DICTAMEN TÉCNICO

PARA LA CONTRATACIÓN DE LA "INFRAESTRUCTURA DE FIRMA ELECTRÓNICA AVANZADA PARA LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, MEDIANTE EL PROCEDIMIENTO DE ADJUDICACIÓN DIRECTA".

Con fundamento en lo señalado en el "Acuerdo General de Administración VI/2008 del Comité de Gobierno y Administración de la Suprema Corte de Justicia de la Nación, por el que se regulan los procedimientos para la adquisición, administración y desincorporación de bienes y la contratación de obras, usos y servicios requeridos por este alto Tribunal, se emite el presente **Dictamen Técnico.**

Acuerdo

La inclusión de esta contratación en el Programa Anual de Ejecución de Adquisiciones, Arrendamientos y Prestación de Servicios 2011 y en el Programa Anual de Trabajo de la Dirección General de Tecnologías de la Información, fue aprobada por el H. Comité de Gobierno y Administración en su sesión efectuada el veintisiete de septiembre del año en curso.

Fundamento

De acuerdo a lo establecido por el nuevo Reglamento Interior en Materia de Administración de la Suprema Corte de Justicia que entró en vigor el 7 de abril de 2011, se dispone en su artículo 20, fracciones I, VI, VII, IX, X, XI y XII, que son atribuciones de la Dirección General de Tecnologías de la Información, atender las necesidades tecnológicas en materia de informática jurídica; ejecutar y actualizar los mecanismos de seguridad informática y vigilar su adecuado funcionamiento; el brindar apoyo técnico, el definir mecanismos de seguridad, impulsar la

actualización y mantener la operación eficiente de todos los sistemas de comunicación electrónica, que comprende, entre otros, la página de intranet e internet de este Alto Tribunal, así como planear el crecimiento armónico de la infraestructura tecnológica que sustente las necesidades actuales y futuras.

Antecedentes

En sesión de fecha dieciséis de mayo de dos mil ocho, el entonces Comité de Archivo, Biblioteca e Informática, ordenó la elaboración del proyecto de implementación de la Firma Electrónica para su uso en este Alto Tribunal.

En sesión de fecha dieciocho de enero de dos mil diez, el Comité de Archivo, Biblioteca e Informática, acordó que el proyecto de Firma Electrónica deberá versar sobre cuestiones administrativas de este Alto Tribunal.

Con fecha ocho de junio de 2010 se solicitó el inicio del Proyecto "Implementación de Servicios de Certificados con Directorio Activo", el cual tenía el siguiente alcance:

- ✓ Emisión de certificados digitales que permitan el firmado digital de correos electrónicos y documentos por parte de los usuarios.
- ✓ Emisión de certificados digitales para los servicios de Microsoft que hoy cuentan con un Certificado emitido con la infraestructura actual.

El cual concluyó el día 26 de octubre de 2010, logrando contar con una Infraestructura de Llave Publica (PKI), para ser usada en la autentificación de programas de red, por ejemplo envío de correo electrónico, firmas digitales, control de acceso a recursos y validación oficial de documentos electrónicos.

A partir de ese proyecto se identificaron los siguientes pasos:

- ✓ Desarrollar las interfaces para administración de firma electrónica
- ✓ Normar y protocolizar el uso de Firma Electrónica en la SCJN
- ✓ Definir los procesos de solicitud, creación y revocación de Firma Electrónica.

Adicionalmente, se elaboró un borrador de los "Lineamientos para la implantación, aplicación y uso de la Firma Electrónica certificada para los asuntos administrativos en la Suprema Corte de Justicia de la Nación".

Criterios de necesidad

Contar con una Infraestructura de Firma Electrónica, que reúna los requisitos para producir los mismos efectos jurídicos que la firma autógrafa, requiere de una solución tecnológica diseñada ex profeso, autorización formal de los lineamientos de Uso de Firma Electrónica y su protocolización formal en este Alto Tribunal.

De acuerdo a las ***Líneas Generales Hacia la Consolidación Institucional del Poder Judicial de la Federación***, se determina que "***Usar adecuadamente las tecnologías de la información debe acompañarse de un nivel de seguridad idóneo, incluso mayor que el proporcionado por los soportes documentales tradicionales. El objetivo es generar más confianza en el uso de las herramientas informáticas***".

Una infraestructura de Firma Electrónica, proporciona los servicios de seguridad que se requieren para contar con elementos de: Confidencialidad, Integridad, Autenticidad, Comunicación segura, Privacidad, No repudio, con un nivel de seguridad superior a los soportes documentales tradicionales.

El Acuerdo Décimo Octavo del Acuerdo General del Comité Coordinador para Homologar Criterios en Materia Administrativa e Interinstitucional del Poder Judicial de la Federación, por el que se establecen las medidas de carácter general de racionalidad y disciplina presupuestal para el ejercicio fiscal 2011, determina a) Promover e impulsar el uso de Firma Electrónica, b) La integración del reconocimiento de las firmas electrónicas de las tres instancias del Poder Judicial de la Federación para trámites administrativos.

Con base en la reunión llevada a cabo el pasado miércoles 13 de julio del presente, personal de la Subsecretaría General de Acuerdos mencionó la necesidad de incorporar el uso de la Firma Electrónica, en función de la próxima publicación de la nueva Ley de Amparo; ya que contempla

procedimientos electrónicos, como el ingreso de asuntos por vía electrónica, usando para ello la Firma Electrónica en la sociedad civil y la comunidad jurídica.

Para dimensionar los elementos tecnológicos de la solución de Firma Electrónica, se identifican las siguientes necesidades a resolver:

Contar una infraestructura de Firma Electrónica con valor similar al de la firma autógrafa para trámites administrativos y trámites jurídicos en la Suprema Corte de Justicia de la Nación.

1. **De acuerdo al número de** usuarios que requiere soportar la Firma Electrónica se tienen identificados los siguientes requerimientos:

   - Para trámites administrativos, es el número de empleados de la Suprema Corte de Justicia de la Nación. Para trámites jurídicos, el número de usuarios llegará a ser ilimitado, en cuanto se ofrezcan servicios a la población. *En este aspecto es indispensable que el costo de la solución no esté determinado por el número de certificados a emitir.*
   - En ambos casos se necesita la integración del reconocimiento de las Firmas Electrónicas de las tres instancias del Poder Judicial. Para la población se requiere validar certificados digitales que se hayan obtenido por medio de otras entidades certificadoras, las cuales deben realizarse por medio de un acuerdo de colaboración y el cumplimiento del estándar **ITFEA** (Mencionado en la sección de análisis).

2. **De acuerdo a las necesidades de la Suprema Corte**, al nivel de seguridad de la infraestructura y nivel de disponibilidad:

   - Una vez iniciada la operación de la Firma Electrónica esta debe mantener la continuidad, por lo que la solución debe diseñarse en un modelo de **alta disponibilidad**.
   - El elemento de seguridad más importante de la infraestructura de Firma Electrónica, es la llave privada de la Autoridad Certificadora, por lo que es necesario resguardarlo en un **dispositivo criptográfico** que garantice su protección.

- Así mismo se debe proteger la llave privada del personal de mando superior, mediante el almacenamiento de las mismas en **dispositivos criptográficos biométricos**.

3. **Plataforma de firma unilateral y multilateral de uso inmediato.** Los procesos en que será usada la firma electrónica, actualmente están en proceso de definición y algunos de los sistemas informáticos no están diseñados para incorporar de manera natural el uso de la Firma Electrónica.

- El ciclo de vida tradicional de implementación de una solución de Firma Electrónica, implica modificar y desarrollar en los sistemas informáticos existentes, con los costos asociados y el impacto en el tiempo, para empezar a operar. Adicionalmente se pueden repetir estos costos si el proceso tiene cambios.
- Se debe contar con una plataforma de software, que permita definir procesos de firma de documentos electrónicos de manera inmediata y flexible a las necesidades que surjan.

4. **De los aspectos legales.**

Proporcionar el carácter legal de la Firma Electrónica para producir los mismos efectos jurídicos que la firma autógrafa, requiere contar con los siguientes documentos mínimos, los cuales se deben elaborar como parte de la solución, aunque quedará a criterio de este Alto Tribunal realizar los ajustes, para dar el carácter legal correspondiente.

- Políticas de Certificación.
- Declaración de Prácticas de Certificación de la Autoridad Certificadora Raíz.
- Declaración de Prácticas de Certificación de la Autoridad Certificadora de la Suprema Corte.

Costo Beneficio

Los beneficios inmediatos derivados del uso de Firma Electrónica se describen a continuación:

- ✓ **Incremento en la seguridad:** La SCJN se beneficiará de la seguridad adicional que se proporciona con la criptografía de llave pública. Los certificados digitales permiten que usuarios puedan firmar y cifrar archivos y correos electrónicos.
- ✓ **Reducción en costos por certificados:** Una infraestructura PKI autoadministrada no requiere el pago de licencias por cada certificado que se emite o renueva, y le dará a SCJN completo control sobre la infraestructura sin dependencia de terceros.
- ✓ **Mejora de procesos.** Los tiempos dedicados a procesos se reducen drásticamente.
- ✓ **Amabilidad con el medio ambiente.** Se disminuye el uso de papel.
- ✓ **Escalabilidad.** Los certificados digitales que se emiten por la PKI se pueden configurar para cubrir los requerimientos de alguna solución en particular, y un diseño jerárquico puede escalarse para cubrir las demandas de una infraestructura creciente y demandas futuras.

Para la elaboración de este dictamen, se analizaron diferentes opciones tecnológicas y su viabilidad de acuerdo a los siguientes criterios:

- ✓ **Cumplir con el estándar ITFEA.** Con lo que se garantiza la intercomunicación entre diferentes Autoridades de Certificación, de tal forma que se puedan aprovechar los certificados digitales generados por Entidades Federales como el Sistema de Administración Tributaria (SAT), Secretaría de la Función Pública (SFP).
- ✓ **Ser un Proveedor de Servicios de Certificación reconocido por la Secretaría de Economía.** Mediante el cual se evalúa que la empresa ha cubierto requisitos de seguridad y madurez en la implementación de Autoridades de Certificación
- ✓ **Ser propietario del código fuente de la solución.**

Acerca del estándar ITFEA

Es la Infraestructura Tecnológica que permite la interoperabilidad y el reconocimiento de Certificados Digitales de Firma Electrónica Avanzada entre las Autoridades o Agencias Certificadoras que la integran

Este es un Acuerdo Interinstitucional por el que se establecen los lineamientos para la homologación, implantación y uso de la Firma Electrónica Avanzada en la Administración Pública Federal (DOF 24/08/2006).

La razón de solicitar este estándar en la solución, es para que la infraestructura pueda interactuar de manera estandarizada con Autoridades Certificadoras de la administración Pública Federal, como el SAT (Sistema de Administración Tributaria), Secretaría de la Función Pública (SFP) y del Poder Judicial de la Federación como es el caso del Consejo de la Judicatura Federal y el Tribunal Electoral.

Evaluación de Soluciones Internacionales

Se realizó la evaluación de soluciones internacionales, sin embargo estas no fueron viables porque no cumplen con el estándar nacional **ITFEA**, lo que impediría hacerlos compatibles entre las implementaciones de las distintas Instituciones de Gobierno en México. **En particular la información que no sería posible validar con la ausencia de este estándar, es el RFC y la CURP del propietario de los certificados.**

Las tecnologías de marca internacional evaluadas que fueron analizadas son Entrust, Verisign y Microsoft. En todos los casos no cumplieron con la norma ITFEA, Adicionalmente se debe resaltar que al ser código desarrollado principalmente en el extranjero, este se sujeta a las legislaciones de su país de origen, el cual como en el caso de Estados Unidos, prohibe el almacenamiento de las llaves privadas de los usuarios, sin embargo también exige que la tecnología si permita guardar las llaves en algunos casos de investigación judicial.

Evaluación de Soluciones Nacionales

Se analizaron las soluciones de empresas que ha sido acreditadas como Proveedores de Servicios de Certificación reconocidos por la Secretaría de Economía.

Las soluciones tecnológicas que fueron analizadas son las siguientes, La empresa PSC Advantage con el producto Certifiel, Seguridata con la misma solución de Seguridata y AB Sistemas con la solución UniSign. Aunque se realizó un análisis exhaustivo de otras alternativas, estas también cuentan con implementaciones en instituciones de gobierno.

Tanto PSC Advantage con el producto Certifiel como AB Sistemas con Unisign, ofrecen una Infraestructura de Firma Electrónica, con los componentes necesarios para implementar una Autoridad Certificadora, pero están limitados, ya que no cuenta con una solución para la conservación de documentos electrónicos firmados a lo largo del tiempo (más de cinco años).

Como se comentó previamente, esta tecnología, permitiría asegurar la integridad de los documentos y las transacciones realizadas, a lo largo de los años, tal como ocurre con los expedientes físicos actualmente; **para la SCJN este es un aspecto relevante por el papel que representa la preservación del valor jurídico de los documentos en su ciclo de vida.** Este aspecto se valida con la existencia de componentes que cumplen con los siguientes estándares:

- Norma ISO 14721.- "reference model for an open archival information system"
- Norma ISO 15489.- "Information and documentation - Records management"
- Moreq 2.- "Model Requirements for the Management of Electronic Records"
- Norma ISO 19005.- "Electronic document file format for long term preservation"

Desde el punto de vista tecnológico, este aspecto es relevante, ya que la fortaleza de los algoritmos criptográficos tiene un tiempo de vida que está en función de los avances científicos en el área del criptoanálisis y el poder de cómputo que se requiere para romper los algoritmos.

Un segundo criterio de evaluación de las soluciones desarrolladas en México, es la propiedad del código fuente de los algoritmos criptográficos, mediante el cual se valora la capacidad de la empresa para responder a problemas de seguridad relacionados con la vulnerabilidad de los algoritmos y su capacidad para responder a la solución de incidentes. La solución desarrollada por PSC World, se basa en los algoritmos criptográficos desarrollados por Microsoft. La solución desarrollada por AB Sistemas con Unisign, se basa en la librería Java JCE desarrollada originalmente por Sun MicroSystems, ahora propiedad de Oracle. La solución desarrollada por Seguridata, es la única que ha desarrollado el código fuente de los algoritmos de cifrado que se usan en sus diferentes componentes.

Como se ha venido mencionando, la fortaleza de la infraestructura de firma electrónica, radica en los algoritmos matemáticos que se implementan en la solución. En este aspecto se resalta que únicamente la empresa Seguridata ha implementado el algoritmo de curvas elípticas, aunque en México esto se menciona como novedad, en otros países se están usando desde el año 2007 y es el único que ha desarrollado la totalidad de los algoritmos.

Por lo anterior, se determina que la empresa que cubre los requerimientos tecnológicos para construir una infraestructura de llave pública son cubiertos por la Solución de Seguridata Privada

S.A. de C.V. ya que no se encontró otra solución que cubriera los aspectos mínimos solicitados, los cuales se formularon a partir de las necesidades de confidencialidad, integridad y disponibilidad que se requiere para garantizar el valor jurídico de los acuerdos que se firmen electrónicamente en este Alto Tribunal.

Dictamen

- ✓ Seguridata Privada S.A. de C.V. es propietario de la marca Seguridata y de tecnología de Firma Electrónica Seguridata y la Entidad Certificadora. Cuenta con los documentos en el Registro Público de Derechos de Autor y los Títulos de Registro de Marca ante el Instituto Mexicano de la Propiedad Intelectual desde el año 2002. Es autor del código fuente que implementa los algoritmos de cifrado, el cual fue desarrollado y registrado en territorio mexicano, por lo que no está sujeto a las leyes internacionales, sobre la revelación de las llaves privadas de los usuarios de su infraestructura. Es la única empresa en México que cuenta con auditorías a su código para la generación de llaves, algoritmos de cifrado y números aleatorios, que demuestran su efectividad. Esta auditoría fue realizada por la Universidad Autónoma Metropolitana.

- ✓ Seguridata Privada S.A. de C.V. es el **fabricante y distribuidor exclusivo** de sus productos y no utiliza otros canales para la venta, implementación, desarrollo y soporte. La comercialización la realiza directamente el fabricante del producto.

- ✓ **Por razones de idoneidad tecnológica**
  - **Es la única empresa que cuenta con la totalidad de los componentes tecnológicos, requeridos para integrar la solución**. Ninguna otra empresa en México ha implementado los estándares requeridos para la conservación de documentos a lo largo del tiempo; ha desarrollado un componente para la creación de flujos de firmas y es desarrollador del código fuente de los algoritmos de cifrado.
  - Adicionalmente a la Infraestructura de Firma Electrónica Avanzada, cuenta con un componente para el Firmado Unilateral, Multilateral y Flujo de Trabajo, la cual será utilizada para resolver de forma transparente para resolver un conjunto de necesidades en las áreas administrativas y jurídicas de la Suprema Corte. Con lo que se reduce el tiempo para iniciar su aplicación. Las otras soluciones, implican el

desarrollo de componentes adicionales de software y el tiempo a esperar en el ciclo de desarrollo.

- Cuenta con interfaces hacia otros componentes tecnológicos, existentes en la Suprema Corte de Justicia y otras soluciones como tecnología de Flujos de Trabajo y Archivado de grandes volúmenes de información, como Alfresco y Sharepoint.
- Cuenta con interfaces hacia plataformas para el resguardo de evidencias criptográficas a lo largo del tiempo. Los algoritmos criptográficos tienen un tiempo de vida limitado, sin embargo la tecnología debe permitir la conservación de la evidencia criptográfica de una forma similar a la que ocurre con documentos físicos, garantizando la confidencialidad e integridad de los documentos aun cuando se alcance la obsolescencia de los algoritmos con los que fueron firmados.

✓ **Otras razones**

- Es el único producto cuyo código fuente ha sido desarrollado por la propia empresa, lo cual permite evaluar el nivel de madurez de la marca en relación a los otros productos, por el nivel de especialización tecnológica y matemática que se requiere para implementar los algoritmos de cifrado.
- Adicionalmente al punto anterior, el código fuente de esta marca ha sido auditado por la Universidad Autónoma Metropolitana, en los siguientes componentes: generación de llaves, algoritmos criptográficos y números aleatorios, demostrado su efectividad.

✓ Seguridad. Ya que esta infraestructura de Firma Electrónica Avanzada para este Alto Tribunal, servirá de soporte para dar el carácter legal a los documentos electrónicos, se deben tomar medidas en cuando a la divulgación de su diseño, alcances y medidas de seguridad.

✓ **Por cuestiones de seguridad de la Infraestructura Tecnológica** de este Alto Tribunal y con la finalidad de disminuir riesgos de intrusión, eliminación o alteración a la información clasificada como confidencial; tal es el caso de expedientes que podrían generar un conflicto jurídico y pérdida de credibilidad de este Alto Tribunal, se recomienda no hacer del conocimiento público la siguiente información:

- Los algoritmos y parámetros de seguridad que se estarán incorporando a la Infraestructura de Firma Electrónica, de este Alto Tribunal

Información clasificada como reservada con fundamento en la fracción V del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como la fracción V del artículo 113 de la Ley General, por contener información relativa a configuraciones de seguridad de la infraestructura de la Firma Electrónica del Poder Judicial de la Federación, podría poner en riesgo la seguridad de las personas que proporcionaron sus datos para que se les otorgue una firma electrónica.

- Arquitectura de dispositivos de seguridad de este Alto Tribunal como Firewall, sistemas de detección y prevención de intrusos (Por sus siglas en inglés Intrusion Detection/Prevention System IDS/IPS), topología de las redes de comunicación, parámetros de configuración de los equipos, configuración de redes y equipos de los actuales proveedores de telecomunicaciones.
- Arquitectura del Directorio Activo y sus políticas existentes en la que se integrará la Solución.
- Parámetros de configuración de la seguridad de cuentas y equipos de cómputo, de funcionarios que manejan información clasificada como confidencial relacionada con los procesos jurídicos.

Los puntos anteriores son necesarios proporcionar, al proveedor a quien se le contratará la arquitectura de la solución requerida, para realizar un buen dimensionamiento del proyecto.

Una Infraestructura de Firma Electrónica proporciona los recursos de seguridad informática, que se requieren para dar el valor jurídico similar al de la firma autógrafa, a los acuerdos efectuados por medios electrónicos. Estos servicios son:

- **Equivalencia Funcional**: Satisface el requisito de firma del mismo modo que la firma autógrafa en los documentos impresos
- **Autenticidad**: Permite dar certeza de que el mismo ha sido emitido por el firmante de manera tal que su contenido le es atribuible al igual que las consecuencias jurídicas que de él deriven
- **Integridad**: Permite dar certeza de que el documento que se firmó ha permanecido completo e inalterado desde su firma, con independencia del flujo que siga durante un proceso, como resultado del proceso de comunicación, archivo o presentación.

- **No Repudio:** Garantiza la autoría del documento y que dicha firma corresponde exclusivamente al firmante, el cual no puede negar que es el firmante del mismo.
- **Confidencialidad:** Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, garantiza que el documento solo pueda ser consultado por la persona a quien fue dirigido.
- **Neutralidad Tecnológica:** Consiste en que la tecnología utilizada para la emisión de Certificados Digitales y para la prestación de los servicios relacionados con la firma electrónica avanzada será aplicada de modo tal que no excluya, restrinja o favorezca alguna tecnología en particular

Estos servicios de seguridad son la esencia de la normatividad de Firma Electrónica de todas las Autoridad Certificadoras de otras instituciones.

Para la Suprema Corte de Justicia, se requiere contar con los más altos niveles de confidencialidad e integridad, ya que se puede convertir en un riesgo de alto impacto para la este Alto Tribunal y sus integrantes al permitir que un documento sea suplantado.

- ✓ **Antecedentes de Asignación Directa.** La implementación de Firma Electrónica en diversas Instituciones de Gobierno, se han realizado de manera directa, para el Caso de la Empresa Seguridata, esta ha sido asignada de manera directa por las siguientes Instituciones:
  - Instituto Federal Electoral
  - Procuraduría General de la República
  - Instituto Mexicano del Seguro Social
  - Gobierno del Estado de Hidalgo, Guanajuato y el Estado de Chiapas

  En el Poder Judicial de la Federación, tanto el Tribunal Electoral, como el Consejo de la Judicatura Federal, asignaron de manera directa la Contratación de la Infraestructura de Firma Electrónica.

La solución propuesta por Seguridata, está integrada por los siguientes elementos:

- ✓ Componentes integrados bajo una arquitectura de alta disponibilidad:

a) **Autoridad Certificadora Raíz.** Autoridad Certificadora que permitirá la homologación de otras Autoridades Certificadoras existentes contemplando:
   - Soporte para una estructura jerárquica de Autoridades Certificadoras. La Autoridad deberá permitir a la SCJN subordinar un número ilimitado de Autoridades Certificadoras, así como la capacidad para mantener la interoperabilidad lateral con otras Autoridades.
   - Compatibilidad con Autoridades Certificadoras externas como por ejemplo el SAT. Para lo cual la SCJN deberá realizar los convenios respectivos y cumplir con los requisitos especificados.
   - Compatibilidad con Directorios Activos bajo el estándar X.500 (LDAP)

b) **Autoridad Certificadora.** Que permitirá la administración de los certificados digitales emitidos a los usuarios internos y externos de la Suprema Corte. Este módulo proveerá los servicios de solicitud, emisión, revocación y validación de certificados digitales. [redacted]

c) **Autoridad de Estampillado de Tiempo.** Que permitirá emitir recibos criptográficos (constancias de tiempo) bajo estándares internacionales y que son la evidencia de la hora y fecha exacta de cualquier transacción.

d) **Componente de Firmas Electrónicas.** Componente que permitirá integrar a cualquier aplicativo de la Suprema Corte los servicios de Firma Electrónica necesarios para proporcionar la integridad, autenticidad, confidencialidad y no-repudio de la información.

e) **Gestor de Firmas Electrónicas.** Componente que gestione flujos de solicitud de firmas electrónicas, permitiendo llevar a cabo procesos de autorización mediante el uso de Firmas Electrónicas.

f) **300 Tokens biométricos para el almacenamiento de llaves de usuario.** Estos tokens permiten el cumplimiento con el estándar FIPS 140 versión 2, nivel 3.

g) **Servicios de consultoría normativos,** necesarios para la generación de las Políticas de Certificación y la Declaración de Prácticas de Certificación de la Autoridad Certificadora Raíz y la Autoridad Certificadora de la Suprema Corte.

h) **Servicios de consultoría de implementación,** necesarios para el análisis, diseño y asesoría de integración de Firma Electrónica en los sistemas de la Suprema Corte

i) **Servicios de asesoría legal,** necesarios para la definición y elaboración del marco normativo que servirá como sustento para el uso de Firma Electrónica.

DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN.

Información clasificada como reservada con fundamento en la fracción V del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como la fracción V del artículo 113 de la Ley General, por contener información relativa a configuraciones de seguridad de la infraestructura de la Firma Electrónica del Poder Judicial de la Federación, podría poner en riesgo la seguridad de las personas que proporcionaron sus datos para que se les otorgue una firma electrónica.

i) **Servicios de transferencia de conocimientos** que permitan a la Suprema Corte operar e integrar los componentes de PKI de manera autosuficiente a todos aquellos sistemas y/o procesos que lo requieran.
k) **Servicios de soporte técnico y mantenimiento** de los productos que la Suprema Corte requiere para la correcta operación del presente proyecto, por tres años.
l) **Servidores y almacenamiento requeridos para implementar la puesta en operación de la Infraestructura de Firma Electrónica.**

Costo Estimado

	Precios en dólares	Precios estimados en
Licenciamiento de software Firma Electrónica, [redacted] (incluye soporte técnico y garantía por 3 años), equipo de cómputo y almacenamiento para instalación de la solución.	$354,489.37	$4'962,851.18

Dictaminó	Autorizó	Fecha
Ing. Isai Fararoni Ramírez Director de Seguridad Informática	Lic. Otilio Esteban Hernández Pérez Director General de Tecnologías de la Información	de octubre de 2011