor en la fecha de su aprobación.

**SEGUNDO.** La implementación de las Notificaciones por Correo Electrónico en las Salas Regionales se realizará en forma paulatina, conforme lo permitan las capacidades técnicas y humanas.

**TERCERO.** Para su debido conocimiento y cumplimiento, publíquese en el *Diario Oficial de la Federación*, en la *Gaceta de Jurisprudencia y Tesis Relevantes en Materia Electoral del Tribunal Electoral del Poder Judicial de la Federación*, en los estrados de las Salas Superior y Regionales, y en las páginas que tiene este órgano judicial en Internet e Intranet.

Así lo acordaron por **mayoría** de votos, los Magistrados que integran la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación, con la ausencia del Magistrado Salvador Olimpo Nava Gomar. El Subsecretario General de Acuerdos autoriza y da fe.

La Magistrada Presidenta, **María del Carmen Alanís Figueroa**.- Rúbrica.- Los Magistrados: **Constancio Carrasco Daza, Flavio Galván Rivera, Manuel González Oropeza, José Alejandro Luna Ramos, Pedro Esteban Penagos López**.- Rúbricas.- El Subsecretario General de Acuerdos, **Rafael Elizondo Gasperín**.- Rúbrica.



**TRIBUNAL ELECTORAL**  
del Poder Judicial de la Federación

---

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

---

**Acuerdo General número 5/2010**

**Anexo 1**

**INDICE**

- 1. Introducción**
- 1.1. Marco legal**
- 1.2. Definiciones y acrónimos**
- 1.3. Nombre de documento e identificación**
- 1.4. Participantes de la PKI**
  - 1.4.1. Unidad de Certificación Electrónica**
  - 1.4.2. Unidades Registradoras**
  - 1.4.3. Usuarios o firmantes**
  - 1.4.4. Relaciones de confianza**
  - 1.4.5. Otros participantes**
- 1.5. Uso válido de certificados digitales**
- 1.6. Lineamientos de administración**
  - 1.6.1. Publicación y actualización de este documento**
  - 1.6.2. Contactos técnicos**
  - 1.6.3. Sobre las adecuaciones a las Prácticas de Certificación**
  - 1.6.4. Procedimiento de aprobación de Prácticas de Certificación**
- 2. Publicación y repositorio de certificados**
  - 2.1. Repositorios**
  - 2.2. Publicación de información de la UCE**
  - 2.3. Frecuencia de publicación**
  - 2.4. Control de acceso a repositorios**
- 3. Identificación y autenticación**
  - 3.1. Nombres**
    - 3.1.1. Tipos de nombres**
    - 3.1.2. Nombres validos**
    - 3.1.3. Suscripciones anónimas y pseudo anónimas**
    - 3.1.4. Reglas de interpretación de varias formas de nombre**
    - 3.1.5. Nombres únicos y no ambiguos**

- 3.1.6. Reconocimiento, autenticación y registro de marcas
- 3.2 Validación inicial de identidad
  - 3.2.1. Método de validación de posesión de llave privada
  - 3.2.2. Autenticación de pertenencia
  - 3.2.3. Autenticación de individuos
  - 3.2.4. Información no verificable de firmantes
  - 3.2.5. Validación de autoridad
  - 3.2.6. Criterios de interoperabilidad
- 3.3. Identificación y autenticación de solicitudes de reuso de llaves
  - 3.3.1. Procedimiento de Identificación y autenticación de firmante para reuso de llaves
  - 3.3.2. Identificación y autenticación de firmante para reuso de llaves posterior a revocación
- 3.4. Identificación y autenticación de solicitudes de revocación
- 4. Requerimientos de operación y ciclo de vida del certificado
  - 4.1. Solicitud de certificado
    - 4.1.1. Quién puede solicitar un certificado
    - 4.1.2. Proceso de inscripción y responsabilidades
  - 4.2. Procesamiento de la solicitud
    - 4.2.1. Validación de identidad y pertenencia
    - 4.2.2. Aprobación o rechazo de solicitudes
    - 4.2.3. Duración del proceso de la solicitud
  - 4.3. Emisión de certificados
    - 4.3.1. Acciones durante la emisión de certificado
    - 4.3.2. Notificación al firmante de la emisión del certificado emitido
  - 4.4. Aceptación del Certificado
    - 4.4.1. Conducta constitutiva de aceptación de certificado
    - 4.4.2. Publicación del certificado por la UCE
    - 4.4.3. Notificación de emisión de certificado a otras entidades
  - 4.5. Uso del certificado y par de llaves
    - 4.5.1. Uso del certificado y llaves privadas de firmantes
    - 4.5.2. Uso de certificados en relaciones de confianza
  - 4.6. Renovación de certificados
    - 4.6.1. Circunstancias para renovación de certificados
    - 4.6.2. Quién puede solicitar una renovación de certificado
    - 4.6.3. Procedimiento para solicitar una renovación de certificado
    - 4.6.4. Notificación de emisión de renovación de certificado
    - 4.6.5. Conducta constitutiva de aceptación de certificado renovado
    - 4.6.6. Publicación de certificados renovados por la UCE
    - 4.6.7. Notificación de emisión de certificado renovado a otras entidades
  - 4.7. Cambio de llaves del certificado
    - 4.7.1. Circunstancias para cambiar llaves a un certificado
    - 4.7.2. Quién puede solicitar cambio de llaves a certificado
    - 4.7.3. Procedimiento de solicitud de cambio de llaves a un certificado

- 4.7.4. **Notificación de emisión de certificado con nuevas llaves**
- 4.7.5. **Conducta constitutiva de aceptación de certificado con nuevas llaves**
- 4.7.6. **Publicación de certificados con nuevas llaves por la UCE**
- 4.7.7. **Notificación de emisión de certificado a otras entidades**
- 4.8. **Modificación de certificados**
  - 4.8.1. **Circunstancias para modificación al certificado**
  - 4.8.2. **Quién puede solicitar una modificación al certificado**
  - 4.8.3. **Procedimiento de solicitud de cambio al certificado**
  - 4.8.4. **Notificación al firmante de la emisión del certificado con cambios**
  - 4.8.5. **Conducta constitutiva de aceptación de cambios en certificado**
  - 4.8.6. **Publicación de certificado con cambios por la UCE**
  - 4.8.7. **Notificación de cambios en certificado por la UCE a otras entidades**
- 4.9. **Revocación y suspensión de certificado**
  - 4.9.1. **Circunstancias de revocación**
  - 4.9.2. **Quién puede solicitar la revocación**
  - 4.9.3. **Procedimiento de solicitud de revocación**
  - 4.9.4. **Periodo de gracia de solicitud de revocación**
  - 4.9.5. **Tiempo de respuesta en el cual la UCE procesará la solicitud de revocación**
  - 4.9.6. **Requerimientos de verificación en relaciones de confianza**
  - 4.9.7. **Frecuencia de emisión de CRL**
  - 4.9.8. **Máxima latencia de CRL**
  - 4.9.9. **Verificación en línea de revocación**
  - 4.9.10. **Requerimientos para verificar en línea la revocación**
  - 4.9.11. **Otras adicionales para anunciar revocaciones**
  - 4.9.12. **Requerimientos para regeneración de llaves comprometidas**
  - 4.9.13. **Circunstancias para suspender certificados**
  - 4.9.14. **Quién puede solicitar suspender un certificado**
  - 4.9.15. **Requerimientos para solicitar suspender un certificado**
  - 4.9.16. **Periodo límite de una suspensión**
- 4.10. **Servicios de validación de certificados**
  - 4.10.1. **Características de operación**
  - 4.10.2. **Disponibilidad de servicios**
  - 4.10.3. **Características opcionales**
- 4.11. **Terminación de suscripción**
  - 4.11.1. **Depósito y recuperación de llaves**
  - 4.11.2. **Política y práctica de recuperación de llaves**
- 5. **Instalaciones, controles y operación**
  - 5.1. **Controles de acceso**
    - 5.1.1. **Ubicación**
    - 5.1.2. **Acceso físico**
    - 5.1.3. **Energía ininterrumpida y entorno ambiental controlado**
    - 5.1.4. **Exposición a inundaciones**
    - 5.1.5. **Control contra incendios**
    - 5.1.6. **Medios removibles**

- 5.1.7. Respaldos fuera de línea
- 5.2. Procedimientos de control
  - 5.2.1. Responsabilidades y roles de operación
  - 5.2.2. Número de personas requeridas por tarea
  - 5.2.3. Identificación y autenticación para cada rol de operación
  - 5.2.4. Separación de funciones
- 5.3. Controles del personal
  - 5.3.1. Calificaciones, experiencia y cumplimiento de requerimientos
  - 5.3.2. Procedimiento de verificación
  - 5.3.3. Capacitación
  - 5.3.4. Actualización de capacitación
  - 5.3.5. Secuencia y frecuencia de rotación de actividades
  - 5.3.6. Sanciones de acciones no autorizadas
  - 5.3.7. Requerimientos contractuales
  - 5.3.8. Documentación proporcionada al personal
- 5.4. Procedimientos de auditorías
  - 5.4.1. Tipos de eventos registrados
  - 5.4.2. Frecuencia de procesamiento de registros
  - 5.4.3. Retención de registros de eventos
  - 5.4.4. Protección de los registros de auditoría
  - 5.4.5. Procedimiento para el respaldo de registros de auditoría
  - 5.4.6. Sistemas de recolección de registros
  - 5.4.7. Notificación de eventos
  - 5.4.8. Evaluación de vulnerabilidades
- 5.5. Respaldo de registros
  - 5.5.1. Tipo de registros a respaldar
  - 5.5.2. Retención de respaldos
  - 5.5.3. Protección de los respaldos
  - 5.5.4. Procedimiento de respaldos de registros
  - 5.5.5. Requerimientos de estampado de tiempo de registros
  - 5.5.6. Sistema de almacenamiento de respaldos
  - 5.5.7. Procedimiento para obtener y verificar la información en los respaldos
- 5.6. Llaves de transición
- 5.7. Manejo de incidentes y recuperación de desastres
  - 5.7.1. Manejo de incidentes de llaves comprometidas
  - 5.7.2. Seguridad de los Recursos informáticos, programas y/o datos
  - 5.7.3. Procedimiento en caso de llave privada de firmante comprometida
  - 5.7.4. Plan de continuidad
- 5.8. Terminación de servicios
- 6. Controles de seguridad lógica
  - 6.1. Generación e instalación del par de llaves
    - 6.1.1. Generación de llaves
    - 6.1.2. Entrega de llaves privadas a firmantes
    - 6.1.3. Entrega de llaves públicas de certificados emitidos

- 6.1.4. Entrega de llave pública de la UCE
- 6.1.5. Tamaño de las llaves
- 6.1.6. Parámetros de generación de llave pública y validación
- 6.1.7. Uso del par de llaves
- 6.2. Protección de la llave privada de certificado raíz y controles del modelo criptográfico
  - 6.2.1. Controles y estándares criptográficos
  - 6.2.2. Control multi-personas (m de n)
  - 6.2.3. Almacenamiento de llave privada
  - 6.2.4. Respaldo de llave privada
  - 6.2.5. Históricos de llaves privadas
  - 6.2.6. Transferencia de llave privada hacia y desde módulo criptográfico
  - 6.2.7. Seguridad de almacenamiento de llave privada
  - 6.2.8. Método de activación de llave privada
  - 6.2.9. Método para desactivar la llave privada
  - 6.2.10. Método para destruir llaves privadas
- 6.3. Otros aspectos de administración del par de llaves
  - 6.3.1. Histórico de llaves públicas
  - 6.3.2. Periodo de vigencia de certificados y par de llaves
- 6.4. Activación de sistemas y datos
  - 6.4.1. Activación para la instalación y generación de certificados
  - 6.4.2. Mecanismos de protección de la activación
  - 6.4.3. Otros aspectos de la activación
- 6.5. Controles de seguridad informática
  - 6.5.1. Requerimientos de seguridad informática
  - 6.5.2. Valoración de la seguridad informática
- 6.6. Controles de ciclo de vida de sistemas
  - 6.6.1. Controles de desarrollo de sistemas
  - 6.6.2. Controles de administración de seguridad
  - 6.6.3. Controles de ciclo de vida de seguridad
- 6.7. Control de seguridad de red
- 6.8. Time-stamping
- 7. Perfil de certificado, CRL y OSCP
  - 7.1. Perfil de certificado
    - 7.1.1. Versión de certificados
    - 7.1.2. Extensiones validas de certificados
    - 7.1.3. Identificadores de objetos algoritmos
    - 7.1.4. Formato de nombre
    - 7.1.5. Limitaciones en formato de nombres
    - 7.1.6. Identificador de objeto de lineamientos del certificado
    - 7.1.7. Definición de política de limitación en extensiones
    - 7.1.8. Definición de política de sintaxis y semántica
    - 7.1.9. Procesamiento semántico de extensiones críticas
  - 7.2. Perfil de CRL
    - 7.2.1. Versión de CRL
    - 7.2.2. Extensiones y campos CRL

- 7.3. Perfil de OCSP**
- 8. Auditorias de cumplimiento técnico**
  - 8.1. Frecuencia o circunstancias de evaluación**
  - 8.2. Consultores y asesores calificados**
  - 8.3. Entidades evaluadoras calificadas**
  - 8.4. Temas a cubrirse en evaluación**
  - 8.5. Acciones a tomar en caso de resultados deficientes**
  - 8.6. Comunicación de resultados**
- 9. Cumplimientos legales**
  - 9.1. Tarifas**
    - 9.1.1. Tarifas de emisión o renovación de certificados**
    - 9.1.2. Tarifa de acceso a certificados**
    - 9.1.3. Tarifa de revocación o acceso a servicios de estatus de certificado**
    - 9.1.4. Tarifas de otros servicios**
    - 9.1.5. Política de reembolso**
  - 9.2. Responsabilidades financieras**
    - 9.2.1. Cobertura de seguros**
    - 9.2.2. Otros activos**
    - 9.2.3. Cobertura y garantías para firmantes**
  - 9.3. Confidencialidad de la información**
    - 9.3.1. Alcance de la confidencialidad de la información**
    - 9.3.2. Información que no se encuentra dentro de este alcance**
    - 9.3.3. Responsabilidades en la protección de la información confidencial**
  - 9.4. Privacidad de la información personal**
    - 9.4.1. Plan de privacidad**
    - 9.4.2. Información tratada como confidencial**
    - 9.4.3. Información no considerada como confidencial**
    - 9.4.4. Responsabilidades sobre información confidencial**
    - 9.4.5. Advertencia y consentimiento sobre uso de información personal**
    - 9.4.6. Divulgación de información de conformidad con procedimientos administrativos o judiciales**
  - 9.5. Propiedad intelectual**
  - 9.6. Representaciones y garantías**
    - 9.6.1. Representaciones y garantías de la UCE**
    - 9.6.2. Representaciones y garantías del firmante**
    - 9.6.3. Representaciones y garantías en relaciones de confianza**
    - 9.6.4. Representaciones y garantías de otros participantes**
  - 9.7. Declaración de garantías**
  - 9.8. Indemnizaciones**
  - 9.9. Terminación de prácticas**
    - 9.9.1. Expiración de prácticas**
    - 9.9.2. Sobre modificaciones**
    - 9.9.3. Circunstancias validas de cambio en OID**

## 9.10. Marco legal

### 1. Introducción

La Unidad de Certificación Electrónica del Tribunal Electoral del Poder Judicial de la Federación, es el órgano encargado de la gestión de certificados de firma electrónica avanzada de uso institucional. La arquitectura de la Unidad de Certificación Electrónica está integrada por un módulo de certificación y un conjunto de unidades registradoras.

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, es de acceso público para ser consultado por los interesados en: hacer uso de los certificados emitidos y conocer las condiciones técnicas de operación.

En base a las mejores prácticas, este documento se encuentra estructurado conforme al **RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"**. En virtud del alcance de la infraestructura de llave pública del Tribunal Electoral, las secciones del **RFC 3647** que no son aplicables serán indicadas como **"No aplica"**.

La **Unidad de Certificación Electrónica** es autónoma e independiente, por lo que no se encuentra subordinada a ninguna autoridad certificadora externa. El certificado raíz de dicha **Unidad** se encuentra formalizado mediante acta del protocolo de inicialización de llaves con fecha del veinte de agosto del dos mil diez.

### 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. Reglamento Interno del Tribunal Electoral del Poder Judicial de la Federación;
- III. Acuerdo de la Comisión de Administración del Tribunal Electoral del Poder Judicial de la Federación 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
- IV. Acuerdo General de la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación número 3/2010, relativo a la Implementación de las Notificaciones por Correo Electrónico.
- V. Acuerdo General número 5/2010, 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. **Agente Registrador:** Servidor público de la Dirección General de Sistemas que realiza las actividades técnicas de recepción de solicitudes, validación de la documentación requerida para la emisión y revocación de certificados dentro de la Unidad de Certificación;
- II. **Autoridades del Tribunal Electoral:** Los Presidentes y Secretarios Generales de Acuerdos de las Salas del Tribunal Electoral;
- III. **Common Criteria:** El marco de referencia que ofrece la garantía de que el proceso de especificación, implementación y evaluación de un producto de seguridad informática se ha llevado a cabo de manera rigurosa y estándar;
- IV. **CN Common Name:** El nombre de la entidad final, en el caso de las personas, se refiere a su nombre completo;
- V. **CRL:** La lista de revocación de certificados;
- VI. **CSR Certificate signing request:** El mensaje electrónico que contiene la información formateada y requerida para procesar un certificado;
- VII. **DGS:** La Dirección General de Sistemas del Tribunal Electoral;
- VIII. **EAL Evaluation Assurance Level:** La evaluación del nivel de garantía de un producto o sistema es un grado numérico asignado tras la finalización de una evaluación de seguridad basada en **Common Criteria**;
- IX. **EAL4:** El que permite obtener la máxima garantía de ingeniería de seguridad positiva basada en buenas prácticas de desarrollo comercial;

- X. 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;
- XI. GMT** *Greenwich Mean Time*: El tiempo referenciado al meridiano de Greenwich;
- XII. 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;
- XIII. OCSP** *Online Certificate Status Protocol*: El servicio en línea que permite evaluar el estado y validez de un certificado;
- XIV. PKI** *Public Key Infrastructure*: El conjunto de hardware, software, personas, políticas, procedimientos necesarios para crear, manejar, distribuir, usar, almacenar y revocar certificados digitales.
- XV. Revocar**: El procedimiento mediante el cual se deja sin efecto el certificado electrónico;
- XVI. 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.
- XVII. Servidor Público**: Los servidores públicos del Tribunal Electoral del Poder Judicial de la Federación.
- XVIII. Firmante**: El Servidor público que tiene un certificado digital autorizado y vigente emitido por la UCE;
- 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.

### 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:** 1.0 liberada el 01 de octubre de 2010.

**OID:** 1.3.6.1.4.1.32639.2.2.3.1.1.1.1

### 1.4. Participantes de la PKI

La **UCE** emitirá los certificados de firma electrónica avanzada para los sistemas informáticos, así como, para los servidores públicos del Tribunal Electoral de conformidad a los acuerdos emitidos por este órgano Jurisdiccional.

#### 1.4.1. Unidad de Certificación Electrónica

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

#### 1.4.2. Unidades Registradoras

La **UCE** dispondrá una **UR** por cada 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, exclusivamente, por servidores públicos del Tribunal Electoral.

La lista de las **UR** se encuentra disponible en la siguiente URL: <https://uce.te.gob.mx/>

#### 1.4.3. Usuarios o Firmantes

La **UCE** únicamente emitirá certificados para los servidores públicos del Tribunal Electoral, a fin de dar cumplimiento a los acuerdos emitidos por dicho órgano jurisdiccional sobre el uso de firma electrónica avanzada.

#### 1.4.4. Relaciones de confianza

Las relaciones de confianza que establezca el Tribunal Electoral con autoridades certificadoras de terceros, se registrarán conforme a lo previsto en las presentes Prácticas y los Acuerdos Generales o convenios que al efecto se emitan.

#### 1.4.5. Otros participantes

**No Aplica.**

#### 1.5. Uso válido de certificados digitales

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

Los agentes registradores 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 correos electrónicos firmados digitalmente por servidores públicos del Tribunal Electoral, y
- III. Proteger documentos y comunicaciones electrónicos mediante el cifrado de datos.

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

#### 1.6. Lineamientos de administración

##### 1.6.1. 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

Las modificaciones a este documento serán propuestas por la **UCE** y aprobadas por la Sala Superior del Tribunal Electoral.

##### 1.6.2. Contactos técnicos

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

- I. Dirección de Seguridad Informática: [seguridad.informatica@te.gob.mx](mailto:seguridad.informatica@te.gob.mx), y
- II. Administración de Unidad de Certificación Electrónica: [admin-ac@te.gob.mx](mailto:admin-ac@te.gob.mx)

##### 1.6.3. Sobre las adecuaciones a las Prácticas de Certificación

La **UCE** elaborará las propuestas de modificación a las presentes **Prácticas de Certificación**.

##### 1.6.4. Procedimiento de aprobación de Prácticas de Certificación

La **UCE** elaborará la propuesta de modificación a las presentes **Prácticas de Certificación** y las someterán a la aprobación 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:

<https://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
----------	----------	---------------

<b>CRL</b>	<a href="https://uce.te.gob.mx/CRL">https://uce.te.gob.mx/CRL</a>	Lista de revocación de certificados
<b>OCSP</b>	<a href="http://uce.te.gob.mx:1350">http://uce.te.gob.mx:1350</a>	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 de la **UCE**, disponible para su descarga en formato **CER**;
- II. Certificados emitidos por **UCE**;
- III. La lista de revocación de certificados **CRL**;
- IV. La versión actualizada de las **Prácticas de Certificación**, y
- V. 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.

La **UCE** administrará y mantendrá actualizada la **CRL** con una periodicidad de 30 días, en caso de procesar la revocación de certificados también emitirá una nueva **CRL**.

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**.

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 estas 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.

Las actividades de mantenimiento se realizarán de 01:00 hrs., a 05:00 hrs. y/o de 22:00 hrs., a 24:00 hrs., en las fechas autorizadas por el Tribunal Electoral.

El acceso a los repositorios de certificados emitidos y **CRL**, así como a este documento es público.

## 3. Identificación y Autenticación

### 3.1. Nombres

#### 3.1.1. Tipos de Nombres

Las cadenas de caracteres validas 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.

Cada certificado emitido por la **UCE** deberá contar con un **Nombre de identificación Common Name (CN)**, el cual debe ser único e irrepetible.

El **Common Name (CN)** tendrá uno de los elementos siguientes:

- I. Para personas, el nombre y apellidos o un texto derivado de su nombre.  
**Ejemplo: CN=Nombre y apellidos de firmante**
- II. Para servidores, el nombre identificador completo **FQDN**, el cual deberá estar en minúsculas, no se acepta direcciones **ip** en este campo.  
**Ejemplo: CN=uce.te.gob.mx**
- III. Para servicios, el nombre del servicio, seguido del carácter "/" y el **FQDN** del servidor, el cual deberá estar en minúsculas, no se acepta direcciones **ip** en este campo.  
**Ejemplo: CN=http/uce.te.gob.mx**

El conjunto de caracteres validos 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 validos

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. Suscripciones anónimas y pseudo anónimas

**No Aplica.**

### 3.1.4. Reglas de interpretación de varias formas de nombre

Con base en la definición establecida en el **punto 3.1.1**

### 3.1.5. 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.

### 3.1.6. Reconocimiento, autenticación y registro de marcas

**No Aplica.**

## 3.2. Validación inicial de identidad

### 3.2.1. Método de validación de posesión de llave privada

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

### 3.2.2. Autenticación de pertenencia

Las **autoridades del Tribunal Electoral** requerirán a la **DGS** para que, a través de la **UCE**, expidan, según corresponda, el certificado de firma electrónica a los Secretarios Generales de Acuerdos, al Subsecretario General de Acuerdos y a los Actuarios, para poder practicar las notificaciones por correo electrónico.

En los demás casos, el servidor público interesado en obtener el certificado de firma electrónica deberá formular la solicitud correspondiente.

El servidor público al que se pretenda dotar de dicho certificado, deberá acreditar el nombramiento que ostenta en el Tribunal Electoral, mediante oficio emitido por la Coordinación de Recursos Humanos y, en su caso, copia de la credencial institucional vigente.

La **UR** validará la información sobre el nombramiento vigente del solicitante con la mencionada Coordinación de Recursos Humanos.

### 3.2.3. Autenticación de individuos

A fin de permitir que la **UR** autentique la identidad de los servidores públicos, estos deberán presentar oficio emitido por la Coordinación de Recursos Humanos y, en su caso, copia de la credencial institucional vigente, en términos del punto **3.2.2**.

### 3.2.4. Información no verificable de firmantes

**No aplica.**

### 3.2.5. Validación de autoridad

Con base a las definiciones establecidas en los **puntos 3.2.2 y 3.2.3**, las **autoridades del Tribunal Electoral o la Coordinación de Recursos Humanos** confirmarán, de manera oficial, a la **UR** la pertenencia del solicitante al Tribunal Electoral.

### 3.2.6. Criterios de interoperabilidad

**No aplica.**

## 3.3. Identificación y autenticación de solicitudes de reúso de llaves

### 3.3.1. Procedimiento de Identificación y autenticación de firmante para reúso de llaves

**No Aplica.**

### 3.3.2. Identificación y autenticación de firmante para reúso de llaves posterior a revocación

**No Aplica.****3.4. 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 portal de la **UCE** o personalmente en la **DGS**.

Las **autoridades del Tribunal Electoral** podrán solicitar la revocación de certificados a la **DGS**.

**4. Requerimientos de operación y ciclo de vida del certificado****4.1. Solicitud de Certificado****4.1.1. Quién puede solicitar un certificado**

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

En alcance a lo establecido en la **sección 1.4.3** de este documento, la **UCE** emitirá certificados solo a servidores públicos del Tribunal Electoral.

**4.1.2. Proceso de inscripción y responsabilidades**

El servidor público respecto del cual las autoridades del Tribunal solicitaron la expedición del certificado o interesado, haciendo uso de un equipo de cómputo institucional, completará la forma de solicitud en línea, y procederá a generar el par de llaves asociadas al certificado, el cual tendrá un tamaño de **2048 bit** y, finalmente, resguardará de manera segura la llave privada en un dispositivo criptográfico **Token** o en repositorio seguro de certificados en el equipo de cómputo en el que se procesó la solicitud.

El servidor público 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 solo 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. Notificar de manera inmediata a la **DGS** de 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 operador en las **UR**, ingresará al módulo de administración de la **UCE** e identificará todas las solicitudes pendientes y en ese sentido; 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 operador de la **UR** deberá:

- I. Verificar se disponga de 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, y
- IV. 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**, así como la comprobación de documentación son exitosas, se tramitará mediante transacción segura firmada por el operador de la **UR** ante el módulo de la **UCE**, la solicitud a fin que ésta proceda con la firma y liberación del certificado.

En caso contrario, se informará al servidor público, 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**

El ciclo de liberación de un certificado desde la solicitud hasta la emisión del certificado dependerá del proceso de validación de la información proporcionada, por lo que la **UCE** emitirá el certificado solicitado, si éste procede, en un máximo de 2 días hábiles siguientes a la recepción de la solicitud.

### **4.3. Emisión de certificados**

#### **4.3.1. Acciones durante la emisión de certificado**

La **CSR** será transferida por medio seguro al módulo de certificación donde reside la llave privada del certificado raíz de la **UCE**. En este sistema, una vez generado y firmado el certificado será transferido de regreso al sitio de la **UCE** para ser publicado en línea.

#### **4.3.2. Notificación al firmante de la emisión del certificado emitido**

La **DGS** emitirá un correo electrónico indicando al firmante la ruta **URL** de descarga del certificado que se le ha autorizado.

### **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 servidor público deberá verificar la integridad del certificado proporcionado, haciendo uso de éste junto con la llave privada que tiene bajo su resguardo, para esto, deberá firmar cualquier archivo con su llave privada y verificará la firma electrónica. Si el resultado de estas pruebas es exitoso, entonces no deberán existir objeciones sobre el certificado emitido, el firmante puede proceder a usarlo, en caso contrario, el servidor público deberá informar a la **DGS** las razones por las cuales el certificado no es funcional a sus necesidades y, en consecuencia, la **UCE** revocará el certificado emitido.

#### **4.4.2. Publicación del certificado por la UCE**

La **UCE** publicará en la página del Tribunal Electoral los certificados emitidos.

#### **4.4.3. Notificación de emisión de certificado a otras entidades**

**No Aplica.**

### **4.5. Uso del certificado y par de llaves**

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

Los certificados emitidos por la **UCE** y sus llaves privadas asociadas deben ser usados únicamente para los fines establecidos en la **sección 1.5** de este documento. Cuando un certificado sea revocado, la llave privada no podrá ser utilizada posteriormente para ningún propósito adicional.

#### **4.5.2. Uso de certificados en relaciones de confianza**

Para el caso del establecimiento de relaciones de confianza con terceros respecto del uso de certificados emitidos por la **UCE**, se deberá:

- I. Verificar que el certificado haya sido firmado por un certificado raíz válido de la **UCE**;
- II. Verificar que el certificado no ha expirado, y
- III. Consultar la **CRL** de la **UCE**, a fin de determinar si es vigente.

### **4.6. Renovación de certificados**

#### **4.6.1. Circunstancias para renovación de certificados**

La **UCE** no dispone de mecanismos de renovación automática de certificados, en consecuencia, para la reexpedición de un certificado, el firmante deberá proceder conforme la **sección 4.1** de este documento.

#### **4.6.2. Quién puede solicitar la renovación de certificado**

**No Aplica.**

#### **4.6.3. Procedimiento para solicitar una renovación de certificado**

**No aplica.**

#### **4.6.4. Notificación de emisión de renovación de certificado**

**No aplica.**

#### **4.6.5. Conducta constitutiva de aceptación de certificado renovado**

**No aplica.**

#### **4.6.6. Publicación de certificados renovados por la UCE**

**No aplica.**

#### **4.6.7. Notificación de emisión de certificado renovado a otras entidades**

**No aplica.**

#### **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 de cambiar algún parámetro del certificado deberá revocar el certificado actual y solicitar un nuevo certificado.

##### **4.7.2. Quién puede solicitar cambio de llaves de certificado**

**No Aplica.**

##### **4.7.3. Procedimiento de solicitud de cambio de llaves a un certificado**

**No aplica.**

##### **4.7.4. Notificación de emisión de certificado con nuevas llaves**

**No aplica.**

##### **4.7.5. Conducta constitutiva de aceptación de certificado con nuevas llaves**

**No aplica.**

##### **4.7.6. Publicación de certificados con nuevas llaves por la UCE**

**No aplica.**

##### **4.7.7. Notificación de emisión de certificado a otras entidades**

**No aplica.**

#### **4.8. Modificación de certificados**

##### **4.8.1. Circunstancias para modificación al 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.

##### **4.8.2. Quién puede solicitar una modificación al certificado**

**No aplica.**

##### **4.8.3. Procedimiento de solicitud de cambio al certificado**

**No aplica.**

##### **4.8.4. Notificación al firmante de la emisión del certificado con cambios**

**No aplica.**

##### **4.8.5. Conducta constitutiva de aceptación de cambios en certificado**

**No aplica.**

##### **4.8.6. Publicación de certificado con cambios por la UCE**

**No aplica.**

##### **4.8.7. Notificación de cambios en certificado por la UCE a otras entidades**

**No aplica.**

#### **4.9. Revocación y suspensión de certificado**

##### **4.9.1. Circunstancias de revocación**

Un certificado puede ser revocado por:

- I. Uso distinto al legalmente previsto;
- II. Baja del firmante o, en su caso, cambio de adscripción;
- III. La llave privada del firmante fue extraviada o está en riesgo su seguridad;
- IV. La información en el certificado es correcta o es imprecisa, o
- V. El sistema (servidor o servicio) asociado al certificado ha sido dado de baja.

##### **4.9.2. Quién puede solicitar la revocación**

La revocación de un certificado puede ser solicitada por:

- I. El firmante propietario del certificado, y
- II. Las autoridades del Tribunal Electoral con base a los acuerdos vigentes sobre el uso del certificado.

#### **4.9.3. Procedimiento de solicitud de revocación**

El firmante puede iniciar la solicitud de revocación a través de los sistemas informáticos que se dispongan en línea para este fin.

El operador de la **UR**, a fin de proceder con la solicitud de revocación, validará la información y, en su caso, registrará la revocación y la tramitará internamente en la **UCE** para publicarse en la **CRL** autorizada, así como a través del protocolo.

Las **autoridades del Tribunal Electoral** solicitarán a la **DGS** la revocación del certificado.

#### **4.9.4. Periodo de gracia de solicitud de revocación**

No hay un periodo de gracia definido para la solicitud de revocación.

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

Una vez recibida la solicitud de revocación, procederá de inmediato a revocar el certificado respectivo.

#### **4.9.6. Requerimientos de verificación en relaciones 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**.

#### **4.9.11. Otras adicionales para anunciar revocaciones**

No aplica.

#### **4.9.12. Requerimientos para regeneración de llaves comprometidas**

No aplica.

#### **4.9.13. Circunstancias para suspender certificados**

No aplica.

#### **4.9.14. Quién puede solicitar suspender un certificado**

No aplica.

#### **4.9.15. Requerimientos para solicitar suspender un certificado**

No aplica.

#### **4.9.16. Periodo límite de una suspensión**

No aplica.

### **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 raíz 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**

**4.10.3. Características opcionales**

**No Aplica.**

**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.

**4.11.2. Política y práctica de recuperación de llaves**

**No Aplica.**

**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 1.6.1**

**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**, 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 riesgos de una inundación.

**5.1.5. Control contra incendios**

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

El hardware se encuentra montado sobre chasis no inflamables.

**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 raíz 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 raíz 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 **DGS**;
- II. Administrador de sistemas. Este rol será asumido por personal de la **DGS**;
- III. Oficial de seguridad. Este rol será asumido por personal de la Dirección de Seguridad Informática de la **DGS**, y

**IV.** Agentes registradores. Se definirá al menos con un responsable de la **DGS** y se integrarán los servidores públicos que se autoricen cumplir estas actividades con base en los acuerdos que en la materia establezcan las Autoridades del Tribunal Electoral.

#### **5.2.2. Número de personas requeridas por tarea**

A fin de ejecutar las tareas de gestión de certificados se requiere de al menos dos participantes: un administrador de la **UCE** y un agente registrador.

#### **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 emisión y revocación de certificados, 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 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 de 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. Secuencia y frecuencia de rotación de actividades**

**No aplica.**

#### **5.3.6. Sanciones de acciones no autorizadas**

Se aplicará la normatividad interna vigente.

#### **5.3.7. Requerimientos contractuales**

**No aplica.**

#### **5.3.8. 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
- VI.** Eliminación de certificados.

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 oficial de seguridad del sistema y el administrador de la **UCE** procesarán 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 **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 y correlación de eventos, a fin de identificar posibles violaciones a la infraestructura de seguridad.

#### **5.4.7. Notificación de eventos**

**No aplica.**

#### **5.4.8. 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**

Unicamente 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. Llaves de transición**

**No aplica.**

### **5.7. Manejo de incidentes y recuperación de desastres**

#### **5.7.1. Manejo de incidentes de llaves comprometidas**

Si la seguridad de las llaves privadas de los operados de la **UR** 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 raíz se encuentra en riesgo, se deberá:

- I. Informar a los operadores de las **UR**, 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.

#### **5.7.2. Seguridad de los Recursos informáticos, programas y/o datos**

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.

#### **5.7.3. 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 revocar del certificado.

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

#### **5.7.4. 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**

#### **5.8. Terminación de servicios**

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

- I. Informar a los registradores, 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 **DGS** garantiza 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 raíz 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 de la **RA**, serán generados utilizando el módulo de solicitud de certificado de su equipo y la llave privada 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 a través del sitio web de la **UCE**.

##### **6.1.4. Entrega de llave pública de la UCE**

El certificado raíz 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 raíz de la **UCE** tendrá 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. Parámetros de generación de llave pública y validación**

**No aplica.**

#### **6.1.7. 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 de **UR** para:

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

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

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

### **6.2. Protección de la llave privada de certificado raíz 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 raíz 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 raíz 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 raíz 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 **DGS**.

#### **6.2.5. Históricos de llaves privadas**

**No aplica.**

#### **6.2.6. Transferencia de llave privada hacia y desde módulo criptográfico**

La llave privada asociada al certificado raíz 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.

#### **6.2.7. Seguridad de almacenamiento de llave privada**

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

### **6.2.8. 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.

### **6.2.9. 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

### **6.2.10. 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 raíz, 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 raíz de la **UCE** tendrá un periodo de vigencia de 12 años, y
- II. Los certificados emitidos para los usuarios tendrán un periodo de vigencia de 2 años y menor en caso que así lo determinen las instancias que correspondan del Tribunal Electoral, mediante acuerdo oficial que autorice dicho cambio.

## **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 raíz de la **UCE** solamente está habilitada para lo establecido en la **sección 6.1.7**

### **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**.

### **6.4.3. Otros aspectos de la activación**

**No aplica.**

## **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 cumplen con la configuración del **common criteria EAL** con **nivel 4** aumentada con características **ALC\_FLR.3**, que ofrecen niveles 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. Valoración de la seguridad informática**

En base al cumplimiento de los perfiles establecidos en el **common criteria** en su **nivel 4**, tal como se comenta en la **sección 6.5.1**.

## **6.6. Controles de ciclo de vida de sistemas**

### **6.6.1. Controles de desarrollo de sistemas**

**No aplica.**

### **6.6.2. Controles de administración de 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 los estándares de 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.

#### 6.6.3. 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.

#### 6.7. 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**. Adicionalmente, la comunicación se establece a través de un esquema de **proxy reverso** de manera que la comunicación la inicia la **UCE** y no en sentido inverso.

El sistema informático de la **UR** se encuentra protegido a través de la infraestructura de seguridad que opera en la red local, ya que estos servidores no se publican en internet.

#### 6.8. Time-stamping

Todos los sistemas en línea de la **UCE** se encuentran sincronizados a través del protocolo **NTP** con la hora oficial 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 Infrastructure: 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 raíz de la **UCE** presentará las siguientes extensiones:

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

Los certificados para uso personal, se extenderán certificados con las siguientes extensiones:

Extensión	Definición/Característica
Basic Constraints:	critical, CA: FALSE
Subject Key Identifier:	Hash

Authority Key Identifier:	Keyid
Key Usage:	Digital Signature, Non Repudiation, Data Encipherment, Client Authentication, email Protection, Object Signing
Extended Key Usage:	SSL Client, S/MIME, Object Signing
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
Explicit Text	String: Texto

En el caso de los certificados de usuario, el texto de la extensión opcional **explicit Text** delimitará el alcance institucional en el cual puede ser utilizado dicho certificado, indicando el acuerdo del Tribunal Electoral que da soporte a dicha actuación, a ser validas las siguientes leyendas:

- I. "Para uso exclusivo de notificaciones por correo electrónico, de conformidad con el Acuerdo General de la Sala Superior número 3/2010, relativo a la Implementación de las Notificaciones por Correo Electrónico", y
- II. "Para uso administrativo, de conformidad con el Acuerdo de la Comisión de Administración del Tribunal Electoral del Poder Judicial de la Federación, 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".

Para sistemas informáticos, los certificados digitales presentarán las siguientes extensiones:

Extensión	Definición/Característica
Basic Constraints:	critical, CA: FALSE
Subject Key Identifier:	Hash
Authority Key Identifier:	Keyid
Key Usage:	Digital Signature, Data Encipherment
Extended Key Usage:	SSL Server , SSL Client, S/MIME, Object Signing
X509v3 CRL Distribution Points:	<b>URI</b>
Subject alternative name:	<b>FQDN</b>
Issuer alternative name:	RFC822 Name =admin-ac@te.gob.mx
Certificate Policies:	OID
Explicit Text	String: Texto

### 7.1.3. Identificadores de objetos algoritmos

- I. **Hash function:** id-sha 1 1.3.14.3.2.26;
- II. **Encryption:** rsaEncryption 1.2.840.113549.1.1.1, y
- III. **Signature:** sha1WithRSAEncryption 1.2.840.113549.1.1.5

### 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.

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

**C** = MX, **O** = Tribunal Electoral del Poder Judicial de la Federación, **OU** = Área de Adscripción, **CN** = Nombre del Servidor Público=Responsabilidad **STREET** = Domicilio de la Sala, **PostalCode** = Código postal, **L** = Ciudad, **S** = Entidad Federativa.

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.

**C** = MX, **O** = Tribunal Electoral del Poder Judicial de la Federación, **OU** = Área de Adscripción, **CN** = FQDN, **STREET** = Domicilio de la Sala, **PostalCode** = Código postal, **L** = Ciudad, **S** = Entidad Federativa.

#### **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.**

#### **7.1.7. Definición de política de limitación en extensiones**

**No aplica.**

#### **7.1.8. Definición de política de sintaxis y semántica**

**No aplica.**

#### **7.1.9. Procesamiento semántico de extensiones críticas**

**No aplica.**

### **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 # 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. Auditorías de cumplimiento técnico**

### **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. Consultores y asesores calificados**

**No aplica.**

### **8.3. Entidades evaluadoras calificadas**

Las evaluaciones de cumplimiento interno serán realizadas por personal 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.

Para efecto de cumplimiento, en caso de establecerse relaciones de confianza con autoridades certificadoras terceras del Poder Judicial de la Federación u otras instituciones, los alcances y condiciones de este tipo de auditoría será parte de los acuerdos que se establecerán con la Institución.

#### **8.4. 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.

#### **8.5. 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.

#### **8.6. 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 emisión o renovación de certificados**

**No aplica.**

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

**No aplica.**

##### **9.1.3. Tarifa de revocación o acceso a servicios de estatus de certificado**

**No aplica.**

##### **9.1.4. Tarifas de otros servicios**

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

##### **9.1.5. Política de reembolso**

**No aplica.**

#### **9.2. Responsabilidades financieras**

**No aplica.**

##### **9.2.1. Cobertura de seguros**

**No aplica.**

##### **9.2.2. Otros activos**

**No aplica.**

##### **9.2.3. Cobertura y garantías para firmantes**

**No aplica.**

#### **9.3. 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.

##### **9.3.1. Alcance de la confidencialidad de la información**

Se aplicará la normatividad vigente que corresponda con base en la definición general de la **sección 9.3**.

##### **9.3.2. Información que no se encuentra dentro de este alcance**

Se aplicará la normatividad vigente que corresponda y declarada en la **sección 9.3**.

**9.3.3. Responsabilidades en la protección de la información confidencial**

Se aplicará la normatividad vigente que corresponda y declarada en la **sección 9.3.**

**9.4. Privacidad de la información personal**

La información recolectada para la suscripción y generación de certificados, será resguardada conforme a lo establecido en la normatividad vigente, declarada en la **sección 9.3.**

**9.4.1. Plan de privacidad**

**No aplica.**

**9.4.2. Información tratada como confidencial**

La información obtenida para la suscripción y generación de certificados será resguardada conforme a lo establecido en la normatividad vigente, declarada en la **sección 9.3.**

**9.4.3. Información no considerada como confidencial**

Se aplicará la normatividad vigente que corresponda con base en la definición general de la **sección 9.3.**

**9.4.4. Responsabilidades sobre información confidencial**

Se aplicará la normatividad vigente que corresponda con base en la definición general de la **sección 9.3.**

**9.4.5. Advertencia y consentimiento sobre uso de información personal**

**No Aplica.**

**9.4.6. 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.

**9.5. Propiedad intelectual**

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

**9.6. Representaciones y garantías****9.6.1. Representaciones y garantías de la UCE**

La **DGS** como administrador de la infraestructura de la **UCE**, sólo garantiza la verificación de la identidad de los firmantes de acuerdo a los procedimientos integrados en este documento.

**9.6.2. 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.

**9.6.3. Representaciones y garantías en relaciones de confianza.**

**No aplica.**

**9.6.4. Representaciones y garantías de otros participantes**

**No aplica.**

**9.7. 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.

**9.8. Indemnizaciones**

**No aplica.**

**9.9. Terminación de prácticas**

En los mismos términos definidos en la **sección 5.8.**

#### **9.9.1. Expiración de prácticas**

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

#### **9.9.2. 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 1.6.1.**

#### **9.9.3. Circunstancias 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.

#### **9.10. 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.



---

### **Manual de Operación de las Notificaciones por Correo Electrónico**

---

#### **Acuerdo General número 5/2010**

##### **Anexo 2**

##### **INDICE**

1. Glosario
2. Expedición del certificado de firma electrónica avanzada a los Secretarios Generales de Acuerdos, Subsecretario General de Acuerdos y Actuarios
3. Revocación del certificado a los Secretarios Generales de Acuerdos, Subsecretario General de Acuerdo y Actuarios
4. Obtención de la cuenta institucional de correo electrónico por las partes
5. Recuperación de la contraseña de la cuenta institucional de correo electrónico por las partes
6. Baja de la cuenta institucional de correo electrónico de las partes
7. Digitalización del acuerdo o resolución a notificar, nombramiento y guarda del archivo
8. Certificación del acuerdo o resolución a notificar
9. Realización de las notificaciones electrónicas
10. Descarga de la constancia de envío y acuse de recibido
11. Elaboración de la razón de notificación por correo electrónico

12. Conocimiento y descarga de las notificaciones electrónicas por las partes
13. Depuración y respaldo de la información generada con motivo de las notificaciones electrónicas
14. Validación y autenticación de las notificaciones electrónicas

#### 1. GLOSARIO.

Para los efectos del presente manual, se entenderá por:

- 1.1. **Actuarios:** Los Actuarios y titulares de la Oficina respectiva, adscritos a las Salas del Tribunal Electoral de Poder Judicial de la Federación;
- 1.2. **Acuerdo General 3/2010:** El Acuerdo General 3/2010 de la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación, relativo a la implementación de las notificaciones por correo electrónico;
- 1.3. **Autoridades electorales:** Las autoridades electorales administrativas y jurisdiccionales;
- 1.4. **Certificado:** El certificado de firma electrónica avanzada que utilizarán los Secretarios Generales de Acuerdos, el Subsecretario General de Acuerdos y los Actuarios del Tribunal Electoral del Poder Judicial de la Federación para autenticar las notificaciones por correo electrónico;
- 1.5. **Constancia de envío y acuse de recibido:** La constancia que genera el sistema de notificaciones del Tribunal Electoral del Poder Judicial de la Federación, en el envío y recepción de las notificaciones por correo electrónico;
- 1.6. **Credencial Institucional.** La credencial oficial que acredita a una persona como servidor público del Tribunal Electoral;
- 1.7. **Cuenta institucional de correo electrónico:** La cuenta de correo electrónico que expida la Unidad de Certificación Electrónica;
- 1.8. **Dirección General de Sistemas:** La Dirección General de Sistemas del Tribunal Electoral del Poder Judicial de la Federación;
- 1.9. **Firmante:** Quien hace uso del certificado de firma electrónica avanzada en el envío de información digital;
- 1.10. **Ley:** La Ley General del Sistema de Medios de Impugnación en Materia Electoral;
- 1.11. **Notificaciones por correo electrónico:** Las comunicaciones procesales que se hacen a las partes que así lo solicitan, con motivo del trámite, sustanciación y resolución de los medios de impugnación en materia electoral;
- 1.12. **Página web del Tribunal:** La página oficial de internet del Tribunal Electoral, cuya dirección es: [www.te.gob.mx](http://www.te.gob.mx);
- 1.13. **Partes:** Todos aquellos que tengan el carácter de actor, responsable, autoridad responsable, tercero interesado o coadyuvante en los medios de impugnación en materia electoral;
- 1.14. **Reglamento Interno.** El del Tribunal Electoral del Poder Judicial de la Federación.
- 1.15. **Sala Superior:** La Sala Superior del Tribunal Electoral del Poder Judicial de la Federación;
- 1.16. **Salas:** A la Sala Superior y las Salas Regionales del Tribunal Electoral del Poder Judicial de la Federación;
- 1.17. **Secretarías Generales de Acuerdos:** Las Secretarías Generales de Acuerdos de las Salas del Tribunal Electoral del Poder Judicial de la Federación;
- 1.18. **Secretarios Generales de Acuerdos:** Los titulares de las Secretarías Generales de Acuerdos y los servidores públicos que los suplan en términos de las disposiciones legales y reglamentarias aplicables;
- 1.19. **Servidores Públicos.** Los Secretarios Generales, Actuarios y Subsecretario General de Acuerdos de la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación;
- 1.20. **Sistema.** Sistema de Notificaciones por correo electrónico del tribunal Electoral;
- 1.21. **Solicitante:** Quien solicite a la Unidad de Certificación Electrónica, la expedición o revocación de la cuenta institucional de correo electrónico;
- 1.22. **Subsecretario.** El titular de la Subsecretaría General de Acuerdos de la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación;
- 1.23. **Token.** El dispositivo criptográfico que almacena llaves privadas de manera segura, a manera de llavero electrónico;
- 1.24. **Tribunal:** El Tribunal Electoral del Poder Judicial de la Federación;

**1.25. Unidad de Certificación Electrónica:** A la Unidad de Certificación Electrónica del Tribunal Electoral del Poder Judicial de la Federación, y

**1.26. Usuario:** A quien cuente con el certificado de firma electrónica avanzada o la cuenta de correo electrónico expedidos por la Unidad de Certificación Electrónica.

**2. EXPEDICIÓN DEL CERTIFICADO A LOS SECRETARIOS GENERALES DE ACUERDOS, SUBSECRETARIO GENERAL DE ACUERDOS Y ACTUARIOS.**

**2.1.** El certificado se otorgará a los Secretarios Generales de Acuerdos, el Subsecretario General de Acuerdos de la Sala Superior y a los Actuarios del Tribunal Electoral.

**2.2.** La Presidencia de las Salas solicitará a la Unidad de Certificación Electrónica, expedir el certificado de los Secretarios Generales de Acuerdos de las Salas y del Subsecretario.

**2.3.** Las Secretarías Generales de Acuerdos de la Sala que corresponda, solicitará la expedición del certificado de los Actuarios de las Salas del Tribunal;

**2.4.** La solicitud de expedición del certificado se hará mediante oficio, el cual deberá contener los elementos siguientes:

**I.** Estar dirigido a la Dirección General de Sistemas;

**II.** Contener la expresión de tratarse de una solicitud de otorgamiento de Certificado;

**III.** Mencionar el nombre completo, cargo y adscripción del servidor público al que se le va a proporcionar el certificado;

**IV.** Adjuntarse la constancia de servicios que haya expedido la Coordinación de Recursos Humanos y Enlace Administrativo del Tribunal, con la cual se acreditará la legitimación del servidor público para obtener un certificado;

**V.** La constancia de servicios no deberá tener una antigüedad mayor a treinta días y, en todo momento, la Unidad de Certificación Electrónica deberá cerciorarse en forma económica de la vigencia de su contenido;

**VI.** Firma autógrafa del titular de la Presidencia de la Sala o del Secretario General de Acuerdos que lo solicite, según sea el caso, y

**VII.** Fecha de la solicitud.

**2.5.** Presentada la solicitud ante la Dirección General de Sistemas, la Unidad de Certificación Electrónica procederá a tramitar la expedición del certificado.

**2.6.** Por su parte, el servidor público al que se va a dotar del certificado, accederá al sitio de la Unidad de Certificación Electrónica, en la liga: <https://uce.te.gob.mx/SGA/>

Unidad de Certificación Electrónica de la Sala Superior del TEPJF		 <b>TRIBUNAL ELECTORAL</b> del Poder Judicial de la Federación	
Solicitud Certificado Digital			
Descarga Certificado Digital			
Solicitar Revocación			
Consulta Certificado Digital			
Descargar Certificado Autoridad			
Políticas y prácticas de certificación			

2.7. En el sitio, seleccionará la opción de **“Solicitud de Certificado Digital”**.



2.8. Seleccionará la opción denominada **“Obtención de datos con base a correo”** y proporcionará su cuenta de correo institucional (\*\*\*\*@te.gob.mx).



2.9. Dará clic en **“Requisitar solicitud”**, para enterarse de los términos y condiciones del uso de los certificados. Si está de acuerdo, dará clic en la opción **“Acepto”**

Unidad de Certificación Electrónica de la Sala Superior del TEPJF

 **TRIBUNAL ELECTORAL**  
del Poder Judicial de la Federación

Solicitud Certificado Digital

Solicitud Certificado Digital

Descarga Certificado Digital

Solicitar Revocación

Consulta Certificado Digital

Descargar Certificado Autoridad

Políticas y prácticas de certificación

**TÉRMINOS Y CONDICIONES DE USO**

- El certificado de firma electrónica avanzada tendrá una vigencia de dos años contados a partir de su expedición.
- El uso adecuado y la guarda de la clave que se le proporciona con motivo de la obtención de dicho certificado de firma electrónica avanzada será responsabilidad del solicitante.
- El solicitante manifiesta conocer el contenido y alcance de las disposiciones legales y reglamentarias relativas al uso del Certificado de Firma Electrónica Avanzada expedidos por el Tribunal Electoral del Poder Judicial de la Federación, por lo que asume plena responsabilidad respecto de la información y contenido de todo documento firmados electrónicamente.
- El solicitante deberá descargar el certificado de la página Web del Tribunal Electoral del Poder Judicial de la Federación [www.te.gob.mx](http://www.te.gob.mx).

©2009 - Todos los derechos reservados

2.10. En la opción “**Guardar en**”, seleccionará la opción “**Guardar en eToken**” y dará clic en “**Siguiente**”.

Unidad de Certificación Electrónica de la Sala Superior del TEPJF

**TRIBUNAL ELECTORAL**  
del Poder Judicial de la Federación

Solicitud Certificado Digital

Solicitud Certificado Digital

Datos del emisor

Nombre: Unidad de Certificación Electrónica del Tribunal Electoral del Poder Judicial de la Federación

Información del solicitante

Requiere los campos solicitados.  
Los campos marcados con un \* son obligatorios.

Nombre \* Prueba Cert

Correo electrónico prueba.cert@te.gob.mx

Institución Tribunal Electoral del Poder Judicial de la Federación

Departamento Dirección General de Sistemas

Título/Puesto Prueba

Dirección Carlieta Armero No. 5000 Col. CTM Culhuacán

Código postal 04480

Localidad/Ciudad Coyacacán

Estado Distrito Federal

Seguridad de la solicitud

Seleccione el medio de almacenamiento para su llave privada

Guardar en: Guardar en token eToken

Atras Siguiente

2.11. Verificará que la información general de la solicitud sea correcta y dará clic en la opción “**Generar y enviar solicitud**”

Unidad de Certificación Electrónica de la Sala Superior del TEPJF

**TRIBUNAL ELECTORAL**  
del Poder Judicial de la Federación

Solicitud Certificado Digital

Solicitud Certificado Digital

Información General de la solicitud

A continuación se muestra la información proporcionada con la que se procesará la solicitud del Certificado Digital, verifique que la información proporcionada sea correcta:

Nombre \* Prueba Cert

Correo electrónico prueba.cert@te.gob.mx

Institución Tribunal Electoral del Poder Judicial de la Federación

Departamento Dirección General de Sistemas

Título/Puesto Prueba

Dirección Carlieta Armero No. 5000 Col. CTM Culhuacán

Código postal 04480

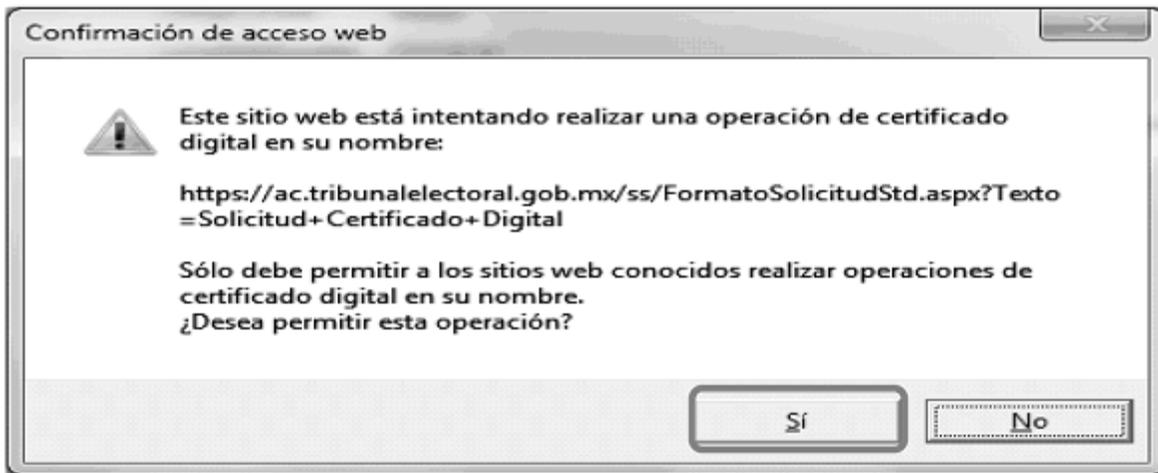
Localidad/Ciudad Coyacacán

Estado Distrito Federal

Atras Generar y Enviar Solicitud

©2008 - Todos los derechos reservados

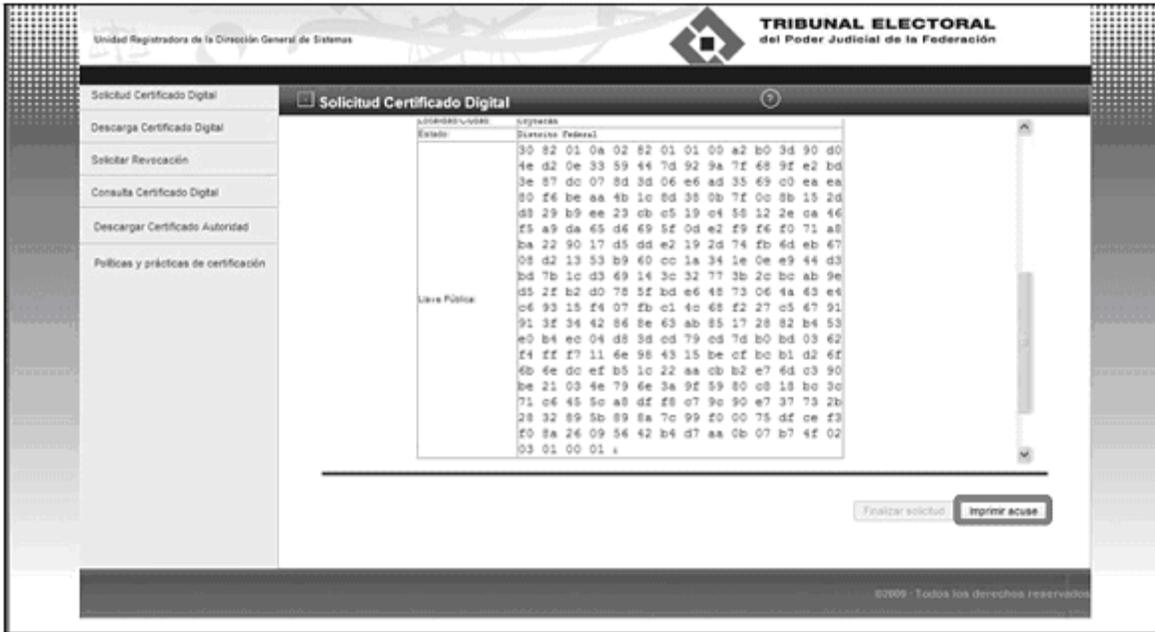
2.12. Hecho lo anterior, dentro del Token se generarán tanto la llave pública como la privada del usuario. Por lo que aparecerá un mensaje de advertencia, el cual debe aceptarse dando clic en la opción "Sí".



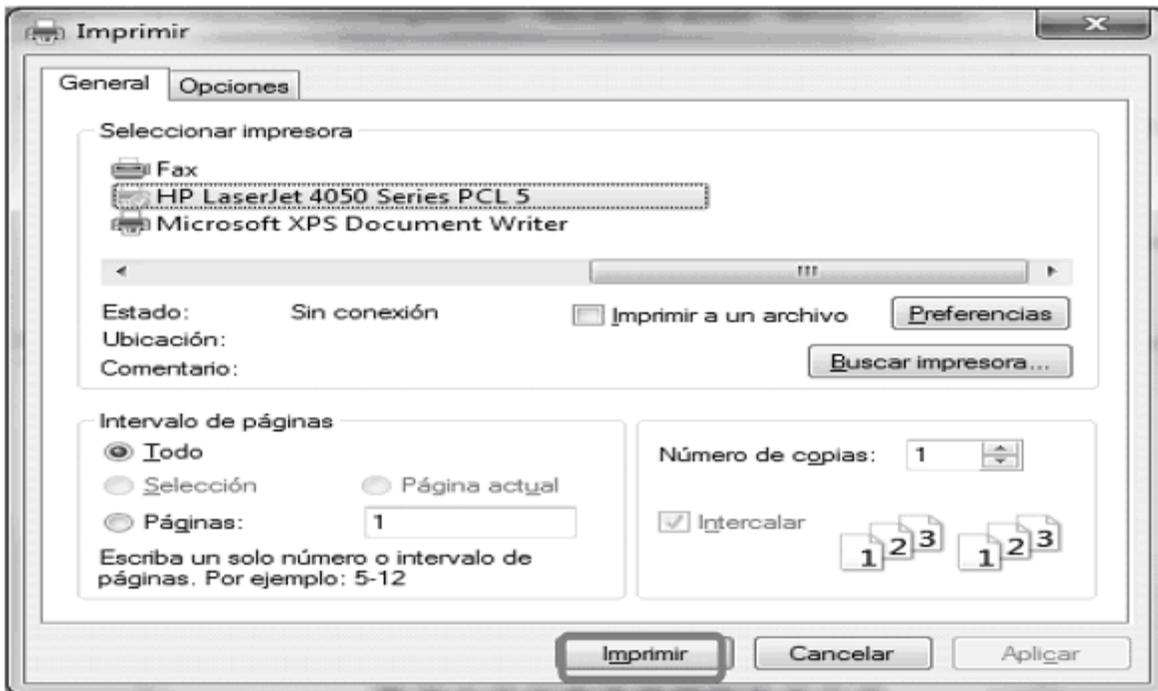
2.13. Ingresará la contraseña del Token y dará clic en la opción "OK"



2.14. Imprimirá el acuse de solicitud de certificado seleccionando la opción “Imprimir acuse”



2.15. Seleccionará la impresora donde enviará dicho documento y seleccionará la opción “Imprimir”



2.16. Obtenida la impresión del acuse de recibo deberá firmarla autógrafamente en el espacio correspondiente.

https://uce.te.gob.mx/ - Recibo de acuse - Windows Internet Explorer



**TRIBUNAL ELECTORAL**  
del Poder Judicial de la Federación

---

**TÉRMINOS Y CONDICIONES DE USO**

- El certificado de firma electrónica avanzada tendrá una vigencia de dos años contados a partir de su expedición.
- El uso adecuado y la guarda de la clave que se le proporciona con motivo de la obtención de dicho certificado de firma electrónica avanzada será responsabilidad del solicitante.
- El solicitante manifiesta conocer el contenido y alcance de las disposiciones legales y reglamentarias relativas al uso del Certificado de Firma Electrónica Avanzada expedidos por el Tribunal Electoral del Poder Judicial de la Federación, por lo que asume plena responsabilidad respecto de la información y contenido de todo documento firmados electrónicamente.
- El solicitante deberá descargar el certificado de la página Web del Tribunal Electoral del Poder Judicial de la Federación [uce.te.gob.mx](http://uce.te.gob.mx).

---

**ACUSE DE RECIBO**

La Unidad de Certificación Electrónica del Tribunal Electoral del Poder Judicial de la Federación a través de la Dirección General de la Unidad de Sistemas ha recibido una solicitud para la generación del certificado digital con los siguientes datos:

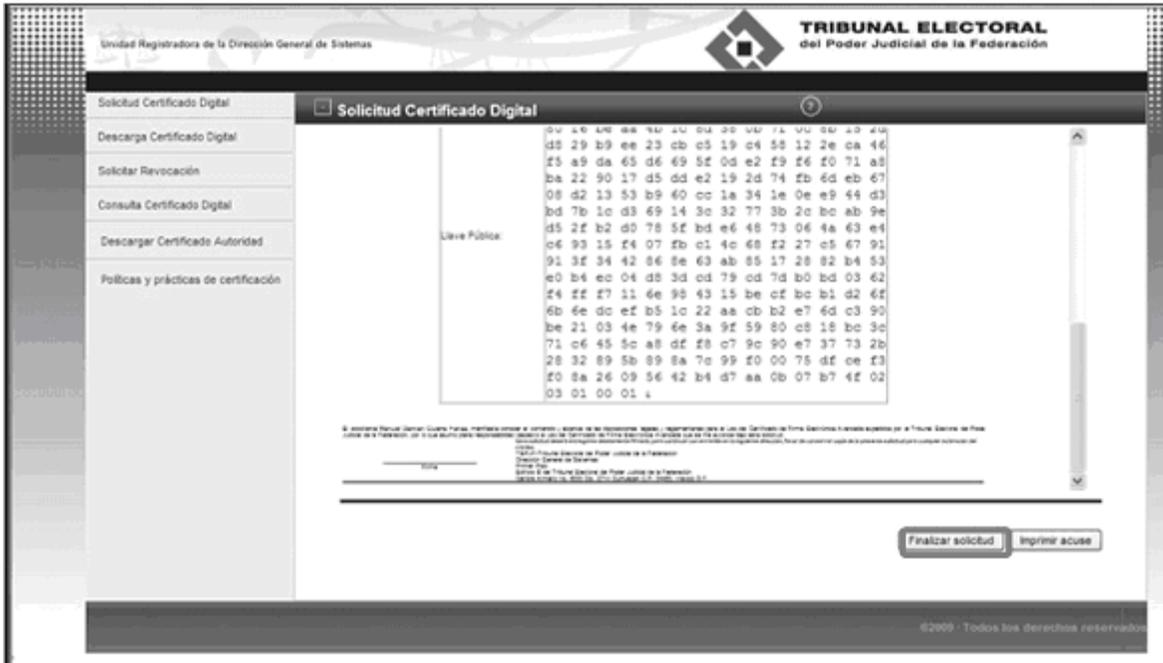
Folio:	64
A nombre de:	Manuel Damian Guerra Farias
Correo electrónico:	manuel.guerra@te.gob.mx
Autoridad Responsable:	Tribunal Electoral del Poder Judicial de la Federación
Departamento:	Dirección General de Sistemas
Título/Puesto:	Asesor
Dirección:	Carlota Armero No.5000 Col. CTM Culhuacán
Código Postal:	04480
Localidad/Ciudad:	Coyoacán
Estado:	Distrito Federal
Llave Pública:	<pre> 30 82 01 0a 02 82 01 01 00 a2 b0 3d 90 d0 4e d2 0e 33 59 44 7d 92 9a 7f e8 9f e2 bd 3e 87 dc 07 8d 3d 06 e6 ad 35 69 c0 ea ea 90 f6 be aa 4b 1c 8d 38 0b 7f 0c 8b 15 2d d8 29 b9 ee 23 cb c5 19 c4 58 12 2e ca 46 f5 a9 da 65 d6 69 3f 0d e2 f9 f6 f0 71 a8 ba 22 90 17 d5 dd e2 19 2d 74 fb 6d eb 67 08 d2 13 53 b9 60 cc 1a 34 1e 0e e9 44 d3 bd 7b 1c d3 69 14 3c 32 77 3b 2c bc ab 9e d5 2f b2 d0 78 5f bd e6 48 72 06 4a 63 e4 e6 93 15 f4 07 fb c1 4c 68 f2 27 c5 67 91 91 3f 34 42 86 8e 63 ab 85 17 28 82 b4 59 e0 b4 ec 04 d8 3d cd 79 cd 7d b0 bd 03 62 f4 ff f7 11 6e 90 43 15 be cf bc b1 d2 ff 6b 6e dc ef b5 1c 22 aa cb b2 e7 6d c3 90 be 21 03 4e 79 6e 3a 9f 59 80 e8 18 bc 3c 71 c6 45 3c a8 df f8 c7 9c 90 e7 37 73 2b 28 32 89 5b 89 8a 7c 99 f0 00 75 df ce f9 f0 8a 26 09 3e 42 b4 d7 aa 0b 07 b7 4f 02 03 01 00 01 i                     </pre>

El solicitante **Manuel Damian Guerra Farias**, manifiesta conocer el contenido y alcance de las disposiciones legales y reglamentarias para el Uso del Certificado de Firma Electrónica Avanzada expedidos por el Tribunal Electoral del Poder Judicial de la Federación, por lo que asumo plena responsabilidad respecto al uso del Certificado de Firma Electrónica Avanzada que se me autoriza bajo esta solicitud.

Esta solicitud deberá entregarse debidamente firmada, para continuar con el trámite en la siguiente dirección, favor de conservar copia de la presente solicitud para cualquier aclaración del trámite:  
TEP/JF-Tribunal Electoral del Poder Judicial de la Federación  
Dirección General de Sistemas  
Primer Piso  
Edificio B del Tribunal Electoral del Poder Judicial de la Federación  
Carlota Armero No. 5000 Col. CTM Culhuacán C.P. 04480, México D.F.

Firma

2.17. Enseguida, seleccionará la opción “Finalizar Solicitud”



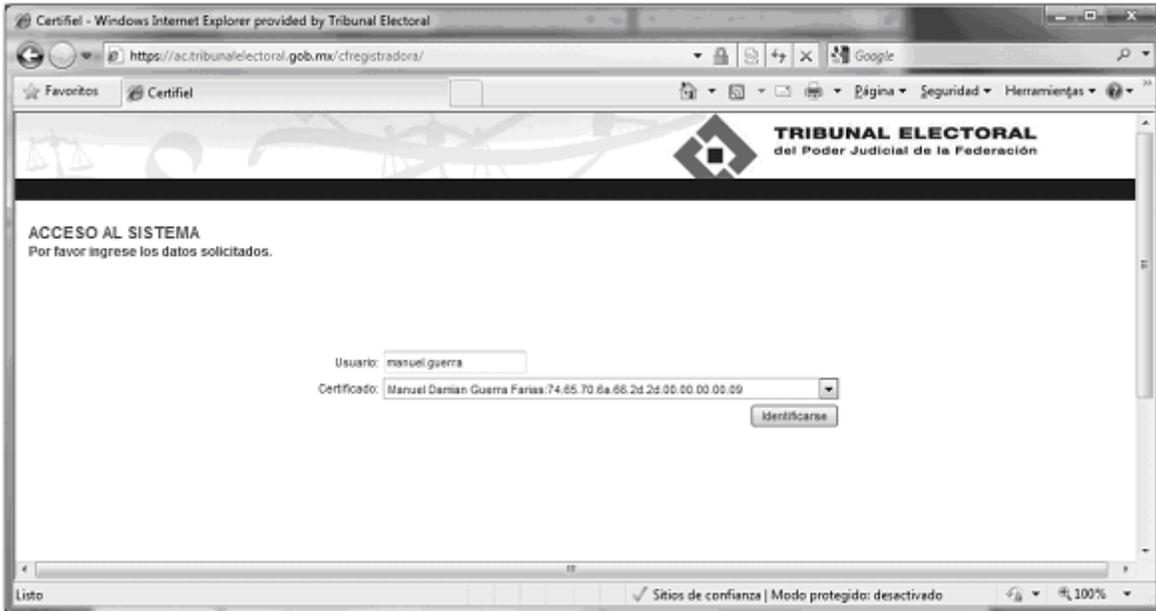
2.18. El sistema informará que la solicitud se ha enviado exitosamente y le indicará el trámite a seguir.



**2.19.** Enviada la solicitud, el servidor público deberá presentar ante la Unidad de Certificación Electrónica, la siguiente documentación:

- I. El acuse de solicitud de certificado firmado autográficamente, y
- II. Una copia de su credencial institucional.

**2.20.** Con estos documentos, la Dirección General de Sistemas validará la información registrada en la solicitud del certificado a través de la siguiente liga: <https://uce.te.gob.mx/cfRegistradora>



**2.21.** Un operador de la Unidad de Certificación Electrónica accederá al sistema, autenticándose a través de su certificado.



2.22. Seleccionará la opción “Acreditación de solicitudes de certificados digitales” y se mostrará una lista de las solicitudes de certificados pendientes de acreditar.

Unidad de Certificación Electrónica del Tribunal Electoral del Poder Judicial de la Federación  
Manuel Damían Guerra Fariás

TRIBUNAL ELECTORAL del Poder Judicial de la Federación

Recepción de solicitudes de certificados digitales  
Carga solicitudes de certificados digitales  
**Acreditación solicitudes de certificados digitales**  
Administración de certificados digitales  
Emisión de certificados digitales  
Consulta certificados digitales  
Funciones de soporte  
Generación de reportes

Acreditación solicitudes de certificados digitales

Folio:  Nombre:

Registros 1 a 1 de 1 coincidentes

Folio	Nombre	Correo	Fecha	Agente
24	Prueba Cert	prueba.cert@te.gob.mx	2010-09-27 19:11:19	*** Recepción en línea

Página:

2.23. Seleccionará la solicitud respectiva, para ver el detalle respectivo y verificará que los datos de las solicitudes correspondan con los documentos presentados y seleccionará la opción “Proceder con la verificación”.

Unidad de Certificación Electrónica del Tribunal Electoral del Poder Judicial de la Federación  
Manuel Damían Guerra Fariás

TRIBUNAL ELECTORAL del Poder Judicial de la Federación

Recepción de solicitudes de certificados digitales  
Carga solicitudes de certificados digitales  
Acreditación solicitudes de certificados digitales  
**Administración de certificados digitales**  
Emisión de certificados digitales  
Consulta certificados digitales  
Funciones de soporte  
Generación de reportes

Acreditación solicitudes de certificados digitales

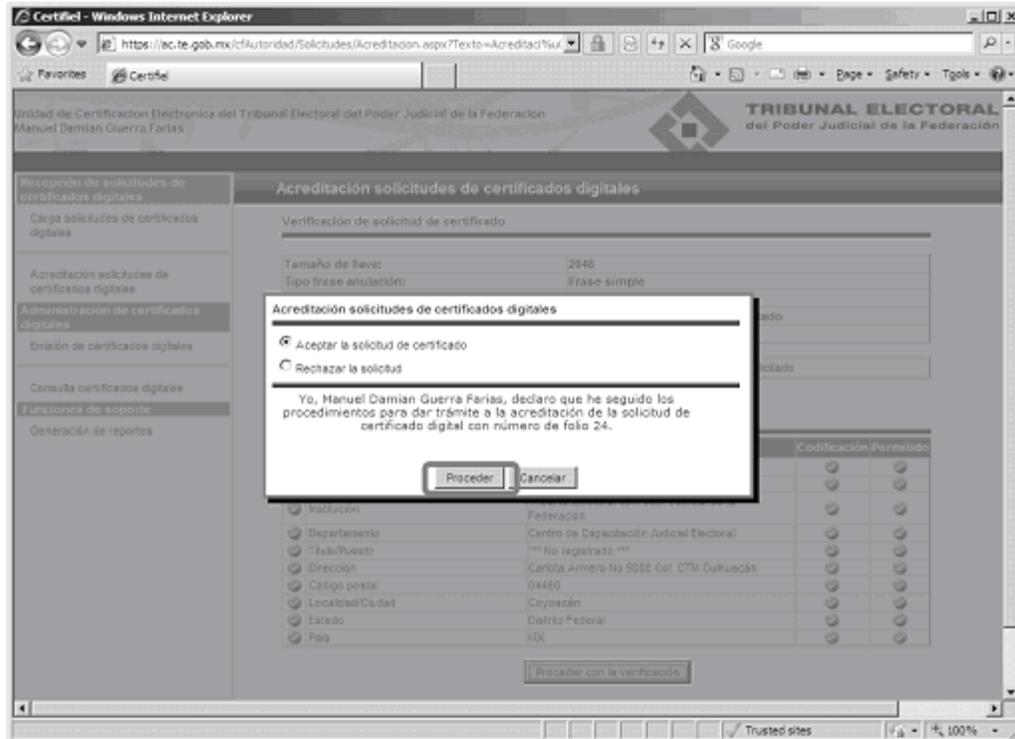
Verificación de solicitud de certificado

Tamaño de llave:	2048
Tipo frase anulación:	Frase simple
Tiene archivo complementor:	SI
Estado operación:	Pendiente de acreditación: Aceptado
Fecha de operación:	2010-09-27 19:11:19

Información de la solicitud

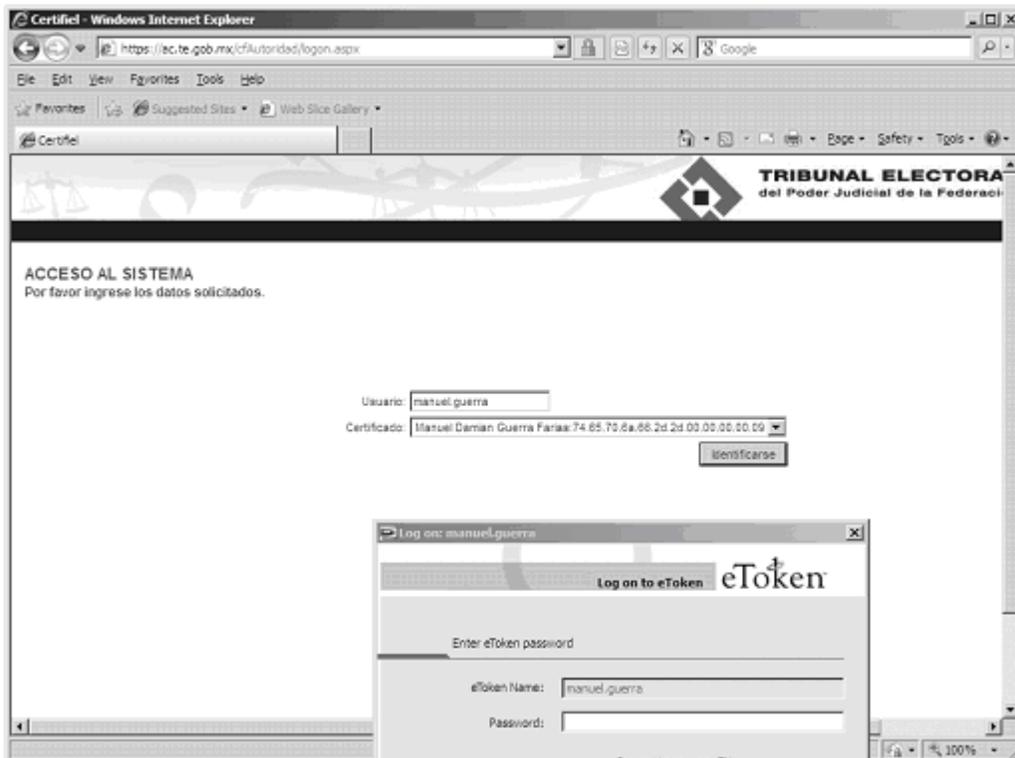
	Descripción	Contenido	Codificación	Permitido
<input checked="" type="checkbox"/>	Nombre	Prueba Cert	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Correo electrónico	prueba.cert@te.gob.mx	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Institución	Tribunal Electoral del Poder Judicial de la Federación	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Departamento	Centro de Capacitación Judicial Electoral	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Título/Puesto	*** No registrado ***	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Dirección	Carlota Armero No.5000 Col. CTM Cuahuacán	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Código postal	04480	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Localidad/Ciudad	Coyoacán	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Estado	Distrito Federal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	País	MX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

2.24. Seleccionará la opción “**Aceptar la solicitud de certificado**” y dará clic en el botón “**Proceder**”.



2.25. Aceptada la solicitud del certificado, ésta será turnada al módulo de autoridad certificadora donde se firmará y emitirá el certificado correspondiente.

2.26. Para emitir el certificado, el operador del módulo de autoridad certificadora accederá, desde la consola del equipo de la Unidad de Certificación Electrónica, a la siguiente liga: <https://ac.te.gov.mx/cfAutoridad>



2.27. Accederá al sistema autenticándose con su certificado.



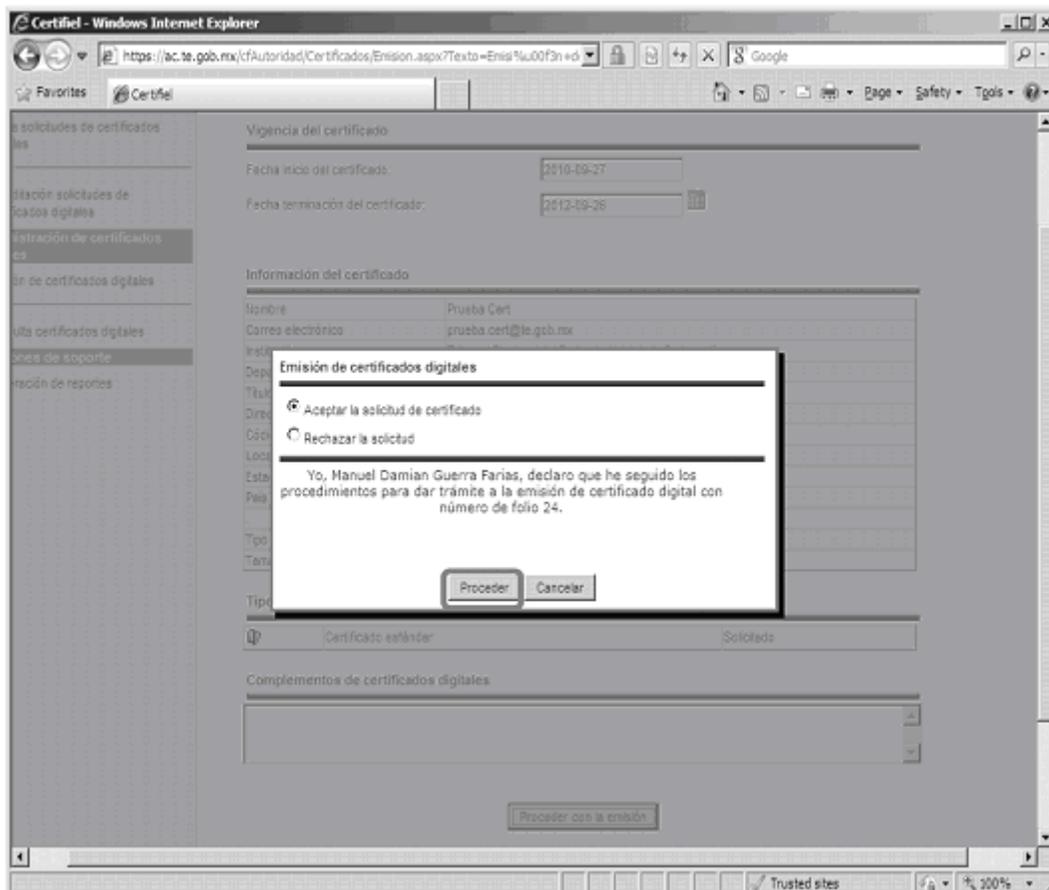
2.28. Seleccionará la opción “Emisión de certificados digitales”, para ver la lista de las solicitudes de certificados pendientes de emitir.



2.29. Seleccionará la solicitud respectiva, para ver los detalles de la misma y, posteriormente, seleccionará la opción **“Proceder en la emisión”**



2.30. Seleccionará la opción **“Aceptar la solicitud de certificado”** y dará clic en el boton **“Proceder”**.



2.31. Una vez emitido el certificado, el usuario recibirá en su cuenta de correo electrónico institucional un aviso indicándole que puede descargar su certificado.

2.32. Una vez emitido el certificado, el usuario acceder al sitio de la Unidad de Certificación Electrónica (<https://uce.te.gob.mx/SGA>) para descargar el certificado e instalarlo.

2.33. En el sitio de Unidad de Certificación Electrónica y seleccionará la opción “**Descarga Certificado Digital**”.



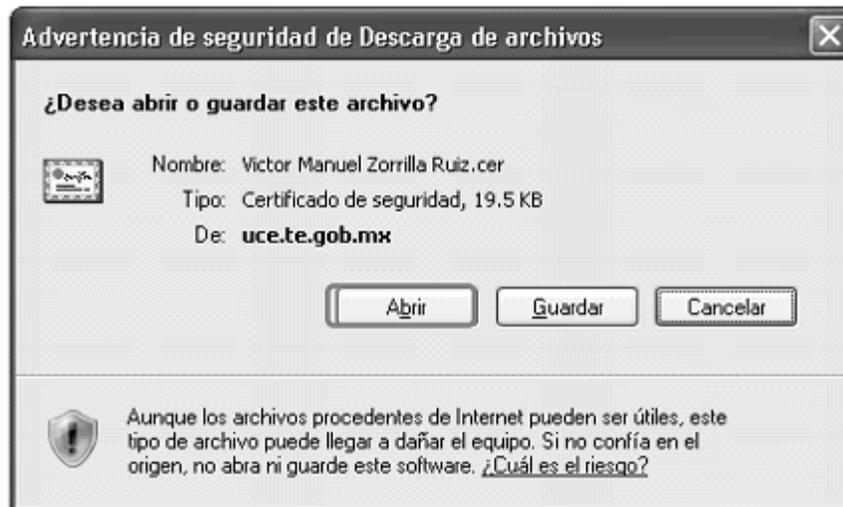
2.34. Indicará su cuenta institucional de correo electrónico y seleccionará la opción “**Descarga Certificado**”.



2.35. Seleccionará el certificado, a través de la liga sobre el nombre del firmante.



2.36. Abrirá el contenido del certificado mediante la opción “Abrir”.



2.37. Instalará el certificado mediante la opción “Instalar certificado”



2.38. Ejecutará el asistente para importación de certificados y continuará con “Siguiente”.



2.39. Seleccionará la opción **“Seleccionar automáticamente el almacén de certificados en base al tipo de certificado”** y continuará con **“Siguiente”**



2.40. El certificado se almacenará en el dispositivo criptográfico Token.



2.41. Proporcionará su contraseña para almacenar el certificado dentro de su Token



2.42. Finalmente, el sistema indicará que el proceso se realizó con éxito y seleccionara “**Aceptar**”.



### 3. REVOCACION DEL CERTIFICADO A LOS SECRETARIOS GENERALES DE ACUERDOS, SUBSECRETARIO GENERAL DE ACUERDOS Y ACTUARIOS.

3.1. Si el servidor público titular del certificado cambia de área de adscripción o termina su relación laboral con el Tribunal, se tendrá por concluida la vigencia del certificado, previa comunicación, expresa y por escrito, que al efecto haga la Presidencia de la Sala o el Secretario General de Acuerdos, según corresponda.

3.2. El uso no autorizado del certificado y/o distinto a lo previsto en el Acuerdo General 3/2010, será causa de revocación, sin perjuicio de la responsabilidad administrativa o penal en que se incurra.

3.3. También será causa de revocación, las señaladas para tal efecto en las Prácticas de Certificación Electrónica de la Unidad de Certificación Electrónica.

3.4. Para llevar a cabo la revocación del certificado, la Presidencia de las Salas o las Secretarías Generales de Acuerdos que correspondan, deberán solicitarlo mediante oficio, el cual deberá contener los elementos siguientes:

- I. Estar dirigido a la Dirección General de Sistemas;
- II. Contener la expresión de tratarse de una solicitud de revocación de Certificado;
- III. Mencionar el nombre completo, cargo y adscripción del servidor público que se le revoque el certificado;
- IV. Mencionar, de manera discrecional, las causas que motivan la revocación, y

V. Fecha de la solicitud.

3.5. Para revocar un certificado, el operador de la Unidad de Certificación Electrónica deberá acceder a la liga siguiente: <https://uce.te.gob.mx/cfRegistradora>

The screenshot shows a web browser window with the following content:

- Header: **TRIBUNAL ELECTORAL** del Poder Judicial de la Federación
- Section: **ACCESO AL SISTEMA**
- Text: Por favor ingrese los datos solicitados.
- Form fields:
  - Usuario:
  - Certificado:
- Button:

3.6. Se autenticará a través de su certificado.

The screenshot shows a dialog box titled "Log on to eToken" with the following content:

- Text: Enter eToken password
- Form fields:
  - eToken Name:
  - Password:
- Text: Current Language: ES
- Buttons:

3.7. Seleccionará la opción “Consulta de certificados digitales”, para visualizar la lista de las solicitudes de certificados con su respectivo estatus, así como el certificado que se desea revocar.

Unidad de Certificación Electrónica del Tribunal Electoral del Poder Judicial de la Federación  
Manuel Damián Guerra Farias

**TRIBUNAL ELECTORAL**  
del Poder Judicial de la Federación

SALIR

Recepción de solicitudes de certificados digitales

Carga solicitudes de certificados digitales

Acreditación solicitudes de certificados digitales

Administración de certificados digitales

Emisión de certificados digitales

**Consulta certificados digitales**

Funciones de soporte

Generación de reportes

**Consulta certificados digitales**

Nombre:  Serie:  Estado Certificado: (Todos)

Registros 1 a 5 de 5 coincidentes

Folio	Nombre	Serie	Estado
7	Prueba Cert	74.65.70.6a.66.2d.2d.00.00.00.00.07	Revocado
11	Yolanda Hortencia Salinas Santos	74.65.70.6a.66.2d.2d.00.00.00.00.0a	Aceptado
23	Rebeca Obdulia Cruz Avilla	74.65.70.6a.66.2d.2d.00.00.00.00.12	Aceptado
24	Prueba Cert	74.65.70.6a.66.2d.2d.00.00.00.00.15	Aceptado
25	Sebastián Baulista Herrera	74.65.70.6a.66.2d.2d.00.00.00.00.14	Aceptado

Página: 1 de 1

3.8. Seleccionará la opción “Revocar certificado”

Unidad de Certificación Electrónica del Tribunal Electoral del Poder Judicial de la Federación  
Manuel Damián Guerra Farias

**TRIBUNAL ELECTORAL**  
del Poder Judicial de la Federación

Recepción de solicitudes de certificados digitales

Carga solicitudes de certificados digitales

Acreditación solicitudes de certificados digitales

Administración de certificados digitales

Emisión de certificados digitales

**Consulta certificados digitales**

Funciones de soporte

Generación de reportes

**Consulta certificados digitales**

Folio: 24

Nombre: Prueba Cert Correo: prueba.cert@te.gob.mx

Serie: 74.65.70.6a.66.2d.2d.00.00.00.00.15

Vigencia: 2010-09-28 00:23 hrs. al 2012-09-27 00:23 hrs.

Entidad: Unidad de Certificación Electrónica del Tribunal Electoral del Poder Judicial de la Federación

Emisor: \*\*\* Emisión en línea 2010-09-27 19:23:24

Agente Emisor: \*\*\* Emisión en línea 2010-09-27 19:23:24

Agente Receptor: \*\*\* Recepción en línea 2010-09-27 19:11:19

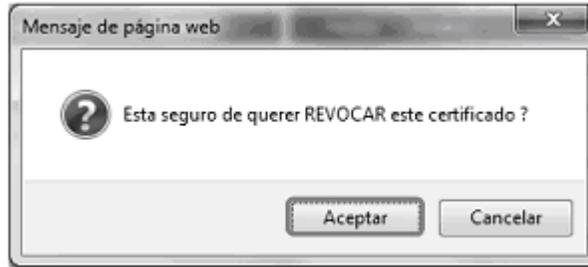
Receptor: \*\*\* Recepción en línea 2010-09-27 19:11:19

Estado: Aceptado

**Bitácora de Estados**

Fecha	Estado	Agente	Fecha	Orden	Tipo	Estado
2010-09-27 19:24	Aceptado	Agente interno del sistema 01	2010-09-27 19:24	1	Registro en active directory	✔
2010-09-27 19:23	En proceso de registro	Manuel Damián Guerra Farias	2010-09-27 19:24	2	Notificación de correo electrónico	✔
			2010-09-27 19:24	3	Publicación certificado	✔

3.9. Seleccionará la opción “Acepta”.



3.10. El certificado cambiará de estado a revocado. Lo cual se podrá verificar al seleccionar la opción “Consulta certificados digitales”



4. OBTENCION DE LA CUENTA INSTITUCIONAL DE CORREO ELECTRONICO POR LAS PARTES

4.1. Para obtener la cuenta institucional de correo electrónico, el interesado deberá ingresar a la página web del Tribunal, acceder al Sistema y dar clic en “Crear nueva cuenta”.



4.2. Llenará los campos que se solicitan para dar de alta la cuenta institucional de correo electrónico.

**Bienvenidos a Sistema de Notificaciones por Correo Electrónico**

Ingrese los siguientes datos para dar de alta su cuenta

\* Nombre

\* Apellido Paterno

\* Apellido Materno

\* Elija una contraseña   
escriba dos veces la contraseña para confirmarla

\* Calle

\* Colonia

\* Ciudad

\* Estado

\* Código Postal

Teléfono

\* Correo Personal   
Este correo sirve para recuperar su contraseña

Sexo  Masculino  Femenino

Fecha de Nacimiento   
DD/MM/AAAA

\* Tipo de Solicitud: Por propio derecho

Especifique Institución:

\* Código de Verificación   
Introduzca las letras siguientes:  
D V M Q E G

Acepto las condiciones del servicio y política de privacidad

**TÉRMINOS Y CONDICIONES DE USO DE LA CUENTA INSTITUCIONAL DE CORREO ELECTRÓNICO PARA RECIBIR NOTIFICACIONES**

- Tiene como única finalidad proporcionar a las partes un buzón con mecanismos de confirmación de envío, que les permita recibir notificaciones;
- No otorga la posibilidad de respuesta, envío o reenvío de información;

- I.- Los campos marcados con un asterisco “\*” son obligatorios, por lo tanto deberá llenarlos para completar el proceso;
- II.- En el campo de “**Correo personal**” deberá escribir 2 veces su correo particular (yahoo, hotmail, gmail, etc.), el cual será utilizado para recibir la notificación de creación de su cuenta para acceso al sistema, recuperar su contraseña en caso de extravío u olvido y recibir avisos de que ha recibido una notificación vía correo electrónico en su cuenta de correo institucional;
- III.- La contraseña deberá tener un mínimo de ocho caracteres alfanuméricos, así como mínimo un número, una mayúscula, una minúscula y deberá escribirse 2 veces para confirmarla.
- IV.- Si algún dato de los marcados como obligatorios falta, el sistema indicará cuál de ellos es, desplegando el mensaje “**Hace falta este campo**” (en color rojo), ubicado debajo de cada etiqueta con el nombre del campo;

\* Calle   
Hace falta este campo.

\* Colonia   
Hace falta este campo.

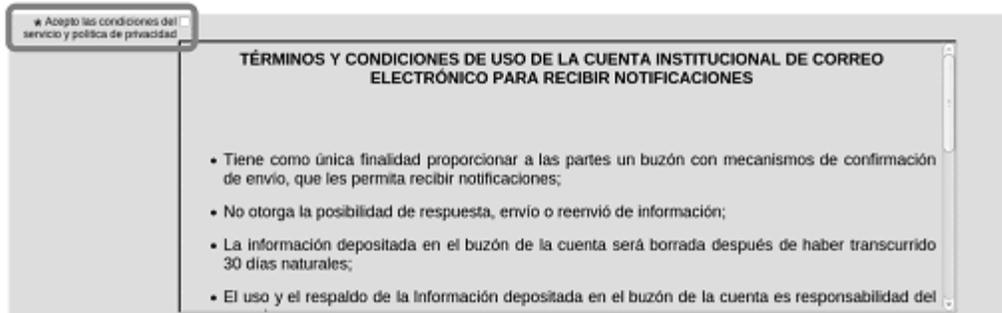
\* Ciudad   
Hace falta este campo.

\* Estado

- V. En el campo “**Código de Verificación**”, deberá capturar las cinco letras que se presentan formadas con caracteres especiales, para evitar suplantaciones o creaciones automáticas de cuentas;

\* Código de Verificación

Introduzca las letras siguientes:  
TKKRT

**VI. Seleccionará la casilla de “Acepto las condiciones de servicio y política de privacidad”.****4.3 Dará clic en el botón “Crear cuenta”**

**4.4.** El sistema la generará, de forma automática y de acuerdo a la información capturada en los campos de Nombre y Apellido Paterno, desplegando un mensaje con el nombre correspondiente. Paralelamente le será enviado un correo electrónico a su cuenta personal con el siguiente mensaje:

“Usted ha generado en el *Sistema de Notificaciones por Correo Electrónico* del Tribunal Electoral la cuenta [luis.cuevas@notificaciones.tribunalelectoral.gob.mx](mailto:luis.cuevas@notificaciones.tribunalelectoral.gob.mx), **la cual deberá señalarla en su demanda o promoción para que pueda ser notificado vía correo electrónico.**

Lo anterior, de conformidad con los artículos 9, párrafo 4, y 26, párrafo 3 de la Ley General del Sistema de Medios de Impugnación en Materia Electoral; 110 del Reglamento Interno del Tribunal Electoral, y el punto de acuerdo Octavo del Acuerdo General de la Sala Superior 3/2010, relativo a la Implementación de las Notificaciones por Correo Electrónico.”

**5. RECUPERACIÓN DE LA CONTRASEÑA DE LA CUENTA INSTITUCIONAL DE CORREO ELECTRÓNICO POR LAS PARTES.**

**5.1.** Antes de iniciar este proceso, es recomendable estar seguro que durante la captura de la contraseña la tecla “**Bloq Mayús**” no se encuentre activada (las contraseñas distinguen mayúsculas de minúsculas).

**5.2.** Para recuperar su contraseña, el usuario ingresará a la página web del Tribunal, accederá al **Sistema** y dará clic en la opción “**¿Ha olvidado la contraseña?**”



5.3. Capturará el **nombre de la cuenta institucional de correo** de la cual quiere restablecer la contraseña y las cinco letras del dígito verificador. Posteriormente dará clic en “Siguiente”

5.4. El sistema enviará un aviso a la cuenta de correo personal que capturó durante el proceso “**Crear cuenta nueva**”, informándole su nueva contraseña.

“Usted ha solicitado la recuperación de contraseña en el *Sistema de Notificaciones por Correo Electrónico* del Tribunal Electoral del Poder Judicial de la Federación la cuenta [luis.cuevas@notificaciones.tribunalelectoral.gob.mx](mailto:luis.cuevas@notificaciones.tribunalelectoral.gob.mx), la cual deberá señalarla en su demanda o promoción para que pueda ser notificado vía correo electrónico.

Lo anterior, de conformidad con los artículos 9, párrafo 4, y 26, párrafo 3 de la Ley General del Sistema de Medios de Impugnación en Materia Electoral; 110 del Reglamento Interno del Tribunal Electoral del Poder Judicial de la Federación, y el punto de acuerdo Octavo del Acuerdo General de la Sala Superior 3/2010, relativo a la Implementación de las Notificaciones por Correo Electrónico.

Nueva Contraseña: \*\*\*\*\*”

## 6. BAJA DE LA CUENTA INSTITUCIONAL DE CORREO ELECTRÓNICO DE LAS PARTES

6.1. Se dará de baja la cuenta de correo institucional de las partes por las causas siguientes:

- I. Por inactividad de más de dos años;
- II. Por existir diversas cuentas relacionadas con la misma persona;
- III. Por solicitud de las partes; y
- IV. Por uso distinto a los fines previstos en el Acuerdo General.

## 7. DIGITALIZACIÓN DEL ACUERDO O RESOLUCIÓN A NOTIFICAR, NOMBRAMIENTO Y GUARDA DEL ARCHIVO

7.1. Para **digitalizar y guardar** el acuerdo o resolución, el Actuario deberá:

7.1.1. Recibir el acuerdo o resolución en la Oficina de Actuarios;

7.1.2. Revisar que el escáner esté configurado correctamente para que el archivo resultante de la digitalización del documento, quede depositado en su carpeta personal; y

7.1.3. Digitalizar el acuerdo o resolución en el escáner correspondiente.

7.2. Para **nombrar el archivo** del acuerdo o resolución digitalizado, el Actuario deberá:

7.2.1. Localizar el archivo que contiene el acuerdo o resolución digitalizada en su carpeta personal.

7.2.2. Dar clic con el botón derecho del ratón sobre el archivo, y seleccionar del menú que aparecerá inmediatamente, la opción “**Cambiar nombre**”.

7.2.3. Capturar el nombre del archivo con base en la siguiente nomenclatura:

I. **Clave del expediente**, compuesto por:

- a. **Sala:** 3 posiciones. Para el caso de las salas que contengan sólo 2 caracteres (SX, SM, ST y SG), se deberá poner un asterisco “\*” al final, para completar las 3 posiciones requeridas;
- b. **Tipo de medio de impugnación:** Para el caso de los medios de impugnación que contengan sólo 2 caracteres (AG y OP), se deberá poner un asterisco “\*” al final para completar las 3 posiciones requeridas;
- c. **Consecutivo:** 5 posiciones. Para completar las 5 posiciones requeridas se deberán poner los ceros a la izquierda necesarios, y
- d. **Año:** 4 posiciones.

**II. Tipo de documento.** Este deberá ser identificado en base al catálogo que a continuación se muestra:

Código	Descripción
J026	Acuerdo de Presidencia ordenando remisión a alguna Sala Regional o al Archivo y notificaciones.
J070	Acuerdo de turno, y notificaciones <ul style="list-style-type: none"> <li>• Diligencias por Cumplimiento</li> <li>• Turno a otro Magistrado</li> </ul>
J090	Acuerdos de Ponencia y/o de instrucción y notificaciones:** <ul style="list-style-type: none"> <li>• Radicación</li> <li>• Admisión</li> <li>• Pruebas</li> <li>• Vistas y/o traslado</li> <li>• Señala fecha y hora de audiencia</li> <li>• Cierre de instrucción</li> </ul>
J110	Audiencia de desahogo de pruebas y notificaciones
J120	Acuerdo plenario y/o Acuerdo de Sala
J130	Acuerdo de Presidencia ordenando archivo y notificaciones.
J150	Copia de opinión y acuse de oficio de presentación ante SCJN.
J170	Acuerdo de trámite de acuse y notificaciones.
J180	Resolución o sentencia
J190	Cumplimientos o incidentes <ul style="list-style-type: none"> <li>• Integrar incidente</li> <li>• Elaborar resolución incidental</li> </ul>
J200	Acuerdos de trámite que: ** <ul style="list-style-type: none"> <li>• Integra constancias y/o agregar a sus autos</li> <li>• Ordena devolución de documentos</li> <li>• Ordena expedición de copias certificadas</li> <li>• Devolución de pieza postal</li> <li>• Ordena archivo</li> </ul>

**III. Fecha.** El formato deberá ser “dd/mm/aaaa”;

**IV. Hora.** El formato deberá ser “HH:mm:ss”;

**V.** En el caso de que el documento esté formado por 2 o más archivos, se agregará un consecutivo alfabético que deberá ser agregado A, B, C..., y un segundo carácter para identificar el número total de archivos en que fue dividido el documento.

Por ejemplo; si el documento fue dividido en 4 partes, se agregará a cada archivo A, B, C y D, respectivamente, seguido de una letra D, la cual indica que el total de partes es 4 (Por la posición que ocupa la letra “D” en el abecedario).

**VI.** Para los archivos en los cuales se vaya a certificar el acuerdo o resolución digitalizado, se deberá agregar la extensión “cert”

**VII.** El archivo deberá quedar con el formato siguiente:

**Ejemplo:** SX\*JDC003252010J18028092010132100Acert

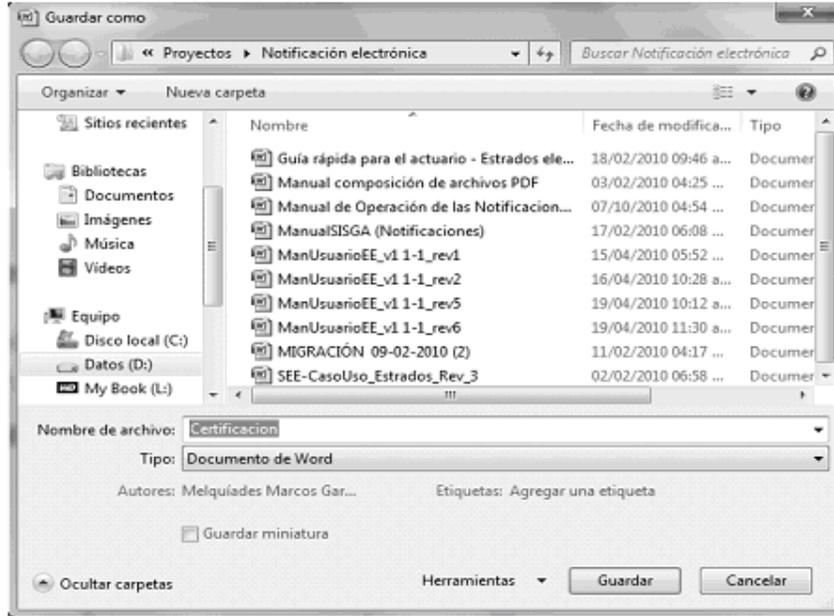
**8. CERTIFICACIÓN DEL ACUERDO O RESOLUCIÓN A NOTIFICAR**

**8.1.** Para certificar el acuerdo o resolución digitalizado y clasificado que se va a notificar, el Actuario deberá:

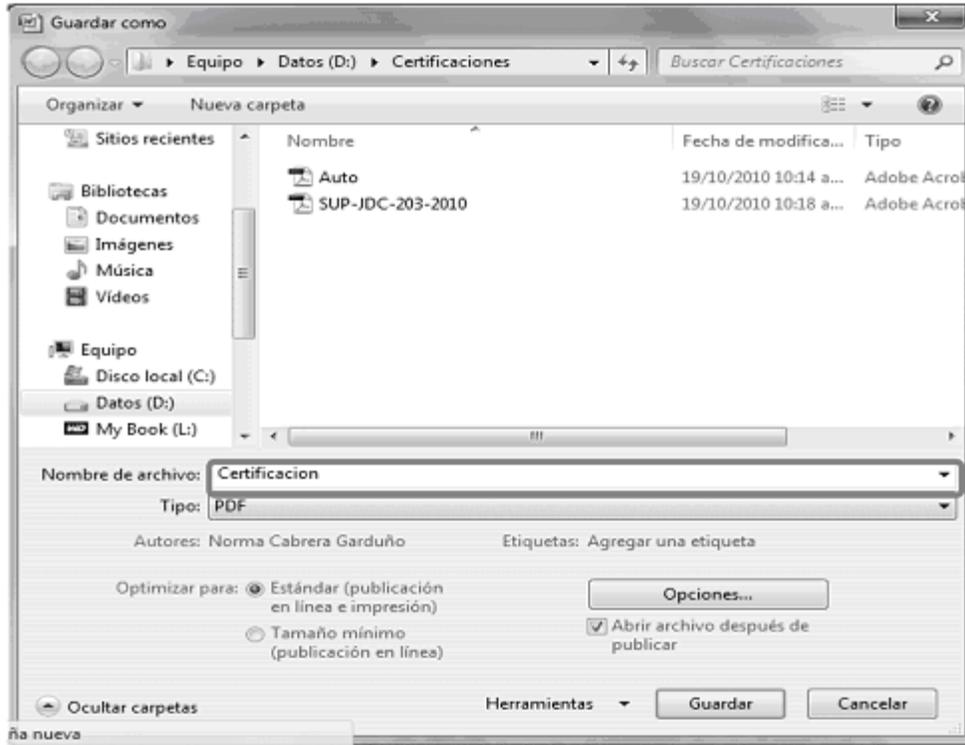
**8.1.1.** Elaborar la propuesta de certificación en un procesador de texto y guardarlo.

**8.1.2.** Convertir el archivo resultante a formato PDF, como a continuación se explica:

I. Seleccionar del menú principal, la opción **“Guardar como”**.



II. En la opción tipo, seleccionar **“PDF”**.



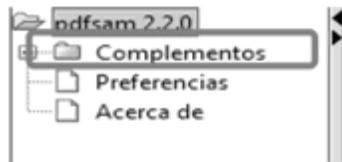
III. Finalmente deberá dar clic en **“Guardar”** y el archivo quedará almacenado en la dirección indicada.

8.1.3. Para insertar el texto de la certificación al archivo que contiene el acuerdo o resolución digitalizada que se va a notificar, el Actuario deberá:

I. Abrir la aplicación que permita unir dos o más archivos en formato PDF, en el caso particular, el programa **“pdfsam”**.



II. Abierta la aplicación, dar doble clic sobre la carpeta **“Complementos”**;



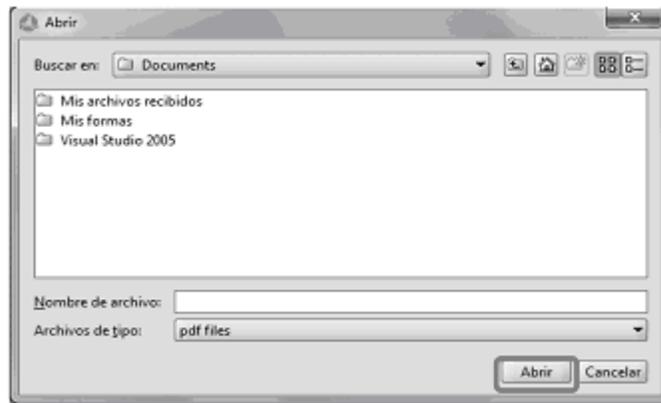
III. De las opciones disponibles que se muestren, seleccionar la de **“Unir/Extraer”** dando clic sobre ésta;



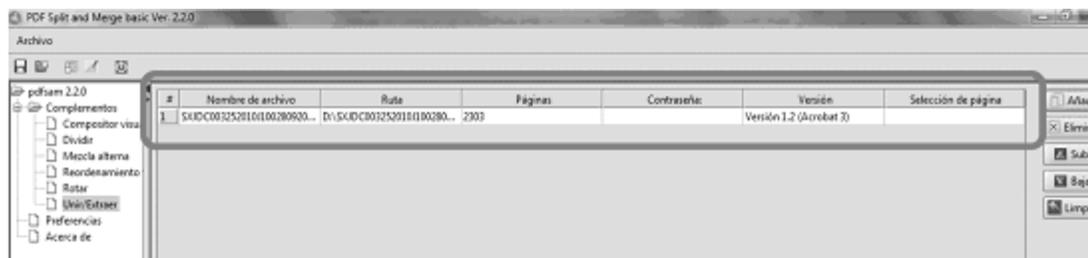
**IV. Dar clic en la opción “Añadir”**



**V. Ubicar y seleccionar el archivo con el acuerdo o resolución correspondiente y dar clic en la opción “Abrir”**



**VI. El archivo seleccionado, aparecerá agregado en la ventana correspondiente (se aplicará el mismo proceso en el caso de ser más de un archivo);**

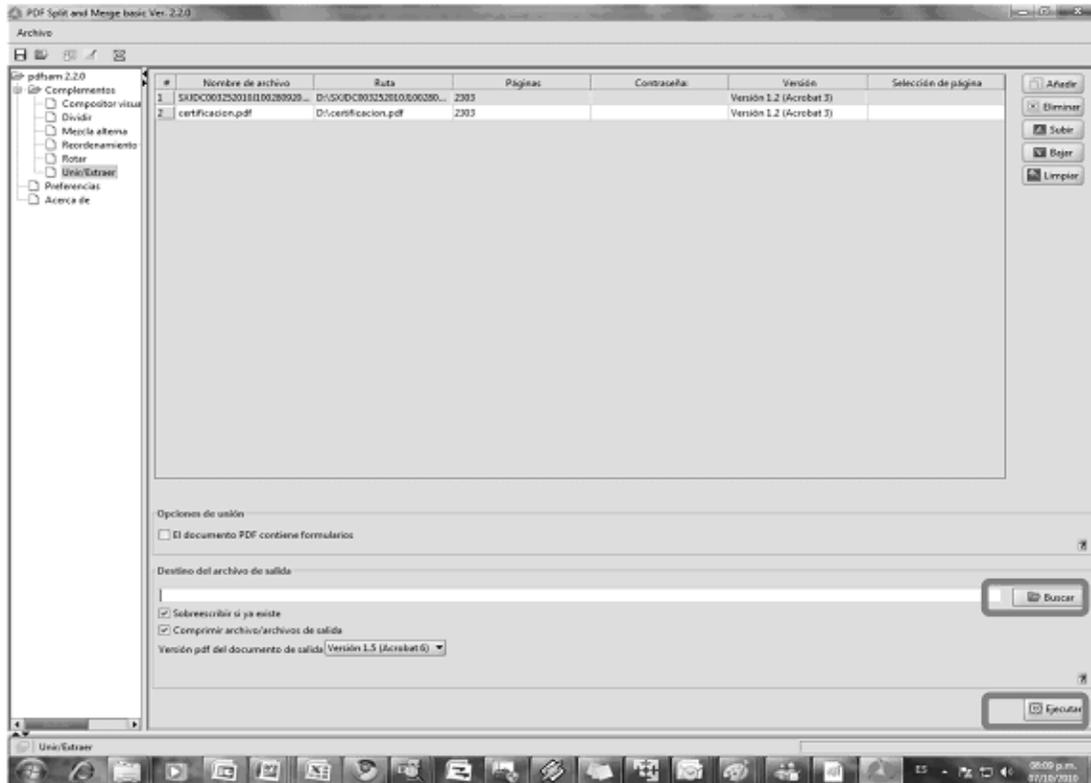


**VII.** Para añadir el archivo de certificación, realizar el mismo proceso desde el inciso f) al i);

**VIII.** Una vez añadidos los archivos necesarios para completar el proceso, se capturará el nombre del archivo de salida (que será el asignado al archivo de la resolución o acuerdo).

**IX.** Localizar la ubicación donde se depositará el archivo resultante, que preferentemente, será en una carpeta de acceso común, y dar clic en **“Buscar”**

**X.** Finalmente, dar clic en **“Ejecutar”** e inmediatamente iniciará el proceso **“Unir”**, dando como resultado el archivo de la resolución o acuerdo con la certificación integrada.

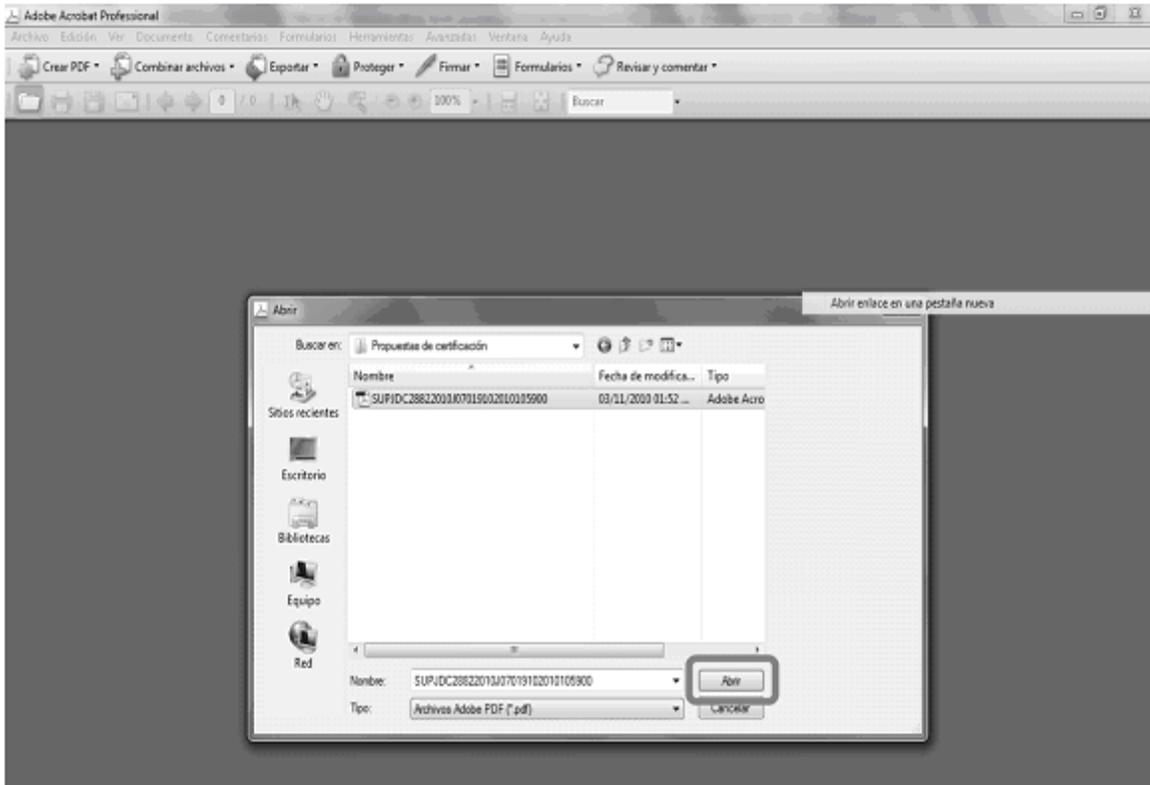


**8.2.** Para **firmar electrónicamente la propuesta de certificación**, el Secretario o Subsecretario General de Acuerdos, deberán:

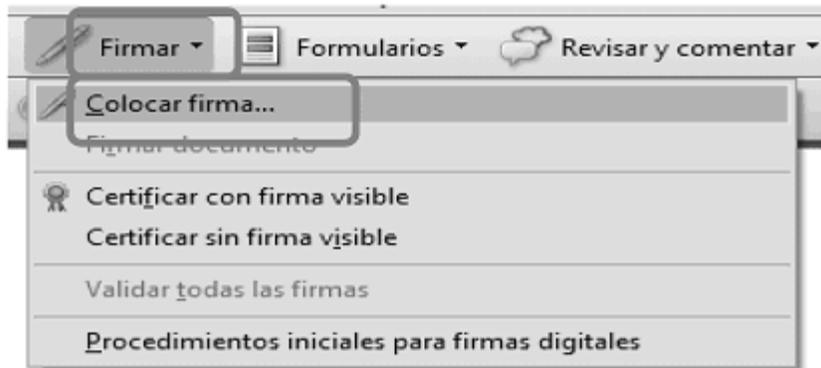
**8.2.1.** Abrir la carpeta de acceso común.



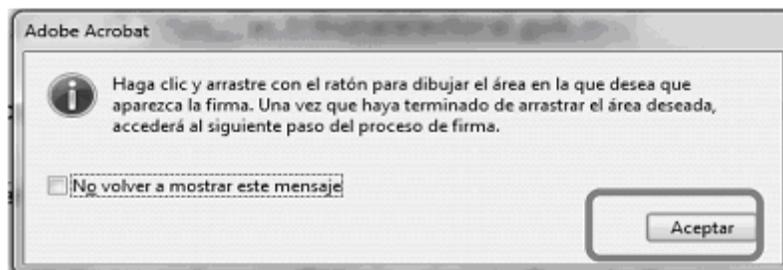
8.2.2. Seleccionar y abrir el archivo respectivo.



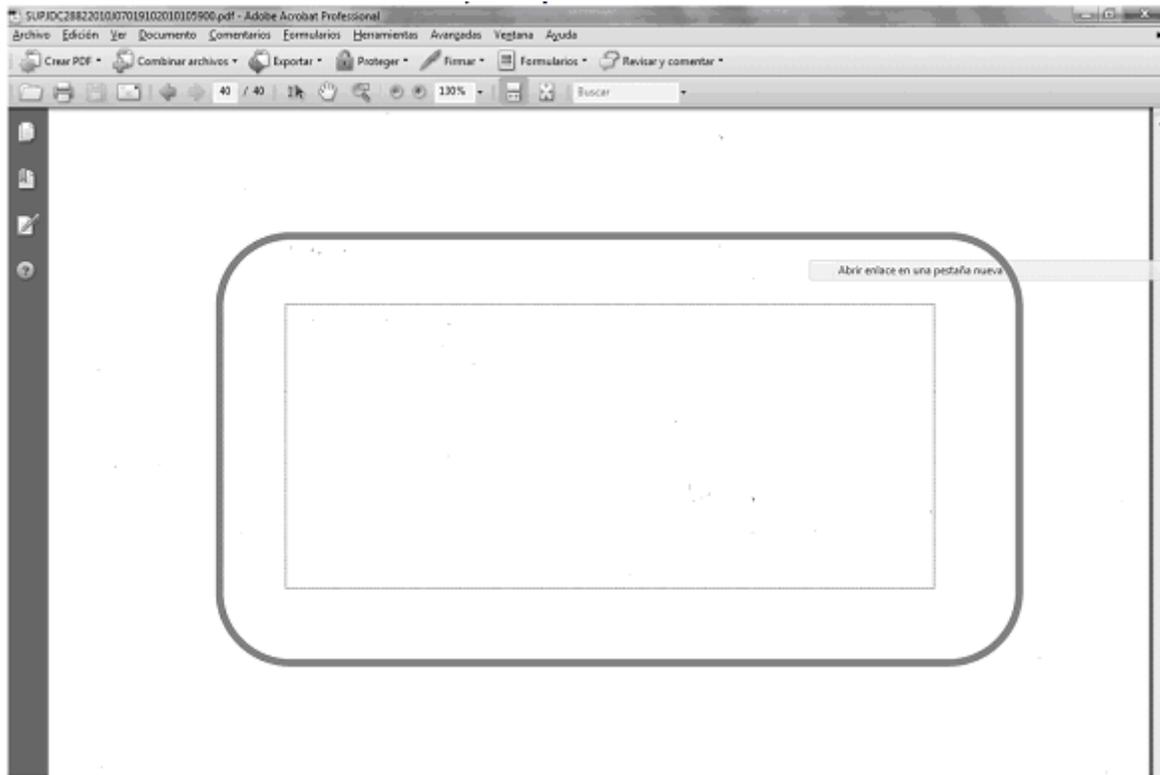
8.2.3. Abierto el documento, dar clic en “Firmar”, y de la lista de opciones desplegadas, elegir “Colocar Firma”.



8.2.4. Dar clic en “Aceptar”.



8.2.5. Ubicar el puntero del ratón y dar clic para iniciar el dibujo del área donde deseamos que aparezca la firma.



8.2.6. Dar clic en el botón "Firmar".



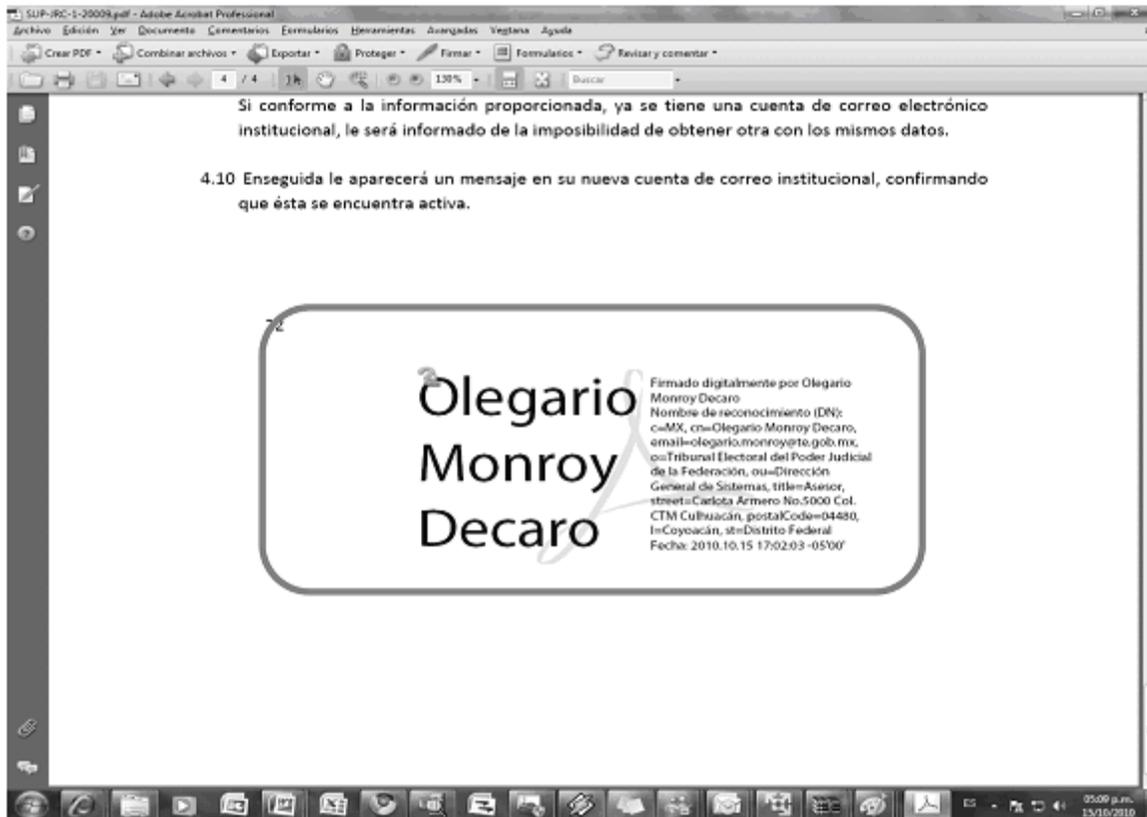
8.2.7. Indicar la ruta y el nombre con el cual se quiere grabar el archivo firmado y dar clic en “Guardar”.



8.2.8. Ingresar la contraseña correspondiente al Token.



8.2.9. Dar clic en el botón “OK” y la firma quedará insertada en el documento.



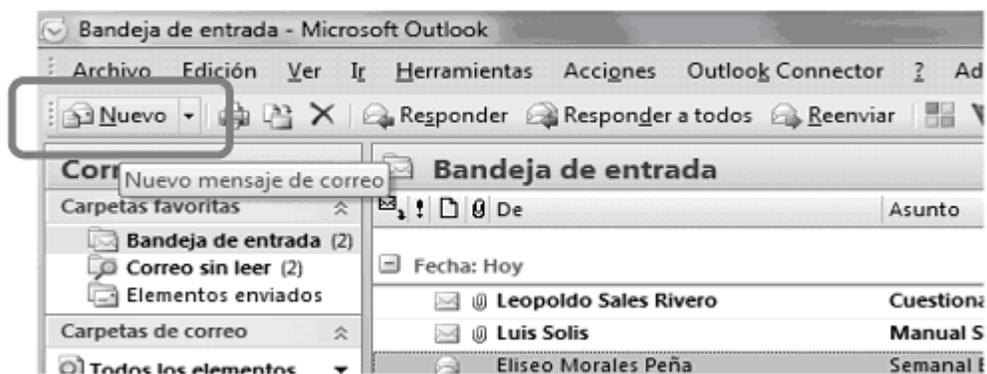
8.2.10. Cerrar el documento.

## 9. REALIZACIÓN DE LAS NOTIFICACIONES ELECTRÓNICAS

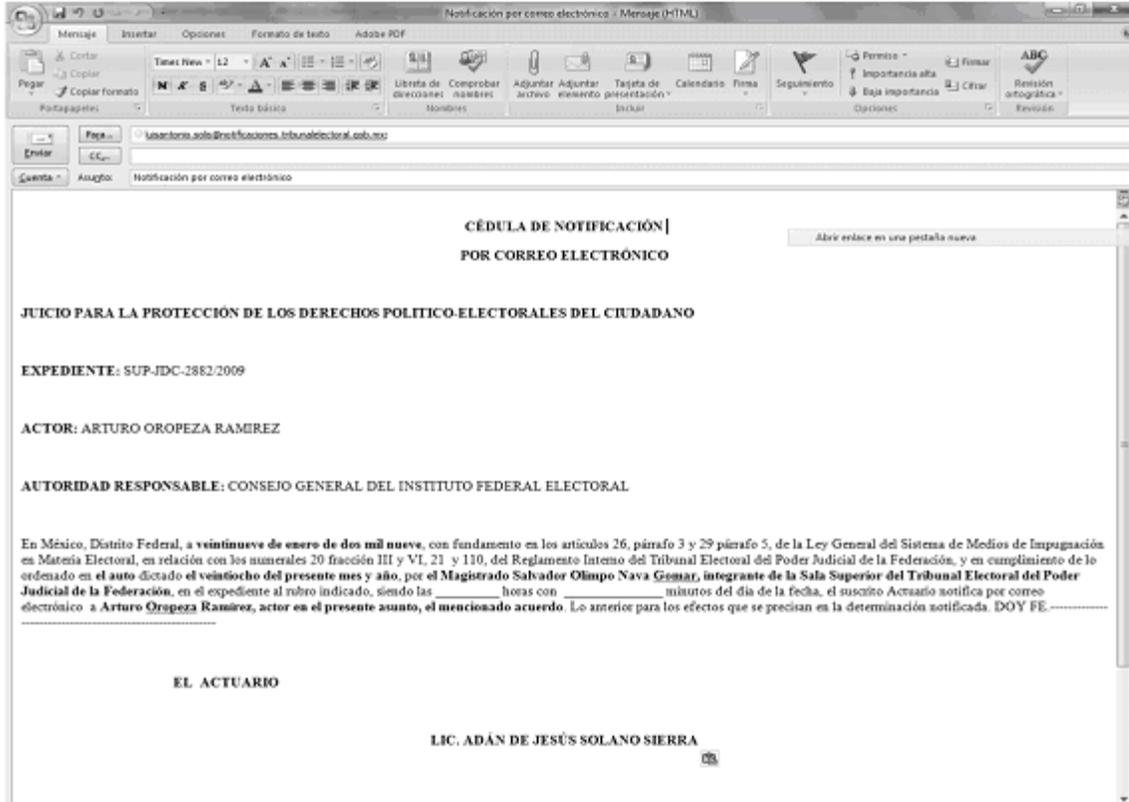
9.1. Para realizar las notificaciones por correo electrónico, los Actuarios deberán:

9.1.1. Ingresar a su cuenta institucional de correo electrónico.

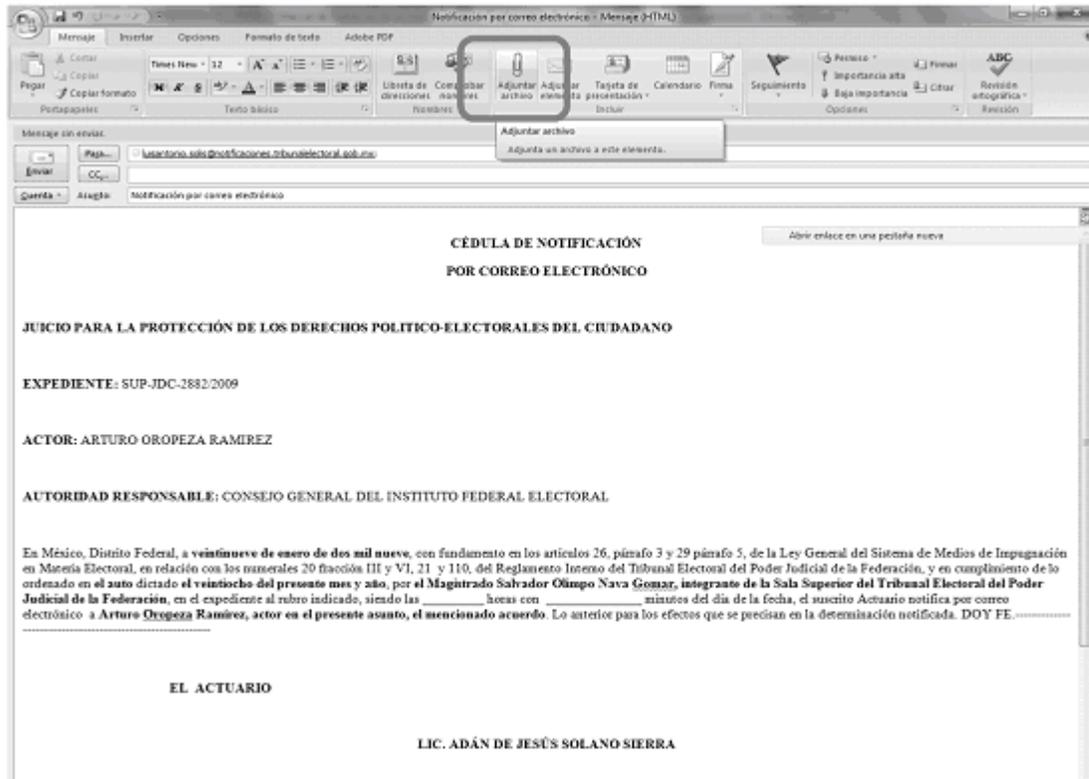
9.1.2. Dar clic en “Nuevo”.



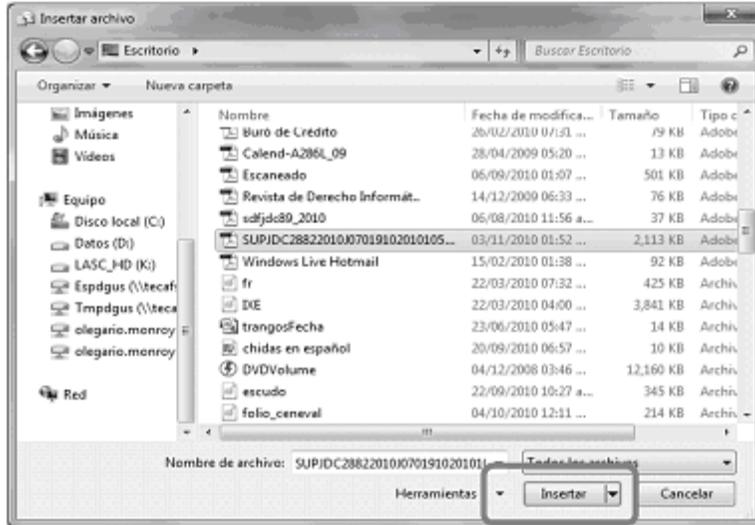
9.1.3. Redactar, en el espacio correspondiente, la **cédula de notificación por correo electrónico**.



9.1.4. Dar clic en el ícono "Adjuntar archivo".



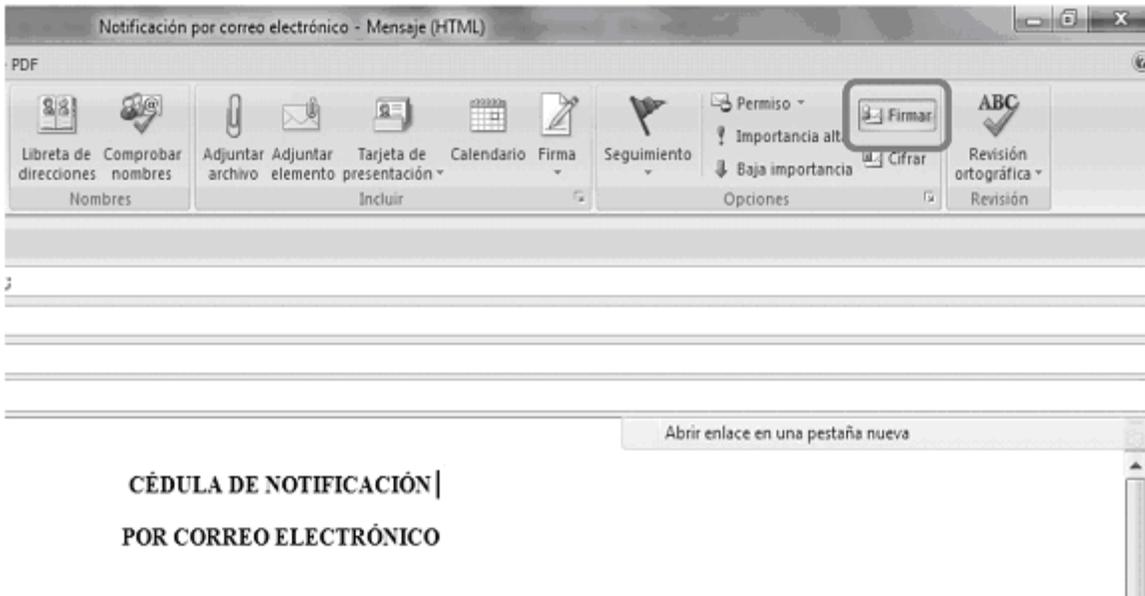
9.1.5. Seleccionar el archivo o archivos que se desean adjuntar y dar clic en “Insertar”.



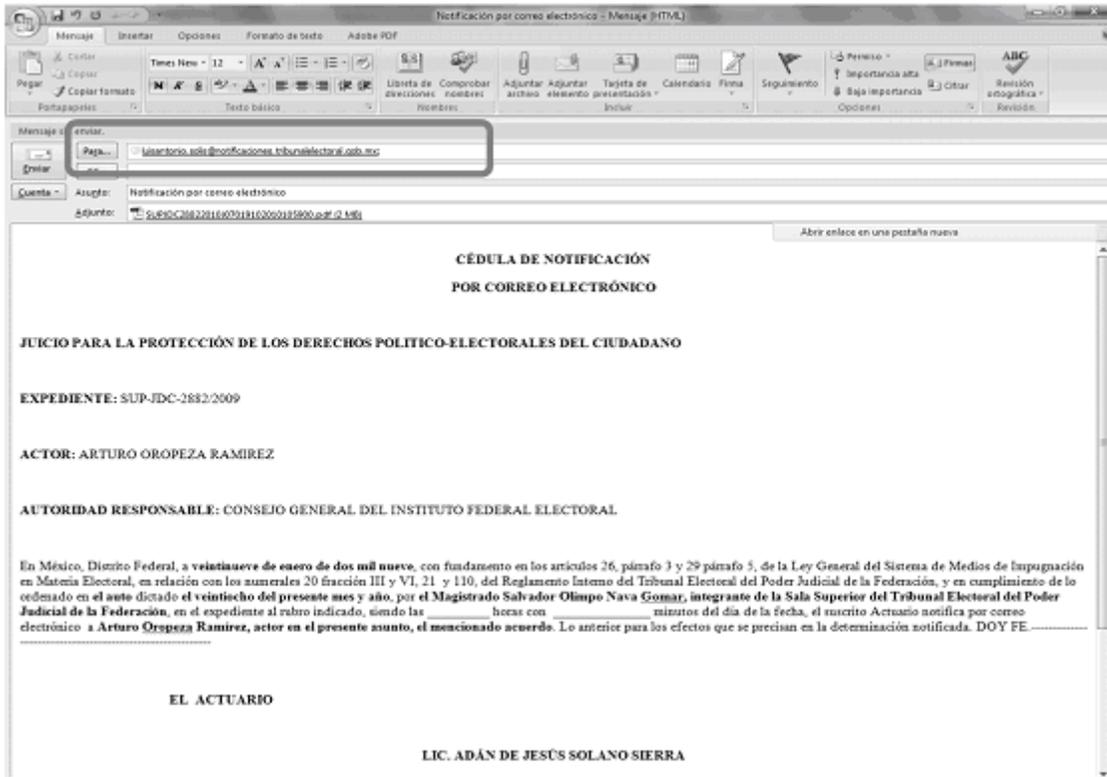
9.1.6. Insertar en el equipo de cómputo su Token.



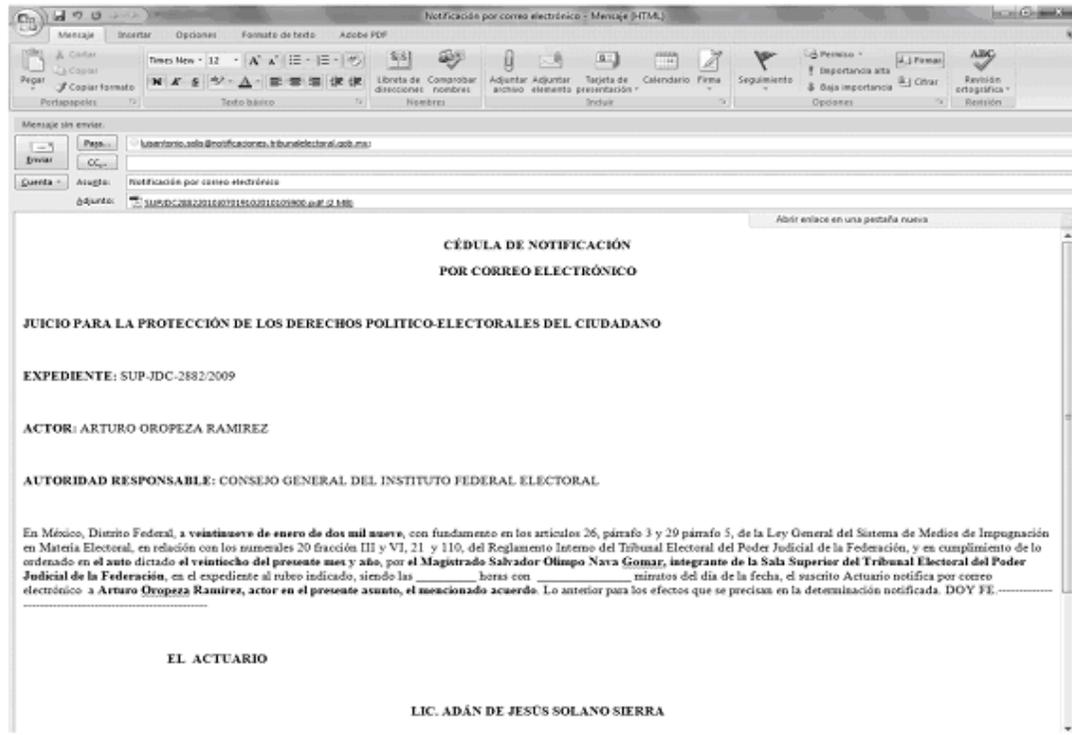
9.1.7. Dar clic en “Firmar”, para firmar el correo electrónico.



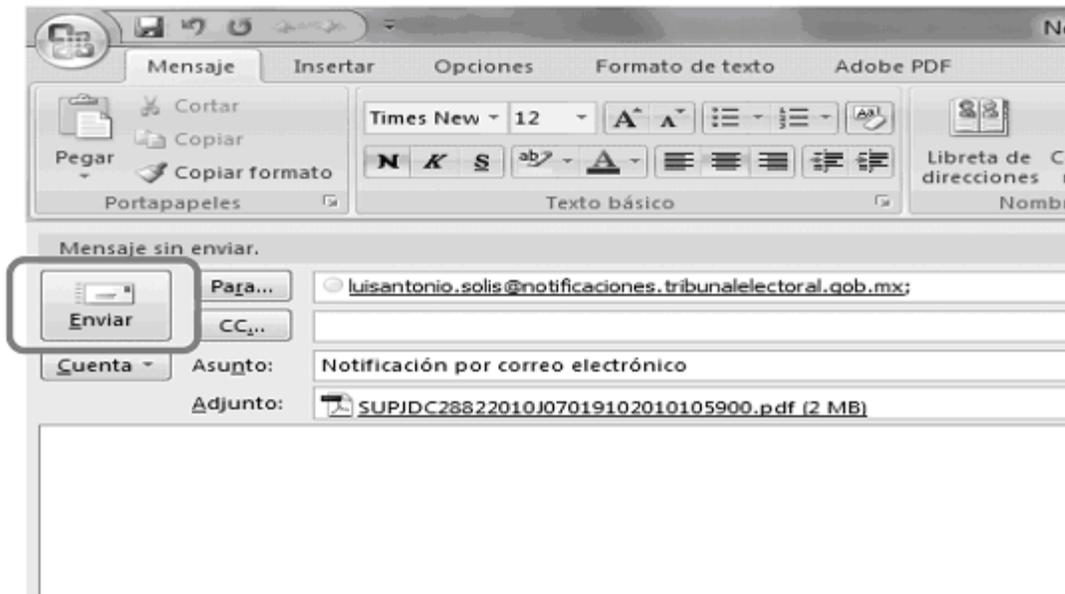
9.1.8. En el espacio correspondiente “Para” redactar la cuenta o cuentas de correo electrónico a quien va dirigida la notificación.



9.1.9. Verificar los datos del correo, destinatarios, archivo o archivos adjuntos y cédula de notificación electrónica firmada.



9.1.10. Dar clic en “Enviar”.



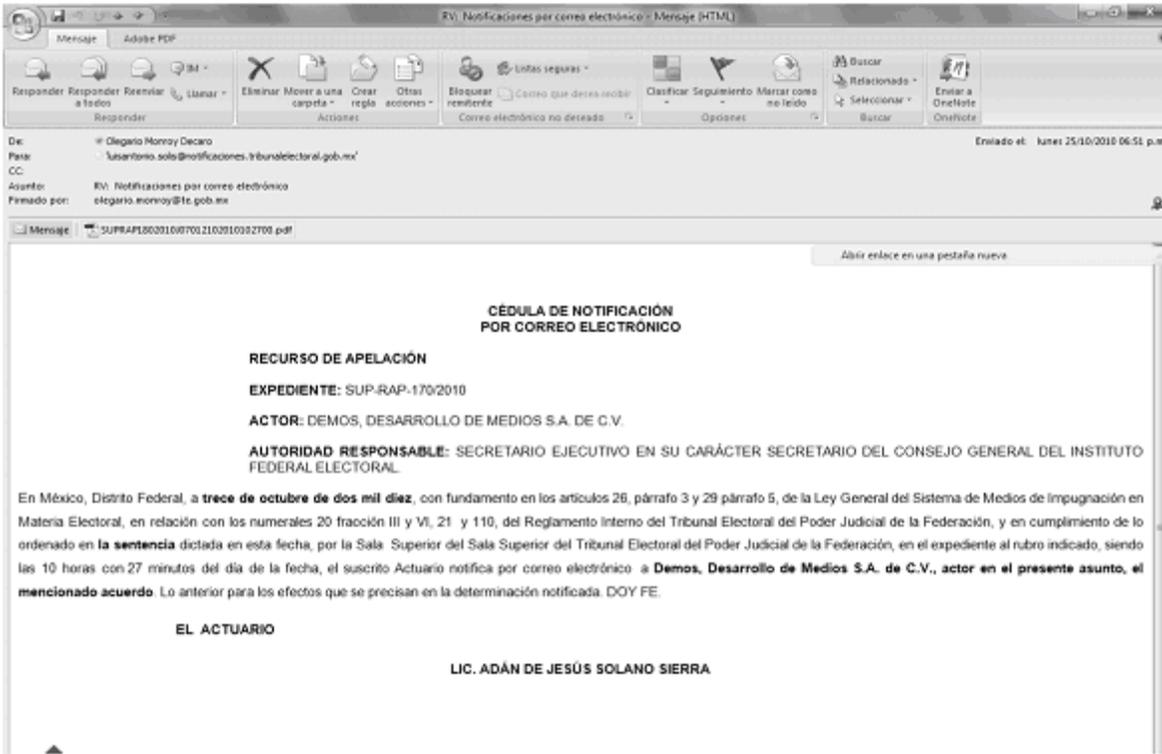
9.1.1. Ingresar la contraseña del Token y dar clic en “OK”.



9.1.12. Dar clic en la bandeja “Elementos enviados”.



9.1.13. Localizar el correo enviado y dar doble clic sobre el mismo.



9.1.14. Seleccionar en el menú principal la opción "Imprimir" para poder obtener copia del correo.



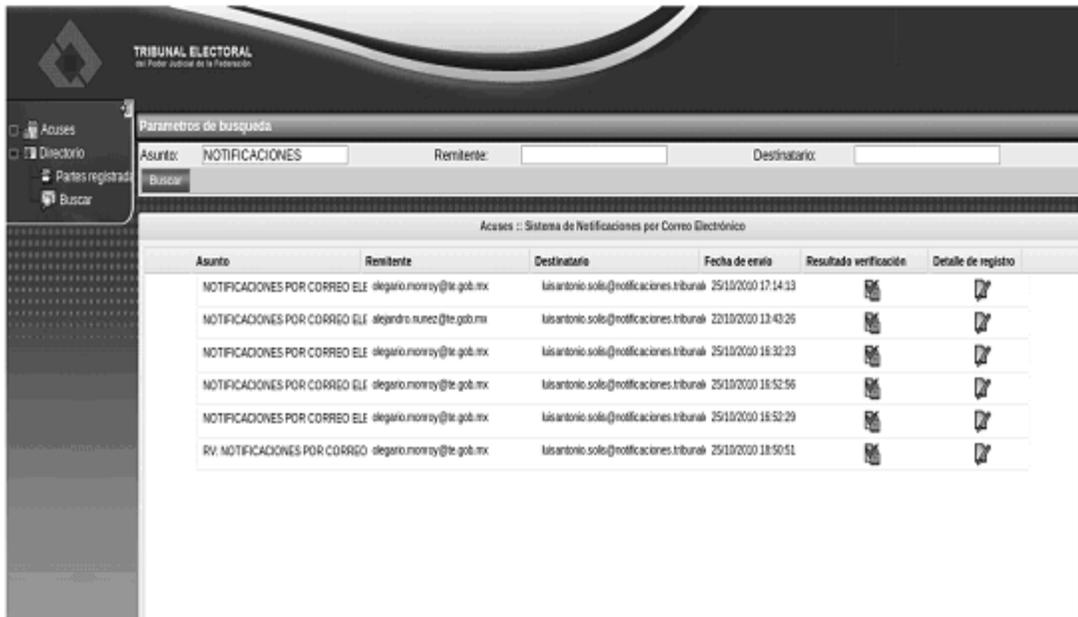
9.1.15. Firmar autógrafamente la impresión.

**10. DESCARGA DE LA CONSTANCIA DE ENVÍO Y ACUSE DE RECIBIDO**

10.1. Para **descargar la constancia de envío y acuse de recibido**, una vez realizada la notificación por correo electrónico, el Actuario deberá:

10.1.1. Acceder al Sistema, mediante la siguiente liga:  
<http://notificaciones.tribunalelectoral.gob.mx/actuario>.

10.1.2. Ingresado al sistema podrá visualizar los acuses de los correos electrónicos enviados.



10.1.3. Seleccionar el o los filtros deseados y capturar la información para identificar el correo.

10.1.4. Dar clic en “**Buscar**”.

10.1.5. Dar clic sobre el ícono “**Detalle de registro**” del correo correspondiente y se desplegará, de forma detallada, la información contenida en el correo.



10.1.6. Dar clic en la opción “**imprimir**”, para obtener las constancia de envío y acuse de recibido.

**11. ELABORACIÓN DE LA RAZÓN DE NOTIFICACIÓN POR CORREO ELECTRÓNICO**

11.1. La razón de notificación por correo electrónico, será elaborada por el Actuario con base en:

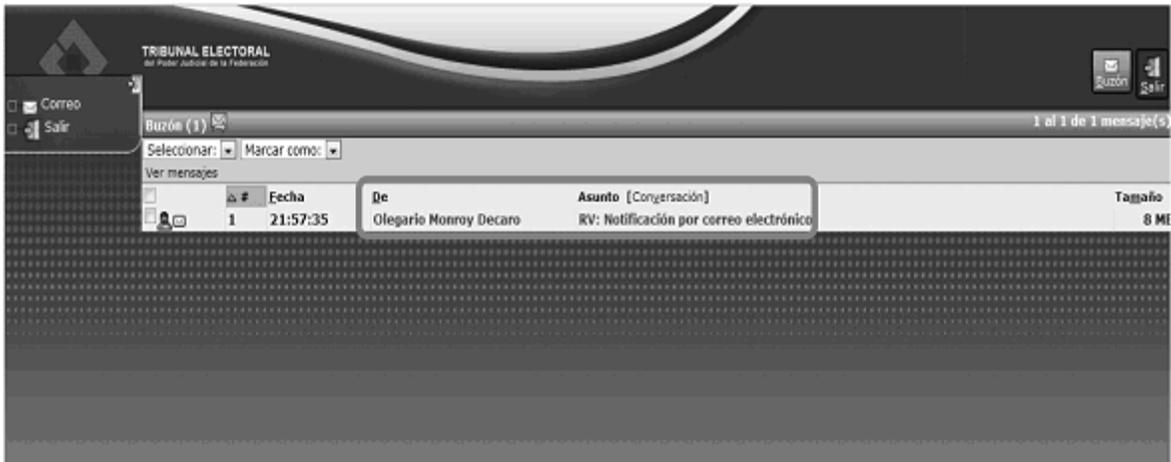
- I. La impresión del correo electrónico enviado;
- II. La impresión de la constancia de envío y acuse de recibo, y
- III. Las impresiones, a que se refieren los puntos que anteceden, se anexarán a la razón a efecto de que sean integradas, junto con ésta, al expediente correspondiente.

**12. CONOCIMIENTO Y DESCARGA DE LAS NOTIFICACIONES ELECTRÓNICAS POR LAS PARTES.**

12.1. Para **conocer y descargar** el contenido de la notificación por correo electrónico, las partes deberán Ingresar a la página web del Tribunal, acceder al Sistema, capturar su cuenta institucional de correo y contraseña, y dar clic en “**Iniciar sesión**”.



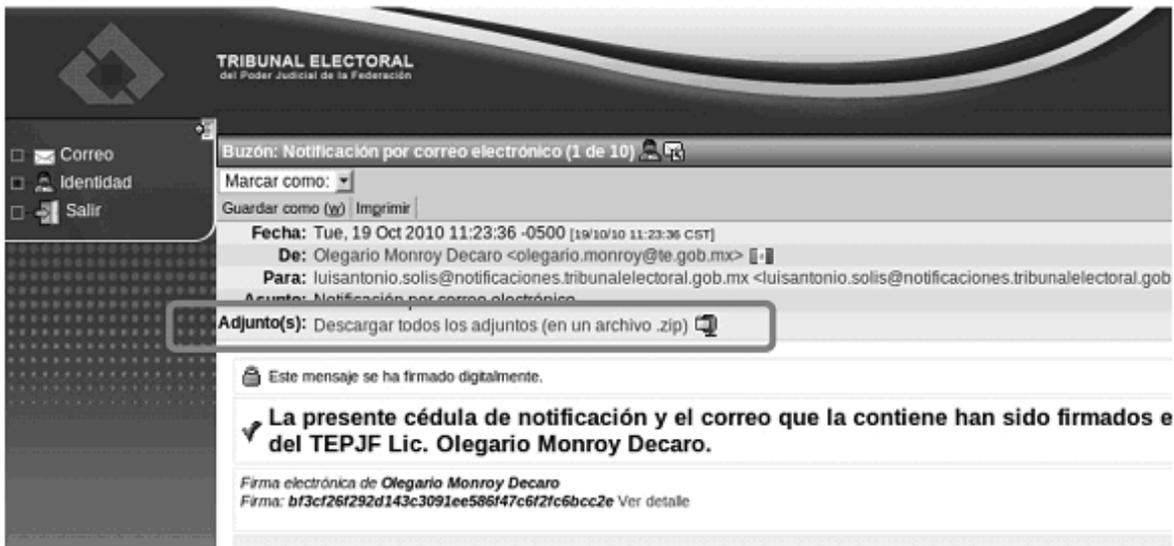
12.2. El sistema presentará los correos con las notificaciones electrónicas que el Tribunal le ha enviado a su cuenta institucional de correo que señaló en su demanda o promoción.



12.3. Darán clic en la columna “De” o “Asunto” del correo electrónico para visualizar el detalle de la notificación electrónica.



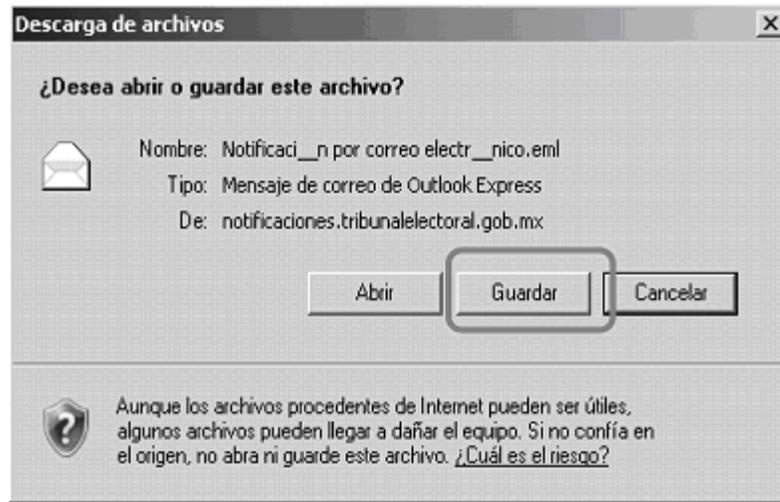
12.4. Para descargar los archivos adjuntos de la notificación, deberán dar clic en el hipervínculo ubicado después de la etiqueta “Adjunto(s)”.



12.5. Para guardar la información del correo y todo su contenido, darán clic en “Guardar Como (w)”.



12.6. El sistema preguntará si se desea abrir o guardar el archivo y presionará la opción “**Guardar**”



12.7. La información permanecerá en la bandeja de entrada durante 30 días naturales, después será borrada.

### 13. DEPURACIÓN Y RESPALDO DE LA INFORMACIÓN GENERADA CON MOTIVO DE LAS NOTIFICACIONES ELECTRÓNICAS.

13.1. El sistema ejecutará una tarea sobre los buzones de los usuarios para depurar las notificaciones al día 31 de la recepción.

13.2. Se realizará **respaldo incremental de la información** cada 24 Hrs. en dos partes;

13.2.1. En la primera, el sistema genera, de manera automática, una copia completa de cada una de las notificaciones electrónicas en archivo de texto en formato MIME.

13.2.2. El nombre de los archivos que contiene cada una de las notificaciones electrónicas está formado por fecha, hora y un identificador de archivo alfanumérico, como se muestra a continuación:

**20101015123329ATX6898418852341117327.MIME**

13.2.3 Las copias se generan con fines de respaldo de las notificaciones electrónicas y se almacenarán en el directorio /respaldo\_notificaciones.

13.2.4 La Dirección General de Sistemas realizará el respaldo de los archivos relativos a las notificaciones electrónicas contenidos en el directorio /respaldo\_notificaciones

13.2.5 En la segunda, el respaldo corresponde a la base de datos del sistema.

13.2.6 El administrador del sistema realizará una copia de la información contenida en la base de datos del sistema de notificaciones.

13.2.7 El respaldo de información del sistema de notificaciones electrónicas serán almacenados en el centro de cómputo del Tribunal Electoral.

13.2.8 Se realizará una copia del respaldo como parte del esquema de continuidad de operaciones de la Dirección General de Sistemas.

### 14. VALIDACIÓN Y AUTENTICACIÓN DE LAS NOTIFICACIONES ELECTRÓNICAS

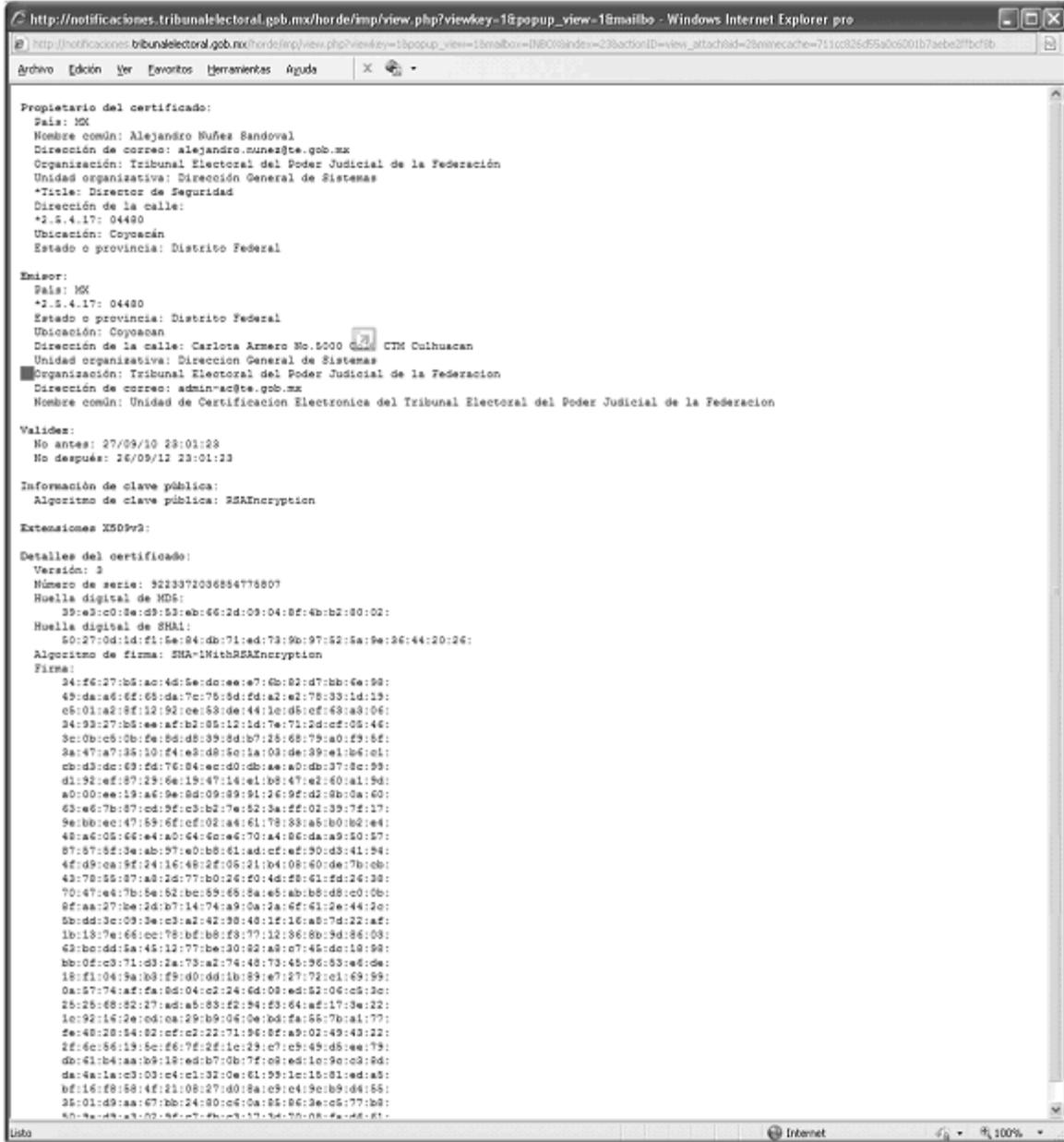
14.1. La validación de las notificaciones se realizará a través del sistema.

14.1.1. Desde el buzón podrá obtenerse el estado de validación de cada una de las notificaciones, para esto, deberá seleccionarse del listado, las notificaciones que se quiera validar su autenticidad.

14.1.2. Al desplegarse el correo electrónico de la notificación, también se desplegará la validación.



14.1.6 La información que se despliegue deberá corresponder al certificado de firma electrónica avanzada del Actuario que ejecutó la notificación.



14.1.7 En caso que el sistema identifique algún problema con el emisor de la notificación electrónica, ésta omitirá la indicación correspondiente.

14.2 Para proveer mayor certeza a las acciones realizadas, el sistema proporcionará mecanismos de validación al acuse de la notificación electrónica, para esto se deberá hacer uso de la sección de **acuses**.



14.2.1 Conforme al procedimiento indicado en la sección 10, de este manual, se deberá ingresar a los detalles de la notificación de interés y descargará el archivo en formato **de timestamp**, que corresponda a la notificación.

**DETALLE DE CORREO** X

Asunto	SUP-JDC-2882/2009
Remitente	alejandro.nunez@te.gob.mx
Destinatario	actuario@notificaciones.tribunalelectoral.gob.mx
Fecha de recibido	25/10/2010 11:22:11 (Hora del centro)
Hash	kYOuMJ9rHP3kb2oUOmBOGijz8h4=
Estatus	Valido
Firma	dSpWFEQSP1XMsU9tPCr3ti5hDbyMUiom++gFyg7i0i4MM49g8ssZSrbLVXoUQbluxx8L+aqke3bNd3+blOGKQ7r6fJBfK1zwhl0Ort9JoF33esDnRzhMRk2JwH2pOm8JTjMsSiz+rXwXlke27vJ3YmOCnHW5EirMravuJNL8u8QtsXJP2BuU2WyaATg1YLrpxROZ1gHmOlrTyO1Q3g6d4QmINJX3oJhUuszNk51+OCaHHQEuv5n9NXkY+s4lOou6jAMJ05AxqViZMQyPvahZ1pOtmwOB+niEakKBk8AZw/4wIUuEQuqxNtm3F4sHRvgwuUDpLXF6ParsF5UvEYcNlpg==

**Correo**

**CÉDULA DE NOTIFICACIÓN**

**POR CORREO ELECTRÓNICO**

**JUICIO PARA LA PROTECCIÓN DE LOS DERECHOS POLITICO-ELECTORALES DEL CIUDADANO**

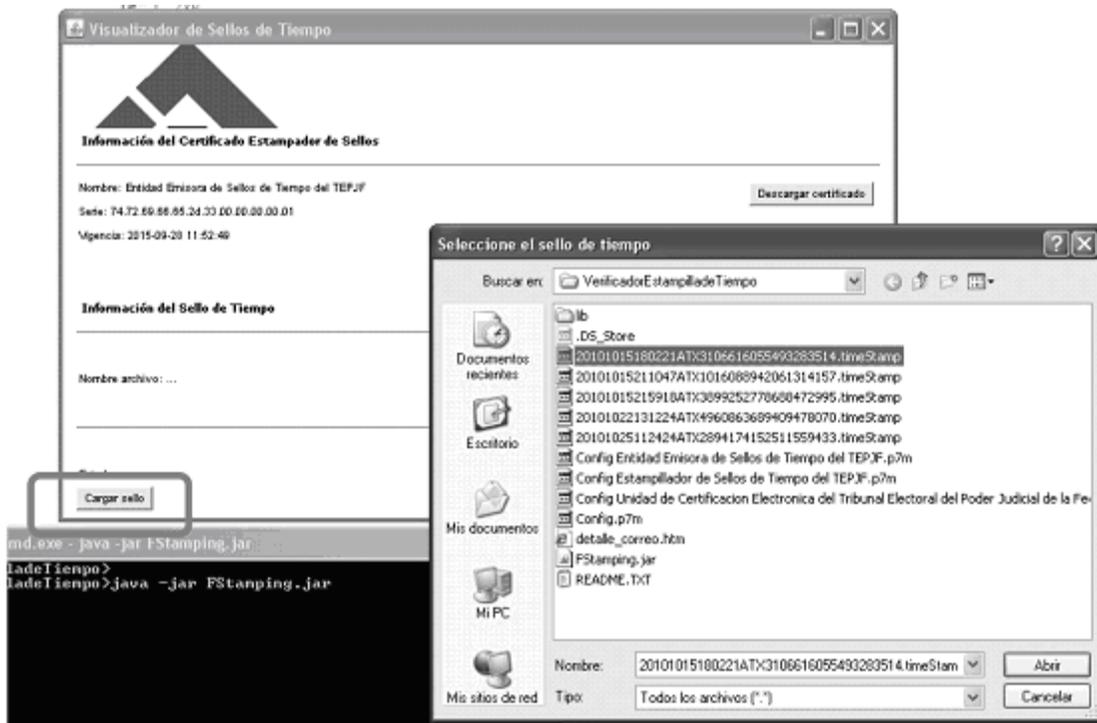
**EXPEDIENTE: SUP-JDC-2882/2009**

Descargar timestamp	Timestamp
Descargar correo	Correo
Imprimir	Imprimir

**14.2.2** A través de una línea de comando ejecutará el programa de validación de estampilla de tiempo **FStamping.jar**, que forma parte de la suite de validación de archivos de la Unidad de Certificación Electrónica.

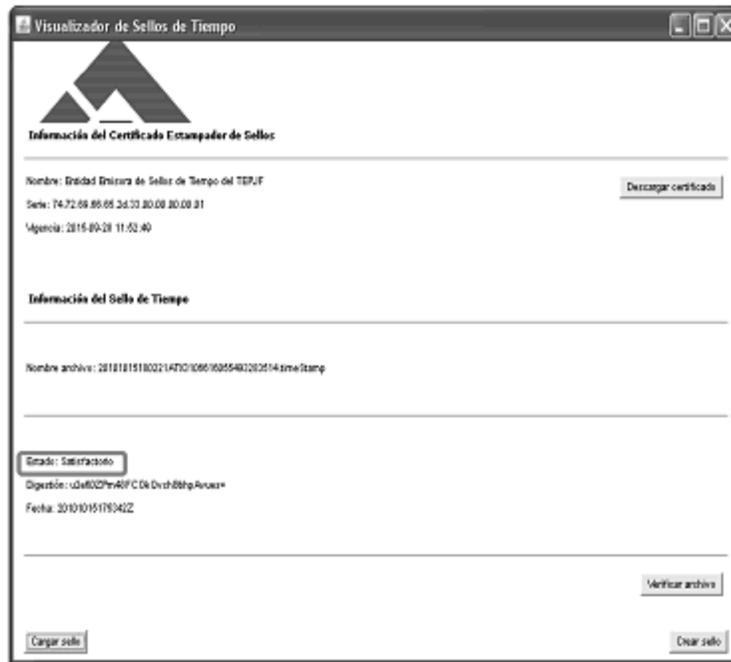


**14.2.3** El programa de validación de estampado de sellos permitirá realizar una validación adicional sobre el acuse de recibido, para ello se deberá cargar el archivo de estampado de firma en el aplicativo a través de la opción **“cargar sello”**.

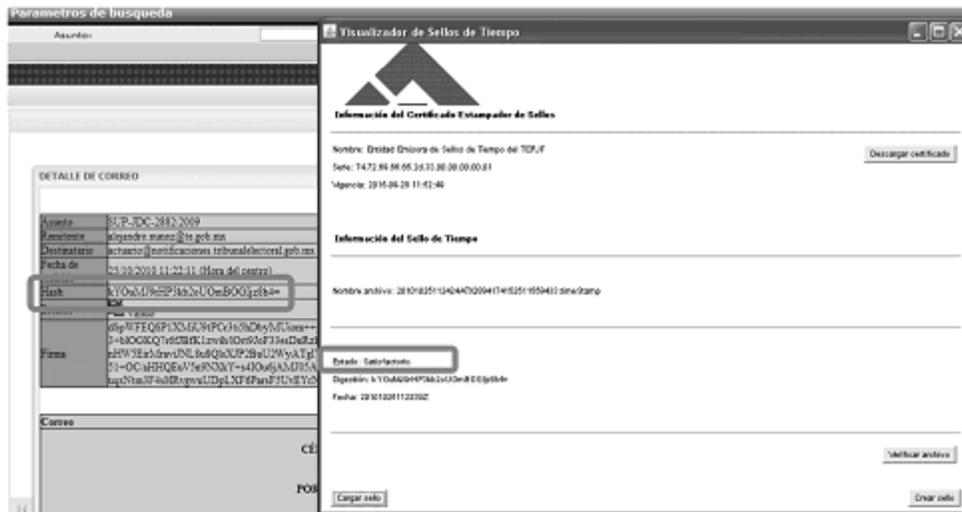


14.2.4 Al cargar el archivo de sello de tiempo, el programa verificará que la firma corresponda al certificado del servicio de "timestamping" con el que se firman los sellos del Tribunal Electoral.

14.2.5 En caso afirmativo el aplicativo mostrará los datos de validación satisfactoria.



14.2.6 La aplicación desplegará la huella digital (hash) del archivo que deberá ser comparada con la correspondiente que se despliega en el detalle del acuse en el sistema de notificaciones.



14.2.3 A través de estos mecanismos de validación se proporcionará la certeza necesaria que se requiere en la recepción de una notificación vía correo electrónico.

EL SUSCRITO, **RAFAEL ELIZONDO GASPERIN**, SUBSECRETARIO GENERAL DE ACUERDOS DE LA SALA SUPERIOR DEL TRIBUNAL ELECTORAL DEL PODER JUDICIAL DE LA FEDERACION, CERTIFICA: Que la presente copia, en ciento catorce folios, debidamente cotejados y sellados, son copia fiel y exacta del Acuerdo General de la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación número **5/2010**, de veintisiete de octubre de dos mil diez, por el que se aprueban las Prácticas de Certificación de la Unidad de Certificación Electrónica y el Manual de Operación de las Notificaciones por Correo Electrónico, y de sus anexos.

Lo que certifico en ejercicio de las facultades previstas en los artículos 202, de la Ley Orgánica del Poder Judicial de la Federación, así como 14, fracción IV, del Reglamento Interno de este Tribunal Electoral, para los efectos legales procedentes.- DOY FE.- México, Distrito Federal, a cuatro de noviembre de dos mil diez.- Rúbrica.