POLÍTICAS PARA LA OBTENCIÓN Y USO DE LA FIRMA ELECTRÓNICA CERTIFICADA DEL PODER JUDICIAL DE LA FEDERACIÓN (FIREL), ASÍ COMO PARA LA OPERACIÓN DE SU INFRAESTRUCTURA TECNOLÓGICA.

1. Aspectos generales.

1.1. Introducción.

El presente documento corresponde a la Política de Certificación (CP por sus siglas en inglés "*Certificate Policy*"), y contiene las políticas que rigen a la Autoridad Certificadora Raíz del Poder Judicial de la Federación así como a las Autoridades Certificadoras Intermedias de la Suprema Corte de Justicia de la Nación, del Tribunal Electoral del Poder Judicial de la Federación y del Consejo de la Judicatura Federal, para llevar a cabo la operación y administración de la Infraestructura de Llave Pública con base en lo dispuesto en el *ACUERDO GENERAL CONJUNTO NÚMERO 1/2013, DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, DEL TRIBUNAL ELECTORAL DEL PODER JUDICIAL DE LA FEDERACIÓN Y DEL CONSEJO DE LA JUDICATURA FEDERAL, RELATIVO A LA FIRMA ELECTRÓNICA CERTIFICADA DEL PODER JUDICIAL DE LA FEDERACIÓN (FIREL) Y AL EXPEDIENTE ELECTRÓNICO.*

La redacción de la presente Política de Certificación está basada en lo dispuesto por la IETF (*Internet Engineering Task Force*) en el documento de referencia RFC (Request For Comments) 3647, denominado "*Internet X.509 Public Key*

Infrastructure Certificate Policy and Certification Practice Framework". Asimismo, para el desarrollo del contenido se tomaron en cuenta los requisitos establecidos en la especificación técnica ETSI *(European Telecommunications Standards Institute) TS 102 042 v2.1.1 (2009-05) – "Electronic Signatures and Infrastructure (ESI); Policy requirements for certification authorities issuing public key certificate".*

1.2. Glosario.

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

1.2.2. **Agente Certificador:** El Servidor Público del PJF por conducto del cual actuará la Unidad de Certificación correspondiente para tramitar la emisión, renovación y revocación de Certificados Digitales de la FIREL.

1.2.3. **Áreas Técnicas:** Las Direcciones Generales de Tecnologías de la Información (DGTI) de la SCJN y del CJF, y de Sistemas (DGS) del TE.

1.2.4. **Autoridad Certificadora del CJF:** La DGTI del CJF, a la que corresponde administrar la infraestructura tecnológica para proporcionar Servicios Relacionados con la FIREL.

1.2.5. **Autoridad Certificadora de la SCJN:** La DGTI de la SCJN, a la que corresponde administrar la infraestructura

tecnológica para proporcionar Servicios Relacionados con la FIREL.

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

1.2.7. **Autoridades Certificadoras Intermedias:** Las autoridades certificadoras de la SCJN, del TE y del CJF.

1.2.8. **Centros de Datos:** Las instalaciones de la SCJN, del TE y del CJF, en donde se alojan los equipos e infraestructura que soportan los Servicios Relacionados con la FIREL y el Sistema Electrónico.

1.2.9. **Certificado Digital de la FIREL:** El Documento Electrónico expedido por alguna de las Autoridades Certificadoras Intermedias que asocia de manera segura y fiable la identidad del Firmante con una Llave Pública, permitiendo con ello identificar quién es el autor o emisor de un Documento Electrónico remitido mediante el uso de la FIREL.

1.2.10. **Certificado Intermedio:** El certificado digital generado a partir del Certificado Raíz del PJF con el cual se emiten los certificados de los usuarios finales.

1.2.11. **Certificado Raíz del PJF:** El certificado digital único emitido por la Unidad del Poder Judicial de la Federación para el Control de Certificación de Firmas, que sirve de base a la infraestructura de firma electrónica de los órganos del Poder

Judicial de la Federación y da origen a los certificados intermedios, los que a su vez servirán para generar los certificados digitales de la FIREL que emitan las Unidades de Certificación correspondientes.

1.2.12. **Certificado Intermedio del CJF:** El Documento Electrónico emitido por la Autoridad Certificadora Raíz del PJF, a partir del cual la Unidad Certificadora del CJF generará los certificados digitales de la FIREL.

1.2.13. **Certificado Intermedio de la SCJN:** El Documento Electrónico emitido por la Autoridad Certificadora Raíz del PJF, a partir del cual la Unidad Certificadora de la SCJN generará los certificados digitales de la FIREL.

1.2.14. **Certificado Intermedio del TE:** El Documento Electrónico emitido por la Autoridad Certificadora Raíz del PJF, a partir del cual la Unidad Certificadora del TE generará los certificados digitales de la FIREL.

1.2.15. **CJF:** El Consejo de la Judicatura Federal.

1.2.16. **Clave de Acceso a la Llave Privada del Certificado Digital de la FIREL:** La cadena de caracteres alfanuméricos del conocimiento exclusivo del titular de un Certificado Digital de la FIREL, que le permite utilizar la Llave Privada para firmar un documento electrónico o, en su caso, para acceder a diversos sistemas que establezcan la SCJN, el TE y el CJF.

1.2.17. **Clave de Revocación:** La cadena de caracteres alfanuméricos que introduce de manera secreta el Firmante durante la solicitud de un Certificado Digital de la FIREL, y que

deberá capturarse al momento de requerir su revocación en línea.

1.2.18. **CURP:** La Clave Única de Registro de Población.

1.2.19. **Dispositivo de Seguridad:** El dispositivo electrónico asignado a los servidores públicos de la SCJN y del TE, para almacenar de forma segura su Llave Privada asociada a su Certificado Digital de la FIREL.

1.2.20. **Documento Electrónico:** El generado, consultado, modificado o procesado por Medios Electrónicos.

1.2.21. **Duplicidad:** La coincidencia plena de la cadena de caracteres correspondiente a la Llave Pública de dos Certificados Digitales de Firma Electrónica, cuya actualización es de mínima probabilidad.

1.2.22. **FIPS** *(Federal Information Processing Standards)***:** Los estándares de referencia internacional. El FIPS 140-2 nivel 3 está enfocado a la acreditación de la seguridad de módulos criptográficos.

1.2.23. **FIREL:** La Firma Electrónica Certificada del Poder Judicial de la Federación.

1.2.24. **Firmante:** La persona física que utiliza su Certificado Digital de la FIREL para suscribir documentos electrónicos y, en su caso, mensajes de datos.

1.2.25. **Hardware:** Los componentes que integran la parte material de una computadora.

1.2.26. **Justiciable:** La persona física que solicite la expedición de un Certificado Digital de la FIREL, distinta a los servidores públicos del PJF.

1.2.27. **Llave Privada:** Los datos que el Firmante genera de manera secreta y bajo su estricto control al solicitar el Certificado Digital de la FIREL, contenidos en el Dispositivo de Seguridad, en cualquier otro dispositivo o en su equipo de cómputo, vinculados de manera única y complementaria con su Llave Pública.

1.2.28. **Llave Pública:** Los datos contenidos en un Certificado Digital de la FIREL que permiten la verificación de la autenticidad de la FIREL del Firmante.

1.2.29. **Medios de Comunicación Electrónica:** La infraestructura tecnológica que permite efectuar la transmisión y recepción de mensajes de datos y de documentos electrónicos.

1.2.30. **Medios Electrónicos:** La herramienta tecnológica relacionada con el procesamiento, impresión, despliegue, traslado, conservación y, en su caso, modificación de información.

1.2.31. **Mensaje de Datos:** La información generada, enviada, recibida, archivada o comunicada a través de Medios de Comunicación Electrónica, que puede contener documentos electrónicos.

1.2.32. **Módulo Criptográfico:** El dispositivo basado en Hardware que genera, almacena y protege llaves criptográficas.

1.2.33. **OCSP** (*Online Certificate Status Protocol*)**:** El protocolo para la verificación en línea del estado del Certificado Digital de la FIREL.

1.2.34. **OID** (*Object Identifier*)**:** El identificador de las presentes Políticas de certificación que fue asignado por la Unidad a partir del otorgado a la Autoridad Certificadora Raíz del PJF, siendo este último el 2.16.484.101.3.

1.2.35. **PFX (***Personal Information Exchange***):** El archivo de intercambio de información que contiene las llaves pública y privada de un Certificado Digital de la FIREL, el cual se encuentra protegido por una contraseña.

1.2.36. **PJF:** El Poder Judicial de la Federación.

1.2.37. **Políticas:** Las directrices que rigen la actuación de la Autoridad Certificadora Raíz del PJF y de las Autoridades Certificadoras Intermedias.

1.2.38. **SCJN:** La Suprema Corte de Justicia de la Nación.

1.2.39. **Sello de tiempo:** Cadena de caracteres emitidos por una TSA que indican la hora y fecha de cuándo se firmó, envió, recibió o consultó un Mensaje de Datos.

1.2.40. **Servidor Público del PJF:** El servidor público adscrito a cualquiera de los órganos jurisdiccionales y administrativos del PJF.

1.2.41. **Servicios Relacionados con la FIREL:** Los servicios de firmado de documentos electrónicos; de verificación de la vigencia de los certificados digitales de la FIREL; de verificación y validación de la unicidad de la Llave Pública; de consulta de certificados digitales de la FIREL revocados, y los demás especificados en las presentes Políticas.

1.2.42. **Sistema AFIS (***Automatic Fingerprint Identification System***):** El Sistema del PJF para la Identificación Automatizada de Huellas Dactilares.

1.2.43. **SEPJF:** El Sistema Electrónico del PJF.

1.2.44. **TE:** El Tribunal Electoral del Poder Judicial de la Federación.

1.2.45. **Tribunales de Circuito:** Los Tribunales Colegiados y Unitarios de Circuito.

1.2.46. **TSA (Time Stamping Authority):** La infraestructura tecnológica encargada de proporcionar, a través de sellos de tiempo, certeza sobre el momento en el que, en su caso, se firma, envía, recibe o consulta un Mensaje de Datos.

1.2.47. **Unidades Certificadoras Intermedias:** La Unidad de Certificación de la SCJN, del TE y del CJF.

1.2.48. **Unidad:** La Unidad del PJF para el Control de Certificación de Firmas conforme al artículo 7 del AGC 1/2013.

1.2.49. **Unidad de Certificación del CJF:** La Unidad para el Control de Certificación de Firmas, dependiente de la Dirección General de Estadística Judicial del CJF, responsable de llevar a cabo los procedimientos para la emisión, renovación, revocación y consulta de los certificados digitales de la FIREL, por sí o, en los términos de la normativa aplicable, por conducto de los agentes certificadores.

1.2.50. **Unidad de Certificación de la SCJN:** La DGTI, responsable de llevar a cabo los procedimientos para su emisión, renovación, revocación y consulta, por sí o, en los términos de la normativa aplicable, por conducto de los agentes certificadores adscritos a la Secretaría General de Acuerdos, respecto de los Justiciables y del área que designe el titular de la Oficialía Mayor, respecto de los servidores públicos de la SCJN.

1.2.51. **Unidad de Certificación del TE:** La Unidad de Certificación Electrónica como la responsable de administrar los procesos de emisión, renovación, consulta y revocación de certificados digitales de la infraestructura de firma electrónica del TE, así como los correspondientes de la FIREL por conducto de los agentes certificadores.

1.2.52. **Usuario Final:** El Servidor Público del PJF o los justiciables que soliciten o hagan uso de un Certificado Digital de la FIREL.

1.2.53. **UTC (*Universal Time Coordinated*):** El tiempo universal coordinado, del inglés. Las zonas horarias del mundo toman como referencia el meridiano cero o meridiano de Greenwich y se expresan como desviaciones positivas o negativas. Para la Ciudad de México el horario correspondiente es -05:00 horas en horario de verano y -6:00 en horario de invierno. La fecha de vigencia de los certificados se expresa en formato UTC.

1.3. Marco legal.

1.3.1. Constitución Política de los Estados Unidos Mexicanos.

1.3.2. Ley Orgánica del Poder Judicial de la Federación.

1.3.3. Ley de Amparo, Reglamentaria de los artículos 103 y 107 de la Constitución Política de los Estados Unidos Mexicanos.

1.3.4. AGC 1/2013.

1.3.5. Reglamento Interno de la Unidad del Poder Judicial de la Federación para el Control de Certificación de Firmas, del veintiuno de noviembre de dos mil trece.

1.4. Nombre del documento e identificación.

1.4.1. **Título.** Políticas para la obtención y uso de la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL), así como para la operación de su infraestructura tecnológica.

1.4.2. **OID:** 2.16.484.101.3.1.1.

1.5. Uso válido de los certificados.

1.5.1. Certificado Raíz del PJF.

El Certificado Raíz del PJF únicamente será utilizado para la generación del Certificado Intermedio de la SCJN, del TE y del CJF.

1.5.2. Certificados Intermedios.

Los certificados intermedios únicamente serán utilizados para la generación de los certificados digitales de la FIREL para usuarios finales y para la operación de los Servicios Relacionados con la FIREL.

1.5.3. Certificados de usuarios finales.

Los certificados de usuarios finales serán utilizados para firmar electrónicamente los documentos que se presenten o que se generen en los procedimientos de la competencia de los órganos jurisdiccionales del PJF, así como para acceder y utilizar el Sistema Electrónico y los diversos sistemas informáticos que establezcan la SCJN, TE y el CJF.

1.6. Autoridad Certificadora Raíz del PJF.

La Autoridad Certificadora Raíz del PJF es el primer objeto de la cadena de certificación con la cual se emitirán, distribuirán y revocarán los certificados de las Autoridades Certificadoras Intermedias. La DGTI del CJF será la responsable de administrar la infraestructura tecnológica de dicha entidad.

1.6.1. **Funciones de la Unidad.**

La Unidad verificará que las actividades de las Unidades Certificadoras Intermedias se apeguen a las presentes Políticas.

1.6.2. **Características del Certificado Raíz del PJF.**

Las llaves pública y privada del Certificado Raíz del PJF deberán tener un tamaño de 4096 bits con algoritmo de firma RSA y algoritmo de digestión SHA-256; generarse dentro de un Módulo Criptográfico que cumpla con las especificaciones de seguridad del FIPS-140-2 nivel 3.

El Certificado Raíz del PJF deberá contener la siguiente información: Su Llave Pública; Nombre Distintivo acorde a lo definido en el numeral 3.1.1.

1.7. Autoridades Certificadoras Intermedias.

Las Unidades Certificadoras Intermedias deberán de operar y apegarse a las presentes Políticas para obtener el Certificado Intermedio correspondiente.

Las Autoridades Certificadoras Intermedias deberán cumplir los mismos niveles de seguridad y algoritmos que la Autoridad Certificadora Raíz del PJF, para mantener coherente la cadena de confianza de todas las autoridades certificadoras del PJF.

1.7.1. **Funciones de las Unidades Certificadoras Intermedias del PJF.**

Las Unidades Certificadoras Intermedias emitirán certificados a los usuarios finales siguiendo la cadena de confianza, como entidad de certificación acreditada por el PJF.

1.7.2. **Características de los Certificados Intermedios.**

La Llave Privada deberá tener un tamaño de 4096 bits con algoritmo de firma RSA y algoritmo de digestión SHA-256; generarse dentro de un Módulo Criptográfico que cumpla con las especificaciones de seguridad del FIPS-140-2 nivel 3. El Certificado Intermedio deberá contener la siguiente información: Su Llave Pública; Nombre Distintivo, acorde a lo definido en el numeral 3.1.2.

1.8. Agente Certificador.

Los agentes certificadores de las Unidades Certificadoras Intermedias deberán apegarse a las presentes Políticas. Únicamente podrán emitir y revocar certificados digitales de la FIREL para usuarios finales, con base en el Certificado Intermedio de la Unidad Certificadora Intermedia a la que se encuentre adscrito o, en su caso, auxilie.

1.9. Estandarización tecnológica.

Las Áreas Técnicas garantizarán el cumplimiento de condiciones de operación tecnológica estandarizada en sus sistemas informáticos, aplicaciones, trámites y servicios electrónicos de procesos administrativos y jurisdiccionales apegados a las presentes Políticas.

1.10. Lineamientos de administración.

1.10.1. Publicación y actualización de las presentes Políticas.

La Unidad es el órgano responsable de la aprobación y modificación del presente instrumento, previa opinión de las Áreas Técnicas en términos de lo previsto en los artículos 7, párrafo cuarto y 9, del AGC 1/2013.

1.10.2. Responsables técnicos.

Las Áreas Técnicas serán responsables de la correcta aplicación de las presentes Políticas en sus secciones 1.6, 1.7 y 1.9, por lo que ante cualquier duda o comentario sobre el particular, deberán someterlo a la consideración de la Unidad.

---

2. Transparencia.

2.1. Repositorios.

2.1.1. **Repositorio de la Unidad.**

El repositorio estará publicado en la dirección electrónica: http*://www.pjf.gob.mx/firel/* y contendrá la información especificada en la numeral 2.1.5.

2.1.2. **Repositorio de la Unidad de Certificación de la SCJN.**

La SCJN publicará la información especificada en el numeral 2.1.6 de las presentes Políticas en la dirección electrónica*: http://www.scjn.gob.mx/firmaelectronica/*

2.1.3. **Repositorio de la Unidad de Certificación del TE.**

El TE publicará la información especificada en el numeral 2.1.6 de las presentes Políticas en la dirección electrónica: *http://uce.te.gob.mx/PracticasCertificacion/*

2.1.4. **Repositorio de la Unidad de Certificación del CJF.**

El CJF publicará la información especificada en el numeral 2.1.6 de las presentes Políticas en la dirección electrónica: *http://www.uncocefi.cjf.gob.mx/PracticasCertificacion/*

2.1.5. **Publicación de información de la Unidad y su frecuencia.**

Los certificados y la información relativa a la Unidad se encontrarán disponibles en línea en la dirección electrónica indicada en el numeral 2.1.1, donde se podrá consultar, y en su caso, descargar:

2.1.5.1 El Certificado Raíz del PJF;

2.1.5.2 Los Certificados Intermedios emitidos por la Unidad;

2.1.5.3 La versión actualizada de las presentes políticas;

2.1.5.4 La información sobre los servicios relacionados con el uso de los certificados; y

2.1.5.5 La demás información relacionada con las Unidades Certificadoras Intermedias respecto de los certificados digitales de la FIREL.

La información señalada en los numerales 2.1.5.1. y 2.1.5.2. se realizará cada vez que se requiera conforme a la vigencia de los Certificados Raíz del PJF e Intermedios.

La información referida en los numerales 2.1.5.3., 2.1.5.4. y 2.1.5.5., se publicará una vez autorizada por la Unidad.

2.1.6. **Publicación de información de las Unidades Certificadoras Intermedias y su frecuencia.**

Los certificados y la información relativa a cada una de las Unidades Certificadoras Intermedias se encontrarán disponibles en línea en la dirección electrónica definida en

cada uno de los repositorios correspondientes, donde se podrá consultar, y en su caso, descargar:

2.1.6.1 Vigencia de certificados de los usuarios finales;

2.1.6.2 Vigencia de certificados OCSP y de TSA.

2.1.6.3 La información sobre los servicios relacionados con el uso de los certificados; y

2.1.6.4 La demás información relacionada con las unidades de certificación intermedias respecto de los certificados digitales de la FIREL.

2.1.7. **Acceso a los repositorios.**

El acceso a los repositorios así como a este documento será público.

Los repositorios se mantendrán en línea y disponibles las veinticuatro horas del día, los siete 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 Unidad o a cada una de las Unidades Certificadoras Intermedias. En ese supuesto, se emitirá el aviso correspondiente en el que se indicará el horario del periodo de mantenimiento.

3. Identificación y autenticación.

3.1. Nombres.

3.1.1. **Nombre distintivo del Certificado Raíz del PJF.**

Nombre Distintivo: CN = Autoridad Certificadora Raíz del Poder Judicial de la Federación; E = acr_pjf@correo.cjf.gob.mx; O = Poder Judicial de la Federación; OU = Unidad del Poder Judicial de la Federación para el Control de Certificación de Firmas; STREET = Av. Insurgentes Sur 2417 Col. San Angel; PostalCode = 01000; L = Alvaro Obregón; S = Distrito Federal; C = MX.

3.1.2. **Nombre distintivo de los Certificados Intermedios.**

El nombre distintivo de los certificados intermedios del PJF contempla los siguientes valores:

3.1.2.1. **Nombre distintivo del Certificado Intermedio de la SCJN.**

Nombre Distintivo: CN = AC de la Suprema Corte de Justicia de la Nación; E = acscjn@mail.scjn.gob.mx; O = Suprema Corte de Justicia de la Nación; OU = Dirección General de Tecnologías de la Información; STREET = Pino Suárez No. 2, Colonia Centro; PostalCode = 06065; L = Cuauhtémoc; S = Distrito Federal; C = MX; 2.5.4.45 = 03 0d 00 53 43 4a 39 35 30 32 30 34 36 50 35.

3.1.2.2. **Nombre distintivo del Certificado Intermedio del TE.**

Nombre Distintivo: CN = Unidad de Certificación Electrónica del TEPJF - PJF; E = admin-ac@te.gob.mx; O = Tribunal

Electoral del Poder Judicial de la Federación; OU = Dirección General de Sistemas; STREET = Carlota Armero No. 5000 Col. CTM Culhuacan; PostalCode = 04480; L = Coyoacán; S = Distrito Federal; C = MX.

3.1.2.3. **Nombre distintivo del Certificado Intermedio del CJF.**

Nombre Distintivo: CN = Autoridad Certificadora Intermedia del Consejo de la Judicatura Federal; E = aci_cjf@correo.cjf.gob.mx; O = Consejo de la Judicatura Federal; OU = Unidad para el Control de Certificación de Firmas; STREET = 1. Av. Insurgentes Sur 2417 Col. San Angel; PostalCode = 01000; L = Alvaro Obregón; S = DF; C = MX; 2.5.4.45 = CJF950204TL0.

3.1.3. **Nombre distintivo de los certificados digitales para usuarios finales de la FIREL.**

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

3.1.3.1. CN = <NOMBRES><APELLIDOS>;

3.1.3.2. E = Dirección de correo electrónico del titular del certificado; y

3.1.3.3. SN = CURP del titular del certificado.

3.1.4. **Nombre distintivo de los certificados digitales para Servicios Relacionados con la FIREL.**

El nombre distintivo de los certificados digitales para Servicios Relacionados con la FIREL contempla los siguientes valores:

3.1.4.1. CN = <NOMBRE DEL SERVICIO>;

3.1.4.2. E = Dirección de correo electrónico del Servicio Relacionado con la FIREL; y

3.1.4.3. C = MX.

3.2. Validación inicial de la Identidad.

3.2.1. **Validación inicial de la identidad del Servidor Público del PJF que solicita un certificado intermedio para la SCJN, el TE y el CJF.**

En la ceremonia de generación del Certificado Intermedio respectivo los referidos servidores públicos se deberán identificar ante el notario público con la credencial oficial vigente que acredite su identidad.

3.2.2. **Validación inicial de identidad de un Agente Certificador de la SCJN.**

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

3.2.3. **Validación inicial de identidad de un Agente Certificador del TE.**

Los agentes certificadores que auxiliarán en estas funciones serán designados por los titulares de las Secretarías Generales de Acuerdos de la Sala Superior y de las Salas Regionales quienes deben ser auxiliados en los aspectos técnicos por personal del área de Sistemas.

3.2.4. **Validación inicial de identidad de un Agente Certificador del CJF.**

Los Coordinadores Técnicos Administrativos asignados a los Tribunales de Circuito y Juzgados de Distrito, con base en el Acuerdo General 23/2013 del Pleno del CJF, así como la cédula de descripción del puesto específico del Manual General de Puestos, son quienes fungirán como agentes certificadores del CJF.

La Unidad de Certificación del CJF podrá designar a servidores públicos adscritos a dicha Unidad para que funjan como agentes certificadores.

3.2.5. **Validación inicial de identidad de los Justiciables.**

El Agente Certificador recibirá los documentos y recabará los registros biométricos para validar la identidad de los Justiciables, previo consentimiento expreso de éste y conforme a lo que señala el numeral 6.2 de las presentes Políticas y el artículo 4 del AGC 1/2013; los Justiciables deberán acudir a las oficinas dispuestas para este fin por la unidad certificadora a la que haya sido enviada la solicitud de certificación.

---

4. Procedimiento para la emisión del Certificado Raíz del PJF.

Deberá ser generado con la participación de los integrantes de la Unidad y ante la presencia de un notario público que de fe de la ejecución del procedimiento para la generación de las llaves pública y privada; acorde a las características especificadas en el numeral 1.6.2. de las presentes Políticas.

4.1. Vigencia del Certificado Raíz del PJF.

El Certificado Raíz del PJF tendrá una vigencia de doce años contados a partir del momento en que sea emitido.

5. Procedimientos del ciclo de vida de los certificados intermedios.

5.1. Órganos facultados para obtener Certificados Intermedios derivados del Certificado Raíz del PJF.

En términos de los previsto en el AGC 1/2013, únicamente los órganos del PJF podrán obtener Certificados Intermedios con base en el Certificado Raíz del PJF.

5.2. Procedimiento de Emisión de Certificados Intermedios del PJF.

5.2.1. La SCJN, el TE y el CJF designarán a los servidores públicos responsables de resguardar el acceso a la Llave Privada de los Certificados Intermedios respectivos.

5.2.2. La Unidad Certificadora Intermedia que corresponda deberá generar su requerimiento de certificación ante la presencia de un notario público, quién dará fe de los pasos a seguir para la generación de las llaves pública y privada, verificará que éstas se generen dentro de un Módulo Criptográfico que cumpla con las especificaciones de seguridad del FIPS-140-2 nivel 3, y tomará nota de la Llave Pública generada.

5.2.3. La Unidad recibirá el requerimiento de certificación y por lo menos tres de los seis servidores públicos responsables de resguardar la Llave Privada del Certificado Raíz ejecutarán los pasos para emitir el Certificado Intermedio ante la presencia de un notario público.

5.2.4. La Unidad Certificadora Intermedia realizará el procedimiento de instalación del Certificado Intermedio en su infraestructura ante la presencia de un notario público, quién validará que el certificado está asociado a la misma Llave Pública generada en el requerimiento de certificación.

5.3. Renovación de un Certificado Intermedio.

Por razones de seguridad la Unidad no dispone de mecanismos para la renovación de un Certificado Intermedio emitido previamente.

5.4. Revocación de un Certificado Intermedio.

La Unidad revocará un Certificado Intermedio cuando existan causas justificadas, las que deberán sustentarse plenamente. Una vez revocado no podrá ser utilizado.

5.5. Vigencia del Certificado Intermedio.

El Certificado Intermedio tendrá una vigencia de diez años contados a partir del momento en que sea emitido por la Unidad.

6. Procedimientos del ciclo de vida del Certificado Digital de la FIREL para usuarios finales.

6.1. Personas que pueden solicitar un Certificado Digital de la FIREL.

Toda persona física, incluyendo a los Servidores Públicos del PJF, en la inteligencia de que sólo podrá ser solicitado y

autorizado a personas físicas, con independencia de que éstas sean representantes de personas morales públicas o privadas.

6.2. Procedimiento de solicitud del Certificado Digital de la FIREL.

6.2.1. El interesado en obtener un Certificado Digital de la FIREL deberá ingresar al SEPJF en la dirección http://www.pjf.gob.mx/firel/, y acceder al vínculo denominado FIREL.

6.2.2. Seleccionará la opción "Solicitud de un certificado digital de firma electrónica (FIREL)" y aceptará los términos y condiciones de uso.

6.2.3. Descargará y ejecutará la aplicación institucional para la generación de su Llave Privada y requerimiento de certificación el cual contendrá la Llave Pública asociada con aquélla. Seleccionará la opción "Requerimiento de certificación FIREL" y capturará la siguiente información: nombre(s); primer apellido; segundo apellido, en su caso; CURP; dirección de correo electrónico; Clave de Acceso a la Llave Privada del Certificado Digital de la FIREL, ruta y nombre del archivo donde almacenará la llave privada (archivo con extensión .key) y el de requerimiento de certificación (archivo con extensión .req). Una vez que haya generado este par de archivos, continuará el procedimiento en el SEPJF.

6.2.4. Al ingresar en la opción "Solicitud de un certificado digital de firma electrónica" en el SEPJF, adjuntará el archivo de requerimiento de certificación (archivo con extensión .req) en

el campo dispuesto para ello y seleccionará la opción "Solicitar certificado digital".

6.2.5. El SEPJF verificará que el archivo de requerimiento de certificación se haya generado correctamente. De ser así, se desplegará la información del solicitante contenida en el mismo, la cual no podrá ser editada. Si el interesado detecta un error deberá ejecutar nuevamente las actividades especificadas en el numeral 6.2.3. de las presentes Políticas.

6.2.6. En caso de que el archivo de requerimiento no se haya generado correctamente, el Sistema Electrónico desplegará un mensaje informando al interesado de esta situación, por lo que éste deberá ejecutar nuevamente las actividades especificadas en el numeral 6.2.3.

6.2.7. El interesado deberá seleccionar la opción de "Formular solicitud de certificado digital".

6.2.8. Deberá llenar el formulario con los siguientes datos: nombres(s); primer apellido; segundo apellido, en su caso; fecha de nacimiento; nacionalidad; CURP; tipo de identificación; número o clave de identificación; dirección de correo electrónico; domicilio; Clave de Revocación; en caso de que sea un servidor público, seleccionar el Órgano del PJF de su adscripción y el número de expediente. A continuación deberá anexar digitalizados y visibles, en archivo electrónico, su identificación oficial vigente (credencial para votar, pasaporte, credencial expedida por la Suprema Corte, por el TE o por el CJF con resello autorizado, cédula profesional o cartilla del servicio militar), copia certificada del acta de nacimiento o, de la carta de naturalización o, del documento de

identidad y viaje, así como su comprobante de domicilio. Los documentos digitalizados deberán ser enviados en formato PDF y con un tamaño no mayor a 1MB en cada uno de ellos.

6.2.9. Al finalizar el solicitante deberá seleccionar la opción "Registrar Información".

6.2.10. El SEPJF validará que la información remitida por el solicitante esté completa y que los documentos no excedan el tamaño establecido; y desplegará la lista de los módulos de atención.

6.2.11. Posteriormente el solicitante deberá seleccionar si la solicitud respectiva la realiza ante la SCJN, el TE o el CJF, tomando en cuenta las ciudades en las que se ubican los módulos de atención en los que se podrá concluir el trámite correspondiente.

6.2.12. Una vez que se seleccione el órgano ante el cual se presentará la solicitud respectiva así como la ciudad en la que se ubica el módulo de atención a la que el Justiciable acudirá para concluir el trámite, el SEPJF desplegará el calendario correspondiente a la unidad seleccionada por el solicitante, indicando los horarios disponibles para cada fecha.

6.2.13. El solicitante deberá seleccionar la fecha y hora deseada para su cita, en la que deberá acudir a la unidad seleccionada para culminar el trámite de solicitud de Certificado Digital de la FIREL.

6.2.14. El tiempo de duración de cada trámite de emisión de Certificado Digital de la FIREL, será de aproximadamente 20

minutos. Las citas iniciarán desde las 9:00 hasta las 14:40 horas y desde las 16:20 hasta las 17:40 horas. Únicamente se permitirá el registro de citas en días hábiles.

6.2.15. El SEPJF generará al solicitante un acuse de recibo del trámite que incluya el número de folio que le corresponda, así como fecha y hora para su presentación al módulo de atención correspondiente. El solicitante deberá imprimir y presentar ante ese módulo, por duplicado, el referido acuse, el cual contendrá el conjunto de caracteres que representan la Llave Pública y la indicación de que previa revisión documental y registro de la información biométrica se ha culminado satisfactoriamente el procedimiento de solicitud de certificado.

6.2.16. Realizado lo anterior, el solicitante acudirá ante al módulo de atención correspondiente en el cual proporcionará al Agente Certificador el acuse de recibo señalado en el numeral inmediato anterior, por duplicado, así como la documentación original o en copia certificada que ingresó al SEPJF y la dirección de correo electrónico indicada en la solicitud del Certificado Digital de la FIREL.

6.2.17. El Agente Certificador localizará en el SEPJF la solicitud de certificado utilizando el número de folio del respectivo acuse de recibo.

6.2.18. El Agente Certificador verificará que el solicitante tiene registrada su cita en ese módulo de atención en la fecha y hora en los que se presente. De lo contrario, en su caso, indicará al solicitante la fecha y hora en la que debe acudir al módulo correspondiente atendiendo a la cita que le fue agendada.

6.2.19. El solicitante entregará al Agente Certificador los documentos requeridos.

6.2.20. El referido agente cotejará los archivos electrónicos de la documentación que obra en el SEPJF con la que le presenta físicamente el solicitante. Si advierte que la documentación presentada en original o copia certificada se remitió en una versión digitalizada que no es legible o incompleta, digitalizará los documentos originales y los ingresará al SEPJF. Si de la lectura de dichos originales se advierte que son incorrectos algunos de los datos ingresados en el formulario, con la autorización del solicitante se realizará la corrección correspondiente. No podrán corregirse los siguientes datos: el nombre, los apellidos, el CURP y la cuenta de correo electrónico, ya que éstos se encuentran asociados a la llave pública previamente generada por el solicitante, por lo que ante un error en esos datos, el agente certificador, por conducto del SEPJF, rechazará la solicitud y remitirá un correo electrónico a la cuenta de correo del solicitante informándole tal situación, para que reinicie el procedimiento de solicitud de certificado digital de la FIREL, ingresando los datos correctos.

6.2.21. Concluida la verificación de la correspondencia de los datos ingresados en la solicitud con los indicados en los documentos que en original o copia certificada presente el solicitante, se realizará la toma de las huellas dactilares, de la fotografía y la digitalización de la firma autógrafa. Posteriormente se validarán las huellas dactilares en el Sistema AFIS. Si de esta validación se advierte la existencia de un Certificado Digital de la FIREL vinculado a las mismas huellas, el Agente Certificador requerirá al solicitante

proporcionar nuevamente sus huellas dactilares. Si de esta segunda lectura de las huellas dactilares se confirma su vinculación con un diverso Certificado Digital de la FIREL dará por concluido el procedimiento e indicará al solicitante que en fecha próxima recibirá el comunicado que corresponda, previa valoración de la Unidad.

6.2.22. Si de la primera o segunda lectura de las huellas dactilares se advierte la inexistencia de vinculación con un Certificado Digital de la FIREL y el registro correcto de los datos biométricos, el Agente Certificador autorizará la emisión del respectivo Certificado Digital, la que únicamente estará condicionada a que no exista duplicidad de la Llave Pública correspondiente a este Certificado Digital respecto de la vinculada a un Certificado Digital expedido previamente. En el caso de actualizarse la referida duplicidad el solicitante deberá reiniciar el procedimiento de solicitud.

6.2.23. Una vez otorgada la autorización mencionada en el numeral inmediato anterior, por conducto del SEPJF se enviará un correo electrónico a la cuenta señalada por el solicitante, en el cual se indicará que su Certificado Digital de la FIREL ha sido emitido así como el procedimiento a seguir para su descarga y generación de su archivo PFX con el Certificado Digital de la FIREL.

6.2.24. Concluido el referido procedimiento el agente certificador y el solicitante suscribirán el acuse de recibo indicado en el punto 6.2.9.4.

6.3. Renovación del Certificado Digital de la FIREL.

6.3.1. La renovación deberá efectuarse dentro de los treinta días anteriores a la conclusión de su vigencia. Si en ese lapso no se renueva el Certificado Digital de la FIREL correspondiente, éste caducará y el interesado deberá formular una nueva solicitud.

6.3.2. Para llevar a cabo dicha renovación el titular del certificado deberá ingresar al SEPJF en la dirección https://www.pjf.gob.mx/firel/ y acceder al vínculo denominado FIREL.

6.3.3. El interesado seleccionará la opción "Renovación de certificado digital de firma electrónica (FIREL)" y aceptará los términos y condiciones de uso.

6.3.4. El interesado descargará la aplicación institucional para la generación de sus llaves pública y privada, para lo cual ejecutará esta aplicación en su computadora con el objeto de generar su Llave Privada y su requerimiento de certificación. A continuación seleccionará la opción "Requerimiento de renovación de FIREL", en la cual se solicitará su archivo PFX vigente y la Clave de Acceso a la Llave Privada del Certificado Digital de la FIREL que está por caducar. La aplicación le solicitará que capture una nueva Clave de Acceso a la Llave Pública del Certificado Digital de la FIREL y que elija la ruta y nombre del archivo donde se almacenará tanto la Llave Privada (archivo con extensión .key) como el requerimiento de certificación (archivo con extensión .req).

6.3.5. Posteriormente, deberá ingresar al SEPJF en la liga "Renovación de certificado digital de firma electrónica (FIREL)" y enviar el archivo de requerimiento de certificación. El SEPJF realizará la validación de que el requerimiento esté firmado por

el Certificado Digital de la FIREL vigente del Usuario Final que realiza el trámite, de esta forma la renovación se realizará de manera inmediata. Una vez emitido el nuevo Certificado Digital de la FIREL, el Usuario Final recibirá en su correo electrónico la dirección electrónica para descargar y generar su nuevo archivo PFX con el Certificado Digital de la FIREL.

6.4. Revocación del Certificado Digital de la FIREL.

La solicitud de revocación sólo podrá ser realizada por el Usuario Final, durante el periodo de vigencia del Certificado Digital de la FIREL, para lo cual deberá ingresar al SEPJF en la liga "Revocación de un certificado digital de firma electrónica (FIREL)" y proporcionar tanto la CURP como la correspondiente Clave de Revocación; de esta forma la revocación se realizará de manera inmediata.

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

El Agente Certificador deberá digitalizar el referido escrito de revocación e ingresarlo en el SEPJF en el registro correspondiente.

Los Agentes Certificadores deberán remitir a las Unidades de Certificación a las que estén adscritos o auxilien, cada tres meses, los originales de los escritos de revocación que hayan recibido.

Sólo podrá revocarse un certificado por causa de muerte de su titular o por diversa que encuentre sustento en una disposición general, cuando la Unidad de Certificación cuente con la documentación que acredite fehacientemente la existencia de dicha causa. El SEPJF revocará un Certificado Digital cuando con motivo de la solicitud de uno diverso se actualice duplicidad entre la Llave Pública de aquél y la del Certificado Digital materia de dicha solicitud, lo que se notificará al Usuario Final de aquél al correo electrónico que hubiere registrado en el formulario correspondiente.

Una vez revocado un certificado no podrá ser utilizado, por lo que si el interesado requiere de otro Certificado Digital de la FIREL tendrá que solicitarlo de nueva cuenta conforme al procedimiento establecido en el numeral 6.2 de estas Políticas.

6.5. Circunstancias para cambiar llaves a un Certificado Digital de la FIREL.

Por razones de seguridad las unidades de certificación correspondientes no disponen de mecanismos para el cambio de la Llave Pública o de la Llave Privada de un Certificado Digital de la FIREL emitido previamente.

6.6. Vigencia del Certificado Digital de la FIREL.

El Certificado Digital de la FIREL tendrá una vigencia de tres años contados a partir del momento de su emisión, deberán tener un tamaño de 2048 bits con algoritmo de firma RSA y algoritmo de digestión SHA-256.

6.7. Depósito y recuperación de la Llave Privada.

Las unidades de certificación no almacenarán la Llave Privada de los usuarios finales, por lo que el propietario de la misma es responsable de su adecuado resguardo y confidencialidad.

7. Controles de seguridad física.

Los Centros de Datos que resguardarán el Módulo Criptográfico de la Autoridad Certificadora Raíz del PJF y de las Autoridades Certificadoras Intermedias deberán contar con las siguientes medidas de seguridad:

7.1. Controles de acceso.

7.1.1. El acceso a los Centros de Datos deberá realizarse mediante un proceso de autenticación. Los dispositivos de acceso utilizados almacenarán las bitácoras respectivas para su consulta.

7.1.2. Todos los accesos de personal al Centro de Datos quedarán registrados en una bitácora, indicando fecha, motivo, y hora de entrada y salida.

7.1.3. El personal externo al PJF que requiera acceso a los Centros de Datos, deberá ser acompañado en todo momento por personal autorizado de los órganos del PJF.

7.1.4. El acceso a los gabinetes que alojan la infraestructura que sirve de soporte a los Servicios Relacionados con la FIREL y el Sistema Electrónico deberán estar bajo llave.

7.2. Monitoreo.

7.2.1. El interior del Centro de Datos y los alrededores, deberán monitorearse mediante un sistema de circuito cerrado.

7.3. Control de temperatura y humedad.

7.3.1. Los sistemas de aire acondicionado de los Centros de Datos deberán mantener a un nivel adecuado la temperatura y humedad del sitio, contando con el monitoreo y envío de alertas en caso de que los umbrales de dichos valores sean rebasados.

7.4. Protección y prevención contra incendios.

7.4.1. Los Centros de Datos deberán contar con medidas de prevención y protección, como sistemas automáticos de detección de humo y extinción de incendios.

7.4.2. El equipo de extinción de incendios deberá evitar el daño a los recursos informáticos.

7.5. Exposición al agua.

7.5.1. Los Centros de Datos deberán ubicarse estratégicamente para minimizar el impacto que resultaría de exponer al agua el cableado y los equipos instalados.

7.6. Suministro eléctrico.

7.6.1. Los Centros de Datos deberán contar con sistemas de alimentación ininterrumpida.

7.7. Protección del cableado eléctrico y de red.

7.7.1. El cableado eléctrico y de red deberá ubicarse estratégicamente para evitar desconexiones accidentales.

7.8. Protección de los respaldos.

7.8.1. Los respaldos de las bases de datos de los Servicios Relacionados con la FIREL y el Sistema Electrónico serán almacenados por las Áreas Técnicas en instalaciones externas destinadas para este fin.

7.8.2. Las Áreas Técnicas deberán establecer el protocolo de seguridad para el traslado de los respaldos a los sitios externos.

7.8.3. Los respaldos deberán protegerse contra daños por magnetismo, agua, incendio y acceso no autorizado.

7.8.4. El acceso a los respaldos deberá realizarse únicamente por personal debidamente autorizado por las Áreas Técnicas.

7.9. Uso de dispositivos electrónicos en Centros de Datos.

7.9.1. El acceso a los Centros de Datos deberá realizarse sin portar equipos telefónicos, fotográficos, de audio o video.

7.9.2. El acceso de medios de almacenamiento extraíble o equipos de cómputo estará restringido a la realización de respaldos, actualizaciones o tareas de mantenimiento.

7.10. Consumo de alimentos y bebidas.

7.10.1. Quedará prohibido consumir alimentos y bebidas dentro de los Centros de Datos.

8. Controles de seguridad informática.

8.1. Análisis de vulnerabilidades.

Se realizarán evaluaciones mensuales de seguridad informática a los distintos sistemas que soportan los Servicios Relacionados con la FIREL y el Sistema Electrónico. Se realizará una prueba anual de seguridad informática que incluya la evaluación de la infraestructura.

Estas pruebas se realizarán bajo estrictas medidas de control que no comprometan la continuidad de la operación de los Servicios Relacionados con la FIREL y el Sistema Electrónico.

8.2. Monitoreo de los servicios.

Se deberá con un sistema de monitoreo de los Servicios Relacionados con la FIREL y el Sistema Electrónico, que

opere en tiempo real las 24 horas del día los 365 días del año, con el consecuente envío de alertas en caso de presentarse cualquier incidente.

8.3. Desarrollo de sistemas.

Los Servicios Relacionados con la FIREL y el Sistema Electrónico, deberán cumplir con las mejores prácticas de desarrollo de sistemas, incluyendo:

8.3.1. Separación de ambientes de desarrollo, pruebas y producción;

8.3.2. Identificación de versiones de código;

8.3.3. Revisiones periódicas de código;

8.3.4. Alinearse a un estándar de desarrollo seguro de aplicaciones;

8.3.5. Contar con un procedimiento de control de cambios; y

8.3.6. Firma de código de las aplicaciones desarrolladas para el SEPJF con certificado digital.

8.4. Registros de auditoría.

Todos los componentes que dan soporte a los Servicios Relacionados con la FIREL y el Sistema Electrónico deberán registrar las actividades, excepciones y eventos de seguridad. Los registros incluirán, en los casos en que aplique, fechas, horas, detalles de los eventos, identidad, ubicación, intentos

fallidos, exitosos y rechazados, cambios en las configuraciones, errores, fallas, uso de privilegios, archivos a los que se tuvo acceso, direcciones y protocolos de red. Todas las actividades realizadas por los administradores y operadores de los sistemas deberán registrarse.

8.4.1. **Protección de los archivos de registro.**

Los archivos de registros deberán protegerse contra lectura, modificación y eliminación por personal no autorizado.

8.4.2. **Revisión de archivos de registro.**

Los registros deberán revisarse mensualmente y generar los reportes necesarios que permitan tomar las medidas preventivas por los responsables de cada parte del proceso para corregir errores y prevenir fallas en los servicios.

8.4.3. **Tiempo de resguardo de los archivos de registro.**

Los registros de auditoría deberán almacenarse por 1 año.

8.5. Análisis de riesgos.

Se deberá realizar un análisis de riesgos a la infraestructura de los Servicios Relacionados con la FIREL y el Sistema Electrónico, que incluya el análisis a las Autoridades Certificadoras Raíz e Intermedias.

8.5.1. **Acciones a tomar como resultado de la detección de riesgos.**

Las Autoridades Certificadoras Intermedias, determinarán su propio procedimiento y plazos apropiados para mitigar los riesgos detectados, dando prioridad a los riesgos de alto impacto.

8.6. Recuperación en caso de desastres.

8.6.1. Identificación de riesgos relacionados con la continuidad de las operaciones.

Deberán identificarse aquellas situaciones que podrían provocar una falla en la continuidad de los Servicios Relacionados con la FIREL y el Sistema Electrónico.

8.6.2. Sitios alternos de recuperación en caso de desastre.

Deberá contarse con instalaciones alternas con el equipamiento de infraestructura necesario, que permita la recuperación de la operación de los Servicios Relacionados con la FIREL y el Sistema Electrónico.

8.6.3. Procedimientos de recuperación.

La Autoridad Certificadora Raíz y las Intermedias deberán contar con los procedimientos necesarios que permitan la recuperación de las operaciones en caso de fallas, incidentes de seguridad o desastres naturales. Estos procedimientos

deberán ser probados una vez al año para evaluar su efectividad e informar los resultados a la Unidad.

---

9. Auditoría de cumplimiento.

Las Autoridades Certificadoras Intermedias se someterán a auditorías anuales efectuadas por terceros certificados en los aspectos técnicos considerados en las presentes Políticas.

9.1. Temas cubiertos por la auditoría.

Los temas cubiertos por una auditoría incluirán, sin carácter limitativo lo siguiente: políticas de seguridad y planificación, seguridad física, evaluación de tecnología y servicios de administración.

9.2. Acciones para el caso de presentarse recomendaciones o hallazgos en los resultados de las auditorías.

Las acciones que deberán tomarse como consecuencia de la existencia de hallazgos serán responsabilidad de las Autoridades Certificadoras Intermedias, en función de la naturaleza y grado del hallazgo identificado. Las Autoridades Certificadoras elaborarán el correspondiente plan de acción para la atención de las observaciones emitidas por los auditores.

10. Controles de personal.

10.1. Uso y operación de los componentes de infraestructura de los Servicios Relacionados con la FIREL y el Sistema Electrónico.

La administración de los módulos criptográficos deberá realizarse únicamente por personal certificado por el fabricante, y autorizado por las Autoridades Certificadoras Intermedias.

La administración de la infraestructura de los Servicios Relacionados con la FIREL deberá realizarse únicamente por personal certificado por el fabricante, y autorizado por las Autoridades Certificadoras Intermedias.

Se deberá proveer capacitación al personal técnico de la Unidad en el uso y manejo de la infraestructura de los Servicios Relacionados con la FIREL y el Sistema Electrónico.

10.2. Cambio de llaves pública y privada de una Autoridad Certificadora.

Por razones de seguridad no se podrán cambiar las llaves pública y privada de la Autoridad Certificadora Raíz ni de las Autoridades Certificadoras Intermedias, por lo cual se deberá seguir el proceso de emisión de certificados conforme a los numerales 4. ó 5.2., según corresponda.

11. Contar con un equipo de respuesta a incidentes.

Con el propósito de identificar, diagnosticar, aislar, remediar e investigar los incidentes que afecten o puedan afectar la confidencialidad de la información o la operación de los sistemas que dan soporte a los Servicios Relacionados con la FIREL, la Unidad contará con un equipo de respuesta a incidentes integrado por personal debidamente capacitado adscrito a las Áreas Técnicas.

Ante una incidencia en materia de seguridad de la información (pérdida de información sensible, falla de algún componente tecnológico, divulgación no autorizada de documentos confidenciales, entre otras), se deberá notificar de inmediato al equipo de respuesta a incidentes señalado en el párrafo anterior.

Los incidentes en materia de seguridad de la información deberán documentarse para crear una base de conocimientos que permita mejorar los procedimientos tecnológicos.

12. Conclusión de las operaciones de las Autoridades Certificadoras.

12.1. Conclusión de las operaciones de la Autoridad Certificadora Raíz.

Antes de concluir la prestación de los servicios de la Autoridad Certificadora, ésta deberá:

12.1.1. Informar a las Autoridades Certificadoras Intermedias;

12.1.2. Informar a los Usuarios Finales sobre la baja del servicio;

12.1.3. Informar sobre las condiciones y terminación del mismo;

12.1.4. Revocar todos los certificados; y

12.1.5. Destruir las llaves privadas y los respaldos.

12.2. Conclusión de las operaciones de las Autoridades Certificadoras Intermedias.

Antes de concluir la prestación de los servicios de las Autoridades Certificadoras Intermedias, éstas deberán:

12.2.1. Informar a los Usuarios Finales sobre la baja del servicio;

12.2.2. Informar sobre las condiciones y terminación del mismo;

12.2.3. Revocar todos los certificados; y

12.2.4. Destruir las llaves privadas y los respaldos.

La Autoridad Certificadora Intermedia deberá emitir el último certificado con una vigencia menor a la de su fecha de vigencia.

Los Servicios Relacionados con la FIREL mantendrán el resguardo de la información generada por las Autoridades Certificadoras Raíz e Intermedias conforme a lo dispuesto en el artículo 6° de la Constitución Política de los Estados Unidos Mexicanos y en la diversa normativa emanada de éste, lo que se tomará en cuenta al proporcionar las evidencias criptográficas de las operaciones realizadas con los Certificados Digitales de la FIREL.

13. Controles técnicos de seguridad.

Se deberán adoptar estándares de seguridad de la información y cumplir con los controles necesarios, siendo recomendables el estándar ISO 27000, el WebTrust o el ETSI.

13.1. Generación e instalación de las llaves pública y privada.

El protocolo para la emisión del Certificado Raíz del PJF se encuentra en la dirección electrónica especificada en el numeral 2.1.1.

Los protocolos para la generación del requerimiento del Certificado Intermedio y para la configuración e instalación del certificado de las Autoridades Certificadoras Intermedias se encuentran en la dirección electrónica especificada en los numerales 2.1.2., 2.1.3. y 2.1.4.

13.2. Protección de la llave privada del Certificado Raíz del PJF y controles de ingeniería de los módulos criptográficos.

13.2.1. Autoridad Certificadora Raíz del PJF.

El Módulo Criptográfico que gestionará el ciclo de vida de las llaves criptográficas de la Autoridad Certificadora Raíz del PJF deberá ser sometido a una pre configuración mediante:

13.2.1.1. Actualización del firmware del Módulo Criptográfico a la última versión estable del fabricante;

13.2.1.2. Utilización de los cables de conexión certificados por el fabricante para la conexión de las consolas; y

13.2.1.3. Documentación de los parámetros de lenguaje de configuración regional de las consolas de acceso.

13.3. Otros aspectos de la gestión de las llaves pública y privada del Certificado Raíz del PJF.

La configuración de parámetros de seguridad para el Módulo Criptográfico de la Autoridad Certificadora Raíz del PJF deberá generarse considerando lo siguiente:

13.3.1. Realización de la configuración de los aspectos de seguridad recomendados de acuerdo al manual del Módulo Criptográfico en los siguientes apartados:

13.3.1.1. Particiones;

13.3.1.2. Contraseñas;

13.3.1.3. Monitoreo;

13.3.1.4. Acceso;

13.3.1.5. Habilitar las alertas necesarias;

13.3.1.6. Alta disponibilidad;

13.3.1.7. Red; y

13.3.1.8. Habilitar las bitácoras necesarias.

13.3.2. Configuración de la API del módulo para acceso únicamente a las aplicaciones autorizadas:

13.3.2.1. Protocolos;

13.3.2.2. IP; y

13.3.2.3. MAC Address.

13.3.3. Controles de acceso basados en roles de usuario:

13.3.3.1. Definición de usuarios administradores / operadores / auditores;

13.3.3.2. Establecimiento del rol del usuario;

13.3.3.3. Niveles de autenticación del usuario;

13.3.3.4. Tipo de autenticación del usuario; y

13.3.3.5. Definición del número mínimo de usuarios para operación del módulo.

13.3.4. Uso de bitácoras de acceso al módulo y actividad.

13.3.4.1. Auditoría de acceso y bitácoras mensuales.

13.3.5. El Módulo Criptográfico deberá estar totalmente reglamentado bajo la normativa del órgano que llevó a cabo su adquisición (asignación de número de inventario y pólizas de garantía vigentes).

13.4. Políticas de respaldo y de recuperación.

13.4.1. **De la Autoridad Certificadora Raíz del PJF.**

13.4.1.1. Se deberá contar con un respaldo del contenido del Módulo Criptográfico en la SCJN, el TE y el CJF.

13.4.1.2. El respaldo será resguardado por un representante de la SCJN, el TE y el CJF.

13.4.1.3. El respaldo deberá ser almacenado en un medio seguro.

13.4.1.4. El respaldo deberá estar accesible las 24 horas de los 365 días del año.

13.4.1.5. Se deberá contar con la disponibilidad de los integrantes de la Unidad, responsables de resguardar las llaves del entorno seguro para el caso de recuperación.

13.4.1.6. Se deberá contar con un plan de recuperación de desastres, y prácticas de verificación del funcionamiento del mismo al menos una vez al año.

13.5. Uso de la Llave Privada.

13.5.1. Requisitos para el uso de la Llave Privada de la Autoridad Certificadora Raíz del PJF.

La Llave Privada de la Autoridad Certificadora Raíz del PJF se activará mediante la puesta en marcha del Módulo Criptográfico acorde a lo especificado en el numeral 4. de las presentes Políticas.

13.5.2. Requisitos para el uso de la Llave Privada de la Autoridad Certificadora de la SCJN.

La llave privada de la Autoridad Certificadora Intermedia del SCJN será protegida en un HSM, en la inteligencia de que para el inicio de sus operaciones se requiere cumplir con una autenticación de doble factor.

13.5.3. Requisitos para el uso de la Llave Privada de la Autoridad Certificadora del TE.

La llave privada de la Autoridad Certificadora Intermedia del TE será protegida en un HSM, en la inteligencia de que para el inicio de sus operaciones se requiere cumplir con una autenticación de doble factor.

13.5.4. Requisitos para el uso de la Llave Privada de la Autoridad Certificadora del CJF.

La llave privada de la Autoridad Certificadora Intermedia del CJF será protegida en un HSM, en la inteligencia de que para el inicio de sus operaciones se requiere cumplir con una autenticación de doble factor.

13.5.5. **Requisitos para el uso de la Llave Privada de los Agentes Certificadores.**

Se requerirá la autenticación del Agente Certificador ante el Dispositivo de Seguridad o archivo PFX que protege el acceso a su Llave Privada, mediante su Clave de Acceso a la Llave Privada del Certificado de la FIREL.

13.5.6. **Requisitos para el uso de la Llave Privada de los usuarios finales.**

Se requerirá proporcionar la Clave de Acceso a la Llave Privada del Certificado de la FIREL que protege el acceso a su Llave Privada.

13.6. Sincronización de tiempo.

La Autoridad Certificadora Raíz del PJF y las Autoridades Certificadoras Intermedias deberán mantener sincronizados los relojes de los equipos que soportan la operación de las mismas, con el tiempo del Centro de la hora oficial de los Estados Unidos Mexicanos proporcionado por el Centro Nacional de Metrología.

13.7. TSA.

Las Autoridades Certificadoras Intermedias deberán contar con una TSA que acredite, a través de un Sello de Tiempo, que un Mensaje de Datos se firmó, envió, recibió o consultó en un momento específico. Estas infraestructuras deberán estar sincronizadas con el tiempo del Centro de la hora oficial proporcionado por el Centro Nacional de Metrología.

13.8. Registro de Llaves Públicas Centralizado.

Las Autoridades Certificadoras Intermedias deberán estar conectadas con un servicio de registro de Llaves Públicas Centralizado a fin de garantizar la unicidad de las llaves de los certificados, el cual se sujetará al protocolo.

14. Perfiles de certificados de Usuario Final, de OCSP y de TSA.

14.1. Perfil de certificado de Usuario Final.

14.1.1. Los certificados digitales de FIREL emitidos a los usuarios finales por un Agente Certificador deberán cumplir con las siguientes normas:

14.1.1.1. Recomendación X.509 ITU-T (2005): Tecnología de información – Interconexión de sistemas abiertos – El directorio: plataforma de autenticación; y

14.1.1.2. RFC 3280: Internet X.509 Infraestructura de llave pública y perfil de certificado.

14.1.2 Los certificados digitales de FIREL utilizan el estándar X.509 versión 3 que incluye la siguiente

información:Versión;Número de serie, este valor es único para cada certificado digital emitido;

14.1.2.3 Nombre del algoritmo de firma utilizado;

14.1.2.4 Nombre distintivo del emisor;

14.1.2.5 Fecha de validez de inicio, el formato de la fecha se encuentra en UTC;

14.1.2.6 Fecha de validez de término, el formato de la fecha se encuentra en UTC;

14.1.2.7 Nombre distintivo del sujeto; y

14.1.2.8 Llave Pública del Usuario Final.

14.1.3 Las extensiones utilizadas son:

14.1.3.1 Uso mejorado de la clave: Correo seguro (1.3.6.1.5.5.7.3.4), Autenticación del cliente (1.3.6.1.5.5.7.3.2); y

14.1.3.2 Tipo de certificado Netscape: Autenticación del cliente SSL, SMIME (a0).

14.1.4 Los valores de las extensiones que deberá calcular la autoridad certificadora intermedia correspondiente son:

14.1.4.1 Nombre alternativo del titular: RFC822 Name=<correo electrónico del usuario final>;

14.1.4.2 Identificador de clave de entidad; y

14.1.4.3 Identificador de clave del titular.

14.1.5 Los valores de las extensiones que deberán colocarse acorde a la autoridad certificadora intermedia son:

14.1.5.1 Puntos de distribución CRL: a) Punto de distribución CRL; b) Nombre del punto de distribución; c) Nombre completo; y d) Dirección URL= <dirección electrónica donde se publica la CRL>;

14.1.5.2 Acceso a la información de la entidad emisora: a) Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1); y b) Nombre alternativo: <dirección electrónica del servicio de OCSP>; y

14.1.5.3 Directivas del certificado: a) Identificador de directiva=<OID de la política respectiva>; b) Información de certificador de directiva; c) Id. de certificador de directiva=CPS; y d Certificador: <dirección electrónica del repositorio donde se encuentre las políticas>.

14.1.6 Los valores para las extensiones críticas requeridas son:

14.1.6.1 Restricciones básicas: a) Tipo de asunto = Entidad Final; y b) Restricción de longitud de ruta = 0; y

14.1.6.2 Uso de la llave: Firma digital, Sin repudio, Cifrado de clave, acuerdo de clave (e8 00).

14.2 Perfil de certificado de OCSP.

14.2.1. Las Autoridades Certificadoras Intermedias del PJF emitirán el certificado para el Servicio OCSP utilizando el estándar X.509 versión 3 que incluye la siguiente información:

14.2.1.1. Versión;

14.2.1.2. Número de serie, este valor es único para cada certificado digital emitido;

14.2.1.3 Nombre del algoritmo de firma utilizado;

14.2.1.4 Nombre distintivo del emisor;

14.2.1.5 Fecha de validez de inicio, el formato de la fecha se encuentra en UTC;

14.2.1.6 Fecha de validez de término, el formato de la fecha se encuentra en UTC;

14.2.1.7. Nombre distintivo del servicio; y

14.2.1.8. Llave Pública.

14.2.2. Las extensiones utilizadas son:

14.2.1.1. Uso mejorado de la clave: Firma de OCSP (1.3.1.5.5.7.3.9); y

14.2.1.2. Tipo de certificado Netscape: Autenticación del cliente SSL, SMIME (a0).

14.2.3. Los valores para las extensiones críticas requeridas son:

14.2.3.1. Restricciones básicas: a) Tipo de asunto = Entidad Final; y b) Restricción de longitud de ruta = 0;

14.2.3.2. Uso de la llave: Firma digital, Sin repudio, Cifrado de clave, acuerdo de clave (e8 00); y

14.2.3.3. Acceso a información de autoridad: a) Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1); y b) Nombre alternativo: <dirección electrónica del servicio de OCSP >.

14.2.4. Los certificados de OCSP que emitan las Autoridades Certificadoras Intermedias tendrán una vigencia de tres años contados a partir del momento de su emisión; deberán tener un tamaño de 2048 bits con algoritmo de firma RSA y algoritmo de digestión SHA-256.

14.3. Perfil del certificado de TSA.

14.3.1. Las Autoridades Certificadoras Intermedias del PJF emitirán el certificado para el Servicio de TSA utilizando el estándar X.509 versión 3 que incluye la siguiente información:

14.3.1.1. Versión;

14.3.1.2. Número de serie, este valor es único para cada certificado digital emitido;

14.3.1.3. Nombre del algoritmo de firma utilizado;

14.3.1.4. Nombre distintivo del emisor;

14.3.1.5. Fecha de validez de inicio, el formato de la fecha se encuentra en UTC;

14.3.1.6. Fecha de validez de término, el formato de la fecha se encuentra en UTC;

14.3.1.7. Nombre distintivo del servicio; y

14.3.1.8. Llave Pública.

14.3.2. Las extensiones utilizadas son:

14.3.2.1. Uso mejorado de la clave: Impresión de fecha (1.3.6.1.5.5.7.3.8); y

14.3.2.2. Tipo de certificado Netscape: Autenticación del cliente SSL, SMIME (a0).

14.3.3. Los valores para las extensiones críticas requeridas son:

14.3.3.1. Identificador de la clave del titular: Id. del titular;

14.3.3.2. Restricciones básicas: a) Tipo de asunto = Entidad Final; y b) Restricción de longitud de ruta = 0; y

14.3.3.3. Uso de la llave: Firma digital, Sin repudio, Cifrado de clave, acuerdo de clave (e8 00).

14.3.4. Los valores de las extensiones que deberán colocarse acorde a la Autoridad Certificadora Intermedia son:

14.3.4.1. Directivas del certificado: a) Identificador de directiva=<OID de la política respectiva>; b) Información de certificador de directiva; c) Id. de certificador de directiva=CPS; y d) Certificador: <dirección electrónica del repositorio donde se encuentre las políticas>.

14.3.5. Los certificados de TSA que emitan las Autoridades Certificadoras Intermedias tendrán una vigencia de tres años contados a partir del momento de su emisión; deberán tener un tamaño de 2048 bits con algoritmo de firma RSA y algoritmo de digestión SHA-256.

15. Otros asuntos legales y comerciales.

15.1 Protección de la información personal.

El tratamiento y protección de la información proporcionada por usuarios finales para el trámite de generación de certificados será resguardada atendiendo a lo previsto en los artículos 6° y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos, así como en la diversa normativa emanada de éstos.

Derechos de propiedad intelectual.

Los Autoridades Certificadoras Intermedias no reclamarán ninguna propiedad intelectual sobre los certificados emitidos.

EL SECRETARIO GENERAL DE ACUERDOS DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN

LIC. RAFAEL COELLO CETINA

LA DIRECTORA GENERAL DE ESTADÍSTICA JUDICIAL DEL CONSEJO DE LA JUDICATURA FEDERAL

LIC. LORENA ANGÉLICA TABOADA PACHECO

EL DIRECTOR GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN

LIC. OTILIO ESTEBAN HERNÁNDEZ PÉREZ

EL DIRECTOR GENERAL DE SISTEMAS DEL TRIBUNAL ELECTORAL DEL PODER JUDICIAL DE LA FEDERACIÓN

MTRO. DAVID AMÉZQUITA PÉREZ

EL DIRECTOR GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN DEL CONSEJO DE LA JUDICATURA FEDERAL

LIC. JUAN JOSÉ GARCÍA MORA

EL SECRETARIO DE LA UNIDAD

LIC. IVÁN ELADIO PALACIOS ALLEC

Esta foja corresponde a las Políticas para la obtención y uso de la Firma Electrónica Certificada del Poder Judicial de La Federación (FIREL), así como para la operación de su Infraestructura Tecnológica.