ULACIT

UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLOGIA

Facultad de Ingeniería Informática

Firma Digital

Un paso más para el expediente electrónico en el Sistema de Gestión de Despachos Judiciales del Poder Judicial.

Marcela Montero Flores

Cédula 303480144

Tutor

Guillermo Oviedo Blanco

2005

INDICE

1 INTRODUCCION

Actualmente existe la ley N° 8454 “LEY DE CERTIFICADOS, FIRMAS DIGITALES Y DOCUMENTOS ELECTRÓNICOS” la cual provee la legislación necesaria en Costa Rica que valide la firma digital, dándole el mismo valor que tiene la firma manuscrita. En ésta Ley se definen los certificados digitales, utilizados para generar y validar las firmas digitales.

Con el fin de estar preparados tecnológicamente para implementar la firma y certificados digitales se inicia en el poder judicial esta investigación que pretende describir el marco teórico-técnico sobre firmas digitales y también esbozar un plan con las consideraciones necesarias para empezar la puesta en marcha del Proyecto de Firma Digital, uno de los fines primordiales es mejorar el Sistema de Gestión de Despachos Judiciales, con el fin de lograr digitalizar por completo el expediente electrónico.

2 ANTECEDENTES

El Poder Judicial, por ser una institución estatal, está regida socio-económicamente, por las disposiciones de la Contraloría General de la República, la cual lleva el presupuesto anual y además aprueba las licitaciones y préstamos del BID y otros.

Por otra parte, desde el punto de vista político, la Asamblea Legislativa dicta las pautas con las cuales se rige, mediante la promulgación de leyes, que el Poder Judicial hace cumplir.

Para finalizar, legalmente debe someterse a las disposiciones de la Corte Suprema de Justicia, que da las normativas con las cuales el Poder Judicial debe regirse, para que este primero pueda ejecutar lo estipulado en las leyes por la Asamblea Legislativa.

2.1 Referencia Organizacional

El Poder Judicial, Supremo Poder de la República, tiene la obligación de hacer respetar las leyes y administrar justicia. Para cumplir con ese objetivo fundamental que le designa la Constitución Política, de administrar justicia, el Poder Judicial conformó una estructura dividida en tres ámbitos diferentes:

- Ambito Jurisdiccional
- Ambito Administrativo
- Ambito Auxiliar de Justicia

2.2 Organigrama

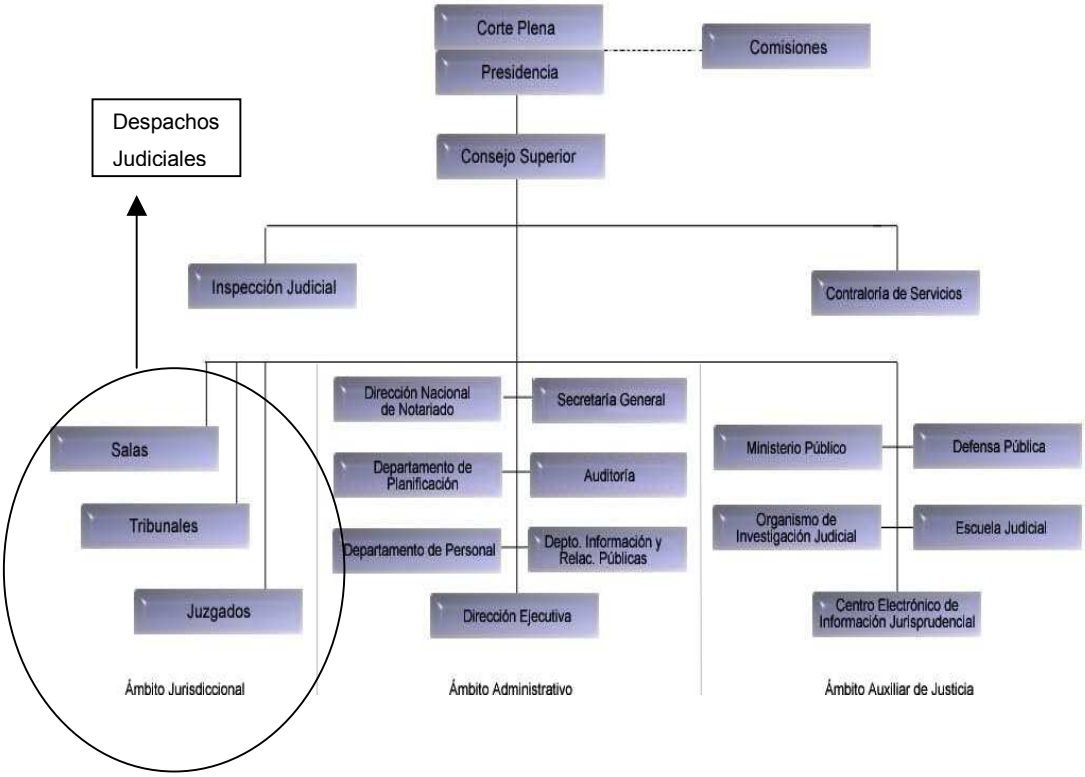

Figura #1: Organigrama del Poder Judicial de Costa Rica
Fuente: Poder Judicial de Costa Rica

2.3 Visión del Poder Judicial

Ser una administración de justicia independiente, imparcial y eficiente, que garantice la protección de los derechos y libertades de las personas con igualdad y plenitud de acceso para todos; integrada por personal consciente de su elevada función en la sociedad, que inspire confianza, contribuya al desarrollo democrático del país y a la paz social.

2.4 Misión del Poder Judicial

Administrar justicia en forma pronta, cumplida, sin denegación y en estricta conformidad con las leyes.

2.5 Valores del Poder Judicial

Los valores son guía fundamental, para el cumplimiento del deber y la cultura organizacional.

Para los usuarios representan garantía y respeto a sus derechos. Para los servidores estar inmersos en un sistema humano, independiente, donde se trabaja con honradez, mística y excelencia; que contribuye a garantizar el Estado de derecho, propiciar la seguridad jurídica y fortalecer la democracia costarricense.

La descripción de los valores que guían el accionar institucional es la siguiente:

Humanización: El ser humano es el eje central de la administración de justicia.

Independencia: Actuar con independencia funcional, imparcialidad y objetividad; el juez en sus decisiones sólo está sometido a la Constitución y a la Ley. El Poder Judicial ejercerá su función con independencia funcional, administrativa, económica y presupuestaria.

Mística: Actuar con vocación, entrega, compromiso con el trabajo e identificación plena con las funciones que desempeñan.

Honradez: Actuar con imparcialidad, decoro, legalidad y rectitud.

Transparencia: Actuar en forma abierta y clara, permitiendo el control ciudadano y de los medios de comunicación. Las servidoras y los servidores judiciales están obligados a rendir cuentas de su gestión.

Excelencia: Actuar promoviendo la calidad y eficiencia en el servicio.

3 SITUACION ACTUAL

El Poder Judicial, consciente del importante papel que cumple en el Estado de Derecho, impulsa un proceso de modernización de la administración de justicia, con el fin de remozar y hacer más eficiente la tutela judicial para todos los sectores sociales y crear el clima de confianza pública, estabilidad, transparencia y respeto a los derechos de cada uno, que constituyen el marco indispensable para propiciar el desarrollo y la expansión democrática.

La necesidad de favorecer y activar una política de modernización, se ha gestado desde el interior de la institución, mediante procesos participativos con los servidores judiciales, que han tomado en consideración la insatisfacción del público por la demora judicial, pero también la necesidad de consolidar un nuevo modelo de administración de justicia más adaptada a las necesidades de la sociedad contemporánea.

Consolidar un sistema jurídico más equitativo, accesible, eficiente y previsible, que permita reducir el retraso y la congestión judicial es el objetivo fundamental de este programa.

3.1 Proceso de Modernización

El Poder Judicial de Costa Rica lleva a cabo un ambicioso Plan de Modernización de las estructuras organizativas, los procedimientos y los sistemas de gestión con que debe hacer frente a su misión constitucional de proporcionar justicia pronta, cumplida y sin denegación.

La decisión de impulsar una política modernizadora, inició en 1993, con una consulta a los servidores judiciales, usuarios y comunidades sobre las necesidades y desafíos de la administración de justicia y la decisión de consolidar una política modernizadora, tanto a nivel legal, como a nivel de la estructura orgánica administrativa y la organización de los despachos judiciales, de acuerdo a las sugerencias dadas en esa consulta.

Paralelamente, se negoció un préstamo con el Banco Interamericano de Desarrollo, para contar con recursos extraordinarios que permitieran hacer frente con mayor solvencia, a los gastos requeridos por el proceso de cambio.

El reto que se asume es muy delicado, ya que aún cuando en términos generales existe consenso en la necesidad del cambio, existen circunstancias que hacen complejo el proceso y que son imprescindibles de tomar en cuenta. Entre ellos destaca el incremento de la litigiosidad, la participación y/o resistencia de los servidores judiciales en el proceso de cambio, la declinante percepción ciudadana acerca del servicio judicial, así como los problemas que conducen a la insatisfacción del usuario con ese servicio, que están dadas en términos generales por la: lentitud en la ejecución de los procedimientos, inadecuado acceso del usuario a la justicia; mala atención al usuario; deficiente organización del Poder Judicial; falta de información al ciudadano; corrupción; y mala calidad de las resoluciones judiciales.

La transformación comprende desde un impulso a la reforma de la legislación vigente, la simplificación y celeridad de los procedimientos, la expansión de los procesos orales, hasta la reestructuración de la oficina judicial, para adaptarla a los avances de la administración moderna y la tecnología de la información. Desde la integración de la información jurídica, relativa a doctrina, legislación vigente y jurisprudencia; pasando por el fortalecimiento de la capacitación judicial, el desarrollo de programas de educación a distancia y el remozamiento de la Escuela Judicial; hasta una reestructuración de la organización administrativa, para hacer procesos más eficientes frente a las necesidades de las oficinas jurisdiccionales.

3.2 Sistema Costarricense de Gestión de los Despachos Judiciales

El objetivo del sistema es crear e implantar nuevos modelos para la tramitación judicial con un avanzado soporte informático que permitan un mejoramiento verificado de la gestión de los despachos judiciales y por ende un mejor servicio al público.

El proyecto se concibió para que los despachos judiciales trabajen con sistemas informáticos que mantengan en forma integra la información de los expedientes, desde una oficina de primera instancia (son las oficinas donde los procesos entran por primera vez a conocimiento del juez para resolver el diferendo entre partes) hasta las salas de casación de la corte (es donde se revisan los posibles vicios, omisiones y violaciones a la ley por parte del tribunal colegiado en un determinado caso). Esto facilita la labor de administrar justicia ya que los servidores judiciales, abogados, partes y público en general cuentan con herramientas informáticas adecuadas para ubicar y conocer el estado de un expediente con sólo digitar el número único.

3.2.1 Descripción general de la funcionalidad del sistema

El sistema de Gestión es una herramienta informática diseñada para dar soporte al modelo organizacional de los despachos judiciales del Poder Judicial. Sus funcionalidades son las siguientes:

Tramita: cuenta con herramientas de productividad que permiten, entre otras utilidades, la emisión de documentos en forma interactiva. Entre sus funciones se puede destacar la integración automática de los documentos por el PJ-Editor (un Editor de texto desarrollado especialmente para el Poder Judicial) con la información de los asuntos almacenados en la base de datos.

Genera libros de registro: las actuaciones de un despacho judicial son "capturadas" de forma automática por el sistema, el cual las incorpora a la base de datos de la que extrae la información utilizada para la confección de diferentes libros y la generación de estadísticas.

Fomenta el impulso procesal: este seguimiento procesal, permite acotar la duración de la tramitación, dando respuesta al problema de paralización o retardo en la tramitación de los expedientes. Esto se logra con:

- La medición de índices de congestión, retraso y productividad según los criterios que se definan.
- Funcionalidades que permiten identificar los casos sobre los que es necesario actuar.
- Un histórico de todos los trámites que se han ido generando en el sistema a lo largo de la vida del expediente.

Independiza el modelo organizativo: el sistema se sustenta en una filosofía de integración y de agregación de oficinas de la misma materia y de servicios comunes. Debido a esto, los modelos organizativos y sus procedimientos, no inciden en su estructura fundamental.

Integra y facilita la comunicación: dispone de medios de transferencia de información a través de su universo para su tratamiento por cualquier despacho que lo requiera, facilitando la agregación, fusión y consolidación de datos dispersos.

Controla las ubicaciones de los expedientes: por medio de mecanismos de señalización efectivos, se puede conocer donde está físicamente el expediente, lo que reduce el tiempo de búsqueda y localización de los mismos.

Archivo: se provee un servicio común de control de los expedientes para los archivos de circuito o despacho, dependiendo de sí se implanta en un circuito judicial o en un despacho independiente.

Integra servicios comunes: permite accesar los servicios comunes de las aplicaciones independientes instaladas en la Oficina de Recepción y Distribución de Documentos(RDD) y en la Oficina de Citaciones y Notificaciones(OCN).

Estimula la dinámica procesal: ofrece la posibilidad de definir avisos del sistema que funciona como alarmas, advirtiendo al usuario del cumplimiento de determinados lapsos y permitiendo la toma de decisiones.
Las alarmas pueden definirse a partir de:

- Secuencialidad y lapsos de ciertos trámites procesales.
- Apuntes de la agenda.
- Escritos pendientes de contestación.

Permite consultas: utiliza filtros predefinidos para poder realizar la búsqueda de la información. Al mismo tiempo, facilita la definición de nuevas consultas mediante la combinación de varios de estos filtros predefinidos. Esto

le brinda al sistema agilidad y versatilidad, al tiempo que incrementa la eficiencia.

Se puede observar que el sistema GDJ (Gestión de Despachos Judiciales) es una herramienta muy completa para el trámite de expedientes en miras al expediente electrónico, sin embargo aunque el sistema puede agregar al expediente electrónico diferentes tipos de archivos, no se cuenta con la infraestructura necesaria para poder adjuntar archivos recibidos externamente, tanto documentos como imágenes y audio.

Es en busca de esta digitalización total del expediente que se piensa en la firma digital como medio para garantizar la fidelidad de los documentos recibidos del exterior electrónicamente y poderlos agregar al sistema.

3.3 Proceso de un Expediente

Se debe tener presente que un expediente pasa por diferentes procesos dependiendo del asunto que trate y el despacho en el cual se tramita, pero a continuación se describe brevemente uno de los procesos comunes por los que pasa un expediente, en la figura #2 se puede ver el proceso gráficamente.

Se tiene la existencia de un ciclo que a lo largo de la tramitación de cada expediente puede repetirse varias veces.

a) El impulso de la actividad de la oficina de Tramitación puede generarse por:
   - a.1. Recepción de un asunto nuevo.
   - a.2. Recepción de un escrito relacionado con un asunto.
   - a.3. Cumplimento de un término en la agenda.
   - a.4. Decisión del Juez Decisor.
   - a.5. Cumplimiento de un acto de comunicación.

b) Apertura de un nuevo expediente o búsqueda del existente.
c) Realizar un acto, por ejemplo, asistir a un juicio.
d) El Juez Tramitador estudia el asunto y decide:
   d.1. Ubica el expediente en casillero en espera de tomar una decisión
   d.2. Ordena la emisión de un documento.
   d.3. Remite el expediente al Juez Decisor para que adopte una decisión.
   d.5. Ordena el archivo (provisional o definitivo).

El Juez Tramitador puede encargar a un auxiliar la tramitación de una determinada etapa procesal de un asunto o parte de ella. En este caso y sólo para estos asuntos, el auxiliar asume la tarea del Juez Tramitador excepto en los asuntos en que necesite consultarlo.

e) Los auxiliares elaboran el documento, consultando y revisando expedientes.
f) Se somete el documento a revisión y firma.
g) Se agregan documentos a los expedientes.
h) Si procede se efectuará una anotación en la agenda.
i) Si procede se ordena acto de comunicación.
j) Se coloca el expediente en el casillero a la espera de un nuevo ciclo o se remite al archivo del circuito.

CICLO DE TRABAJO DENTRO DE LA OFICINA DE TRAMITACIÓN DEL DESPACHO JUDICIAL

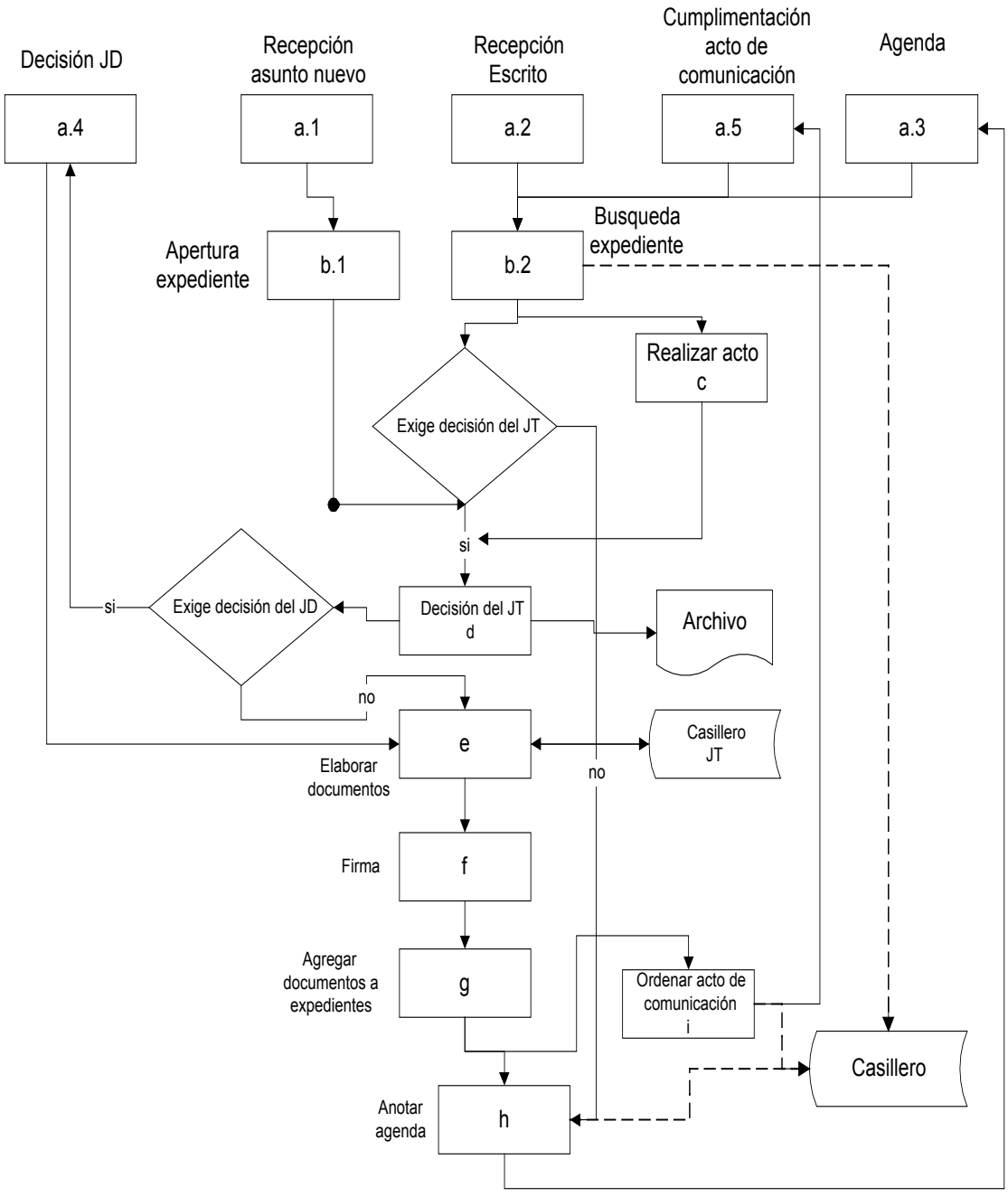

Figura #2: Proceso de trámite de un expediente

Fuente: Area de Normalización del Sistema de Gestión de Despachos Judiciales

4 MARCO TEORICO

4.1 Definiciones

4.1.1 Función hash

Una función hash es un algoritmo que se utiliza para dotar a un documento digital de integridad, esto es, poder detectar cualquier alteración posterior a su firma. Este algoritmo produce un número en función del documento, el largo del número depende de la versión del algoritmo hash, este número es un resumen del documento, si el algoritmo se aplica siempre al mismo documento produce el mismo número en cuestión, pero si el documento variase en tan sólo un bit de información el número producido va a diferir completamente del anterior. El número creado por este algoritmo determina al documento en forma unívoca.

Estos algoritmos se encuentran categorizados dentro de una clase de funciones que se conocen como funciones de un solo sentido (One way function) puesto que dado un documento es posible obtener siempre su número resumen pero, por el contrario, es prácticamente imposible deducir el documento original a partir del número resumen. Esto permite garantizar la unicidad e integridad del documento que se esta por firmar.

4.1.2 Sistema criptográfico asimétrico

En un sistema criptográfico asimétrico, cada usuario posee un par de claves propias, llamadas clave privada y clave pública, las cuales son dos claves numéricas representadas generalmente por una larga secuencia de dígitos y letras y que además cumplen dos propiedades.

La primera propiedad que cumplen es que la vinculación entre ellas es biunívoca, no habiendo dos claves privadas que se correspondan con una

misma pública o viceversa. De esta forma no pueden ser elegidas al azar, sin embargo, hay algoritmos, o programas, que se encargan de generar este par de claves.

La segunda propiedad que cumplen es que, a pesar de ser únicas, conociendo solamente una de ellas y el algoritmo que las generó es imposible deducir cual es la otra clave ni tampoco a partir de los documentos cifrados con cualquiera de ellas.

El sistema opera de tal modo que la información cifrada con una de las claves sólo puede ser descifrada con la otra. De este modo si un usuario cifra determinada información con su clave privada, cualquier persona que conozca su clave pública podrá descifrar la misma. En consecuencia, si es posible descifrar esa información utilizando la clave pública correspondiente y sabiendo fehacientemente que pertenece a una persona determinada, entonces esa información solo pudo haber sido generado por esa persona utilizando la única clave privada que se corresponde con esa pública.

Por este motivo una vez generado el par de claves, la clave pública debe ser entregada a una Autoridad Certificante, que actúa como tercera parte confiable, quien la incluirá en un certificado digital de manera que pueda asegurar que esa clave pública pertenece a su titular y no a otra persona.

El algoritmo más utilizado en este procedimiento de encriptación asimétrica es el RSA, llamado así por sus autores: Rivest, Shamir y Adleman.

4.2 Firma Electrónica (Digital)

Hay diversas definiciones de Firma Digital o Firma Electrónica a continuación se presentan varias:

“Cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico.”(Ley de Certificados, Firma Digitales y Documentos electrónicos, ley Nº 8454 Costa Rica, 2005, artículo 8°)

“La firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, permitiendo que estos gocen de una característica que únicamente era propia de los documentos en papel.

Una firma digital es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje.

La firma digital no implica asegurar la confidencialidad del mensaje; un documento firmado digitalmente puede ser visualizado por otras personas, al igual que cuando se firma holográficamente.

La firma digital es un instrumento con características técnicas y normativas, esto significa que existen procedimientos técnicos que permiten la creación y verificación de firmas digitales, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen. “ (Subsecretaría de la Gestión Pública de Argentina . (2005). ¿Qué es firma digital?. Recuperado el 15 de septiembre del 2005, de http://www.pki.gov.ar/index.php?option=content&task=view&id=322&Itemid=180)

En este documento se utilizará el término Firma Digital y Firma Electrónica como iguales.

4.2.1 Funcionamiento de la firma digital

La firma digital se puede utilizar en cualquier documento digital, por ejemplo, correos electrónicos, archivos de imágenes, archivos de audio, páginas web, programas de software, etc. Cualquier archivo digital que requiera ser autentificado por su autor.

"La firma digital funciona utilizando complejos procedimientos matemáticos que relacionan al documento firmado con información propia del firmante, y permiten que terceras partes puedan reconocer la identidad del firmante y asegurarse que los contenidos no han sido modificados. El firmante genera, mediante una función matemática, una huella digital del mensaje. Esta huella digital se cifra con la clave privada del firmante, y el resultado es lo que se denomina firma digital la cual se enviará adjunta al mensaje original. De esta manera el firmante va a estar adjuntando al documento una marca que es única para ese documento y que sólo él es capaz de producir. "(Subsecretaría de la Gestión Pública de Argentina . (2005). ¿Cómo funciona la firma digital?. Recuperado el 15 de septiembre del 2005, de http://www.pki.gov.ar/index.php?option=com_content&task=view&id=331&Itemid=180&lang=es&PHPSESSID=5047f01e974a14b3c5ab08b966b31178)

En el proceso de firmar digitalmente se utilizan las funciones hash para asegurar la integridad del archivo digital y algoritmos de encriptación asimétrica para asegurar su autenticidad.

4.2.2 Pasos a seguir al realizar la firma

El procedimiento de firmar se resume así:

- Para firmar un documento el software del firmante aplica un algoritmo hash sobre el archivo a firmar obteniendo un extracto de longitud fija, y absolutamente específico para ese mensaje.
- Este extracto que se obtiene de la función hash se somete a continuación a cifrado mediante la clave privada. De esta forma se

obtiene un extracto final cifrado con la clave privada del autor el cual se añadirá al archivo para que se pueda verificar el autor e integridad del documento por aquella persona interesada que disponga de la clave pública del autor.

- El receptor del archivo, requiere comprobar que la firma realizada es válida. Es necesario que el receptor conozca la clave pública del autor. El software del receptor, previa introducción en el mismo de la clave pública del remitente (obtenida a través de una autoridad de certificación), descifraría el extracto cifrado por el autor; a continuación calcularía el extracto hash que le correspondería al archivo, y si el resultado coincide con el extracto anteriormente descifrado se consideraría válida, en caso contrario significaría que el archivo ha sufrido alguna modificación posterior al firmado.

En la figura #3 se muestra el proceso que se sigue al firmar y verificar la firma digital.

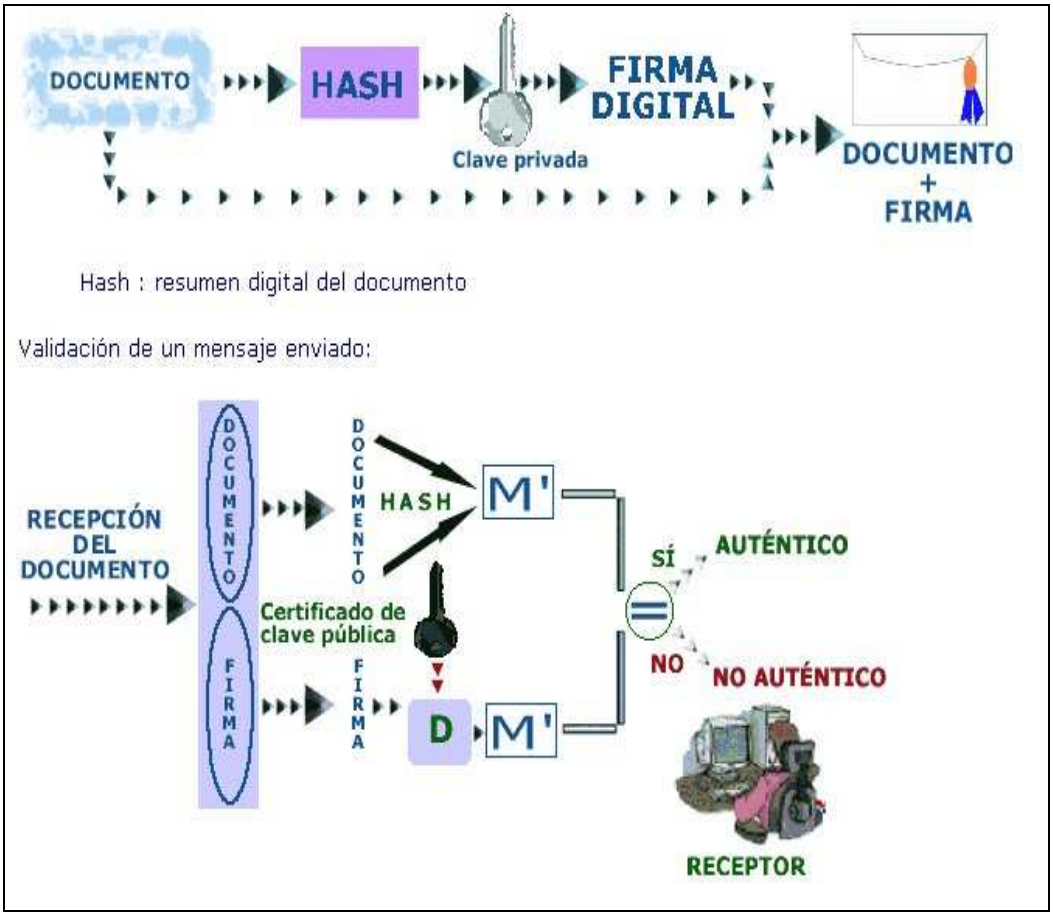

Figura #3: Diagrama de Firma Digital

Fuente: Asociación de Asesores de Empresas en Internet. http://www.internautas.org

En la firma digital se cumplen tres características fundamentales:

1. **Autenticación del Firmante**: Se autentifica en el momento que el receptor logra desencriptar con la clave pública proporcionada en el certificado digital. Por la propiedad de correspondencia biunívoca entre claves privadas y públicas, se puede asegurar que la clave pública proporcionada es la pareja irrefutable de la clave privada con que se encriptó. Y la Autoridad Certificante certifica la identidad de la persona a la que pertenece la clave privada.
2. **Integridad del Archivo**: Se determina al aplicar en el destino el algoritmo hash, el resultado debe ser igual a lo obtenido de desencriptar con la clave pública. Debido a que en el emisor, se encriptó con la

clave privada el resultado del algoritmo hash. Por tanto al coincidir estos resultados se asegura, que el archivo no fue alterado.

3. **No repudio en Origen:** Se debe verificar que el certificado digital sea válido, es decir, no se haya vencido, revocado o anulado. De estar activo, el firmante no puede negar su firma.

En términos generales al firmar digitalmente se requiere:

- La pareja de claves privada y pública
- Contar con el certificado digital emitido por una autoridad certificante autorizada.
- Software que permita realizar la firma digital
    - Se deben establecer los tipos de archivos que requieren firma digital.

En términos generales al verificar la firma digital se requiere :

- Certificado digital que contenga la clave pública del firmante.
- Software que permita realizar la verificación

4.3 Certificados Digitales y Autoridades de Certificación

En el esquema de la figura #3 en la verificación de la firma, se puede notar que un elemento necesario es que el certificado digital debe ser emitido por una autoridad certificadora autorizada. El propósito del certificado es proporcionar la clave pública al receptor, y por parte de la entidad certificadora legitimar que es la clave pública que corresponde a la clave privada asociada al autor de la firma. Si no se cuenta con un certificado digital la firma no es de confianza.

4.3.1 Certificados digitales

En la Ley de Certificados, Firmas Digitales Y Documentos Electrónicos de Costa Rica, se define, en el **artículo 11,** un certificado digital como: "el mecanismo electrónico o digital mediante el que se pueda garantizar, confirmar o validar técnicamente:
a) La vinculación jurídica entre un documento, una firma digital y una persona.
b) La integridad, autenticidad y no alteración en general del documento, así como la firma digital asociada.
c) La autenticación o certificación del documento y la firma digital asociada, únicamente en el supuesto del ejercicio de potestades públicas certificadoras.
d) Las demás que establezca esta Ley y su Reglamento. "

Pueden haber diferentes formas de certificar, así como puede variar el contenido de los certificados, sin embargo se hará mención de la forma más utilizada:

- El contenido de los certificados digitales abarca la clave pública de la persona a la cual se le emitió, el nombre completo, una fecha de expiración y datos relevantes de la autoridad certificante que emitió el certificado.

Es importante aclarar que el certificado en si está firmado digitalmente por su emisor, de esta manera se asegura la integridad de la información contenida en él.

El formato de estos certificados está definido por el estándar internacional ITU-T **X.509**. De esta forma, los certificados pueden ser leídos o escritos por cualquier aplicación que cumpla con el estándar.

Hay diversos tipos de certificados, existen certificados de correo electrónico, usuario, servidor, sitio web, etc. estos certificados varían

dependiendo de las necesidades del solicitante y de los requerimientos de registro exigidos por la autoridad.

Los certificados digitales de correo electrónico certifican simplemente el origen de un mensaje, es decir, certifican que el mensaje proviene de la cuenta correo que se indica en el certificado digital, en estos casos el interesado en obtener un certificado de esta clase puede realizar su registro por medios electrónicos.

Los certificados de usuario certifican la identidad del firmante, debido a esto en el proceso de registro se debe establecer la presencia física ante la oficina de registro de la entidad certificadora.

Las políticas de certificación deben estar contenidas en un documento que debe publicar las autoridades certificadoras, en el cual se definen los procedimientos de certificación, requisitos para obtener certificados, etc, y se deben establecer para cada tipo de certificado a emitir.

4.3.2 Autoridades certificadoras

En la Ley De Certificados, Firmas Digitales Y Documentos Electrónicos de Costa Rica, se define, en el **artículo 18,** una Autoridad Certificadora como "la persona jurídica pública o privada, nacional o extranjera, que emite certificados digitales y está debidamente autorizada según esta Ley o su Reglamento; asimismo, que haya rendido la debida garantía de fidelidad."

Las autoridades de certificación deben cumplir con una serie de tareas tales como: Recibir solicitudes, emitir, revocar, renovar, anular certificados. Estas funciones se basan en políticas y normas que la misma autoridad certificante debe crear. En la figura #4 se muestra un esquema de las

actividades relacionadas a los certificados que debe realizar una entidad certificadora.

Figura #4: Diagrama de Certificados

Fuente: Asociación de Asesores de Empresas en Internet. http://www.internautas.org

Las autoridades de certificación utilizan oficinas de registro como delegadas o mediadores entre usuarios y la entidad certificante, existen porque en ocasiones por la ubicación física de la entidad se hace lejano acceder a sus servicios. Las oficinas reciben solicitudes directas de los usuarios interesados en certificados que posteriormente las hacen llegar a la autoridad certificante. En tipos de certificado donde se autentifica la firma de una persona se establece como requisito indispensable la presentación física de dicha persona ante alguna oficina de registro autorizada, oficina donde se valida y autentifica al individuo.

Las autoridades certificantes deben procesar solicitudes de emisión, revocación, anulación, renovación de los certificados. Las solicitudes se procesan a través de las oficinas de registro autorizadas.

En el artículo 12 inciso “e” del Proyecto de Ley se autoriza a las instituciones del estado a ser autoridades certificadoras:

“Fungir como un certificador respecto de sus despachos y funcionarios, o de otras dependencias públicas, en el caso del Estado y las demás instituciones públicas.”

4.4 Infraestructura de Claves Públicas (PKI)

Es común ver que la mayoría de productos de seguridad y soluciones globales seguras están relacionadas a PKI. Las infraestructuras de clave pública (PKI en inglés) se están poniendo de moda. ¿Es todo una nueva palabra mágica en labios de sonrientes comerciales? ¿Qué hay detrás de las PKI? ¿Qué significa PKI exactamente?

PKI tiene sus orígenes en la criptografía de clave pública, cuyos orígenes se remontan al artículo seminal de Diffie y Hellman en 1976, donde se explica la idea revolucionaria de servirse para las operaciones criptográficas de una pareja de claves, una pública, conocida por todos, y otra privada, sólo conocida por el usuario a quien le es asignada. Un mensaje puede ser cifrado por cualquier persona usando la clave pública, ya que es públicamente conocida, aunque sólo el poseedor de la clave privada podrá descifrarlo. Recíprocamente, un mensaje cifrado con la clave privada sólo puede ser cifrado por su poseedor, mientras que puede ser descifrado por cualquiera que conozca la clave pública.

Estas propiedades de la clave pública, cuyo uso más común se plasma en la firma digital, la convierten en candidata ideal para prestar servicios como la autenticación de usuarios (para asegurarse de la identidad de un usuario, bien como signatario de documentos o para garantizar el acceso a servicios distribuidos en red, ya que sólo él puede conocer su clave privada, evitando así

la suplantación), el no repudio (para impedir que una vez firmado un documento el signatario se retracte o niegue haberlo redactado), la integridad de la información (para prevenir la modificación deliberada o accidental de los datos firmados, durante su transporte, almacenamiento o manipulación), la auditabilidad (para identificar y rastrear las operaciones, especialmente cuando se incorpora el estampillado de tiempo), y el acuerdo de claves secretas para garantizar la confidencialidad de la información intercambiada, esté firmada o no. Si se desea todos estos servicios de seguridad PKI puede ser la respuesta.

Sin embargo surgen muchas dudas fundamentadas, ¿cómo podemos estar seguros de que la clave pública de un usuario, que hemos encontrado por ejemplo en un directorio o una página web, corresponde realmente a ese individuo y no ha sido falsificada por otro? ¿Cómo fiarnos de esa clave pública antes de confiarle algún secreto nuestro? La solución más ampliamente adoptada consiste en recurrir a una tercera parte confiable, erigida en la figura de una autoridad de certificación (AC). La función básica de una AC como ya se ha mencionado anteriormente reside en verificar la identidad de los solicitantes de certificados, crear los certificados y publicar listas de revocación cuando éstos son inutilizados.

Los mayores obstáculos a los que se han enfrentado las empresas pioneras en la implantación de soluciones PKI para sus necesidades de negocio electrónico han sido tradicionalmente:

- La falta de interoperabilidad, ya que el mero hecho de ceñirse al estándar X.509.v3 no garantiza en absoluto que dos certificados generados por dos sistemas desarrollados por casas distintas sean mutuamente compatibles. Además, existen problemas de confianza entre AC de distintas organizaciones, que puede imposibilitar la verificación con éxito de cadenas de certificación cuya AC raíz sea desconocida o no confiable, invalidándose todo el esquema de PKI.
- El coste ha sido un problema desde el principio. Al no existir un mercado suficientemente maduro en PKI, cada empresa que ofrece soluciones de

clave pública tiene su tarifa en función de criterios diversos (por certificado, por uso de certificado, por servidores instalados, etc.) y cobra honorarios también dispares, de manera que la inversión en PKI como respuesta a las necesidades de seguridad y accesibilidad a los activos informáticos de la empresa puede resultar cuando menos inesperadamente elevada.

- PKI termina presentando problemas de escalabilidad, cuando el número de certificados emitidos a los usuarios va creciendo, debido a que las listas de revocación deben ser consultadas en cada operación que involucre certificados y firmas digitales, si se desea una implantación seria y robusta de PKI.
- Finalmente, la tecnología PKI se le antoja un tanto enigmática al usuario final, que no terminan de entender del todo la jerga relacionada. Acostumbrado a autenticarse sin más que introducir su nombre y contraseña, puede sentirse fácilmente rebasado por la complejidad tecnológica de las firmas digitales y demás funciones criptográficas. Por demás, en la medida en que no se instauren las tarjetas chip, controles biométricos y otros dispositivos similares criptográficamente robustos, el problema de los usuarios anotando su contraseña (en este caso para acceder a su clave privada) en un post-it pegado en el monitor persistirá por mucho tiempo.

Se puede decir que PKI puede constituir la solución a los problemas de una empresa dependiendo de qué problemas afronte. No existen fórmulas mágicas ni soluciones generales aptas para todo tipo de negocio.

La PKI resulta ideal en una intranet, en la que se comparten documentos (trabajo en grupo), se accede a recursos de red (cálculo, servidores de archivos, bases de datos, etc.), se intercambia correo certificado entre los empleados, etc. PKI resulta mucho más ágil que los sistemas tradicionales de control basados en nombre y contraseña y listas de control de acceso.

En el caso de extranets o de Internet, PKI es de uso obligado. De hecho, es la única forma conocida actualmente de prestar confianza a los actores de las relaciones telemáticas que no se conocen entre ellos, tanto en el business-to-business entre empresas, como en el comercio al por menor, entre vendedores y compradores particulares por Internet.

Las últimas iniciativas de las Administraciones Públicas para descargar procedimientos administrativos, realizados en papel y sometidos a la venalidad burocrática, hacia procesos digitales interactivos, hacen uso también de tecnología PKI.

5 CONSIDERACIONES TÉCNICAS

Se debe contar con equipo y herramientas de software que permitan implementar una infraestructura de clave pública en forma segura y eficiente. La institución ha comprado tecnología Microsoft, tomando en cuenta este aspecto, se consultó la factibilidad de crear una infraestructura de clave pública con la misma tecnología para disminuir el costo del proyecto. Con la versión Microsoft Windows Server 2003 Enterprise Edition se puede implementar completamente la infraestructura de claves públicas, software que si se tiene en la institución. Para una instalación y configuración correcta del conjunto de herramientas de Microsoft Windows Server 2003 se debe contar con una capacitación o asesoría.

Las entidades certificantes deben implementar un diseño de acuerdo a sus necesidades. Dependiendo del diseño que se proponga así será el equipo que se requiera, por tanto, primero se debe diseñar la infraestructura para determinar la necesidad de equipo. Como mínimo se requerirá un servidor con Microsoft Windows Server 2003, Enterprise Edition.

Se debe considerar también aspectos de cableado y equipos de comunicación, procurando la seguridad y eficiencia.

Un aspecto de suma importancia es tener un plan de contingencia ante sucesos de comunicación, equipo, software, e inclusive ante una violación física al lugar donde se encuentren los equipos de la institución.

La implementación técnica depende de la definición de los procedimientos, políticas y normas definidas para la autoridad, por tanto no se puede empezar a efectuar configuraciones en las herramientas de software ni en el equipo sin que inicialmente exista un esclarecimiento de esos aspectos.

5.1 Proyecto de Firma Digital

El proyecto de Firma Digital tiene como fin definir la utilización de la firma digital en el Poder Judicial, así como proporcionar herramientas para realizar la firma y verificación en los archivos que se solicite. Establecer normas y procedimientos que controlen este proceso junto con la comunicación de los documentos firmados, e inclusive el control de seguridad y respaldo de los directorios donde se almacenen. Se debe tener presente que un efecto de la utilización de la firma digital es la despapelización, por tanto se deben crear y regular los nuevos procedimientos de comunicación electrónica.

La firma digital se puede utilizar en cualquier documento electrónico, por ejemplo:

- Un mensaje de e-mail
- Una página Web
- Archivos de Microsoft Word
- Archivos de PJ-Editor

- Una imagen (bmp, jpg, etc.)

Se puede tener una herramienta que permita firmar cualquier archivo electrónico, o bien utilizar la funcionalidad de firma digital que provea la misma herramienta con que se crea el archivo, si es que cuenta con una.

En el Poder Judicial se puede utilizar la firma digital en el correo electrónico, en todos los archivos de texto utilizados para la comunicación interna y recepción externa, en las sesiones de las aplicaciones creadas en la institución, en los servicios que se brinden a través del sitio web y al iniciar la sesión con los servidores al ingresar a la red.

5.1.1 Correo electrónico

Se puede hacer uso de la herramienta Microsoft Outlook para administrar los correos electrónicos del personal y de los despachos. Al personal autorizado en poseer una dirección de correo electrónico se le instala y configura esta herramienta para que pueda recibir, enviar, reenviar, eliminar, y demás acciones con los correos electrónicos provenientes de otros empleados u oficinas, así como de direcciones externas a la institución.

La firma digital en el correo electrónico se puede realizar por medio de un certificado digital para correo electrónico, la firma le garantiza al receptor que el correo proviene del emisor que firma. El certificado digital en el correo también se puede utilizar para cifrar mensajes, al cifrar los mensajes se previene que información sensible o altamente confidencial incluida en el mensaje sea vista o alterada por intrusos. Para enviar un correo cifrado, tanto el remitente como el destinatario deben poseer un certificado digital válido.

Para configurar en Microsoft Outlook la utilización de un certificado digital se deben seguir los siguientes pasos extraídos de la ayuda de esta herramienta:

- Tener un certificado digital para correo electrónico, este debe ser emitido por una autoridad certificante.
- En el menú **Herramientas**, haga clic en **Opciones** y, después, en la ficha **Seguridad**.
- Haga clic en **Configurar correo electrónico seguro**.
- Escriba un nombre en el cuadro **Nombre de configuración de seguridad**.
- En la lista **Formato de mensaje seguro**, haga clic en **S/MIME**.
- Haga clic en **Elegir** junto al tipo de seguridad que desea configurar y seleccione su certificado digital.

Estos pasos configuran el Outlook para que en adelante se utilice el certificado digital seleccionado para firmar y cifrar sus correos electrónicos. Después de realizar esta configuración podrá firmar y cifrar correos, para conseguir esto debe seguir los siguientes pasos que se indican en la ayuda de esta herramienta:

- Redacte un mensaje.
- En el mensaje, haga clic en **Opciones**.
- Active la casilla de verificación **Agregar firma digital al mensaje saliente**.
- Para modificar las opciones de seguridad, en el menú **Archivo** haga clic en **Propiedades** y, después, en la ficha **Seguridad**.
- Haga clic en **Enviar**.
-

De esta manera ha enviado un correo firmado digitalmente utilizando el certificado digital que configuró para estos fines.

Técnicamente es muy sencillo para los usuarios utilizar la firma digital y cifrado en los correos electrónicos. El único inconveniente es obtener en este momento un certificado digital válido para estos fines. Se debe definir que usuarios u oficinas deben poseer esta clase de certificados.

El correo electrónico actualmente es muy utilizado para intercambiar información de interés para todos los empleados, estos procedimientos son regulados por **"El Manual de Procedimientos de las Comunicaciones por medios electrónicos de las Oficinas Judiciales".** La utilización de la firma digital en los correos electrónicos implica cambios en este manual debido a que se debe autorizar y regular su uso.

5.1.2 Archivos de texto

En la institución se utilizan dos editores de texto, el Microsoft Word y el PJ-Editor. El primero es de la familia de productos Microsoft Office, el segundo es un producto hecho a la medida para la institución. También se utiliza en gran medida el Microsoft Excel para rendir informes, reportes, etc.

El PJ-Editor se utiliza en las oficinas donde se tiene instalado el Sistema Costarricense de Gestión de los Despachos Judiciales. Con este editor se crean todos los documentos creados en el proceso judicial, así como las resoluciones, las solicitudes del ministerio público, etc.

El Microsoft Word y el Microsoft Excel se utilizan en el resto de oficinas para crear todos los documentos necesarios en la comunicación interna y externa. Toda el área administrativa lo utiliza para crear sus oficios, informes, comunicados, actas, etc.

Se debe desarrollar un módulo en el Sistema de Gestión de Despachos Judiciales que permita firmar digitalmente estas clases de archivos.

5.1.3 Recepción de documentos

La institución recibe gran cantidad de documentos de origen externo tanto en el área administrativa como en el área jurisdiccional. Por lo que se vuelve de gran interés brindar un servicio de recepción de documentos electrónicos en el área jurisdiccional, donde los usuarios no requieran trasladarse hasta los diferentes despachos para hacer entrega de escritos.

Para ofrecer este servicio se deben definir medios de entrega electrónica, sea correo electrónico, aplicación vía web, etc. Se debe definir el tipo de formato en que deberán ser entregados los escritos, debido a que no se puede aceptar formatos de archivos que la institución no pueda procesar. Otro aspecto a considerar es uno de los más importantes y es la comprobación de la firma digital de los escritos. Para comprobar la firma se requiere el certificado digital correspondiente, el mismo debe ser emitido por alguna de las autoridades certificadoras que sean clasificadas como autoridades de confianza.

Con la aprobación de la ley de Firmas y Certificados Digitales de Costa Rica, se debe proceder a establecer las normas y procedimientos que permitan el proceso de recepción electrónica. Los procedimientos definirán las necesidades técnicas necesarias para implantar el servicio, así por ejemplo, si se decide establecer como medio de recepción un servicio en el sitio web, se deberá crear una aplicación que cumpla con esos requerimientos.

5.2 Propuesta: Herramienta de Firma Digital Genérica

La opción más sencilla para firmar digitalmente es contar con una herramienta de escritorio que simplemente realice el proceso de firma a cualquier tipo de archivo, el cual se instala en las máquinas que así lo requieran.

Para realizar el proceso de la firma solicita al usuario la escogencia del documento más el certificado digital con el cual se realizará la firma.

Un problema con este tipo de herramientas es el manejo de firmas múltiples, generalmente las herramientas de firma digital de escritorio no poseen esta característica, debido a que es una herramienta monousuario. Cada usuario es responsable de almacenar e identificar posteriormente sus documentos firmados.

5.3 Propuesta: Herramienta de Firma Digital Genérica y control del Flujo de Trabajo

Una opción más compleja que la anterior es crear una herramienta que controle la firma digital en los documentos así como el flujo de trabajo que se genera a partir de ellos. Sería deseable que tuviera como mínimo las siguientes características:

- Permitir aplicar la firma digital a cualquier clase de archivo válido, así como la verificación de la misma.
- Permitir y controlar la Firma Múltiple, en casos en que los archivos requieren la firma de más de un firmante.
    - Controlar la secuencia de firmado.

- Crear una herramienta en ambiente WEB, que se pueda utilizar abriendo el Internet Explorer desde la intranet del Poder Judicial, permitiendo el firmado desde cualquier oficina o despacho conectado a la red interna mediante acceso a la intranet.
- Controlar el ingreso de usuarios con acceso a las funcionalidades del sistema dependiendo de su perfil.
- Utilizar encriptación en la transmisión de información sensible por la red para lograr una mayor seguridad.
- Comprimir los archivos para la transmisión de información logrando así un ahorro en ancho de banda.
- Controlar los diversos estados de la firma.
    - Pendiente
    - Realizada
    - Revocada
    - Firmado Completo
    - Archivar
- Registrar información relevante a cada documento
    - Emisor y destinatarios.
    - Fecha de firma.
    - Fecha de envío para firmar.
    - Etc.
- Interactuar con Outlook para realizar la entrega de los Documentos Firmados a los destinos seleccionados.
- Registrar el acuse de recibo de los documentos firmados, al ser entregados a sus destinos.
- Consultar y generar los reportes según se requieran.
    - Por firmante
    - Por estado
    - Por documento
- Poseer un certificado digital por cada usuario.

- Agregar documentos a firmar, al agregarlo a firmar el usuario que hizo el movimiento se convierte en el custodio del documento.
- Visualizar los documentos correspondientes al usuario que tiene en:
  - Pendiente de firma
  - Revocados, estos son los que envío a firmar por otro usuario y le fueron revocados con alguna observación.
  - Firmado Completo, documentos firmados y listos para enviar a su destino.
- Controlar los respaldos de todos los documentos ingresados al sistema para firmar.

Con una herramienta que cumpla esas características se controlaría no solo el proceso de firma sino también el proceso de comunicación de los documentos a sus destinos respectivos, por lo menos en el ámbito interno de la institución.

Asimismo se manejaría un control de respaldo del archivo electrónico que se crearía a partir de la acumulación de documentos firmados digitalmente

Podría ampliarse las características para que se ofrezca el servicio de firmado y entrega en el sitio Web de la institución, permitiendo la recepción electrónica de escritos a los despachos judiciales.

6 CONCLUSIONES

Este documento es un recuento general de los temas que intervienen en el proceso de los certificados y firma digital. El tema es amplio y puede convertirse en complicado si no se tienen las bases necesarias para comprender la teoría expuesta. Por otro lado, imaginar su empleo en el Poder

Judicial requiere un amplio conocimiento del trabajo que se realiza en todas las áreas de la institución.

Esta investigación preliminar hace comprender que se debe realizar un gran proyecto. El cual consiste en proporcionar una herramienta de software que permita controlar el proceso de la firma y verificación de cualquier clase de archivo permitido.

Este proyecto requiere un equipo de trabajo multidisciplinario, es decir, se requiere personal de todas las áreas del departamento de Tecnología de la Información: Soporte Técnico, Telemática, Sistemas de Información, Apoyo a la Gestión e inclusive en algún momento asesoría legal. Claro que una vez realizadas la preparación de la plataforma tecnológica y la reglamentación de los nuevos procesos, el trabajo recae sobre los analistas que puedan realizar todo el desarrollo normal de un sistema: Etapa de análisis, diseño y desarrollo que permita realizar la firma digital de cualquier archivo y cumpla con todos los requerimientos propuestos, tomando en cuenta que la administración está interesada en ofrecer servicios de recepción electrónica de documentos dirigidos a las oficinas y despachos judiciales.

Los requisitos fundamentales para realizar la firma es tener el certificado digital con el cual efectuar la firma así como tener la herramienta de software que permita realizarla. Asumiendo que se va a contar con los certificados digitales, lo siguiente pendiente sería contar con una herramienta de software que permita realizar la firma y verificación de las firmas digitales.

En primer lugar se debe de realizar un análisis cuidadoso de la clase de archivos a firmar digitalmente. En el Poder Judicial como se mencionó con anterioridad se trabajan con Archivos de Microsoft Word, Archivos del PJ-Editor, Correo Electrónico de Outlook, etc. Se debe evaluar las opciones que existen para firmar esta clase de archivos, y cualquier otros que posteriormente se definan.

Algunos aspectos de consideración:

- Investigación de las herramientas que existen para realizar la firma y verificación de cada uno de los tipos de archivos.
- Definir Características deseables
    - Herramientas en ambiente WEB
    - Permitiendo el acceso remoto (Internet o Intranet)
    - Control de Ingreso (Usuarios Registrados)
    - Claves Encriptadas con algoritmos de un solo sentido.
    - Encriptación en la transmisión (seguridad)
    - Compresión en la transmisión (ahorro ancho de banda)
- Definir todas las funciones que deberá cumplir la herramienta.
- Definir despachos, oficinas y usuarios que requieren la utilización de esta herramienta.
- Investigar el manejo de los documentos en los diversos despachos y oficinas. Procedimiento utilizado para archivar los documentos, controles utilizados para dar seguimiento a los documentos, información que registran en los controles, etc.

7 BIBLIOGRAFÍA

Asociación de Internautas (2003) Recuperado el 14 de septiembre del 2005, de http://www.internautas.org

Carlino B. (1998). *Firma digital y derecho societario electrónico*. Buenos Aires: Rubinzal-Culzoni Editores.

Criptonomicón. (1999). *PKI Los cimientos de una criptografía de clave pública*. Recuperado el 10 de octubre del 2005, de http://www.iec.csic.ex/criptonomicon/susurros/susurros11.html

Ellison, C., y Scheneier, B. (2000). Teen Risk of PKI: What You're not Being Told about Public Key Infrastructure. *Computer Security Journal*, XVI, 1-8

Martínez, A.(1998). *Comercio electrónico, firma digital y autoridades de certificación (Colección Estudios de derecho mercantil).* España: Cívitas.

República de Costa Rica. ley N° 8454. *Ley de certificados, firmas digitales y documentos electrónicos*.

Simon, H. (2005). *Negocios En Internet: E-Commerce, Correo Electrónico, Firma Digital*. España: Editorial Astrea