Proyecto de Grado

Ingeniería en Sistemas – IUA

Tema:

Análisis, Diseño e Implantación de Firma Digital en Documentos Electrónicos

Alumna: María Laura Irigoitia

Tutor: Ing. Eduardo Casanovas

Noviembre 2016

Declaración de Derechos de Autor

Dedicatoria

A mi familia.

Resumen

El uso de la Firma Digital ha tenido una creciente evolución en los últimos años debido a las necesidades de un mundo globalizado, en donde las transacciones y la interacción entre los individuos son impersonales, sin vínculos físicos, y la tendencia a la "despapelización" de las tareas es cada vez mayor. Es así que surgieron una diversidad de herramientas tecnológicas, que permiten garantizar la autoría e integridad de los documentos digitales y que buscan cubrir las expectativas de personas, empresas y entidades.

En este contexto, surge la necesidad y la conveniencia de plantear el presente Proyecto Final de Grado para la implementación de Firma Digital de documentos electrónicos en el Instituto Universitario Aeronáutico. El mismo permitirá agilizar la burocracia de algunos procesos existentes, garantizando la autenticidad del firmante e integridad de los datos y replanteando el modo en el que se desarrollan las tareas, enfocándose hacia procedimientos mucho más dinámicos y eficientes.

De este modo, para desarrollar este proyecto, se ha realizado una investigación en base a diversas fuentes bibliográficas analizando el concepto de Firma Digital, algoritmos y estándares tecnológicos, los requisitos legales exigidos por las leyes vigentes, procedimientos de seguridad y herramientas disponibles en el mercado y analizando los costos y beneficios asociados.

Así, en pos de desarrollar una solución, se aplicó un proceso en cascada, el cual permite clarificar el modelo, planteando el diseño del mismo. Finalmente, se realiza el despliegue mediante la configuración de un servidor de claves para la generación y el almacenamiento de las mismas, su distribución y la simulación de los procesos que involucran la Firma Digital de documentos y correos electrónicos en la Institución.

El resultado final del proyecto es un modelo teórico para la implantación de la Firma Digital en el IUA, fundamentado en las beneficios, que de su uso se desprenden, y defendiendo la idea de que la tendencia hacia la implementación de Firma Digital es una necesidad actual y la vía más apropiada para garantizar la autoría e integridad de los documentos digitales, posibilitando que éstos gocen de una característica que únicamente era propia de los documentos en papel, que es la garantía de identidad.

Índice

Índice de Figuras

Índice de Tablas

1. Introducción

1.1. Antecedentes

Con la sanción de la Ley N° 25.506[1], denominada de Firma Digital, la Argentina se incorpora al grupo de países que ha encarado la regulación normativa de la denominada sociedad de la información, nacida a partir de la digitalización de las comunicaciones y caracterizada por la facilitación y la velocidad de las comunicaciones a lo largo y a lo ancho del planeta, con acceso a una cantidad infinita de información por un infinito universo de usuarios. Esta realidad se ha multiplicado y adquiere importancia relevante desde la apertura al público de las redes de computación abiertas, tal como Internet.

La Ley de Firma Digital en Argentina ha atravesado un largo camino con idas y vueltas. Recién en el año 2009 se ha comenzado a transitar por la Ley propiamente dicha, con todo lo que implica su aplicación. Al incorporarse las primeras Autoridades Certificantes, operadas por los certificadores licenciados nacionales, todo el escenario ha cambiado literalmente. Las perspectivas, también.

Así, las primeras iniciativas relacionadas con la Firma Digital en el ámbito de la Secretaría de Gabinete y Gestión Pública (SGP) comenzaron en Marzo de 1997. En esa fecha, la entonces Secretaría de la Función Pública (SFP, actualmente SGP) dictó la Resolución N°45, que establecía pautas técnicas para elaborar una normativa sobre Firma Digital, a fin de difundir esta tecnología en el ámbito de la Administración Pública Nacional (APN).

Posteriormente, en Abril de 1998, el Poder Ejecutivo Nacional dictó el Decreto N° 427, que autorizaba la utilización de la Firma Digital en la instrumentación de los actos internos del Sector Público Nacional, otorgándole los mismos efectos que la firma ológrafa y estableciendo las bases para la creación de la Infraestructura de Firma Digital de la República Argentina (IFDRA) para el Sector Público Nacional.

[1] Anexo 1: Ley N° 25.506.

La SFP era la Autoridad de Aplicación del decreto mencionado y asumía las funciones de organismo licenciante, es decir, de otorgar las licencias a las autoridades certificantes que se constituyeran en el ámbito de la APN.

En cumplimiento de lo dispuesto en dicha normativa, la SFP dictó la Resolución N° 194/98 (Estándares sobre Tecnología de Firma Digital para la APN) y la Resolución N° 212/98 (Política de Certificación del Organismo Licenciante) y se desarrolló un software de autoridad certificante de libre distribución en el ámbito de la Administración Pública.

Al mismo tiempo, son numerosas las asistencias técnicas que se efectuaron a fin de asesorar sobre la implementación de la Firma Digital en las aplicaciones internas de distintos organismos.

Con el fin de difundir el uso de la tecnología, se creó una autoridad certificante de correo electrónico (que no requiere identificación personal), que permite a cualquier ciudadano gestionar un certificado digital de prueba y experimentar su utilización.

La creación del laboratorio de Firma Digital, que permite a los asistentes probar la gestión y utilización de un certificado digital, asistidos por un instructor experto en el tema, es otro de los instrumentos de difusión que han probado su éxito.

En marzo de 2000 se inició la distribución de una lista de novedades sobre Firma Digital, que permitió difundir las noticias más relevantes del ámbito nacional e internacional sobre el tema.

A inicios de 2001 comenzó el desarrollo de una Autoridad Certificante que emitiera certificados con identificación personal y constancia de cargo, destinados a agentes y funcionarios públicos. Esta implementación impulsó la necesidad de crear un marco normativo adecuado, que reflejara los procedimientos a cumplir para la administración de los certificados, así como la creación del indispensable entorno de seguridad.

En julio de 2001, con la creación de la Oficina Nacional de Tecnologías de Información (ONTI), en jurisdicción de la Secretaría de Gabinete y Gestión Pública, se da nuevo impulso al proyecto de digitalización de aplicaciones internas en el Estado Nacional con garantía de autoría e integridad. Con lo que se hizo necesario avanzar en el desarrollo de la

Autoridad Certificante (AC) que pudiera proveer de certificados digitales personales. Dentro de este marco, resulta destacable la firma del Convenio de Comunicación Electrónica Interjurisdiccional, entre la Jefatura de Gabinete de Ministros y los Poderes Judiciales provinciales, en el cual se estableció que las comunicaciones electrónicas entre los funcionarios judiciales serán firmadas digitalmente, utilizándose certificados digitales emitidos por la Autoridad Certificante de la Secretaría de Gabinete y Gestión Pública. A tal fin, los Poderes Judiciales provinciales debían constituirse como Autoridades de Registro de la AC.

A partir de abril de 2002 comenzó a implementarse un esquema de Autoridades de Registro remotas de la AC-ONTI, mediante el cual se descentraliza el proceso de validación de la identidad de los solicitantes de certificados digitales. Al mes de agosto de 2004, ya eran veinticuatro los organismos que utilizaban esta operatoria.

De este modo, hemos llegado al escenario que hoy se presenta en nuestro país, donde existen dos Autoridades Certificantes, operadas por los certificadores licenciados nacionales por la ONTI, como lo son la Administración Federal de Ingresos Públicos (AFIP) y la Administración Nacional de la Seguridad Social (ANSES); a las cuales se les otorga la potestad de emitir certificados digitales con peso de Ley, de modo tal que aquel que firme con estos certificados será exactamente lo mismo que si lo hubiera firmado en forma ológrafa. Así, en una primera etapa se aplicará Firma Digital en la documentación y procesos internos, que luego intercambiaran funcionarios de gobierno, y a partir de ese punto se irá trasladando esta práctica al sector privado.

A nivel mundial, se han aprobado en los últimos años nuevas Leyes que soportan las firmas digitales y electrónicas como medio de autenticar datos y transacciones electrónicas. Tal es así que en Latinoamérica, ya son 18 los países de la región que han trabajado normativas acerca de la Firma Digital, lo que muestra un pronóstico de su desarrollo en los próximos años. La validación que entrega al traspaso de información vía Internet, entre otros beneficios, impulsarían a los gobiernos a su implementación, y fomentarían el crecimiento de un nuevo nicho de mercado.

Finalmente, a nivel local, en Córdoba, en julio de 2007 se sancionó la Ley Provincial N° 9.401[2], por la cual la provincia adhirió a la Ley Nacional N° 25.506 sobre Firma Digital. Más adelante, en diciembre de 2011 la Legislatura Provincial aprobó la Ley N° 10.019 que incorporó el artículo 9 bis a la Ley Nº 5.350 que regula los procedimientos administrativos en la provincia, el cual dispone que: "Los actos preparatorios, los actos administrativos y los actos de los administrados que se realicen en soporte digital y sean suscriptos mediante Firma Digital conforme a la Ley Nº 9401, se considera que cumplen con los requisitos de forma escrita y firma en los que la presente Ley disponga estos últimos formalismos".

Reconociéndose de este modo que la Firma Digital representó un avance significativo para la inserción de la Argentina en la sociedad de la información y en la economía digital, brindando una oportunidad para el desarrollo del sector productivo vinculado a las nuevas tecnologías.

1.2. Situación Problemática

La firma manuscrita es todavía la forma más utilizada y "confiable" para relacionar un documento con una persona en particular de manera legal. Sin embargo, este método padece de diversas imperfecciones, entre ellas la posibilidad de falsificación y las dificultades en el proceso de verificación de la firma.

La firma en sí, involucra dos acciones: la acción de firmar y la acción de verificación de la firma. La acción de firmar, en el caso de la firma manuscrita, consiste en que una persona deje su rúbrica; mientras que la acción de verificación es más complicada ya que se requiere, en algunos casos, la utilización de tecnología altamente sofisticada o la participación de peritos calígrafos altamente calificados, y siempre con probabilidad de error.

Otra limitación que se presenta en las transacciones comerciales (como la firma de contratos) es la necesidad de contar con la presencia física y simultánea de las personas involucradas y un notario que garantice la validez del acto, todo lo cual hace lenta y costosa una transacción entre organizaciones ubicadas en diferentes localidades.

[2] Anexo 3: Ley Provincial N° 9.401.

Precisamente como solución a estos problemas, nace una nueva tecnología que puede reemplazar a la firma manuscrita y que se ha denominado Firma Digital. Esta tecnología va llegando poco a poco a diferentes lugares del mundo, y los gobiernos, conscientes de las claras ventajas de ésta, hacen los esfuerzos necesarios para implantarla en sus naciones, promulgando Leyes y promoviendo su uso.

Tal es así, que muchas entidades dependen hoy en día de una metodología más ágil y sencilla para desarrollar parte de su actividad cotidiana, debiendo vincular la identidad de un individuo a un segmento de información, otorgando garantía de autenticidad e integridad de la información.

Es por ello que surge la necesidad de desarrollar un proyecto que cubra dichas expectativas para el Instituto Universitario Aeronáutico (IUA).

1.3. Problema

El problema planteado radica en la necesidad de implementar un esquema de Firma Digital en el IUA, de modo de facilitar y agilizar determinados procesos administrativos existentes al brindar autenticación de la identidad del firmante, integridad de la información y el no repudio de ésta.

1.4. Objeto de Estudio

Se basa en la investigación y en el análisis de requerimientos, tecnologías y algoritmos de seguridad, necesarios para la implementación de Firma Digital en el IUA.

1.5. Campo de Acción

Se plantea la implementación de un esquema de Firma Digital en el IUA, para la autentificación de documentos electrónicos.

1.6. Objetivos

1.6.1. Objetivo General

Se busca realizar un estudio de los certificados digitales y un análisis, diseño e implementación de Firma Digital, como medida de seguridad para la autenticación de documentos electrónicos firmados por el personal y las autoridades del IUA.

1.6.2. Objetivos Específicos

Con el desarrollo de este proyecto se pretenden alcanzar los siguientes objetivos específicos:

- Investigar la situación actual de la Firma Digital, su uso y aplicación, algoritmos y estándares vigentes.
- Recopilar información de los avances tecnológicos y procedimientos para obtener la Firma Digital y el cifrado de documentos electrónicos.
- Analizar la Infraestructura de Firma Digital, llamándose así al conjunto de Leyes, normativa legal complementaria, obligaciones legales, hardware, software, bases de datos, redes, estándares tecnológicos y procedimientos de seguridad, que permiten que distintas entidades (individuos u organizaciones) se identifiquen entre sí de manera segura al realizar transacciones en redes (por ej. Internet).
- Elaborar una prueba de concepto (PoC) como estrategia de diseño e implementación de Firma Digital.

1.7. Propuesta a Justificar

A partir de la implementación de un esquema de Firma Digital, se simplificarán y agilizarán determinados procesos administrativos existentes, brindando mayor seguridad en el de envío y recepción de documentos, reduciendo riegos de falsificación, tiempo y delitos informáticos, garantizando así, la autenticación de la identidad del firmante, la integridad de la información y el no repudio de la misma.

1.8. Delimitación del Proyecto

Implementar un esquema de Firma Digital involucra un concepto muy amplio, por lo que se hace necesario limitar el alcance del proyecto, centrándose en los objetivos específicos mencionados y no contemplando, a los efectos del presente trabajo académico, los siguientes conceptos/actividades:

- Pago de licencias del software requerido.
- Implementación en hardware definitivo.
- No se implementará una entidad certificante.
- Emisión de certificados para otras personas físicas o jurídicas.
- No se implementará en ningún área operativa.
- No se generaran manuales de utilización para usuarios.

1.9. Aporte Teórico

El uso Firma Digital ha tenido una creciente evolución en los últimos años debido a la necesidad de un mundo globalizado, en donde las transacciones y la interacción entre los individuos son impersonales, sin vínculos físicos, y la tendencia a la "despapelización" de las tareas es cada vez mayor. Así, en este contexto, surgieron una diversidad de herramientas tecnológicas que permiten garantizar la autoría e integridad de los documentos digitales y que buscan cubrir las expectativas de personas, empresas y entidades; haciendo interesante y conveniente, en este sentido, la implementación de un proyecto de esta índole en el ámbito del IUA.

De este modo, el presente proyecto contribuirá a brindar los conocimientos sobre las nuevas tecnologías y tendencias del mercado, sentando las bases necesarias que podrán ser generalizadas y aplicadas a otros proyectos de características similares, con posibilidad de expansión dentro del mismo dominio en estudio.

1.10. Aporte Práctico

El impacto que genera la implementación de Firma Digital en el ámbito del IUA supone un beneficio significativo para alumnos, profesores y empleados del Instituto, permitiendo agilizar aquellos procesos institucionales y administrativos para los que se requiere la necesidad de la aplicación de una firma.

Resulta necesario destacar, además, los siguientes beneficios asociados a la aplicación de la Firma Digital:

- Una significativa contribución al proceso de "despapelización" de determinadas tareas administrativas, equiparando la firma de documentos electrónicos con los rubricados en forma manuscrita. Alineando así al IUA a la Ley de Firma Digital, la cual propone en su art. 48 la progresiva despapelización del Estado para sus actos internos, brindando validez legal a todos los documentos electrónicos en donde se cumplan los requisitos que fija la Ley.
- Garantía de autoría e integridad de los documentos digitales.
- Validez legal a la documentación electrónica, y la introducción de estándares de seguridad en las transacciones electrónicas.

1.11.Métodos de Investigación

El desarrollo del proyecto se basa en métodos de investigación empíricos y lógicos.

MÉTODOS CIENTÍFICOS	FUNDAMENTACIÓN TEÓRICA
Método Analítico Sintético	Ayudará al entendimiento de los conceptos administrativos que utilizará la Firma Digital para el proceso de autentificación de documentos electrónicos, para posteriormente extraer una síntesis de los temas que se podrán adaptar y sintetizar lo más importante para aplicarlo al tema investigado.
Método Inductivo Deductivo	Porque se partirá de la recolección de información sobre la Firma Digital que se está llevando en el país, y a lo largo del desarrollo de la investigación se buscará particularizar sobre

	la viabilidad del estudio de Firma Digital para el proceso de autentificación de documentos.
MÉTODOS EMPÍRICOS	
Recolección de la Información	Permitirá recoger, procesar, analizar la información del proyecto que se está llevando a cabo; ya que la recolección de la información enfocará a una idea de la emisión de mensajes de datos.
METODOLOGÍA DE INVESTIGACIÓN	**DIAGNOSTICO SITUACIONAL**
Método Histórico Lógico	Permitirá conocer el proceso que se llevará a cabo, así como cuando comenzó el proyecto de firma electrónica, quienes son los involucrados para realizar este proceso en nuestro país. Se realizará el estudio y la verificación de los problemas que se han venido suscitando dentro de las empresas, entidades o personas naturales a lo largo de su funcionamiento.
Observación Científica	Este método ayudará a encontrar los principales problemas y necesidades existentes en el país, mediante la observación de hechos o acontecimientos.
METODOLOGÍA DE INVESTIGACIÓN	**PROPUESTA**
Analítico Sintético	Con la ayuda de este método se podrá obtener toda la información referente al tema de Firma Digital, para el proceso de autentificación de documentos.

Tabla 1. Métodos de Investigación

1.12.Enfoque Metodológico

1.12.1. Paradigma

La implementación del proyecto plantea un paradigma sobre el uso de Firma Digital como medio que permite garantizar la identidad del firmante y la integridad del mensaje, en tal sentido se apuntará a su investigación, comprensión y aplicación.

1.12.2. Proceso

En post de alcanzar los objetivos planteados, resulta conveniente proponer un esquema secuencial a seguir. Así, se comenzará realizando un análisis del concepto de Firma

Digital, su funcionamiento, algoritmos de encriptación, claves públicas y privadas, certificados digitales, legislación vigente y el valor legal de la Firma Digital. A continuación, se empleará un desarrollo en cascada para la implementación de la solución, el cual permite clarificar el modelo:

- *Identificación de requerimientos:* se definirán los requerimientos en base a las necesidades ya descriptas y patrones de diseño, como primera etapa del desarrollo, los cuales servirán de guía para las etapas posteriores.
- *Análisis:* en base a los requerimientos identificados, se procederá al análisis del sistema para brindar una solución al problema planteado.
- *Diseño:* se procederá al diseño de la solución, seleccionando las herramientas, tecnologías, algoritmos, Leyes y estándares necesarios para la implementación, así como también las herramientas necesarias para la simulación.
- *Despliegue:* se generará la simulación de una implementación del esquema de Firma Digital para la autentificación de documentos electrónicos, considerando lo desarrollado.

1.12.3. Métodos

La metodología a aplicar es en cascada, considerando en cada etapa el alcance del proyecto. Asimismo, se tendrán en cuenta el marco normativo vigente de la República Argentina, algoritmos y tecnologías disponibles en el mercado, como también su análisis costo-beneficio.

1.12.4. Técnicas

Las técnicas a aplicar son las siguientes:

- *Recopilación de requerimientos:* se generará un listado de los requerimientos del sistema en relación a las tecnologías de hardware y software disponibles en el mercado, el marco normativo, los costos asociados, entre otros.
- *Análisis, diseño y modelado:* aquí se generará un modelo del sistema, un plano general del objeto en estudio, el cual refleje cómo van a interactuar los usuarios con el sistema, a quiénes afectara y cómo les afectara.

- *Implementación:* en base a lo desarrollado en el punto anterior, se procede a la simulación del proyecto, la cual va a reflejar claramente el funcionamiento del proyecto, como si la implementación se hubiese realizado in situ.
- *Herramientas:* para el desarrollo del proyecto se utilizarán las siguientes herramientas:
    - Microsoft Word 2010: permite el desarrollo de la presentación del anteproyecto y del proyecto de grado, siendo este uno de los procesadores de texto más potentes y usuales en el mercado.
    - Microsoft Project 2010: esta aplicación es utilizada para el desarrollo de la planificación del proyecto mediante diagramas de Gantt.
    - Ubuntu Server 12.04.3: este Sistema Operativo nos permite correr una aplicación que demuestre efectiva y económicamente la generación y manipulación de certificados.
    - OpenSSL, GnuPG, Gpgp4win, Mozilla Thunderbird: Herramientas para la generación y manipulación de certificados.

2. Marco Contextual

2.1. Entorno del Objeto de Estudio

En la actualidad es cada vez más frecuente el uso de documentos digitales para cualquier tipo de actividad o trámite a realizar. Así es como el quehacer diario nos involucra frecuentemente con el intercambio de documentos digitales entre personas o instituciones, debido a la necesidad de un mundo globalizado en donde las transacciones y la interacción entre los individuos son impersonales, sin vínculos físicos y donde la tendencia a la "despapelización" de las tareas es cada vez mayor. Pero a pesar de que trabajamos con gran cantidad de documentos digitales no lo hacemos habitualmente con los mínimos requisitos de seguridad. Así es como el uso de la Firma Digital se presenta como una herramienta que nos posibilita tomar las medidas de seguridad adecuadas, manteniendo la privacidad e integridad de nuestra información.

De esta forma, el proyecto propuesto surge a partir de la necesidad de implementar un esquema de Firma Digital en el IUA, tras el análisis y estudio de nuevas tecnologías y algoritmos de seguridad que satisfacen dichas necesidades, y resuelven la problemática planteada, involucrando a los alumnos y empleados del instituto. Todo ello en un marco donde existe un fuerte crecimiento a nivel regional y nacional, donde cada vez son más aquellas personas e instituciones que la utilizan como herramienta para tomar las medidas de seguridad adecuadas a fin de mantener la privacidad e integridad de la información a la que acceden. Alineando así al IUA con las directivas que el Gobierno Nacional ha emanado a tal efecto, brindando validez legal a todos los documentos electrónicos en donde se cumplan los requisitos que fija la Ley.

2.2. Relación entre la Tesista y el Objeto de Estudio

Con la Ley de Firma Digital se da validez legal a todos los documentos electrónicos donde se cumplan los requisitos que fija la Ley. A partir de esta Ley, es posible despapelizar al Estado para sus actos internos y crear mecanismos de comunicación electrónica con terceros que cumplan los requisitos de legalidad y formalidad. En este contexto, como

alumna del IUA y miembro de una sociedad donde existe un fuerte crecimiento a nivel regional y nacional en este aspecto, reflejado en el hecho de ser cada vez más las personas e instituciones que utilizan esta herramienta para tomar las medidas de seguridad adecuadas, a fin de mantener la privacidad e integridad de la información a la que acceden, es que surge este proyecto con la intención de alinear a la Institución hacia esta creciente tendencia, dentro del marco propuesto por las directivas del Gobierno Nacional en dicho sentido.

2.3. Análisis de Problemas Observados

Como ya se ha mencionado anteriormente, existe la necesidad en el IUA de implantar un esquema de Firma Digital que agilice la burocracia de algunos procesos existentes, garantizando la autenticidad del firmante e integridad de los datos y replanteando el modo en el que se desarrollan las tareas, enfocándose hacia procedimientos mucho más dinámicos y eficientes.

Cuando se habla del proceso de despapelización, el mismo implica pasar de un esquema de trabajo apoyado en soporte papel a un esquema digital basado en el uso de documentos electrónicos, donde la tecnología utilizada ocupa un rol central. De este modo, la utilización del documento electrónico, como soporte sustituto del papel, supone beneficios múltiples tales como:

- Aumento de la eficiencia en el tratamiento de los procesos: Se reducen los tiempos en el ingreso a las bases de datos y en la autenticación y control de integridad de la información. Se facilita el seguimiento de las tramitaciones, pudiéndose determinar su ubicación y estado fácilmente. Además, se minimiza la posibilidad de errores en la información suministrada, dada la existencia de pruebas de validación y consistencia de la misma.
- Ahorro de recursos: el incremento en la eficiencia de los procesos genera reducción en los tiempos de tramitación y respuesta a las solicitudes. Adicionalmente, se producen ahorros de dinero derivados de un menor costo de captura y mantenimiento de la información.

- Mayor confidencialidad de la información contenida en los documentos: se ofrece mayor control en cuanto a los accesos permitidos a los datos.
- Mejora las condiciones de trabajo de los empleados: producto de procesos ágiles y facilitados.
- Perdurabilidad de los documentos: por su naturaleza digital y la seguridad que puede rodearlos, los documentos electrónicos se encuentran expuestos a una menor cantidad de factores que puedan dañarlos o destruirlos.
- Preservación del medio ambiente: el menor consumo de papel supone una menor demanda de recursos naturales para su elaboración y un menor consumo eléctrico producto del menor uso de fotocopiadoras e impresoras.

Sumado a los beneficios brindados por el documento electrónico, la Firma Digital favorece significativamente el proceso de despapelización, brindando garantía de autoría e integridad de los documentos electrónicos, bajando la tasa de repudio, otorgando validez legal a la documentación electrónica y contribuyendo a la introducción de estándares de seguridad en las transacciones electrónicas. Destacándose así, los puntos claves que representan dicha tecnología:

- Autentificación: la Firma Digital es equivalente a la firma física de un documento, de modo tal que permite verificar la identidad del firmante.

- Integridad: es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el original.

- No repudio en origen: el emisor no puede negar haber enviado el mensaje o haber realizado una determinada transacción.

Actualmente no existe implementado en el IUA un esquema de Firma Digital, por lo cual se expone el presente proyecto como una solución para abordar dicho problema, planteándose como el medio más aproximado para cubrir dicha necesidad.

2.4. Antecedentes de Proyectos Similares

A nivel mundial y regional, existe una tendencia creciente sobre la temática en desarrollo, pues cada vez es mayor la cantidad de personas e instituciones que desean implementar la

Firma Digital como una herramienta para brindar seguridad a sus procesos. En este sentido, podemos encontrar una diversidad de proyectos similares, aplicados en su gran mayoría en otros países y por lo tanto sujetos a sus correspondientes legislaciones.

A nivel nacional, para citar algunos ejemplos de casos similares, se puede consultar en https://pki.jgm.gov.ar, proyectos implementados en AFIP y ANSES. En el ámbito provincial la implementación de Firma Digital en la Universidad Nacional de Córdoba y la Universidad Nacional de Río Cuarto.

3. Marco Teórico

3.1. Introducción

El desarrollo del marco teórico permitirá describir antecedentes, teorías, tecnologías, tendencias y otros conceptos teóricos referentes a la Firma Digital; que es necesario estudiar, analizar y dominar para posteriormente plantear un modelo teórico, que servirá como base para la implementación de una solución al problema planteado que satisfaga los requerimientos del proyecto.

De este modo, en esta sección se buscará abordar las siguientes temáticas:

- Estudiar y comprender el concepto de Firma Digital y sus principales usos.
- Estudiar y comprender las Leyes y normativas que conforman el marco legal en la implementación de Firma Digital.
- Estudiar y comprender los estándares tecnológicos implicados en su implementación.

3.2. Seguridad

Se puede definir a la seguridad como la protección de un conjunto de propiedades o características de algo en particular, descripta por un conjunto de reglas destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño . En tal sentido, la Seguridad Informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables para el procesamiento de datos en sistemas informáticos; permitiendo asegurar que los recursos del sistema de información de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización[3].

[3] http://seguridad-informatica-1-iutll.blogspot.com.ar Instituto Universitario de Tecnología de los Llanos.

Así, la Seguridad Informática se convierte en un concepto importante en el contexto actual donde existen personas ajenas a la información, también conocidas como piratas informáticos o Crackers (mal llamados comúnmente "hackers"), que buscan tener acceso a la red empresarial para modificar, sustraer o borrar datos. Tales personas pueden, incluso, formar parte del personal administrativo o de sistemas, de cualquier compañía. De acuerdo con expertos en el área, más de 70 por ciento de las violaciones e intrusiones a los recursos informáticos se realiza por el personal interno, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible de su empresa, es decir, a todos aquellos datos cuya pérdida puede afectar el buen funcionamiento de la organización. Esta situación se presenta gracias a los esquemas ineficientes de seguridad, con los que cuentan la mayoría de las compañías a nivel mundial, y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente, que proteja los recursos informáticos de las actuales amenazas. El resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor de miles o millones de dólares.

3.2.1. Objetivos de la Seguridad Informática

Generalmente, los sistemas de información incluyen todos los datos de una compañía y también el material y los recursos de software que permiten a una compañía almacenar y hacer circular estos datos. Los sistemas de información son fundamentales para las compañías y deben ser protegidos.

La Seguridad Informática consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

Dicha Seguridad se fundamenta en cinco principios, que debe cumplir todo sistema informático:

- **Integridad**: es necesario asegurar que los datos no sufran cambios no autorizados. La pérdida de integridad puede acabar en fraudes, decisiones erróneas o dar paso a otros ataques. El sistema contiene información que debe ser protegida de modificaciones imprevistas, no autorizadas o accidentales.
- **Confidencialidad**: se refiere a la protección de los datos frente a la difusión no autorizada; la pérdida de confidencialidad puede resultar en problemas legales,

pérdida del negocio o de credibilidad. El sistema contiene información que necesita protección contra la divulgación no autorizada.

- **Disponibilidad**: se refiere a la continuidad operativa de la entidad. La pérdida de disponibilidad puede implicar la pérdida de productividad o de credibilidad de la entidad. El sistema contiene información o proporciona servicios, que deben estar disponibles a tiempo para satisfacer requisitos o evitar pérdidas importantes.
- **No Repudio**: cuando se recibe un mensaje, no sólo es necesario poder identificar de forma unívoca al remitente, sino que éste asuma todas las responsabilidades derivadas de la información que haya podido enviar. En este sentido, es fundamental impedir que el emisor pueda repudiar un mensaje, es decir, negar su autoría sobre el mismo.
- **Autenticación**: debido a la naturaleza insegura de los canales de comunicación, es necesario asegurarse de que la información que se recibe en la computadora viene de quien realmente se cree que viene.

Estos aspectos, además de lidiar con el riesgo que representan los atacantes remotos, se ven amenazados también por los riesgos derivados de desastres naturales, empleados desleales, virus y sabotaje, entre otros.

La Información

Se ha convertido en uno de los elementos más importantes dentro de una organización, se la considerada uno de los principales activos y de valor estratégico en las empresas; como soporte para la toma decisiones es susceptible de ser perdida, deteriorada, revelada o incluso de robada. Así, la información puede ser considerada como el bien más preciado de una organización.

La Seguridad Informática debe ser administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario, la organización corre el riesgo de que la información sea utilizada maliciosamente, para obtener ventajas de ella, o que sea manipulada, ocasionando lecturas erradas o incompletas de la misma. Otra función de la Seguridad Informática, en esta área, es la de asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la misma en caso de que esta sufra daños o pérdida, producto de accidentes, atentados o desastres.

La Infraestructura Computacional

Es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la Seguridad Informática en esta área, es velar que los equipos funcionen adecuadamente y prever, en caso de falla, planes de robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

Los Usuarios

Son las personas que utilizan la estructura tecnológica, las comunicaciones y son quienes gestionan la información. La Seguridad Informática debe establecer normas que minimicen los riesgos a la información o a la infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de Seguridad Informática; minimizando así el impacto en el desempeño de los funcionarios y de la organización en general. Todo ello contribuyente al uso de programas realizados por programadores.

3.2.2. Amenazas

Una amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, como lo son los referidos a la información, atentando contra su confidencialidad, integridad y disponibilidad.

El hecho de conectar una red a un entorno externo, da la posibilidad de que algún atacante pueda entrar en ella, pudiendo acceder, alterar, robar información o afectar funcionamiento de la red. Sin embargo, el hecho de que la red no sea conectada a un entorno externo no garantiza la seguridad de la misma. En tal sentido, existen dos tipos de amenazas:

- **Amenazas Internas**: Generalmente estas amenazas pueden ser más serias que las externas por varias razones:
    - Los usuarios conocen la red y saben cómo es su funcionamiento.
    - Tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo.

- Los IPS (Intrusion Prevention System) y Firewalls son mecanismos no efectivos en amenazas internas.

Esta situación se presenta gracias a los esquemas ineficientes de seguridad, con los que cuentan la mayoría de las compañías a nivel mundial, y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente, que proteja los recursos informáticos de las actuales amenazas combinadas. El resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor de miles o millones de dólares.

- **Amenazas Externas:** son aquellas amenazas que se originan afuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso consiste en que el administrador de la red puede prevenir una buena parte de los ataques externos.

3.2.3. Autentificación

Se refiere a la verificación de la autenticidad de las identificaciones, realizadas o solicitadas por una persona física o entidad, o sobre los datos, tales como un mensaje u otros medios de transmisión electrónica. El proceso de autenticación es el segundo de dos etapas que comprenden:

- La presentación de una identificación ante el sistema de seguridad.
- La presentación o generación de información que corrobora la relación entre la entidad y el identificado.

La autenticación de una firma presenta a menudo consecuencias legales, en tanto que la autenticación del sitio de Internet de origen, de destino, así como de la identidad del que accede a los mismos, puede perseguir objetivos vinculados con la seguridad. Autentificación, o mejor dicho acreditación, en términos de seguridad de redes de datos, se puede considerar uno de los tres pasos fundamentales (AAA) a saber:

- Autenticación: es la verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos. Involucra el proceso de

intento de verificar la identidad digital del remitente de una comunicación, como una petición para conectarse. El remitente, siendo autenticado, puede ser una persona que usa una computadora, una computadora por sí misma, o un programa de computadora. En un sitio web de confianza, "autenticación" es un modo de asegurar que los usuarios son quién ellos dicen ser; donde el usuario que intenta realizar funciones en un sistema es, de hecho, el usuario que tiene la autorización para poder realizarlo.

- Autorización: es el proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma, determinando de este modo, qué, cómo y cuándo, un usuario autenticado puede hacer uso de los recursos del sistema.
- Auditoría: es el proceso mediante la cual la red o sistemas asociados registran todos y cada uno de los accesos a los recursos que realiza el usuario, autorizado o no; permitiendo a los administradores verificar que las técnicas de autenticación y autorización utilizadas, se realizan según lo establecido y se cumplen los objetivos fijados por la organización.

3.3. Marco Legal de la Firma Digital en Argentina

3.3.1. Introducción

En la actualidad, muchos países y regiones están dejando de lado el uso del papel como soporte para realizar sus tramitaciones, tanto en el ámbito local como en el internacional. En su reemplazo, comenzaron a utilizar herramientas más sofisticadas que aseguran una mayor eficiencia en sus procesos y un menor tiempo de respuesta, lo que se traduce en intercambios de información mucho más dinámicos. Este pasaje de la “sociedad del papel” hacia la “sociedad digital” pone en escena a las tecnologías de la información y de la comunicación, con el documento electrónico y la Firma Digital a la cabeza.

De este modo, los avances tecnológicos en materia informática, vienen planteando diversos retos al ser humano, tanto sociales como jurídicos, especialmente debido a la creciente demanda de operaciones electrónicas por medio de las llamadas redes abiertas. Para enfrentar estas nuevas situaciones, que en muchos casos generan consecuencias legales de gran magnitud, se viene regulando el uso de la firma electrónica, así como de las firmas y

certificados digitales. Al respecto, en Argentina se han aprobado una serie de cambios legislativos que permiten el uso de tales elementos técnicos, con la finalidad de acreditar fehacientemente a las personas que manifiestan su voluntad por medios electrónicos, y evitar de esta forma el repudio de sus operaciones.

Ejemplo de ello es la promulgación de la Ley N° 25.506 - Ley de Firma Digital, publicada en el Boletín Oficial el 14/12/2001 (Anexo 1: Ley de Firma Digital); continuando en forma específica, el desarrollo legislativo, con la aprobación del decreto Nº 2.628/2002 (Anexo 2: Decreto 2.628/2002).

Los aspectos regulados por la Ley de Firma Digital han permitido que en Argentina comience un desarrollo legislativo paulatino y constante, a través de la aprobación de una serie de normas con carácter jurídico-informático, que vienen siendo aplicables a los diferentes ámbitos de la vida en sociedad.

3.3.2. Valor Legal de la Firma Digital

Para la legislación Argentina, la Firma Digital implica que existe una presunción “iuris tantum” en su favor. Esto significa que si un documento firmado digitalmente es verificado correctamente, se presume, salvo prueba en contrario, que proviene del suscriptor del certificado asociado y que no fue modificado. En cambio, en la firma electrónica, en caso de ser desconocida la firma, corresponde a quien la invoca acreditar su validez.

Además, es importante tener en cuenta que, para reconocer que un documento ha sido firmado digitalmente se requiere que el certificado digital del firmante haya sido emitido por un certificador licenciado. A su vez, el certificado digital permite identificar quién es el propietario de la clave privada.
Cabe aclarar que la legislación argentina emplea el término "Firma Digital" en equivalencia al término "Firma Electrónica Avanzada" o "Firma Electrónica Reconocida" utilizado por la Comunidad Europea, o "Firma Electrónica" utilizado en otros países como Brasil o Chile.
El marco normativo de la República Argentina en materia de Firma Digital está constituido por la Ley Nº 25.506, el Decreto Nº 2.628/02 y sus modificaciones, junto con un conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos.

3.3.3. Legislación Asociada

La Ley N° 25.506 crea una nueva forma de interactuar entre las personas privadas y entre éstas y la Administración Pública, al reconocer validez y valor probatorio al documento digital, y autorizar el uso de la Firma Digital (diseñando una infraestructura que la hace posible); al tiempo que, bajo ciertas condiciones, reconoce la Firma Digital y certificado digital extranjeros. Regula también el uso de la firma electrónica, con una acepción más amplia que la digital.

Esta norma no sustituye las formas tradicionales, por el contrario, se complementa a las formas documentales ya existentes, agregando, al documento escrito, el documento digital, y a la firma, la firma electrónica y la Firma Digital.

Dichas situaciones ya estaban incorporadas en el ámbito de la Administración Pública, pero la Ley posee la virtud de extenderlas a todos los actos jurídicos.

A partir de ella, se podrán firmar contratos en un documento de Word o en un e-mail, con plena validez.

La Firma Digital requiere una infraestructura compleja para funcionar, razón por la cual un alto porcentaje de la Ley está dedicado a su organización.

Es fundamental para el desarrollo del comercio electrónico, el reconocimiento legal del documento electrónico, su equivalencia con el documento impreso en papel y su admisibilidad como prueba en juicio.

No parece ser razonable, actualmente, la existencia de diferencias entre el valor jurídico de un documento impreso en papel a un documento otorgado electrónicamente, salvo por supuesto, por aquellos documentos que requieren ser otorgados cumpliendo ciertas solemnidades, como la concurrencia de un notario público, mientras éstos no tengan facultades en el mundo electrónico.

La Firma Digital tiene algunas ventajas sobre la firma manuscrita, como la inalterabilidad del mensaje, la fecha y hora de la firma.

La finalidad de la Ley al admitir el documento digital y difundir el uso de la Firma Digital en la Argentina, es facilitar el comercio exterior, la contratación a distancia, y bajar el costo argentino.

Algunos de los aspectos más relevantes de la Ley son:

- Es tecnológicamente neutra, de acuerdo a la última tendencia internacional.

- Establece una IFDRA, a fin de brindar condiciones de uso confiable de los documentos digitales, de acuerdo con estándares tecnológicos internacionalmente aceptados.
- Establece requisitos para la emisión y administración de los certificados digitales.
- Regula la actividad de las entidades prestadoras de servicios de certificación, determinando los alcances de la responsabilidad y las exigencias para obtener la respectiva licencia.
- Prevé mecanismos de reconocimiento de certificados digitales extranjeros.
- Fija un plazo de 5 años para la "despapelización" de la Administración Nacional.
- Otorga a la Jefatura de Gabinete de Ministros las funciones de Autoridad de Aplicación.

3.3.4. Infraestructura de Firma Digital

En nuestro país se denomina Infraestructura de Firma Digital al conjunto de Leyes, normativa legal complementaria, obligaciones legales, hardware, software, bases de datos, redes, estándares tecnológicos y procedimientos de seguridad, que permiten que distintas entidades (individuos u organizaciones) se identifiquen entre sí de manera segura al realizar transacciones en redes (por ej. Internet).

Así, IFDRA está conformada por un conjunto de componentes que interactúan entre sí, permitiendo la emisión de certificados digitales para verificar firmas digitales en condiciones seguras, tanto desde el punto de vista técnico como legal.

Básicamente, la estructura está constituida por un certificador licenciado, dependiente de una Autoridad de Aplicación (Jefatura de Gabinete), y sometido a un régimen de auditoría y sanciones. Una Comisión Asesora asistirá a la Autoridad de Aplicación en todo lo relativo a la aplicación de la Ley.

Las firmas digitales, así como los certificados que permiten su verificación, son herramientas fundamentales a la hora de otorgar validez a los documentos electrónicos. Por ello, la tecnología que viabiliza su utilización requiere de especial cuidado y atención. Este cuidado se vincula fundamentalmente a la utilización de estándares tecnológicos basados en normas y protocolos internacionalmente aceptados.

Esto último asegura no sólo el correcto funcionamiento de la Infraestructura de Firma Digital, sino también la interoperabilidad entre las aplicaciones, y entre Certificadores Licenciados nacionales con las infraestructuras de Claves Públicas de otros países.

Frente a cualquier transacción que involucre el uso de una Firma Digital o de un certificado digital, la adopción de estándares tecnológicos internacionalmente aceptados, permite asegurar un proceso efectivo de verificación de dichas firmas, otorgando seguridad técnica y legal a las transacciones electrónicas.

En este marco, la IFDRA ha adoptado los siguientes estándares tecnológicos:

- Para el formato de los certificados y de las listas de certificados revocados: ITU–T X509.
- Para la generación de las claves: RSA, DSA o ECDSA.
- Para la protección de las claves privadas de certificadores y suscriptores: FIPS 140.
- Para las políticas de certificación: RFC 5280 y 3739.

El listado completo de los estándares aprobados para la IFDRA, así como las condiciones bajo las cuales deben ser utilizados, se encuentra descripto en la Decisión Administrativa Nº 6/2007[4].

3.3.5. Principios Normativos Básicos

Los principios normativos que debería contemplar una legislación referida a la Firma Digital pueden resumirse de la siguiente manera:

a) *Compatibilidad con el marco jurídico internacional:* se refiere a la dimensión global o internacional del tema desde el punto de vista legislativo y tecnológico, a fin de permitir la inserción del país en el mercado mundial del comercio electrónico.

b) *Neutralidad tecnológica:* se hace referencia a la no discriminación entre distintas tecnologías y, en consecuencia, la necesidad de producir normas que regulen los diversos entornos tecnológicos. Este principio refiere a la flexibilidad que deben tener las normas, es decir, que las mismas no estén condicionadas a un formato, una

[4] Anexo 2: Otras Normas y Decretos de interés.

tecnología, un lenguaje o un medio de transmisión específico. No se debe favorecer a una determinada tecnología para las firmas y certificados electrónicos.

c) *Establecer la equivalencia de la Firma Digital a la firma manuscrita:* se considera que la misma satisface el requerimiento de firma, respecto de los datos consignados en forma electrónica, y que tiene los mismos efectos jurídicos que la firma manuscrita, con relación a los datos consignados en papel.

d) *Establecer la libre competencia:* referida a todos los servicios relacionados con la certificación de las firmas electrónicas.

e) *Respeto a las formas documentales existentes:* significa no obligar a la utilización de la firma electrónica en lugar de la manuscrita, sino que su utilización es voluntaria.

f) *Libertad contractual:* permite a las partes convenir la modalidad de sus transacciones, es decir, si aceptan o no las firmas electrónicas.

3.3.6. Conceptos y Terminología

La firma es una forma de exteriorización de la voluntad humana, pero la manifestación de la voluntad en relación a un documento electrónico obviamente no puede ser la firma manuscrita; por ello la Ley debe reconocer una forma electrónica de consentir, como válida y eficaz para la suscripción de documentos electrónicos. Esta forma de consentir es la llamada firma electrónica.

La doctrina jurídica conviene en que la firma es el género, la firma electrónica una especie y dentro de ésta encontramos subespecies, tales como las denominadas, en algunas legislaciones, Firma Digital, firma electrónica avanzada, ó firma electrónica certificada.

La firma es la prueba de la manifestación de la voluntad que permita imputar la autoría e identificar al firmante de un instrumento.

La firma electrónica es un método o símbolo, basado en medios electrónicos, utilizado o adoptado por una persona con la intención de vincularse o autenticar un documento. Es una forma de manifestar la voluntad mediante medios electrónicos.

La Firma Digital es la firma electrónica que utiliza una técnica segura, que permite vincular e identificar fehacientemente al firmante del documento electrónico, garantizando así la autenticación, integridad y no repudio del documento firmado. Es una forma segura y verificable de manifestar la voluntad mediante medios electrónicos.

El ordenamiento jurídico argentino no se refiere exclusivamente al valor jurídico de la firma en sí misma, sino con relación al instrumento en el cual dicha firma está estampada. En líneas generales, establece que un documento firmado es un instrumento privado, con validez jurídica, y que quien se oponga al contenido de un instrumento por él firmado, es quien debe probar que las declaraciones u obligaciones que se encuentran en él no son las que ha tenido intención de hacer o contratar.

En materia de Firma Digital, el mismo procedimiento que verifica la titularidad de la firma, acredita también la autenticidad e inalterabilidad del documento. Ambos términos son inseparables.

Se debe señalar que las distintas legislaciones le han dado a la Firma Digital o electrónica avanzada, dos tratamientos diferentes:

> 1) otorgarle simplemente validez probatoria, sujeta a la valoración según los criterios comunes de apreciación establecidos en las normas procesales. Esto implicaría que quien quiere sostener la validez de la Firma Digital deberá probar los extremos necesarios;
>
> 2) otorgarle un juego de presunciones, en virtud de las cuales:
>
> > a) la Firma Digital pertenece efectivamente al titular del certificado digital correspondiente;
> >
> > b) el documento digital firmado digitalmente no ha sido modificado desde el momento de su escritura;
> >
> > c) la firma fue añadida por dicha persona con la intención de manifestar su acuerdo con los datos obrantes en el documento.

La Asociación Argentina de Derecho de Alta Tecnología considera que la segunda opción, a la que se le otorga una presunción "*iuris tantum*" de validez y autenticidad a la Firma

Digital, sería adecuada y beneficiaría la seguridad jurídica en el tráfico mercantil por medios electrónicos. La primera opción se aplicaría a las firmas electrónicas, que deberían ser probadas por quien las alega.

En cuanto al documento, podemos considerar que en general es el género, mientras que el instrumento es el documento firmado. En este sentido, instrumento privado es todo escrito que da constancia de un hecho o un acto con consecuencias jurídicas, que ha sido firmado por particulares sin intervención de un funcionario público competente y que no tiene otro requisito que la firma.

Un documento electrónico no podría considerarse un instrumento privado, si no existe una Ley que dé efectos jurídicos de firma al procedimiento de firma electrónica o digital. Es decir que, la eficacia jurídica del documento informático viene condicionada por la necesidad de suscripción digital del mismo. Verificada la firma, el documento electrónico sería eficaz desde el punto de vista probatorio.

3.3.7. Firma Digital vs Firma Tradicional.

La utilización del papel como soporte de información en trámites y procedimientos exige disponer de espacio físico para su archivo, a la vez que vuelve ineficaz su procesamiento. Hoy en día, las tecnologías de información permiten mudar la información en soporte papel a otros medios digitales.

Así, un documento en papel puede ser digitalizado y enviado a través de medios electrónicos, como por ejemplo: el correo electrónico, agilizando de esta manera su envío y recepción. En el caso de los documentos firmados hológrafamente, el problema que plantea esta práctica es que, al ser digitalizados, pierden todo valor legal; ya que durante el proceso esa firma, originalmente efectuada de puño y letra, pudo ser editada, alterada, borrada o reemplazada por otra diferente.

Por este motivo, los documentos digitalizados o producidos sobre medios electrónicos se encuentran en desventaja con respecto a aquellos producidos en papel, cuando éstos están firmados hológrafamente. En este sentido, la Firma Digital resulta la herramienta eficaz que nos permite equiparar esa asimetría, haciendo posible que un documento electrónico

resulte "firmado digitalmente", dotándolo del mismo valor legal que el que posee el papel con firma hológrafa.

Si, para establecer su voluntad sobre un documento en papel, el signatario estampa una firma de puño y letra para su identificación, de modo similar puede hacerlo con una Firma Digital en el documento electrónico. Esa marca, efectuada sobre dicho documento electrónico, permite detectar cualquier alteración producida sobre éste en forma posterior a su firma, evitando así la comisión de cualquier tipo de fraude.

Sumado a los beneficios brindados por el documento electrónico, la Firma Digital favorece significativamente el proceso de despapelización del sector público. Brinda garantía de autoría e integridad de los documentos electrónicos, bajando la tasa de repudio. Adicionalmente, otorga validez legal a la documentación electrónica y contribuye a la introducción de estándares de seguridad en las transacciones electrónicas.

A continuación se detallan algunos puntos claves que representan el uso de Firma Digital a diferencia de la firma tradicional de puño y letra:

- Reducción de costos: la eliminación del uso de papel involucrado en los procesos y el espacio físico necesario para archivar dichos papeles.
- Reducción de errores: se logra una amplia reducción de errores administrativos producidos durante la manipulación del papel.
- Eficiencia en los procesos: se logra agilizar el envío y recepción de documentos de una forma notable. La cantidad de papeles utilizados para un solo expediente y el tiempo que demora el expediente en pasar por cada proceso, dependiendo del flujo que tenga que seguir, es minimizado y organizado.
- Mejora el control y visibilidad: se logra una mejora en el control y visibilidad de los procesos involucrados.
- Aumenta la Seguridad: el soporte electrónico es resguardado por medios de copias de seguridad (backups) y almacenados en cofres ignífugos, facilitando su recuperación en caso necesario. Al contrario, el papel está compuesto básicamente por celulosa, que es degradable y se expone a hongos y bacterias que agilizan el

proceso de degradación natural, haciendo que este tipo de soporte no sea el más indicado para almacenar información por periodos largos de tiempo.

3.3.8. Antecedentes legales Internacionales de la Firma Digital

- Naciones Unidas - UNCITRAL - Ley Modelo de Firma Digital.
- Directiva de Firma Digital de la Comisión Europea del 13 de diciembre de 1999.
- Ley de Firma Digital de la República Federal Alemana.
- Ley Reglamentaria de Firma Digital de la República Federal Alemana.
- Ley de Firma Digital de la República Francesa.
- Ley de Firma Digital de Hong Kong.
- Ley de Firma Digital del Perú.
- Ley de Firma Digital del Estado de Utah, EE.UU.
- Ley de Firma Digital de los EE.UU.
- Normativa de Firma Digital de la ABA, American Bar Association (Asociación Americana de Abogados) - Sección de Ciencia y Tecnología, Comité de Seguridad en la Información.

3.4. Criptografía

3.4.1. Introducción

La palabra criptografía proviene del griego “kryptos” que significa ocultar y “grafos” que significa escribir, literalmente sería “escritura oculta”.
La criptografía es el arte o ciencia de cifrar y descifrar información, utilizando técnicas matemáticas que hace posible que la transferencia de información sea segura y que sólo pueda ser leída por las personas a quienes va dirigida.
La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y, en segundo lugar, asegurar que la

información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.
Así, podemos decir que la "Criptografía es el estudio de técnicas matemáticas relacionadas con aspectos de seguridad de la información, tales como la confidencialidad, la integridad de datos, la autenticación de entidades y la autenticación del origen de datos"[5].

La criptografía no es el único medio de garantizar la seguridad de la información sino, más bien, un conjunto de técnicas.

3.4.2. Criptosistema

Un criptosistema, o sistema criptográfico, consiste en los fundamentos y procedimientos de operación algorítmica que participan en el cifrado y descifrado de un mensaje. Todo sistema criptográfico consta de cinco componentes: M, C, K, E y D[6].

- **M** representa el conjunto de todos los mensajes sin cifrar (texto plano) que pueden ser enviados.
- **C** representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
- **K** representa el conjunto de claves que se pueden emplear en el criptosistema.
- **E** es el conjunto de transformaciones de cifrado o familia de funciones, que se aplica a cada elemento de M para obtener un elemento de C. Existe una transformación diferente Ek para cada valor posible de la clave K.
- **D** es el conjunto de transformaciones de descifrado, análogo a E.

Todo criptosistema cumple la condición Dk (Ek (m))=m es decir, que si se tiene un mensaje m, se cifra empleando la clave K y luego se descifra empleando la misma clave, obteniendo así el mensaje original m.

3.4.3. Tipo de Criptosistemas

A lo largo de la historia, se han utilizado cientos de criptosistemas diferentes, pero a grandes rasgos pueden dividirse en dos tipos:

[5] Handbook of Applied Cryptography, by A. Menezes, P. van Oorschot, and S. Vanstone pág. 4.
[6] Criptografía y Seguridad en Computadores, Manuel J. Lucena López pág. 30.

- **Criptosistemas de clave privada**: utilizan la misma clave para cifrar y descifrar el mensaje. La clave secreta es compartida con el emisor y el receptor del mensaje. Este tipo también se conoce como criptografía simétrica.
- **Criptosistemas de clave pública:** utilizan una clave pública para cifrar el mensaje y una clave privada para descifrarlo o viceversa. La clave privada debe mantenerse en secreto y la clave pública debe ser conocida por todas las restantes entidades que van a comunicarse con ella. Los sistemas de clave pública se conocen también como criptografía asimétrica.

3.4.4. Criptografía Simétrica

Los cripstosistemas simétricos, o llamados también de clave secreta, privada o clásicos, se caracterizan por que en ellos se usa la misma clave para cifrar y para descifrar.

Un esquema de cifrado simétrico tiene cinco componentes[7] (Figura 1):

- **Texto claro:** es el mensaje o los datos originales que se introducen en el algoritmo como entrada.
- **Algoritmo de cifrado:** el algoritmo de cifrado realiza varias sustituciones y transformaciones en el texto claro.
- **Clave secreta:** la clave es también una entrada del algoritmo. Las sustituciones y transformaciones realizadas por el algoritmo dependen de ella.
- **Texto cifrado:** es el mensaje ilegible que se produce como salida. Depende del texto claro y la clave secreta. Para un mensaje determinado, dos claves diferentes producirían dos textos cifrados diferentes.
- **Algoritmo de descifrado:** es básicamente, el algoritmo de cifrado ejecutado a la inversa. Toma el texto cifrado y la misma clave secreta, y genera el texto claro.

[7] Fundamentos de Seguridad en Redes Aplicaciones y Estándares, William Stallings pág. 29.

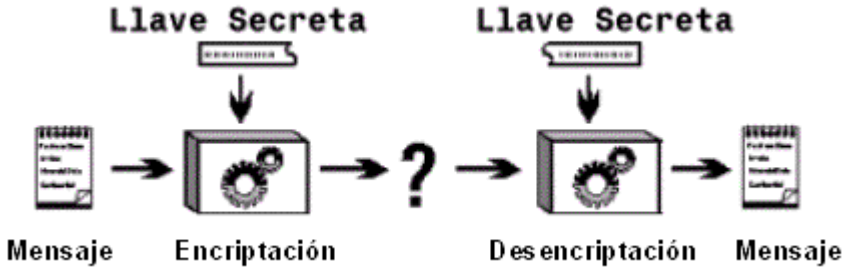


Figura 1: Criptografía Simétrica.

Existen dos requisitos para el uso seguro de este cifrado:

- Se necesita un algoritmo de cifrado robusto. Es decir, el atacante no debería poder descifrar el texto o averiguar la clave, aunque estuviera en posesión de textos cifrados y su correspondiente original.
- El emisor y receptor deben haber obtenido copias de clave secreta de manera segura y guardarlas de la misma forma.

Dado que toda la seguridad se centra en la clave, ésta tiene que ser difícil de adivinar. Esto quiere decir que el abanico de claves posibles, es decir, el espacio de posibilidades de claves, debe ser amplio. Existen varios algoritmos capaces de realizar cifrado simétrico como: DES, AES, IDEA, Blowfish, 3DES, Twofish, RC2, entre otros. Los diferentes algoritmos tienen distintos grados de seguridad de acuerdo al tamaño de bits de la clave (64 a 256 bits).

La seguridad del cifrado simétrico depende de la privacidad de la clave, no de la privacidad del algoritmo. Es decir, se asume que no es práctico descifrar un mensaje teniendo el texto cifrado y conociendo el algoritmo de cifrado/descifrado. En otras palabras, no es necesario que el algoritmo sea secreto; lo único que hay que mantener en secreto es la clave. Esta característica del cifrado simétrico es la causa de su uso tan extendido.

Así, encontramos las siguientes ventajas y desventajas:

Ventajas:

Entre las principales ventajas de la criptografía simétrica se tiene:

- El mensaje en texto cifrado mantiene un tamaño igual o menor al mensaje en texto plano.
- Una clave simétrica, con menor tamaño, entrega el mismo nivel de resistencia a un ataque que una clave asimétrica de mayor tamaño.
- La criptografía simétrica garantiza la confidencialidad de la información.
- Gran velocidad de Cifrado / Descifrado.

Desventajas:

Entre las principales desventajas de la criptografía simétrica se tiene:

- La administración de claves simétricas es compleja.
- El intercambio de claves es susceptible a interceptación.
- Para que el intercambio se lleve a cabo, el emisor y el receptor deben establecer una comunicación previamente.
- Debido a que se utiliza la misma clave para cifrar y descifrar, la criptografía simétrica no permite la utilización de firmas digitales.
- No se puede garantizar integridad de los mensajes utilizando criptografía simétrica.

3.4.5. Criptografía de Clave Pública

La criptografía de clave pública utiliza un par de claves (clave pública y clave privada) para el envío del mensaje, una para cifrar y otra para descifrar el mensaje; lo que se cifra en emisión con una clave, se descifra en recepción con la clave inversa. De este modo, estas claves tienen la propiedad de que, cada una de ellas, invierte la acción de la otra pero, y aquí está el punto más relevante, a partir de una no se puede obtener la otra.

Un esquema de cifrado de clave pública tiene seis componentes[8] (Figura 2.):

- **Texto claro:** es el mensaje o los datos legibles que se introducen en el algoritmo como entrada.
- **Algoritmo de cifrado:** el algoritmo de cifrado realiza diferentes transformaciones en el texto claro.
- **Clave pública y privada:** es una pareja de claves que han sido seleccionadas, de las cuales una se usa para el cifrado y la otra para el descifrado. Las

[8] Fundamentos de Seguridad en Redes Aplicaciones y Estándares, William Stallings pág. 72.

transformaciones exactas llevadas a cabo por el algoritmo de cifrado dependen de la clave pública o privada que se proporciona como entrada.

- **Texto cifrado:** es el mensaje desordenado producido como salida. Depende del texto claro y la clave secreta. Para un mensaje determinado, dos claves diferentes producirían dos textos cifrados diferentes.

- **Algoritmo de descifrado:** este algoritmo acepta el texto cifrado y la clave correspondiente y produce el texto claro original.

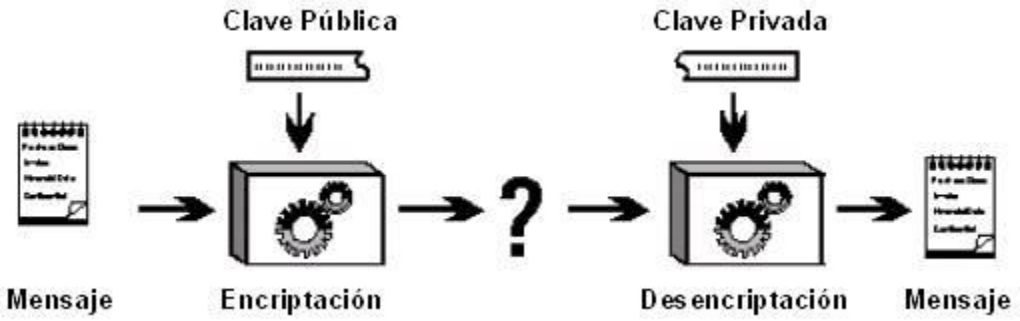


Figura 2: Criptografía asimétrica.

Las claves públicas y privadas son otorgadas por la autoridad de certificación.

La clave privada deberá ser custodiada por el usuario y es imprescindible que se mantenga en secreto. La clave pública, por el contrario, se publicará junto con la identidad del usuario. Así, cuando se quiera enviar un mensaje seguro a un usuario, se tomará la clave pública de éste y se utilizará para cifrar el mensaje que se quiera enviar. El resultado de esta operación será el texto cifrado, que sólo el propietario de la clave privada correspondiente a esa clave pública podrá descifrar

Esto no implica ningún problema de seguridad dado que es imposible deducir la clave privada a partir de la pública.

La clave privada y la pública están relacionadas matemáticamente, pero esta relación debe ser suficientemente compleja para que el criptoanalista no la pueda encontrar.

También se puede cifrar con la clave privada y descifrar con la clave pública, lo cual no proporciona confidencialidad, ya que cualquiera puede descifrar un mensaje cifrado con una clave secreta, al poder obtener siempre la componente pública de su interlocutor. Sin embargo, el hecho de cifrar un mensaje con la clave secreta de un usuario, implica una

identificación del usuario al igual que lo hace una firma, por lo que este proceso se conoce con el nombre de Firma Digital.

La Criptografía asimétrica es muy usada, siendo sus principales servicios la confidencialidad, la integridad y la autenticación del origen de los datos, además del uso del mecanismo de Firma Digital. Para cada servicio se cifra de manera diferente:

- **Confidencialidad:** el emisor cifra el texto con la clave pública del receptor y el receptor lo descifra con su clave privada. Así, cualquier persona puede enviar un mensaje cifrado, pero solo el receptor, que tiene la clave privada, y el emisor que lo ha creado, puede descifrar el contenido.
- **Autenticación**: Se cifra texto, o un resumen de éste, mediante la clave privada y cualquier persona puede comprobar su procedencia utilizando la clave pública del emisor. El mensaje es auténtico porque solo el emisor verdadero puede cifrar con su clave privada.
- **Firma Digital:** Igual que la autenticación, pero siempre se cifra el resumen del mensaje, cuyo criptograma es la firma del emisor. Así, el emisor no puede negar la procedencia ya que se ha cifrado con su clave privada. Por otro lado, el receptor no puede modificar el contenido porque el resumen sería diferente y se observaría que no coincide con el descifrado de la firma. Pero el receptor sí puede comprobar que el resumen coincide con la firma descifrada para ver si es auténtico y goza de integridad.

Cabe aclarar que, el receptor puede tener confianza sobre la autoría del emisor en el cifrado de los datos de origen, pero no en que haya sido el emisor quien los ha enviado a través de un medio de transferencia de datos; éste es otro servicio, el de **no repudio de envío**, que exige otro escenario de comunicaciones y la presencia de terceras partes de confianza (Autoridad Certificadora, AC).

Las principales ventajas de este tipo de criptografía consisten en que la clave secreta ya no tiene que transmitirse entre los interlocutores, y tampoco es necesario tener claves diferentes para cada pareja de interlocutores, siendo suficiente con que cada usuario tenga su clave pública y su clave privada.

Algunos ejemplos de algoritmos asimétricos son: Diffie-Hellman, RSA, DSA, ElGamal, Criptografía de curva elíptica.

Así, encontramos las siguientes ventajas y desventajas:

Ventajas:

Entre las principales ventajas de la criptografía asimétrica se puede mencionar lo siguiente:

- La administración de claves asimétricas tiene menor complejidad.
- El número de claves involucradas en un sistema que utiliza criptografía asimétrica es el doble del número de participantes y cada uno de ellos posee una pareja de claves. Esto permite mejor escalabilidad.
- La clave de cifrado no es igual a la de descifrado, por lo tanto puede ser conocida públicamente.
- Debido a que la clave pública está disponible para todos los usuarios, la criptografía asimétrica no es susceptible a interceptación de claves.
- La criptografía asimétrica permite la utilización de firmas digitales.
- Con criptografía asimétrica se puede garantizar confidencialidad y autenticación.
- Utilizando criptografía asimétrica se puede garantizar la integridad de los mensajes.

Desventajas:

Entre las principales desventajas de la criptografía asimétrica se tiene:

- El tamaño del mensaje en texto cifrado es mayor al tamaño del mensaje en texto plano.
- La criptografía asimétrica consume mayores recursos.
- Requiere de claves de mayor tamaño para brindar el mismo nivel de seguridad.
- La necesidad de autenticar las claves públicas para lograr datos de autenticación de origen de las claves públicas

3.4.6. Algoritmos de Clave Pública

Históricamente el problema de la distribución de claves siempre ha sido el punto débil de la mayoría de los criptosistemas. Por más robusto que sea un criptosistema, si un intruso puede robar la clave, el sistema no tiene validez suficiente. Los criptólogos siempre daban por hecho que las claves de encriptación y desencriptación eran la misma (o que se podría derivar de manera fácil una de otra). Pero al tener que distribuirse la clave a todos los usuarios del sistema, se planteaba un problema inherente: las claves se tenían que proteger contra robo, pero también tenían que distribuirse.

En 1976, dos investigadores de la Universidad de Stanford, Diffie y Hellman, propusieron una clase de criptosistema en donde las claves de encriptación y desencriptación eran diferentes, y la clave de desencriptación no podía derivarse de la clave de encriptación. El algoritmo de encriptación (con clave) *E,* y el algoritmo de desencriptación (con clave) *D*, tenían que cumplir con los tres requisitos siguientes:

1. *D(E(P))=P*
2. Es excesivamente difícil deducir *D* de *E*.
3. *E* no puede descifrarse mediante un ataque de texto llano seleccionado.

El primer requisito define que si aplicamos *D* a un mensaje cifrado *E(P)*, obtenemos nuevamente el mensaje de texto original *P*. Sin esta propiedad, el receptor legítimo no podría desencriptar el texto cifrado. El segundo requerimiento no necesita explicación. El tercer requisito es necesario porque los intrusos pueden experimentar a placer con el algoritmo. En estas condiciones, no hay razón para que una clave de encriptación no pueda hacerse pública.

El algoritmo de encriptación y la clave aplicada se hacen públicos, de ahí que se denomina Criptografía de clave pública**.**

La criptografía de clave pública requiere que cada usuario tenga dos claves: una clave pública, usada por todo el mundo para encriptar mensajes a enviar a ese usuario, y una clave privada, que necesita el usuario para desencriptar los mensajes.

Cabe aclarar que este tipo de cifrado, a primera vista, puede resultar más seguro que cualquier otro esquema de cifrado. Pero la seguridad del cifrado depende de la longitud de la clave y del coste computacional necesario para romper un cifrado. No existe nada que indique que hay uno superior, en lo que respecta a la resistencia del criptoanálisis, entre el cifrado convencional o de clave pública. Aunque los métodos de clave pública sean poderosos, tienen un coste computacional elevado, lo que demuestra que el cifrado convencional no va a abandonarse.

Actualmente, la mayoría de los protocolos de seguridad utilizan ambos esquemas de cifrado. La criptografía de clave simétrica se usa para cifrar grandes cantidades de datos y la criptografía asimétrica se aplica para acordar una clave de sesión.

3.4.6.1. Diffie- Hellman

La finalidad del algoritmo es hacer posible que los usuarios intercambien de manera segura una clave secreta, que luego pueda ser usada para el cifrado de mensajes. El algoritmo está limitado al intercambio de claves.

Este algoritmo depende, para su efectividad, de la dificultad de calcular logaritmos discretos. Podemos definir el logaritmo discreto de la siguiente manera: definimos una raíz primitiva de un número primo *p* cuyas potencias generan todos los enteros desde 1 a *p* -1. Es decir, si *a* es una raíz primitiva del número primo *p*, entonces los números

$$a \bmod p, a^2 \bmod p \ldots, a^{p-1} \bmod p$$

son distintos y consisten en los enteros desde 1 hasta *p* -1 en alguna de sus permutaciones.

Entonces podemos definir el intercambio de clave de Diffie-Hellman[9], resumiendo en la Figura 3. Para este esquema, hay dos números conocidos públicamente: un numero primo *q* y un entero α que es una raíz primitiva de *q*. Supongamos que los usuarios A y B quieren intercambiar una clave. El usuario A selecciona un entero aleatorio $X_A < q$ y computa $Y_A=\alpha^{XA} \bmod q$. De igual forma, el usuario B selecciona independientemente un entero aleatorio XB < *q* y calcula YB=α XB. Cada parte mantiene el valor X en privado y hace público el valor Y a la otra parte. El usuario A computa la clave como $K= (Y_B)^{XA} \bmod q$ y el usuario B computa la clave como $K= (Y_A)^{XB} \bmod q$.

[9] Fundamentos de Seguridad en Redes Aplicaciones y Estándares, William Stallings pág. 78.

Elementos públicos globales	
q	numero primo
α	$\alpha < q$ y $\alpha <$ una raíz prima de q
Generación de la clave del usuario A	
Seleccionar X_A privada	$X_A < q$
Calcular Y_A pública	$Y_A = \alpha^{XA} \bmod q$
Generación de la clave del usuario B	
Seleccionar X_B privada	$X_B < q$
Calcular Y_B pública	$Y_B = \alpha^{XB} \bmod q$
Generación de la clave secreta por el usuario A	
$K = (Y_B)\, X^A \bmod q$	
Generación de la clave secreta por el usuario B	
$K = (Y_A)\, X^B \bmod q$	

Figura 3: Algoritmo de intercambio de claves Diffie-Hellman

3.4.6.2. El Algoritmo RSA

El Algoritmo RSA es el más ampliamente conocido para realizar criptografía de clave pública. Su nombre se debe a sus inventores, Ronald **R**ivest, Adi **S**hamir y Leonard **A**dhelman. Es utilizado tanto para cifrado (confidencialidad) como para autenticación (firmas digitales) y usa dos tipos de claves, una pública y una privada. En la actualidad RSA emplea claves de 1024 bits (1024 bits, equivale a un número de 308 dígitos), consideradas lo bastante largas como para resistir ataques de fuerza bruta (se han roto claves de hasta 512 bits, aunque se necesitaron más de 5 meses y casi 300 computadoras trabajando juntos para hacerlo).

Su método se basa en ciertos principios de la teoría de los números:

1. Seleccionar dos números primos grandes *p y q* (generalmente de 1024)
2. Calcular $n = p$ X q y z=(p-1) X (q-1)
3. Seleccionar un número primo con respecto a *z*, llamándolo *d*.
4. Encontrar *e* tal que *e* X *d* = 1 mod *z*.

5. Para algún bloque de texto claro M y un bloque de texto cifrado C, el cifrado y el descifrado son de la siguiente forma:

$$C = M^e \ mod \ n$$

$$M = C^d \ mod \ n = (M^e)^d \ mod \ n = M^{ed} \ mod \ n$$

El uso del RSA es semejante a usar un algoritmo simétrico en modo ECB: el mismo bloque de entrada da el mismo bloque de salida. Por tanto, se requiere una forma de encadenamiento para la encriptación de datos. En la práctica, la mayoría de los sistemas basados en RSA usan criptografía de clave pública, principalmente para distribuir claves de sesión de una sola vez, para su uso con algún algoritmo de clave simétrica como el AES o el triple DES. El RSA es demasiado lento para poder encriptar grandes volúmenes de datos, pero se utiliza con amplitud para la distribución de claves.

Su seguridad se basa en la dificultad de factorizar números primos de gran tamaño. En principio, se puede deducir la clave secreta conocida la clave pública pero, solamente, por medio de la factorización de números de gran longitud (centenares de cifras). Una gran ventaja del RSA es que permite asegurar las cualidades de No Repudio, Autenticidad e Integridad de los criptosistemas, cuando se lo utiliza para firmar mensajes; razón por la cual lo convierte en un sistema muy completo y uno de los más seguros que existen.

Los servicios de autenticación y Firma Digital sólo se pueden implementar con estos sistemas. Para confidencialidad se puede utilizar también clave simétrica (DES, IDEA, RC4, etc.), siendo estos mucho más rápidos que el RSA. En la actualidad se utilizan sistemas mixtos, simétricos para confidencialidad y asimétricos para distribución de claves simétricas, autenticación y Firma Digital.

3.4.6.3 Criptografía de Curva Elíptica

La Criptografía de Curvas Elípticas (ECC) fundamenta su seguridad, en el alto grado de dificultad que supone resolver el problema del logaritmo discreto en el grupo abeliano, formado por curvas elípticas definidas sobre campos finitos.

De forma general, una curva elíptica E(Fq) se define como el conjunto de puntos que satisface la ecuación:

$$E: y^2 = x^3 + ax + b;$$

donde a y b están en un campo finito apropiado Fq de orden q, el cual puede ser el grupo de los números racionales, números complejos, enteros modulo n. Los coeficientes a y b caracterizan de manera unívoca cada curva.

La atracción principal de la ECC, en relación al RSA, es que parece ofrecer igual seguridad en un tamaño de bit menor, reduciendo así los costes de procesamiento. Por otra parte, aunque la teoría de la ECC ha estado presente durante algún tiempo, ha habido un interés por probar sus debilidades. A nivel confianza, ECC todavía no alcanza al del RSA.

3.5. Autentificación

La principal meta de la criptografía es garantizar que se cumplan los cinco servicios de la seguridad computacional: Confidencialidad, Integridad de los datos, Disponibilidad la Autentificación y el No-Repudio. La autentificación, es la técnica mediante la cual un proceso verifica que su compañero de comunicación sea quien se supone que debe ser y no un impostor.

La autentificación es necesaria en los sistemas de clave pública, aunque suele creerse que los sistemas de clave pública son ideales y no requieren de un canal seguro para transportar la clave de cifrado. Esto nos haría pensar que dos entidades pueden comunicarse dentro de un canal inseguro, sin haberse encontrado para intercambiar claves.

Desafortunadamente, este pensamiento no es posible. El ataque conocido como “hombre en el medio”, nos demuestra como un adversario activo puede burlar el modelo sin romper el criptosistema. De esta manera se verifica la necesidad de autenticar a las claves públicas, para lograr una certificación del origen de datos de las claves públicas en sí.

3.5.1. Métodos de Autentificación

La autentificación es cualquier proceso a través de cuál se demuestra y se verifica cierta información referente a un objeto como: el origen de un documento, la identidad del remitente, el momento en que un documento fue enviado y/o firmado, la identidad de una computadora o usuario, etc.

Se dice que un mensaje, archivo, documento o cualquier otro grupo de datos es auténtico cuando es genuino y procede de la fuente original. La autentificación de mensajes es un procedimiento que permite la comunicación entre las partes para verificar que los mensajes recibidos son auténticos. Los dos aspectos importantes son verificar que los contenidos del mensaje no han sido alterados y que la fuente es auténtica.[10]

Los métodos de autentificación se clasifican en cinco tipos:

- Autentificación del origen de datos: es un tipo mediante el cual se corrobora una de las partes como la fuente (original) de los datos especificados, creados en algún momento en el pasado (por lo general sin especificar). Por definición, la autenticación del origen de datos incluye la integridad de los datos.

- Autentificación de mensaje: es un término utilizado de forma análoga con la autenticación de origen de los datos. Ofrece autenticación del origen de datos con respecto a la fuente del mensaje original (y la integridad de los datos, pero no se garantiza la línea de tiempo).

- Autentificación por transacción: denota la autenticación de mensajes, además de ofrecer garantías, singularidad y oportunidad de los datos (es decir identifica el momento preciso de creación).

- Autentificación de entidad: es el proceso por el cual una de las partes, mediante la adquisición de evidencia que se puede corroborar, está seguro de la identidad de la otra parte involucrada en el protocolo y que esa otra parte está activa en ese justo momento. Los términos *Identificación* y Autentificación de entidad se usan comúnmente como sinónimos. La identificación está basada en una o más de estas características: *algo que se conozca* (contraseña, NIP, etc.); *algo que se posea* (por ejemplo, una tarjeta de identificación); y *algo que sea inherente* a un individuo (huellas digitales u otras características biométricas).

[10] Fundamentos de Seguridad en Redes Aplicaciones y Estándares, William Stallings pág. 56.

- Autentificación de clave: también llamada autentificación de llave, es la propiedad por la cual una parte está segura de que ninguna otra entidad, además de una segunda parte identificada (o un conjunto de partes confiables), tiene acceso a una llave secreta particular.

3.5.2. Funciones de Hash

Una función hash es aquella que toma, como entrada, un mensaje de tamaño variable, *M* y produce un resumen del mensaje de tamaño fijo H*(M)* como salida, conocido como valor hash. Para autentificar un mensaje, el resumen se envía con el mensaje, con lo cual se verifica la autenticidad del resumen.[11]

Con el uso de funciones hash y criptografía asimétrica, se puede garantizar el servicio de integridad de los datos con el establecimiento de firmas digitales. Una función hash sólo comprime los textos en un bloque de longitud fija. No son reversibles, es decir, no se puede recuperar el texto desde el resumen.

La finalidad de una función de hash es la de obtener una "huella" de un archivo, mensaje u otro bloque de datos. Para que resulte útil a la autentificación de mensajes, una función de hash *H* debe poseer las siguientes propiedades:

- Transformar un texto de longitud variable en un bloque de longitud fija.
- Ser irreversibles.
- Conocido un mensaje y su función Hash, debe ser imposible encontrar otro mensaje con la misma función Hash. Esto se debe cumplir para evitar que los criptoanalistas firmen un mensaje propio como si fueran otra persona.
- Es imposible inventar dos mensajes cuya función Hash sea la misma

Dadas las características de una función hash, queda claro que si se aplica una función hash a un mensaje, el valor hash obtenido es como la huella digital del mensaje; si se altera tan solo un bit del mensaje original, el valor hash será diferente.

Se puede verificar la integridad de un mensaje enviando el mensaje y su valor hash al receptor; en el destino, el receptor puede aplicar la misma función hash al mensaje y luego comparar su resultado con el valor recibido. Para evitar que un atacante cambie el mensaje

[11] Fundamentos de Seguridad en Redes Aplicaciones y Estándares, William Stallings pág. 61.

y el valor hash introduciendo valores falsos, el valor hash debe enviarse cifrado con la clave privada del emisor.

Esquema:

Mensaje = M

Función Resumen = h(M)

Firma (rúbrica): r = EdE{h(M)}

dE es la clave privada del emisor que firmará h(M)

¿Cómo se comprueba la identidad en destino?: se descifra la rúbrica r con la clave pública del emisor eE. Al mensaje en claro recibido M' (si viniese cifrado, se descifra) se le aplica la misma función hash que en emisión. Si los valores son iguales, la firma es auténtica y el mensaje íntegro:

Calcula: EeE(r) = h(M)

Compara: h(M') = h(M)

Las funciones, o algoritmos de hash, son usadas en múltiples aplicaciones como, los arrays asociativos, criptografía, procesamiento de datos y firmas digitales, entre otros. Los algoritmos de hash MD5 y SHA-1 son dos de los más populares.

3.5.3. MD5

En criptografía, MD5 (acrónimo de **M**essage-**D**igest Algorithm **5**, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente utilizado.

Opera truncando los bits de una manera tan complicada que cada bit de salida es afectada por cada bit de entrada. Muy brevemente, comienza por rellenar el mensaje a una longitud de 448 bits (módulo 512). Después la longitud original del mensaje se agrega como entero de 64 bits para dar una entrada total, cuya longitud es un múltiplo de 512 bits. El último paso del cálculo previo es la inicialización de un búfer de 128 bits a un valor fijo.

El cálculo se inicia desde que cada ronda toma un bloque de 512 bits de entrada y lo mezcla por completo con el búfer de 128 bits. Además, se introduce una tabla construida a partir de la función seno. El objetivo de la función conocida como el seno, no es porque sea más aleatoria, sino para evitar especulaciones acerca de que el diseñador creo otra

puerta trasera[12]. Se hacen cuatro rondas por cada bloque de entrada. Este proceso continúa hasta que todos los bloques de entrada se han consumido. El contenido del búfer de 128 bits forma el compendio del mensaje.

MD5 ha existido aproximadamente por una década y muchas personas lo han atacado. Se han encontrado algunas vulnerabilidades, pero ciertos pasos internos evitan que sea violado. Sin embargo, si cayeran las barreras restantes dentro de MD5, éste podría fallar con el tiempo.

3.5.4 SHA-1

La otra función principal para el compendio de mensajes es SHA-1 (Algoritmo Seguro de Hash 1), desarrollado por la National Security Agency (NSA) y aprobado por el National Institute of Standards and Technology (NIST) en FIPS 180-1. Al igual que MD5, SHA-1 procesa datos de entrada en bloques de 512 bits, sólo a diferencia de MD5, genera un compendio de mensaje de 160 bits. En la Figura 4 se ilustra una forma típica para que Alice envíe a Bob un mensaje no secreto, pero firmado. Aquí su mensaje de texto llano se alimenta en el algoritmo SHA-1 para obtener un hash SHA-1 de 160 bits. A continuación, Alice firma el hash con su clave privada RSA y envía a Bob tanto el mensaje de texto llano como el hash firmado.

Después de recibir el mensaje, Bob calcula el hash SHA-1 él mismo y también aplica la clave pública de Alice al hash firmado para obtener el hash original, H. Si los dos concuerdan, el mensaje se considera válido. Puesto que no hay forma de que Trudy modifique el mensaje (de texto llano), mientras está en tránsito, y producir uno nuevo que haga hash a H, Bob puede detectar con facilidad cualquier cambio que Trudy haya hecho al mensaje. Por un costo de cómputo relativamente bajo, garantiza que cualquier modificación hecha al mensaje de texto llano en tránsito pueda detectarse con una probabilidad muy alta.

[12] Una puerta trasera o *BackDoor* es una característica oculta de algunas aplicaciones o algoritmos que permite a su creador acceder a opciones especiales que son inaccesibles para los usuarios.

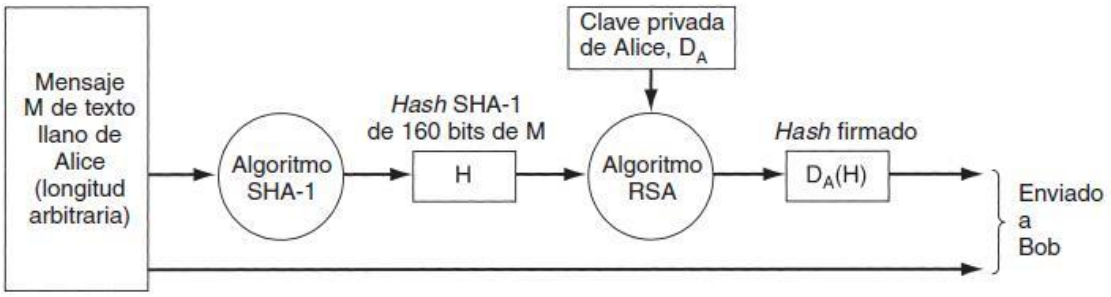


Figura 4: Uso de SHA-1 y RSA para firmar mensajes no secretos.

3.6. Firma Digital

La autenticidad de documentos legales, financieros y de cualquier otro tipo se determina por la presencia o ausencia de una firma holográfica autorizada. Para que los sistemas computarizados reemplacen el transporte físico de papel y tinta, debe encontrarse un método para que la firma de los documentos sea infalsificable.

El problema de idear un reemplazo para una firma manuscrita es complicado, ya que se requiere un sistema en el cual una parte pueda enviar un mensaje "firmado" a otra parte, de modo que:

- El receptor pueda verificar la identidad del transmisor: Propiedad de autenticidad.
- El transmisor no pueda repudiar (negar) después el contenido del mensaje: Propiedad de no repudio.
- El receptor no haya podido elaborar el mensaje él mismo: Propiedad de integridad.

Así podemos afirmar que una Firma Digital es una primitiva de cifrado, fundamental en la autenticación, autorización y no repudio. El propósito de una Firma Digital es, proporcionar un medio para que una entidad pueda relacionar su identidad a un segmento de información[13].

De este modo, la Firma Digital es una herramienta tecnológica, que permite garantizar la autoría e integridad de los documentos digitales, posibilitando que éstos posean la misma característica que la firma hológrafa, exclusiva de los documentos en papel. Así, una Firma

[13]Handbook of Applied Cryptography, by A. Menezes, P. van Oorschot, and S. Vanstone pág. 22.

Digital es un conjunto de datos asociados a un mensaje digital, que permite garantizar la identidad del firmante y a 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.

El proceso de firma, dentro de los esquemas de clave pública, se puede ver como el proceso de cifrado con la clave privada; y el proceso de verificación, se puede ver como el proceso de descifrado con la clave pública. El esquema general de Firma Digital se muestra en la Figura 5. Como se observa, al mensaje se le aplica una función hash, cuyo resultado será firmado con la clave privada del signatario y anexado al mensaje para ser enviados al destinatario. El destinatario separa los dos componentes: el mensaje y la firma. Le aplica la misma función hash al mensaje obteniendo el valor v1 y a la firma la verifica con la clave pública del signatario obteniendo el valor v2; si v1 = v2 se diría que el mensaje no ha sido alterado en la transmisión y que la autenticidad del origen ha sido confirmada.

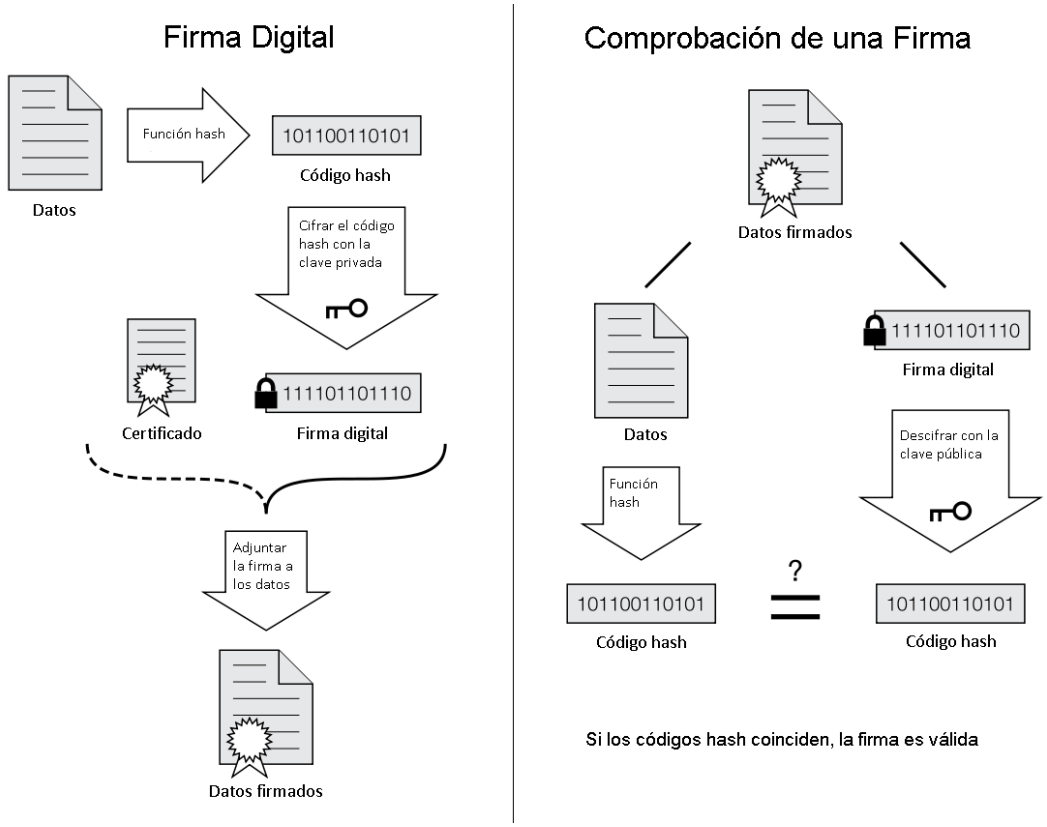


Figura 5: Esquema de Firma Digital.

Cabe destacar que:

- Cualquiera que posea la clave pública del emisor puede constatar que el mensaje proviene realmente de él.
- La Firma Digital es distinta en todos los documentos: si A firma dos documentos produce dos criptogramas distintos; y si A y B firman el mismo documento también producirán dos criptogramas diferentes.

Actualmente se recomienda utilizar firmas de al menos 128 bits (38 dígitos) siendo 160 bits (48 dígitos) el valor más utilizado.

La Firma Digital debe cumplir los siguientes requisitos:

- Debe ser fácil de generar.
- Será irrevocable, no repudiable por su propietario.
- Ser única, sólo posible de generar por su propietario.
- Será fácil de auténtica o reconocer por su propietario y los usuarios receptores.
- Debe depender del mensaje y del autor.

Las funciones de la Firma Digital son garantizar:

- **Autenticidad***:* poder atribuir el documento únicamente a su autor, de forma fidedigna, de manera de poder identificarlo.
- **Integridad:** estar vinculada a los datos del documento digital, poniendo en evidencia su alteración luego de que fue firmado.
- **Exclusividad:** garantizar que la firma se encuentre bajo el absoluto y exclusivo control del firmante.
- **No repudio:** garantizar que el emisor no pueda negar o repudiar su autoría o existencia; ser susceptible de verificación ante terceros.
- **Validez:** haber sido producida con un certificado emitido por un Certificador Licenciado.

Así, se pueden firmar diferentes elementos:

- Datos enviados a través de un formulario web.
- Una imagen, fotos o música.

- Un base de datos.
- Un disco rígido, un CD o un DVD.
- Una página o un sitio de Internet.
- Una transacción electrónica o un e-mail.
- Una hoja de cálculo o un documento de texto.
- El código fuente de un programa o un software.
- Uno o varios archivos en general.
- Además, podemos afirmar que una Firma Digital No es lo siguiente:
- Una Firma Digitalizada (una firma manuscrita escaneada).
- Una contraseña o password.
- Un sistema biométrico.
- Un sistema de autenticación: este requisito sólo no alcanza.
- Una firma electrónica.
- Un documento encriptado (sólo se garantiza la confidencialidad).

3.6.1. El algoritmo de Firma Digital (DSA)

En agosto de 1991, en los EE.UU., el Instituto Nacional de Estándares y Tecnología (NIST) propuso un algoritmo de Firma Digital (DSA). La DSA se ha convertido en un Estándar de información federal (FIPS 186) llamado Digital Signature Standard (DSS), y es el primer esquema de Firma Digital reconocida por un gobierno. El algoritmo es una variante del esquema de ElGamal.

El mecanismo de la firma requiere de una función hash h: {0, 1} * - → Zq para algún entero *q*. El DSS exige explícitamente el uso del algoritmo de hash seguro (SHA-1).

Para generar el par de claves de DSA se debe seguir una fase de inicialización:

Cada entidad crea una clave pública y una clave privada correspondiente.

Cada entidad A debe hacer lo siguiente:

1. Seleccione un número primo q tal que 2159 <*q* <2160.
2. Elija t para que $0 \leq t \leq 8$, y seleccionar un número primo p, donde $2^{511+64\,t}$ <p <

$2^{512+64\,t}$, con la propiedad de que *q* divide a (p - 1).

3. (Seleccione una α generador del único grupo cíclico de orden q en Z *p.)

3.1 Seleccionar un elemento g pertenezca Z *p y calcular $\alpha = g^{(p-1)/q} \bmod p$.

3.2 Si α = 1, entonces vaya al paso 3.1.

4. Seleccionar un entero aleatorio a tal que $1 \leq a \leq q - 1$.

5. Calcular $y = \alpha^a \bmod p$.

6. Una clave pública es (p, q, α, y); Una clave privada es a.

A firma un mensaje m con el siguiente procedimiento:

(a) Seleccionar un número entero k aleatorio secreto, 0 <k <q.

(b) Calcule $r = (p\,\alpha^k \bmod p) \bmod q$.

(c) Calcular $k^{-1} \bmod q$.

(d) Calcular $s = k^{-1}\{h(m) + ar\} \bmod q$.

(e) La firma de A para m es (r; s), la cual se envía a B junto con m.

Para que B v u2erifique la firma debe:

(a) Obtener los datos públicos de A (p, q, α, y).

(b) Verificar que 0 <r <q, 0 <s <q, si no es así, rechazar la firma.

(c) Calcule $w = s^{-1} \bmod q$ y h (m).

(d) Calcular $u_1 = w \cdot h(m) \bmod q$ y $u_2 = rw \bmod q$.

(e) Calcular $v = (\alpha^{u1} y^{u2} \bmod p) \bmod q$.

(f) Aceptar la firma si y sólo si v = r.

3.6.2. Firma con RSA

Si se utiliza el esquema de llave pública RSA para Firma Digital, los pasos son los siguientes:

1. Recapitulando, A genera dos primos grandes p; q y calcula n = pq. A elije e_A tal que $1 < e_A < \phi(n)$ con *mcd*(e_A; ϕ (n)) = 1, y calcula d_A tal que $e_A d_A \equiv 1 \pmod{\phi(n)}$. A publica ($e_A$; n) y mantiene privado d_A; p; q. El proceso de generación de claves se da por hecho al iniciar el procedimiento de firma.

2. La firma de A es $y \equiv m^{dA} \pmod{n}$:

3. Entonces el par (*m; y*) se hace público.

B puede verificar que A firmó el mensaje siguiendo los siguientes pasos:

1. Obtener (e_A; *n*) de A.

2. Calcular z ≡y e_A (mod *n*). Si z = *m*, entonces B puede aceptar la firma como válida; de otra manera la firma no es válida.

El sistema criptográfico RSA presenta algunos inconvenientes para las firmas digitales parecidos a los que presenta como sistema de cifrado. En particular, no se sabe a ciencia cierta si es tan difícil de romper como la factorización de grandes enteros. Incluso, aunque así fuera, dados un mensaje original elegido *m* y la llave de cifrado de otro usuario (*e; n*), calcular la Firma Digital *s* tal que $m - s^e$(mod *n*) puede ser mucho más fácil si se tiene, además, (*s' ;m'*), donde *s'* es la Firma Digital del usuario legitimo para un mensaje *m'* muy parecido al mensaje *m*. En otras palabras, podría resultar fácil falsificar firmas digitales para algún mensaje dado después de haber visto las firmas digitales auténticas de varios mensajes parecidos.

Lo mencionado sugiere que podría resultar más favorable, para el diseño de esquemas de firmas digitales, el empleo de sistemas probabilísticos, en vez de los sistemas de llave pública. Sin embargo, ésta es una tarea difícil, ya que, por ejemplo, se ha demostrado que el sistema probabilístico de Blum-Goldwasser es inútil para firmas digitales. Debido a este tipo de ataques para la firma y verificación, el estándar de criptografía de RSA **PKCS** #1 versión 2:1 da recomendaciones para la implementación de los esquemas criptográficos de clave pública basados en RSA: primitivas criptográficas, esquemas de cifrado, esquemas de firma, y la sintaxis ASN.1 para representar a las llaves.

Para cifrar el mensaje *m*, se digiere con una función *hash* dando como resultado un digesto que es codificado de acuerdo al estándar en una cadena de octetos.

A continuación, el resultado se divide en bloques y cada cadena de octetos es transformada a enteros. A partir de ahí, se aplica la primitiva de firma de RSA, vista anteriormente, y el resultado es convertido de enteros a octetos, teniendo de esta manera la Firma Digital. Para el proceso de verificación, dentro del estándar a partir de la firma y el mensaje *m*, el primer paso es convertir la cadena de octetos de la firma en cadena de enteros, a lo cual se le

aplica la verificación de RSA, la cadena resultante de enteros se convierte a cadena de octetos nuevamente y se le aplica un análisis para recuperar del bloque la digestión *h*(*m*)*0*, se digiere el mensaje *m* y el resultado, *h*(*m*) debe ser idéntico a *h*(*m*)*0*.

Estos esquemas resisten los ataques, principalmente al dar formato a los bloques, ya que todos los mensajes grandes o pequeños se codifican a bloques de tamaño normalizado de *k* bytes (a través del uso de bits de relleno).

3.7. Certificados.

Se entiende por certificado digital al documento digital firmado digitalmente por un una tercera parte de confianza, el cual vincula los datos de verificación de firma a su titular. Los certificados de Firma Digital deben ser emitidos por un Certificador Licenciado, cuya licencia este certificada por el Ente Licenciante.

Un certificado es esencialmente una clave pública y un identificador, firmados digitalmente por una autoridad de certificación, y su utilidad es demostrar que una clave pública pertenece a un usuario concreto[14].

En otras palabras, es un documento digital mediante el cual, la autoridad de certificación asegura la vinculación entre la identidad del usuario, su clave pública y privada.

La clave privada, es la clave confidencial que mantiene en privado el usuario. Es usada generalmente para descifrar los mensajes codificados y también para generar la Firma Digital.

La clave privada, empleada para enviar mensajes, debe estar exclusivamente bajo el poder del firmante. Para ello, dicha clave se guarda en un dispositivo seguro, en una tarjeta criptográfica, que no se pueden duplicar y está protegida por un ping.

La clave pública, es la parte del certificado digital que se utiliza para la verificación de la firma electrónica y el cifrado de datos.

Por otra parte, la clave pública debe ser conocida por el resto de las personas, por lo que se incluye en un certificado digital público y accesible. Este certificado avala que la clave contenida en él, pertenece a la persona indicada en el mismo; esto quiere decir que lo identifica unívocamente.

[14] Criptografía y Seguridad en Computadores, Manuel J. Lucena López pág. 169.

Los certificados digitales permiten efectuar comunicaciones electrónicas seguras, proporcionando y garantizando:

- **Autenticación:** permite que la identidad del emisor y el receptor sean reconocidas y autorizadas, así como la información que de ellos proviene. El certificado digital asocia los datos del usuario a una clave pública, que permite a otros verificar que esa clave es válida.
- **Confidencialidad:** de la información transmitida mediante el uso de algoritmos de cifrado, con el propósito de que sólo el destinatario del documento pueda acceder a su contenido
- **No repudio o irrenunciabilidad**: permite probar la participación de las partes en una comunicación, existiendo dos posibilidades:
    - No repudio en origen: el emisor no puede negar que envío porque el destinatario tiene pruebas del envío.
    - No repudio en destino: el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.
- **Integridad:** de la información que se transfiere, garantizando que no se ha producido manipulación alguna en el mensaje original.

Los certificados ayudan a prevenir que alguien utilice una clave para hacerse pasar por otra persona. En algunos casos, puede ser necesario crear una cadena de certificados, cada uno certificando el previo, para que las partes involucradas confíen en la identidad en cuestión. En su forma más simple, el certificado contiene una clave pública y un nombre. Habitualmente, también contiene una fecha de expiración, el nombre de la Autoridad Certificante que la emitió, un número de serie y alguna otra información.

Pero lo más importante es que el certificado propiamente dicho, está firmado digitalmente por el emisor del mismo.

Su formato está definido por el estándar internacional ITU-T X.509. De esta forma, puede ser leído o escrito por cualquier aplicación que cumpla con el mencionado estándar.

Para obtener un certificado digital, debemos en primer lugar saber quién o quienes intervienen en este proceso, los cuales analizamos a continuación:

- **Autoridad de Certificación (AC):** es quién emite el certificado digital y quién interviene como tercero de confianza.

- **Autoridad de Registro (AR):** persona o entidad delegada por la AC para la verificación de la identidad de los solicitantes y otras funciones, dentro del proceso de expedición y manejo de certificados digitales.
- **Suscriptor:** es la persona para la cual se expide el certificado.
- **Solicitante:** persona física que solicita la expedición del certificado, puede ser distinta que el suscriptor.
- **Usuario:** Persona que voluntariamente decide confiar en un certificado.

3.7.1. Clases de Certificados

Los certificados pueden ser clasificados según qué medios hayan sido utilizados para verificar la veracidad de los datos:

- **Clase 0**: se utilizan para probar el procedimiento de Firma Digital. Son gratuitos.
- **Clase 1**: certifican que la persona que posee el Certificado es quien dice ser, y que la dirección de correo electrónico está bajo su control. Para cerciorarse la identidad de la persona, la Autoridad de Registro solicita un documento que lo acredite.
- **Clase 2**: certifican que la persona que posee el Certificado es quien dice ser, y que la dirección de correo electrónico está bajo su control. Para cerciorarse la identidad de la persona, la Autoridad de Registro requiere que el solicitante se presente con Documentación de Identificación Oficial en el ámbito nacional.
- **Clase 3**: tienen la ventaja de no necesitar ningún hardware especial, sin costos, posibilitando su uso masivo. Solo requiere instalar el certificado en la PC que utilizará para firmar digitalmente documentos. El sistema solicitará el ingreso de la clave privada para firmar documentos.
- **Clase 4:** Brindan una mayor seguridad ya que los datos privados del titular son almacenados en un dispositivo criptográfico especial. Para firmar digitalmente el sistema solicitará que conecte el dispositivo criptográfico e ingrese la clave privada.

3.7.2. Usos de los Certificados

Los certificados permiten realizar una gran cantidad de acciones a sus titulares, entre los cuales tenemos:

- **Identificación**: control de accesos a sitios Web o servicios en línea restringidos. Desarrollo de comunidades cerradas, intranets corporativas. Control de acceso físico de tarjetas inteligentes. Firma de software para su uso en Internet, de manera que se puedan realizar acciones en el navegador del usuario que de otro modo le serían negadas.
- **Transacciones electrónicas**: como por ejemplo los movimientos en una cuenta corriente o las transacciones comerciales seguras.
- **Trámites fiscales**: como por ejemplo declaraciones juradas de impuestos, pago on-line de tributos.
- **Seguridad en servidores Web**: se trata de tener la certeza de que se está en el verdadero sitio y no en una copia, permitiendo realizar interacciones seguras.
- **Documentos electrónicos**: da la posibilidad de firmar contratos, órdenes de compra o cualquier otro documento de uso público o privado, en forma digital con los mismos efectos que los celebrados por escrito y en soporte de papel. Así mismo, se puede asegurar la confidencialidad en procesos administrativos o consultas de información de importancia, en servidores de la Administración.
- **Correo Seguro:** permite enviar correo electrónico cifrado y firmado, de manera de proteger este canal, identificando a quién emite, a quién recibe y además cifrando el contenido del mensaje.

3.7.3. Estándar X.509

Si todas las personas que desean algo firmado fueran a la AC, con un tipo diferente de certificado, administrar todos los formatos diferentes pronto se volvería un problema. Para resolverlo se ha diseñado un estándar para certificados, el cual ha sido aprobado por la ITU. Dicho estándar se conoce como X.509**,** solo define la sintaxis de los certificados, por lo que no está atado a ningún algoritmo en particular y se utiliza ampliamente en Internet. La versión IETF del X.509 se describe en el RFC 3280. En esencia, el X.509 es una forma de describir certificados. Los campos principales en un certificado se listan en la Figura 6. Las descripciones dadas allí proporcionan una idea general de la función que cumplen los campos.

Campo	Significado
Versión	Cuál versión del X.509
Número de serie	Este número junto con el nombre de la CA identifican de manera única el certificado
Algoritmo de firma	El algoritmo que se utilizó para firmar el certificado
Emisor	El nombre X.500 de la CA
Validez	Las fechas de inicio y final del periodo de validez
Nombre del sujeto	La entidad cuya clave se está certificando
Clave pública	La clave pública del sujeto y el ID del algoritmo usado para generarla
ID del emisor	Un ID opcional que identifica de manera única al emisor del certificado
ID del sujeto	Un ID opcional que identifica de manera única al sujeto del certificado
Extensiones	Se han definido muchas extensiones
Firma	La firma del certificado (firmada por la clave privada de la CA)

Figura 6: Campos de un certificado X.509

Los certificados están codificados mediante la **ASN.1** (**Notación de Sintaxis Abstracta 1**) de la OSI, que puede considerarse como si fuera una estructura de C, pero con una notación peculiar y poco concisa.

El certificado está compuesto de tres áreas principales:

- El Certificado *TBS*, que contiene la *versión* del certificado, el *número de serie*, el *identificador del algoritmo* de la firma, el *nombre del emisor*, el periodo de *validez* del certificado, el *usuario* que está siendo certificado, la *información de la llave pública* del usuario. Es opcional la presencia del *identificador único* del emisor, del *identificador único* del usuario y de las extensiones.
- El *Identificador del Algoritmo de Firma* que toma un código preestablecido.
- El *Valor de la Firma* que es una cadena de bits.

Estos certificados se estructuran de forma jerárquica, de tal forma que es posible verificar la autenticidad de un certificado comprobando la firma de la autoridad que lo emitió, que a su vez tendrá otro certificado expedido por otra autoridad de rango superior. De esta forma se va subiendo en la jerarquía hasta llegar al nivel más alto, que deberá estar ocupado por un certificador que goce de la confianza de toda la comunidad. Normalmente las claves

públicas de los certificadores de mayor nivel se suelen publicar incluso en papel para que cualquiera pueda verificarlas[15].

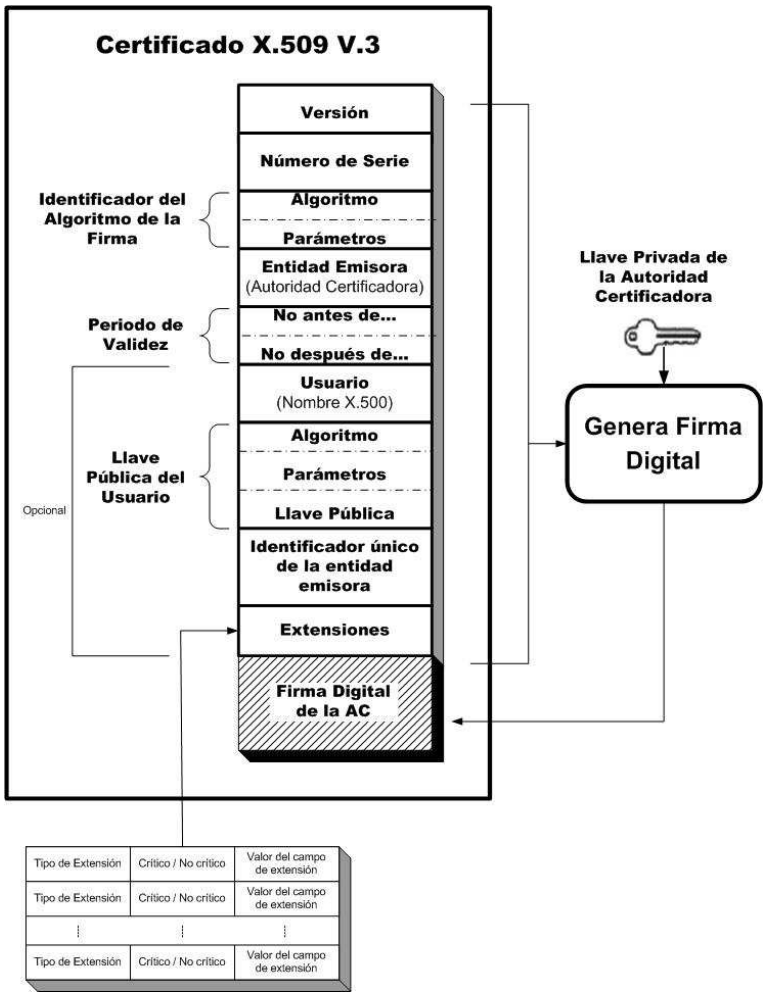


Figura 7: Formato certificado X.509

3.8. Infraestructura de Clave Pública (PKI).

Se define Infraestructura de Firma Digital o Infraestructura de Claves Públicas, al conjunto de normas jurídicas, hardware, software, bases de datos, redes, estándares tecnológicos, personal calificado y procedimientos de seguridad, que permiten que distintas entidades (individuos u organizaciones), mediante el uso de certificados digitales como herramienta,

[15]Criptografía y Seguridad en Computadores, Manuel J. Lucena López pág. 170.

se identifiquen entre sí de manera segura al realizar transacciones en redes, especialmente Internet, permitiendo además dotar de autoría e integridad a los documentos digitales[16].

El sistema de autenticación debe tener:

- **Una política de certificación.**
- **Un certificado de la AC.**
- **Los certificados de usuarios (X.509).**
- **Los protocolos de autenticación, gestión y obtención de certificados.**

El objetivo de cualquier PKI es proporcionar a cada usuario las claves necesarias para:

1. Identificarse, frente a los servidores que lo soliciten y bajo el pleno control del titular.

2. Firmar Digitalmente pedidos, órdenes de pago, correo electrónico, entre otras cosas.

3. Disponer de Correo Electrónico Seguro, haciendo que los demás puedan enviar mensajes que sólo el destinatario genuino puede abrir y leer.

4. Establecer canales de comunicación realmente privados entre usuarios, sin la supervisión de ningún otro agente que pudiese aprovecharse de lo que a través de ese canal se comunica.

Una PKI consta de:

- Política de seguridad.

- Autoridad de Certificación.

- Autoridad de Registro.

- Sistema de Distribución de Certificados.

[16] http://www.jgm.gov.ar Laboratorio de Firma Digital.

- Aplicaciones aptas para PKI.

Una infraestructura PKI es una infraestructura de seguridad, basada en criptografía de clave pública, que permite la gestión de certificados digitales. La meta de una infraestructura de clave pública es cumplir las necesidades del *control de acceso*, de la *identificación automatizada* y de la *autentificación* de manera determinista

Una PKI tiene múltiples componentes, entre ellos usuarios, ACs, certificados y directorios. La tarea principal de una PKI es proporcionar una forma para estructurar estos componentes y definir estándares para los diversos documentos y protocolos. Una forma, particularmente simple, de PKI es una jerarquía de ACs, como se muestra en la Figura 8. La AC de nivel superior, la raíz, certifica a ACs de segundo nivel, llamadas **Ras** (**Autoridades Regionales**), que pueden cubrir alguna región geográfica, como un país o un continente. Estas Ras, a su vez, certifican a las ACs reales, las cuales emiten los certificados X.509 a organizaciones e individuos. Cuando la raíz autoriza una nueva RA, genera un certificado X.509 donde indica que ha aprobado la RA, e incluye en él la nueva clave pública de la RA, la firma y se la proporciona a la RA. De manera similar, cuando una RA aprueba una AC, produce y firma un certificado que indica su aprobación y que contiene la clave pública de la AC.

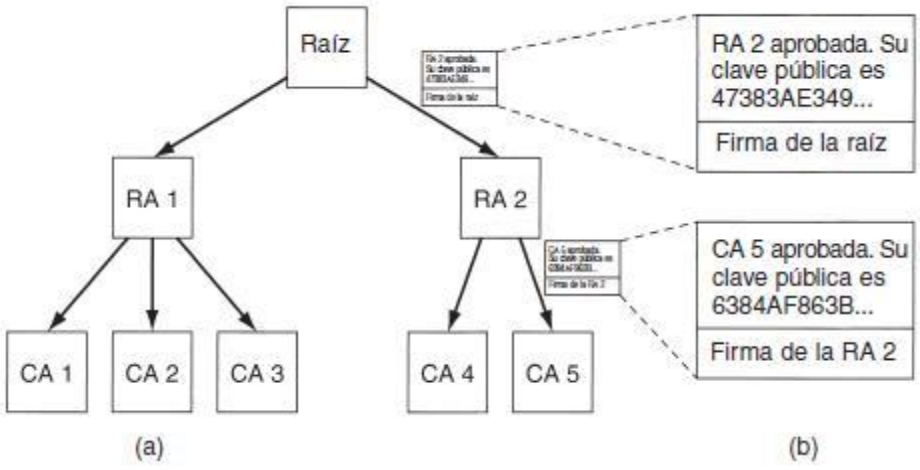


Figura 8: a) PKI jerárquica. b) Cadena de certificados.

Directorios

Un problema de cualquier PKI es en dónde están almacenados los certificados (y sus cadenas hacia un ancla de confianza [17]conocida). Una posibilidad es hacer que cada usuario almacene sus propios certificados. Si bien esto es seguro (es decir, no hay forma de que los usuarios falsifiquen certificados firmados sin que esto se detecte), también es inconveniente. Una alternativa que se ha propuesto es utilizar DNS como un directorio de certificados. Una alternativa es dedicar servidores de directorio, cuyo único trabajo sea manejar los certificados X.509. Tales directorios podrían proporcionar servicios de búsqueda, utilizando propiedades de los nombres X.500. LDAP podría ser seleccionado para almacenar esta información.

Revocación

Algunas veces estos certificados pueden anularse, es decir, el otorgante de un certificado podría decidir revocarlo porque la persona u organización que lo posee, ha abusado de alguna manera. También puede revocarse si la clave privada del sujeto se ha expuesto o si la clave privada de la AC está en peligro. Por lo tanto, una PKI necesita tratar el problema de la revocación.

Un primer paso en esta dirección es hacer que cada AC emita periódicamente una CRL (lista de revocación de certificados), que proporcione los números seriales de todos los certificados que ha revocado. Puesto que los certificados contienen fechas de vencimiento, la CRL sólo necesita contener los números seriales de los certificados que no han expirado. Una vez que pasa la fecha de vencimiento de un certificado, éste se invalida de manera automática, por lo que no hay necesidad de hacer una distinción entre los certificados que han expirado y los que fueron revocados. Ninguno de esos tipos de certificados puede utilizarse.

Introducir CRLs significa que un usuario, que está próximo a utilizar un certificado, debe adquirir la CRL para ver si su certificado ha sido revocado. Si es así, dicho certificado no debe utilizarse. Sin embargo, si el certificado no está en la lista, pudo haber sido revocado justo después de que se publicó la lista. Por lo tanto, la única manera de estar seguro

[17] Es una clave pública y el nombre de una autoridad de certificación que es usado para validar el primer certificado en una secuencia de certificados.

realmente es preguntar a la CA. Y la siguiente vez que se utilice ese mismo certificado, se le tiene que preguntar nuevamente a la CA, puesto que dicho certificado pudo haber sido revocado segundos antes.

Otro inconveniente es que un certificado revocado puede reinstalarse nuevamente, por ejemplo, si fue revocado por falta de pago, pero ahora se ha puesto al corriente. Tener que tratar con la revocación (y, posiblemente, con la reinstalación) elimina una de la mejores propiedades de los certificados, principalmente, que pueden utilizarse sin tener que contactar a una AC.

¿Dónde deben almacenarse las CRLs? Un buen lugar sería el mismo en el que se almacenan los certificados. Una estrategia es que una AC quite, de manera activa y periódica, CRLs y hacer que los directorios las procesen con sólo eliminar los certificados revocados. Si no se utilizan directorios para almacenar certificados, las CRLs pueden almacenarse en caché, en varios lugares convenientes alrededor de la red. Puesto que una CRL es, por sí misma, un documento firmado, si se altera, ésto puede detectarse con facilidad. Si los certificados tienen tiempos de vida largos, las CRLs también los tendrán. Una forma estándar para tratar con CRLs grandes es emitir una lista maestra ocasionalmente, pero emitir actualizaciones con más frecuencia. Hacer esto reduce el ancho de banda necesario para distribuir las CRLs.

4. Modelo Teórico

4.1. Introducción

A partir del desarrollo del marco teórico se ha logrado comprender el concepto de Firma Digital, sus algoritmos relacionados, estándares vigentes e infraestructura de Firma Digital, como base teórica de apoyo para el presente proyecto.

En pos de los objetivos planteados, se desarrollara en esta sección un modelo teórico apropiado para cumplimentar dichos objetivos.

De este modo, se busca cumplimentar los siguientes objetivos específicos:

- Definir los requerimientos para la implementación de Firma Digital en el IUA.
- Modelar un esquema de Firma Digital, considerando la infraestructura, leyes, normativas y estándares tecnológicos estudiados.

4.2. Planificación

A continuación, se definen las actividades a llevar adelante para cumplimentar cada etapa del proyecto, en un lapso de tiempo considerado aceptable.

4.2.1. Etapas, actividades y duración

	Nombre de tarea	Duración
1	**Proyecto**	**190 días?**
2	Introducción	6 días?
3	Marco Contextual	4 días?
4	Marco Teórico	40 días?
5	**Modelo Teórico**	**72 días?**
6	Planificación	5 días?
7	Requerimientos	10 días?
8	Análisis	20 días
9	Diseño	35 días
10	**Concreción del Modelo**	**44 días**
11	Simulación del Proyecto	30 días
12	Revisión del Modelo	14 días
13	**Revisión**	**24 días**
14	Revisión de documentación	9 días
15	Conclusiones	5 días
16	Revisión Final	10 días

Tabla 2: Etapas y actividades y duración del proyecto

4.2.2. Diagrama Gantt

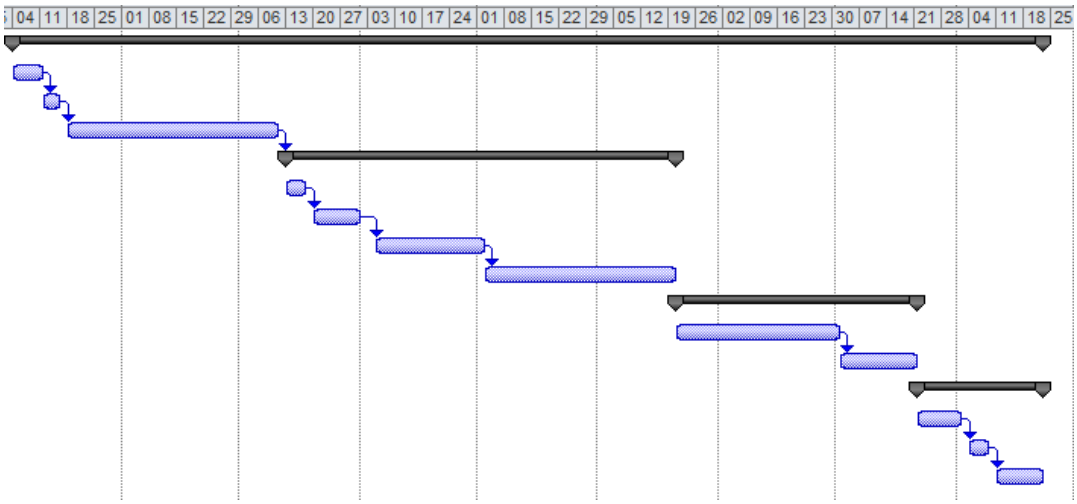


Figura 9: Diagrama Gantt del proyecto

4.3. Requerimientos

Los requerimientos de este proyecto surgen a partir de la necesidad de implementar un esquema de Firma Digital en el IUA, con el objetivo de simplificar y agilizar determinados procesos administrativos existentes. Brindando mayor seguridad en el de envío y recepción de documentos, reduciendo riegos de falsificación, tiempo y delitos informáticos; garantizando así, la autenticación de la identidad del firmante, la integridad de la información y el no repudio de la información.

En tal sentido, en los requerimientos de este modelo se describen los servicios proporcionados por el sistema y sus restricciones operativas; los cuales reflejan las necesidades de los usuarios y representan la base para la prueba de concepto, que propone una solución que ayudará a resolver la problemática planteada.

Así, se pueden definir diferentes niveles de descripción para los requerimientos:

- Requerimientos del usuario: están definidos por las declaraciones de los servicios que se espera que el sistema proporcione y de las restricciones bajo las cuales debe funcionar.
- Requerimientos del sistema: donde se define exactamente qué es lo que se va a implementar, las funciones, servicios operativos.

En las secciones posteriores se realizará un análisis detallado sobre dichos requerimientos.

4.3.1 Requerimientos funcionales y no funcionales

Los requerimientos se pueden clasificar en funcionales y no funcionales, de acuerdo a las declaraciones y restricciones de los servicios brindados por el sistema.

4.3.1.1 Requerimientos funcionales

Describen lo que el sistema debe hacer:

- El usuario deberá tener la posibilidad de firmar digitalmente todo documento que se le solicite.
- El usuario podrá verificar el certificado, vigencia y la autenticidad del mismo en el mismo documento.
- El usuario podrá verificar que dicho documento no haya sido modificado o alterado.
- El sistema generará una clave privada que se asignará a cada usuario de manera única.

4.3.1.2 Requerimientos no funcionales

Son aquellos que se refieren a las restricciones y limitaciones del sistema en su desarrollo y operación:

- Requerimientos de uso: refieren el grado de utilidad del sistema de Firma Digital, es decir, que tan fácil puede ser aplicado y utilizado, reemplazando la firma manuscrita.
- El esquema de Firma Digital no deberá revelar, al personal que lo utilice, ninguna información sobre las claves privadas de otros usuarios, ni transacciones realizadas, más allá de los datos como nombre, apellido y referencia de cargo; como así también, todos los datos (campos) definidos y emitidos en el certificado digital que acompañará a cada documento.

- Requerimientos legislativos: el proceso de desarrollo de Firma Digital, los documentos firmados mediante esta metodología a implementar y los requisitos para cumplimentarla, deberán ajustarse a las normativas de Firma Digital de la República Argentina de acuerdo con la Ley N° 25.506.

- El proceso de desarrollo de Firma Digital debe cumplir con los procedimientos, normativas de verificación y gestión de cada área, dispuestos por el IUA.

4.3.2. Actores Participantes

Los actores participantes son aquellos implicados con el sistema de Firma Digital.

Entre ellos, se pueden definir 4 actores principales:

- Quien firma (el suscriptor): es la persona física o jurídica, titular de un certificado. Es la encargada de firmar digitalmente los documentos que desee, por ejemplo: el Decano de la Facultad, los directores, secretarios, jefes de departamentos del IUA, AIT, etc.

- Quien(es) necesita(n) verificar la firma: es la/s persona/s física o jurídica, titular de un certificado. Es quien desea realizar una identificación del firmante, para autentificar que el que rubrica es quién dice ser, por ejemplo: el Decano de la Facultad, los directores, secretarios y jefes de departamentos del IUA.

- Quien testimonia que una Firma Digital pertenece a una cierta persona: tiene el carácter de validar la identidad y autenticar los datos de los titulares de certificados, como así también de los solicitantes de revocación de certificados.

- Quien controla y audita el sistema: en nuestro país, existe un órgano rector (ONTI) para generar un marco tecnológico, legal y procedimental adecuado, conforme la **IFDRA** con el fin de poder utilizar esta tecnología en forma segura.

A continuación, se muestra un esquema de parte del Organigrama del IUA que permite reflejar la estructura de la organización a la que pertenecen los actores participantes, haciendo énfasis en la Facultad de Ingeniería. El objetivo de mostrar el organigrama esta dado porque cualquier documento necesario, debe ser solicitado y firmado por su superior inmediato.

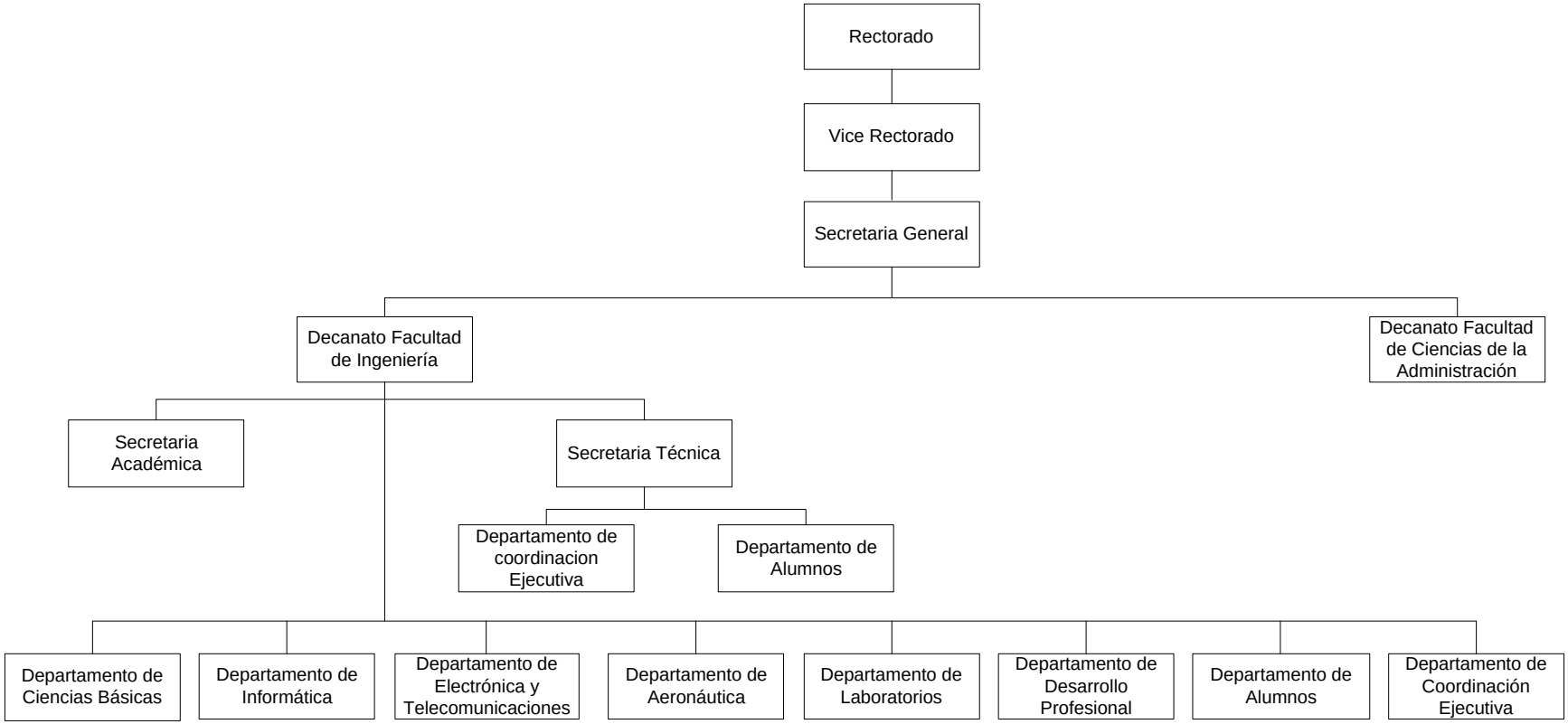


Figura 10: Organigrama.

4. Modelo Teórico

4.4 Análisis y Diseño

En esta etapa se realizará el análisis y el diseño de los diferentes pasos necesarios para llevar adelante la implementación de un proyecto de Firma Digital en el IUA.

En el siguiente diagrama se presentan a nivel general las etapas a considerar:

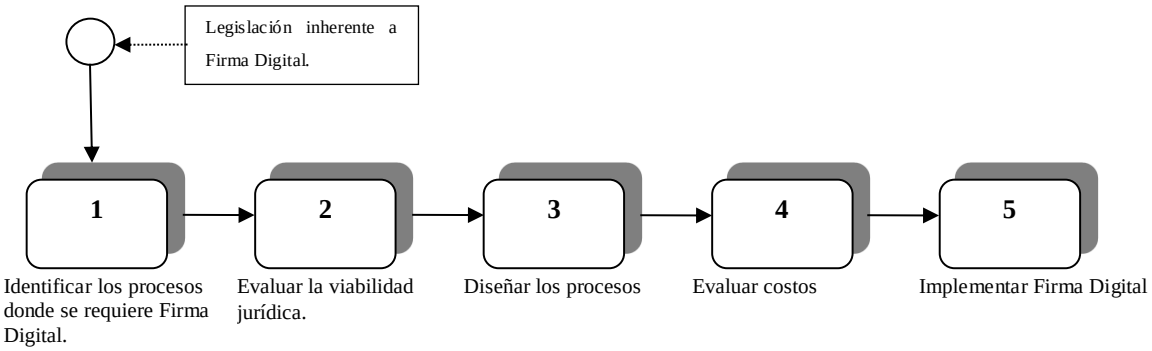


Figura 11: Etapas para la implementación de Firma Digital

Donde:

- Etapa 1: Hace referencia a la necesidad de identificar y relevar los procesos donde se quiere implementar la Firma Digital, evaluando su nivel de impacto dentro de la organización.
- Etapa 2: Se refiere a la elaboración de un diagnóstico acerca de la viabilidad jurídica que tiene el cambio de proceso de firma manuscrita en un documento.
- Etapa 3: En esta etapa se debe elaborar un diseño de los procesos que requieren implementar la Firma Digital.
- Etapa 4: Es necesario identificar, por medio de un diagnóstico de requerimientos, los principales costos asociados a la implementación de Firma Digital.
- Etapa 5: Hace referencia al proceso de desarrollo, puesta en marcha y operación de Firma Digital en la organización.

4.4.1. Identificación y Relevamiento de Procesos

La documentación que fue analizada para este proyecto corresponde a muchos de los documentos administrativos realizados por el Departamento de Alumnos de la Facultad de Ingeniería ya sea de forma independiente, en interacción con otras áreas de la Institución, o bien, en pudiendo intervenir también la AIT. Cabe aclarar, la Firma Digital podrá ser aplicada no solamente a los documentos aquí analizados sino también a cualquier Comunicación Escrita interna que fluya dentro de las áreas de la Institución.

Dichos documentos, comparten una estructura similar y pueden ser generados por ejemplo, a partir de algunos de los siguientes casos que se describen a continuación:

Certificado de Alumno Regular

Es un certificado que se extiende a pedido del interesado, donde consta que el alumno se encuentra matriculado en la carrera correspondiente y a la fecha de emisión mantiene su condición de alumno regular en el IUA.

Certificado Parcial de Estudios

Es un certificado de estudios cursados y aprobados, correspondientes a un nivel educativo incompleto, que se extiende a pedido del interesado, donde consta la totalidad de las materias rendidas por el alumno y sus correspondientes calificaciones. No se emite en un papel planilla otorgado por el Ministerio de Educación de la Nación.

Intervienen en su elaboración y validación el Departamento de Alumnos, el Decano y la Secretaría General.

Constancia de Título en Trámite

Se extiende a pedido del interesado, donde consta que el alumno ha finalizado sus estudios en la correspondiente carrera dictada en la Facultad y su título se encuentra en trámite.

Intervienen en su elaboración y validación el Departamento de Alumnos y la Secretaría General.

Programas de Estudio

Es un documento donde constan los programas de estudios correspondientes a los años de cursado y se extiende a pedido del alumno, generalmente cuando el mismo desea solicitar equivalencias, ya sea un alumnos del Instituto que desea cambiar de carrera, como así también un alumno que desea ingresar desde otra institución.

Intervienen en su elaboración y validación el Departamento de Alumnos, el Decano y la Secretaría General.

Pedido de Análisis de Excepción

Refiere a la solicitud de excepción que requiere el alumno, la cual puede darse por los siguientes motivos:

Art.5: se podrán cursar materias del año *i* si se tienen aprobadas todas las del año *i-2*.

Art.12: toda materia puede ser cursada hasta tres veces.

Art. 10 inciso a]: haber aprobado en el año académico, como mínimo dos asignaturas.

Art. 10 inciso b]: no tener más de diez (10) aplazos en exámenes finales de materias correspondientes a los tres primeros años de la carrera.

Art. 10 inciso c]: no tener más de seis (6) aplazos en el examen final de una misma materia.

Intervienen en su elaboración y validación el Departamento de Alumnos, el Decano y el Director de Carrera según correspondan.

Solicitud de Equivalencias

Este documento se elabora a pedido del alumno o interesado que desea solicitar equivalencias de materias dictadas en una determinada carrera dentro de la Facultad, ya sea porque es alumno de la misma y desea cambiarse de carrera o proviene de otra institución y desea ingresar.

Intervienen en su elaboración y validación el Departamento de Alumnos, el Decano y el Director de Carrera.

Transferencia de Legajos de Alumnos Egresados

Corresponde a la comunicación escrita interna, mediante la cual el Departamento de Alumnos eleva a la Secretaria General los legajos de los alumnos egresados de la Institución, que corresponden a la siguiente colación de Grado.

Libre deuda

Refiere al certificado que solicita el alumno donde consta la libre deuda tanto en Biblioteca como en AIT.

4.4.1.1 Problemas Identificados

A partir de la definición de los procesos a desarrollar, se identificaron los siguientes problemas:

- Todos los documentos son realizados en papel y firmados en forma manuscrita.
- Existe cierta burocracia y estructura para todos los documentos, lo cual genera ciertos cuellos de botella en los procesos administrativos.
- Existen ciertos documentos que están relacionados con otras organizaciones, instituciones, etc.

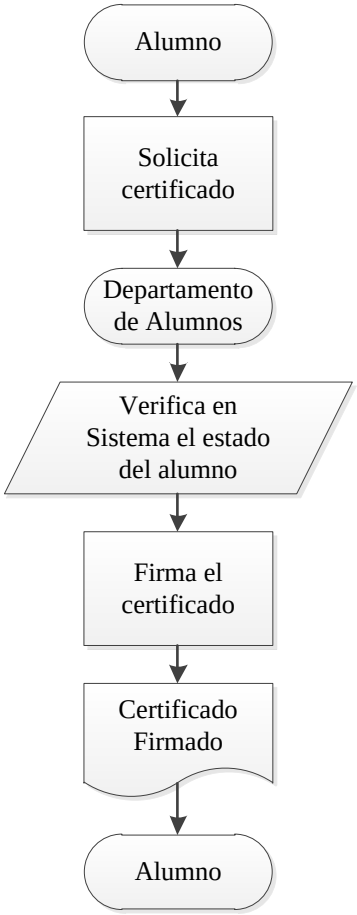
4.4.2 Evaluación de la viabilidad jurídica

El proyecto es viable jurídicamente en la medida en que el proceso de desarrollo de Firma Digital, los documentos firmados mediante esta metodología a implementar y los requisitos para cumplimentarla, se ajusten a las normativas de Firma Digital de la República Argentina de acuerdo con la Ley Nº 25.506.

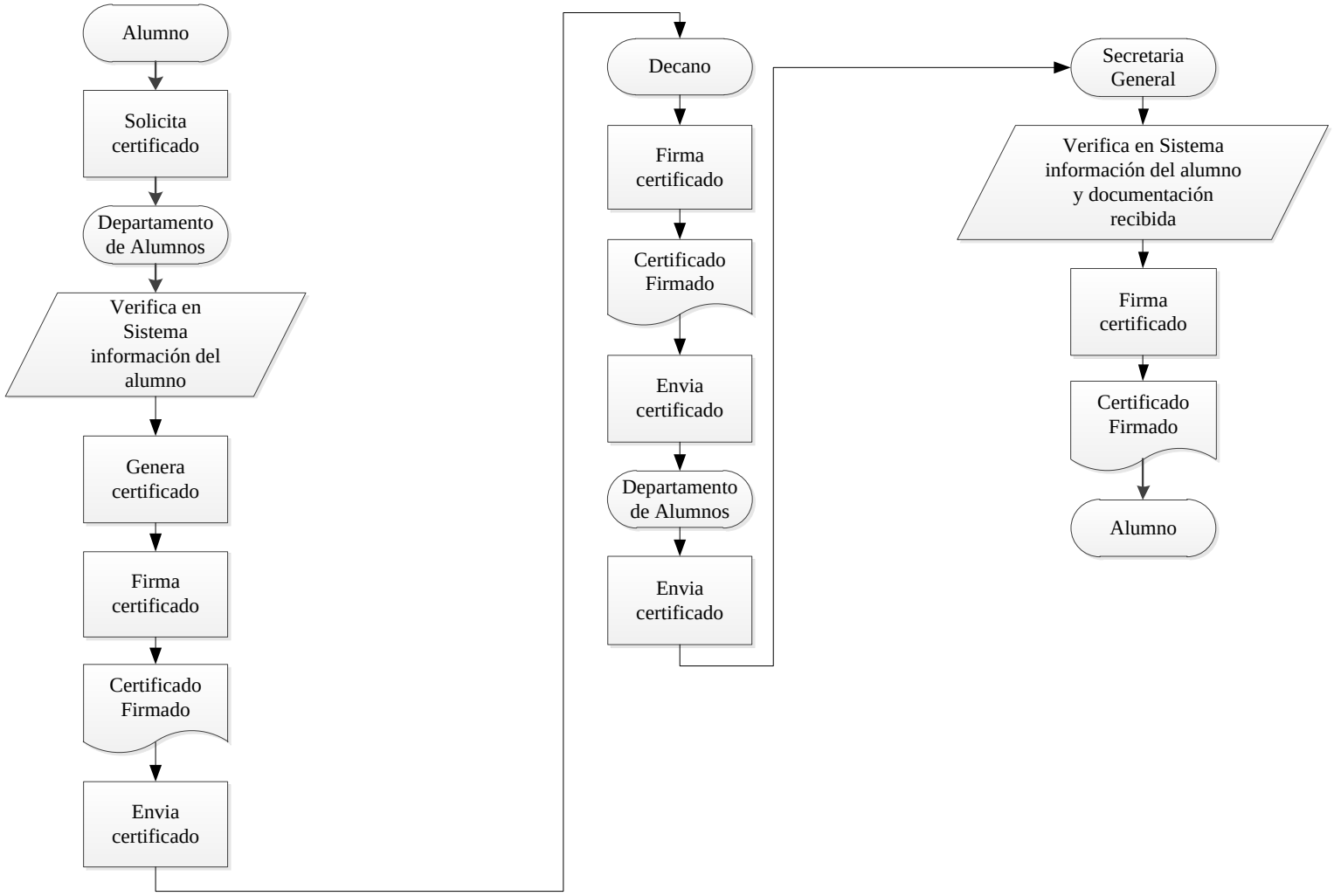
4.4.3 Diseño de Procesos

A partir de la identificación y el relevamiento de los procesos para los cuales se implementará la utilización de la Firma Digital, se expone a continuación el diseño de los mismos:

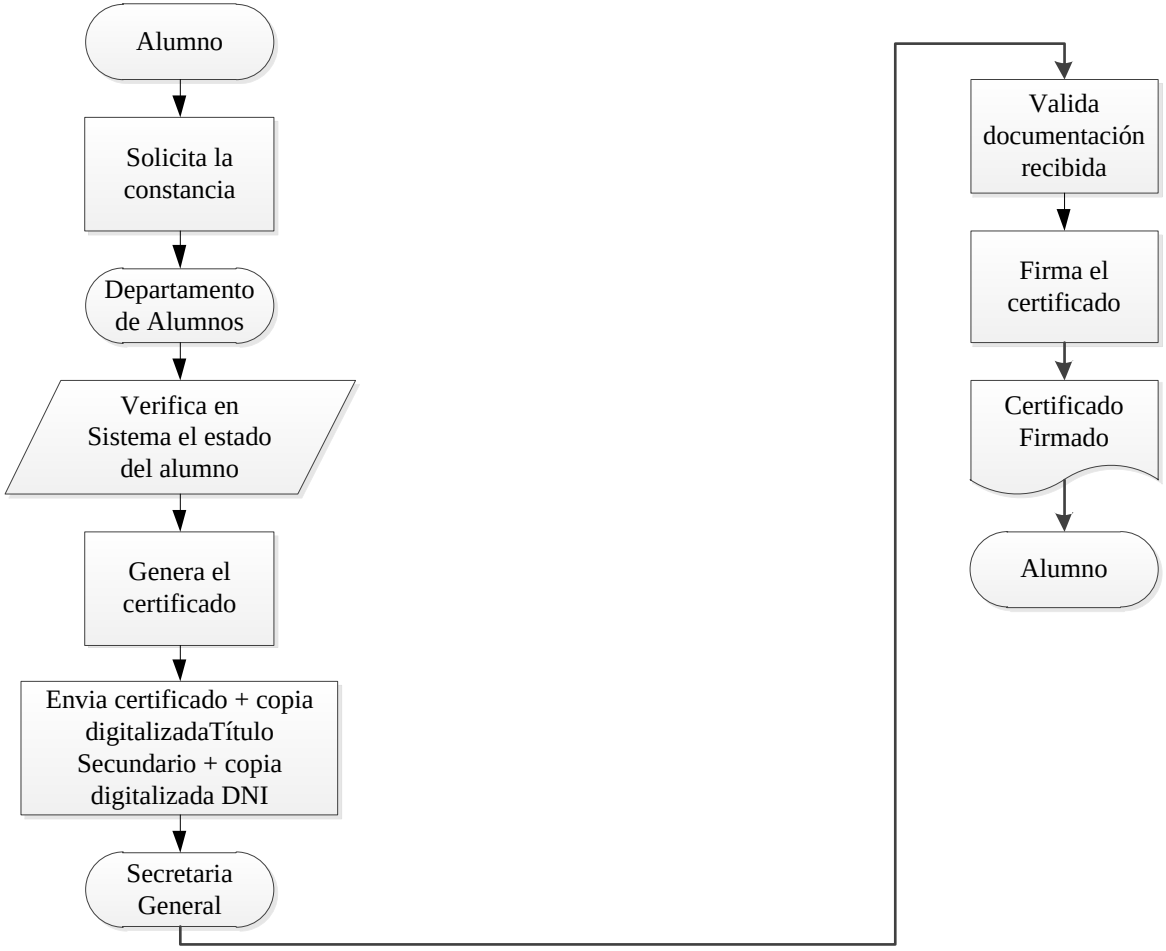
Certificado de Alumno Regular



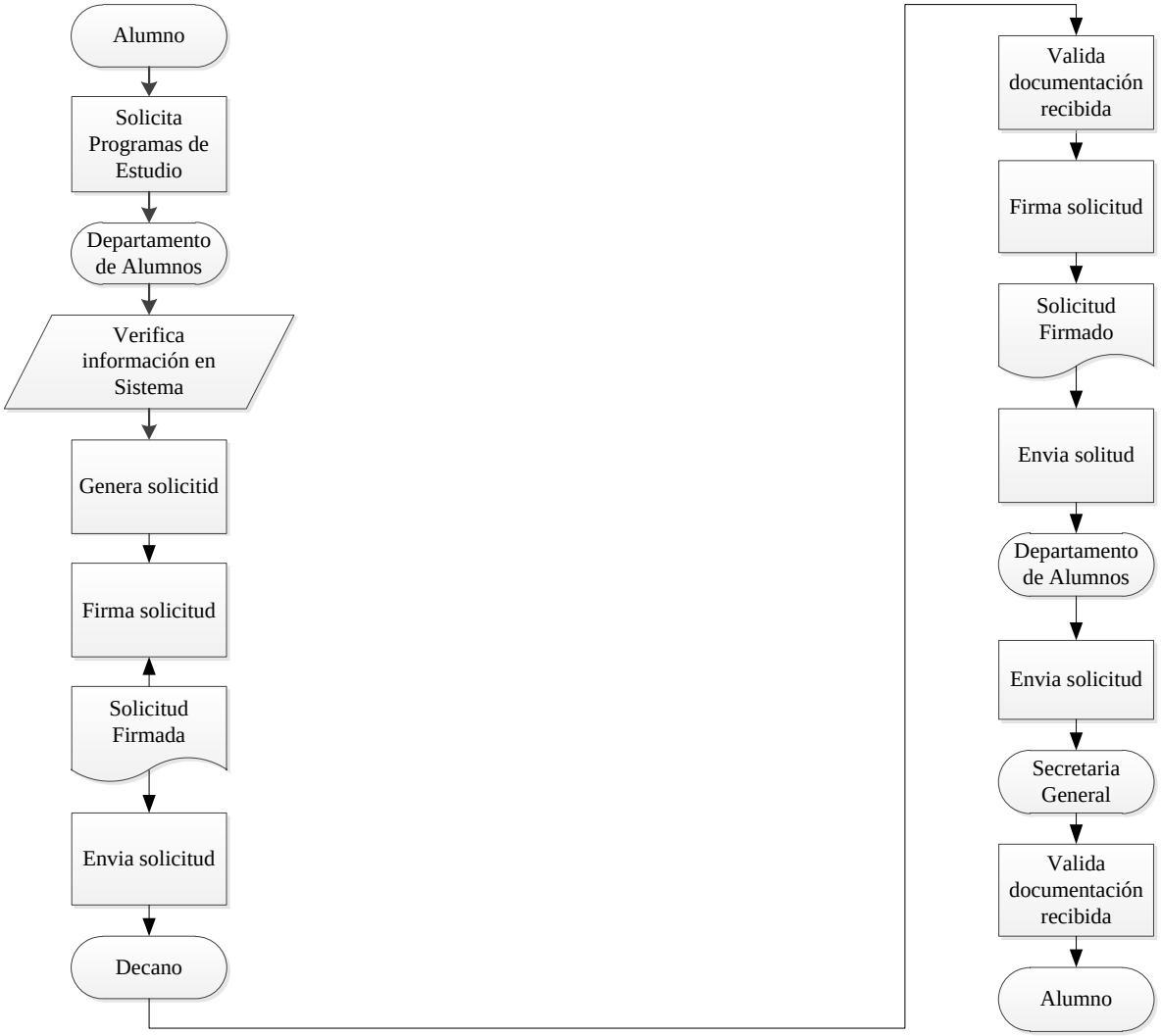
Certificado Parcial de Estudios



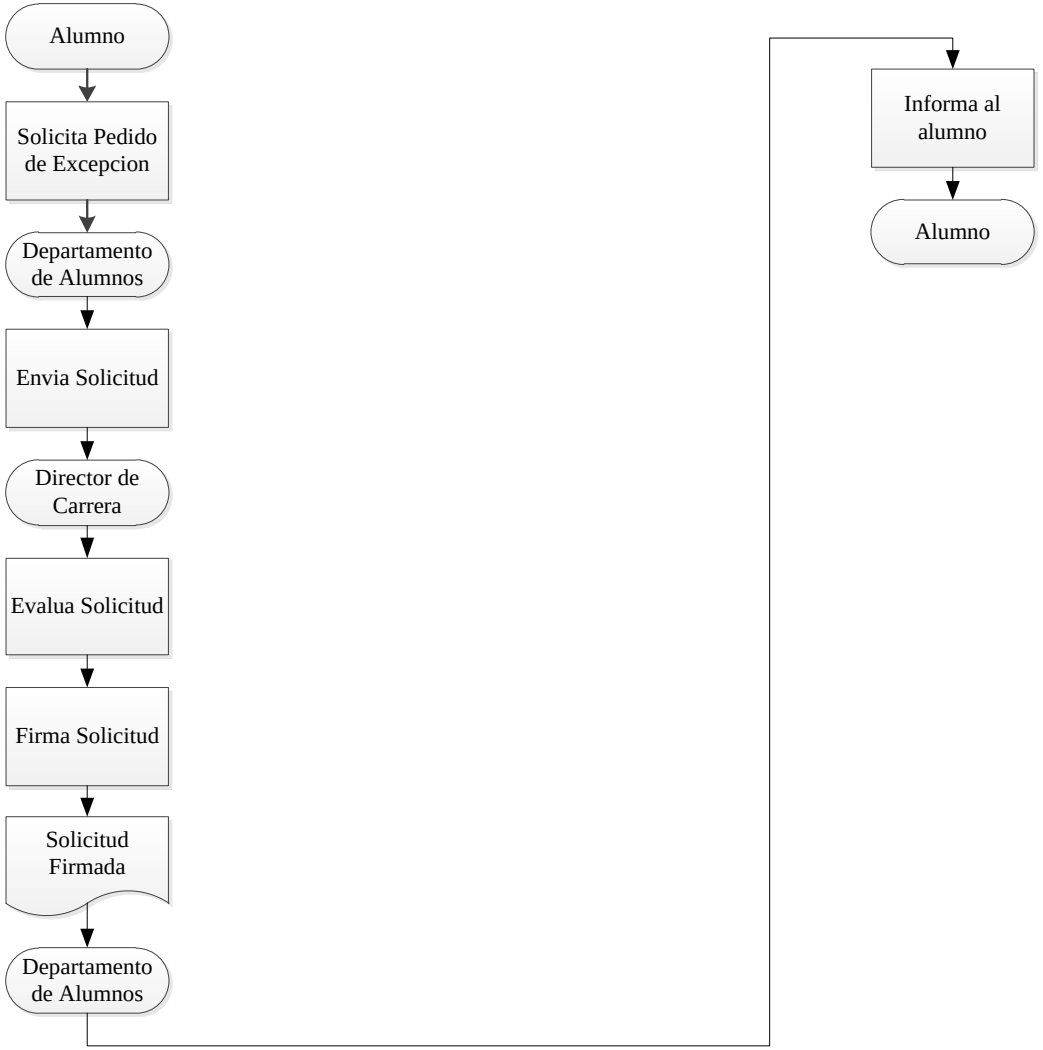
Constancia de Título en Trámite



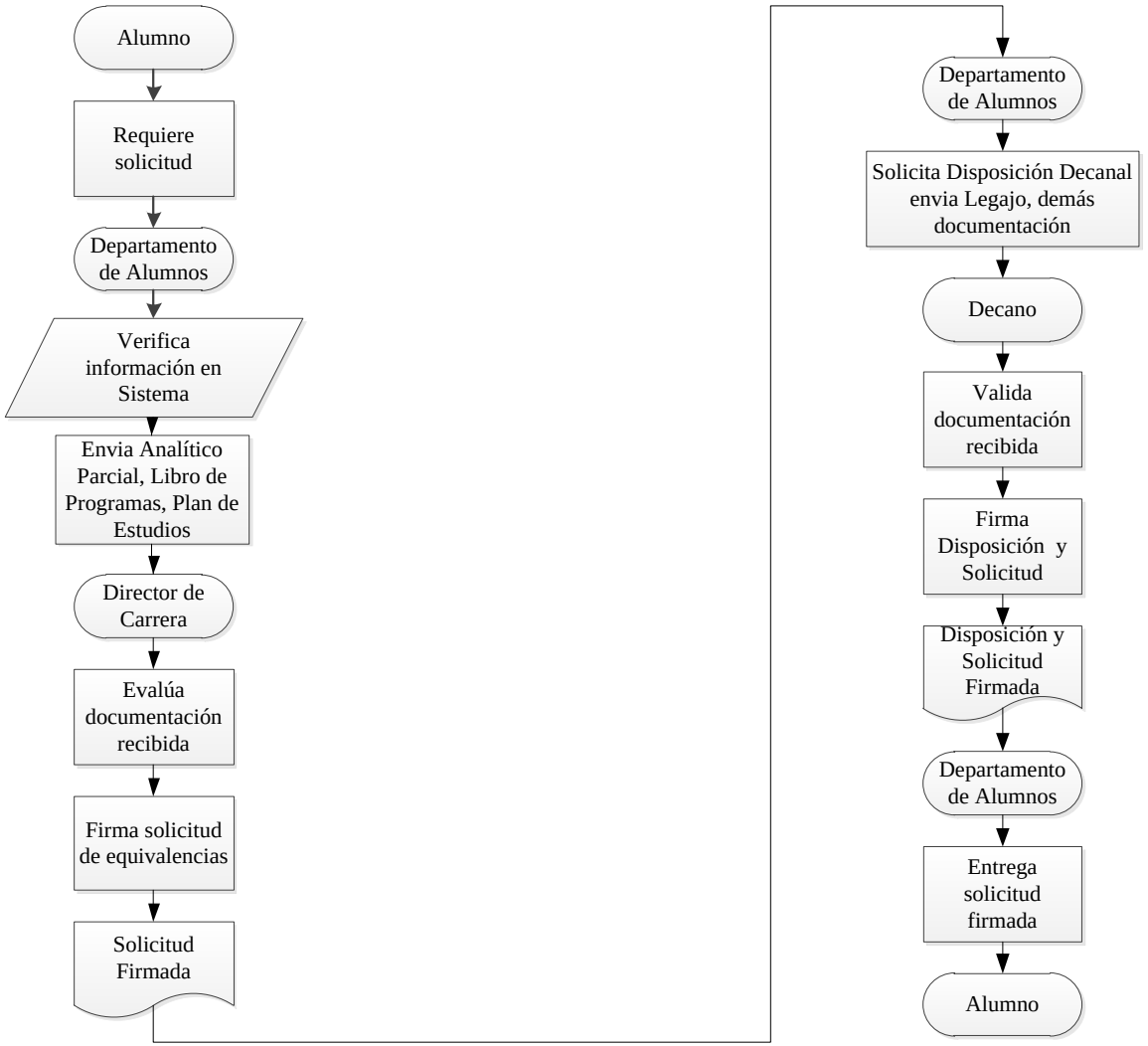
Programas de Estudio



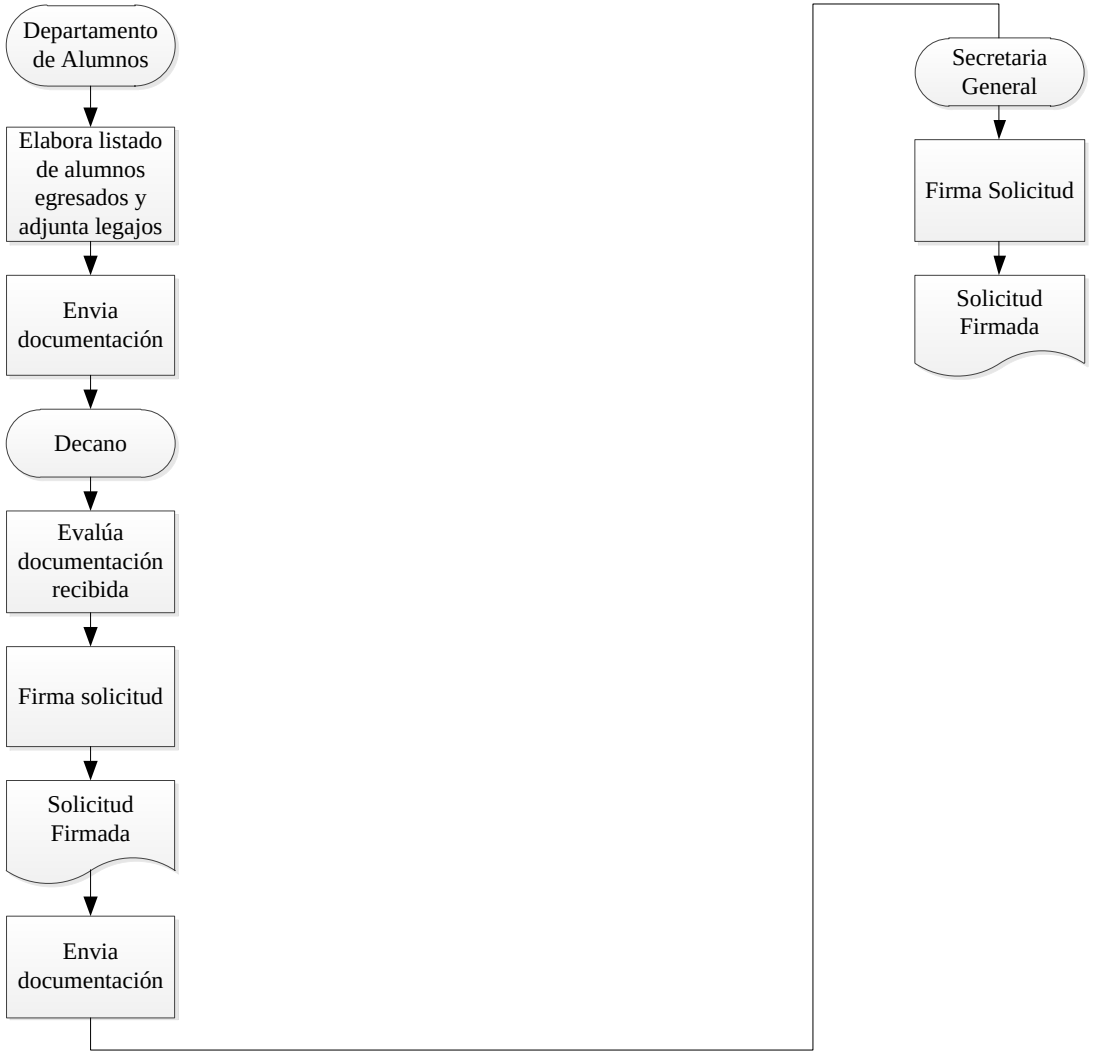
Pedido de Análisis de Excepción



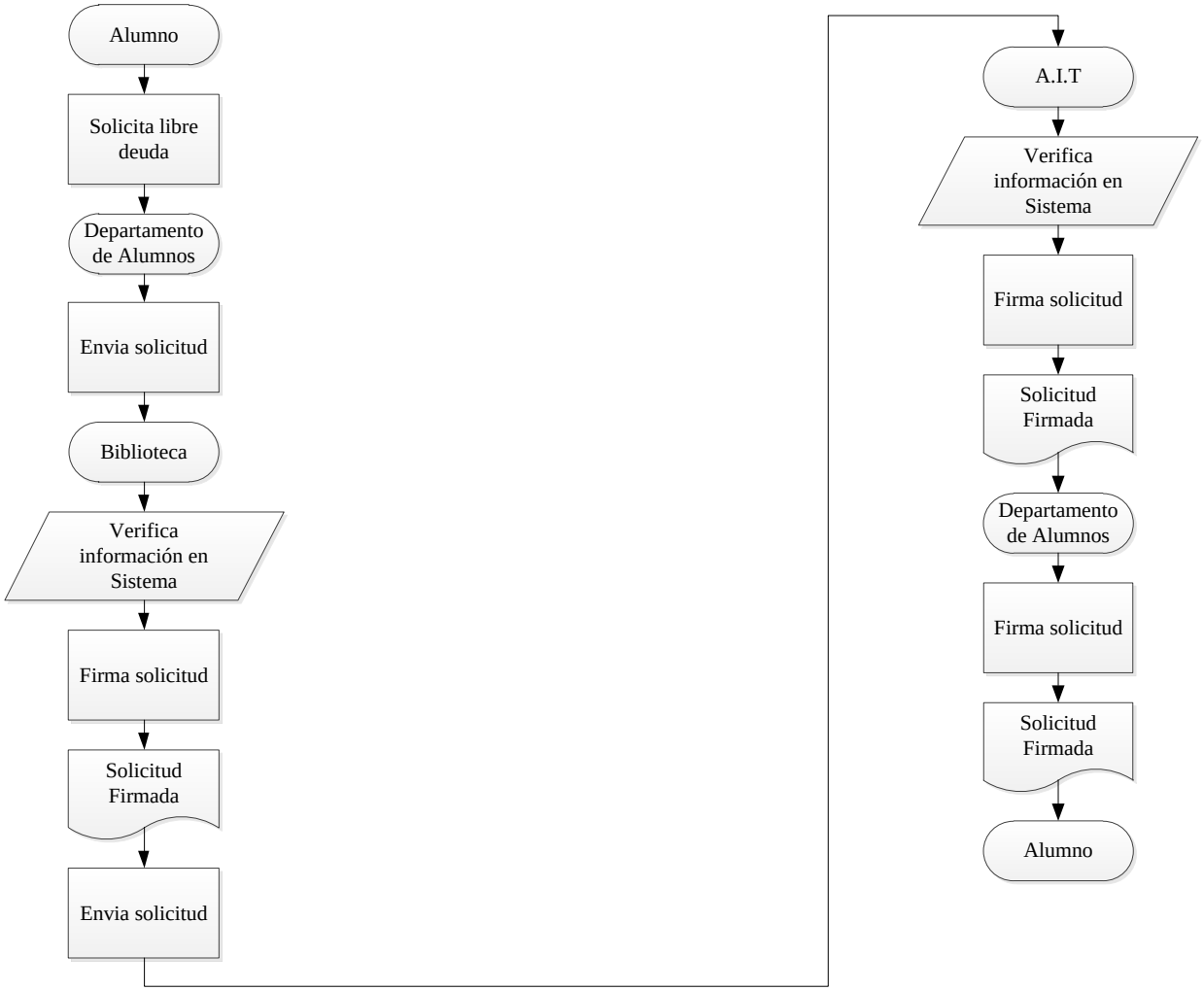
Solicitud de Equivalencias



Transferencia de Legajos Egresados



Libre deuda para solicitud de Baja



4.4.4 Evaluación de Costos

La evaluación de los costos asociados al proyecto se realizará de forma pertinente en la siguiente etapa. [18]

4.4.5 Implementación

El proceso de desarrollo, puesta en marcha y operación de Firma Digital en la organización se desarrollará en la siguiente etapa.[19]

4.4.6. Plataforma Tecnológica

4.4.6.1. Servidores

El modelo de HP Proliant DL580 G7, con grandes capacidades de desempeño y rendimiento, resulta conveniente para empresas y medianas corporaciones. Además, cuenta con hasta un 70% de ahorro energético respecto a otros modelos.

HP ProLiant DL580 G7 ofrece fiabilidad, capacidad de gestión y rendimiento, con la última tecnología de procesador Intel; y es la opción ideal para clientes que están preparados para desplegar grandes bases de datos que requieren procesamiento informático de escalabilidad vertical, gran memoria y aplicaciones de E/S intensivas.

Sus principales características son:

- ✓ Rendimiento y escalabilidad excepcionales

  - Las capacidades de expansión de E/S, los últimos procesadores Intel de 10 núcleos y la memoria DDR3 ampliable permiten ampliar la infraestructura de TI a medida que crece el negocio.
  - La arquitectura 4S de HP, nuevas memorias de 2 TB, 10 Gb NIC de ampliación opcional, hasta 11 ranuras de E/S y las soluciones de gestión líderes en la industria hacen que este sistema sea ideal para la virtualización.

[18] Ver 5.5.3 Prefactibilidad Económica.

[19] Ver 5. Concreción del Modelo.

- Procesador Intel® Xeon® de alto rendimiento E7-4800 y Serie 7500, acceso más rápido a memoria, anchos de banda de red y E/S más elevados que habilitan al DL580 G7 para aplicaciones y cargas de trabajo críticas.

✓ Fiabilidad y disponibilidad avanzadas

- Double Device Data Correction (Corrección de datos de dispositivo doble) - DDDC: esta función amplía la capacidad de resistencia ante fallos en dos dispositivos DRAM. DDDC puede corregir errores de memoria de dispositivo de DRAM, tanto individual como doble.
- Los ventiladores redundantes de conexión en caliente (3+1) estándar, más las fuentes de alimentación de ranura común añaden más disponibilidad al sistema.
- Lo último en tecnología de caché de escritura respaldada por flash, ofrece retención de datos de caché indefinidos, en comparación con la retención de dos días con el caché de escritura respaldada por batería de generaciones anteriores.

✓ Soluciones de gestión líder del sector

- Insight Control mide y limita el uso energético en servidores individuales o de grupo, con el fin de optimizar el consumo, lo que aporta grandes beneficios a la capacidad del centro de datos

  Insight control ofrece ahora la posibilidad de visualizar las secuencias de inicio y de error grabadas y encender y apagar el equipo de forma remota, permitiendo así que los clientes reduzcan de manera espectacular el tiempo y coste de la resolución de problemas, además de los gastos de desplazamiento.

Especificaciones Técnicas	
Procesador	Intel® Xeon® E7520 (4 núcleos, 1,86 GHz, 18 MB , 95 W)
Número de procesadores	2
Processor core available	4
Memoria de serie	16 GB
Ranuras de memoria	32 ranuras DIMM
Memoria	DDR3 PC3-10600E
Ranuras de expansión	11

Controlador de red	(1) 4 puertos 1GbE NC375i multifunción
Tipo de fuente de alimentación	(2) Fuente de alimentación redundante de 1200 W de conexión en caliente
Controlador de almacenamiento	(1) FBWC Smart Array P410i/512 MB
Internal mass storage	4 TB
Software de gestión	Software HP Insight Control (incluido)
Tipo de unidad óptica	SATA DVD ROM compacto
Software de gestión remota	Insight Control con iLO Advanced (iLO 3)

Tabla 3: Especificaciones técnicas - Servidor HP Proliant DL 580 G7

4.4.6.2. Almacenamiento, Respaldo y Recuperación

En un esquema de Firma Digital resulta de gran importancia mantener el control exclusivo sobre las claves criptográficas, durante su almacenamiento, y sobre sus copias de respaldo. Implementando, a su vez, procedimientos para realizar la recuperación de las claves a partir de copias de respaldo.

Para cumplir con los requisitos mencionados, se definirá el siguiente esquema de almacenamiento, que se aplicará a todos los documentos y datos en soporte magnético y/o digital de valor para el esquema Firma Digital:

- Almacenamiento Full + Diferencial: Un almacén de tipo full + diferencial inversa es similar al almacén completo-incremental. La diferencia está en que, en vez de hacer una copia full seguida de series incrementales, este modelo ofrece un full que refleja el estado del sistema a partir de la última copia y un historial de copias diferenciales. Una ventaja de este modelo es que solo requiere una copia de seguridad full inicial. Cada copia diferencial es inmediatamente añadida al full y los ficheros que son remplazados son movidos a una copia incremental inversa. Una copia diferencial puede sustituir a otra copia diferencial más antigua sobre la misma copia total.

- Almacenamiento full: Respaldo completo de los archivos sujetos a resguardo en frecuencias predefinidas.

- Almacenamiento Full + Incremental: Un almacén completo-incremental propone hacer más factible el almacenamiento de varias copias de la misma fuente de datos. En primer lugar se realiza la copia de seguridad full del sistema. Más tarde se realiza una copia de seguridad incremental, es decir, sólo con los ficheros que se hayan modificado desde la última copia de seguridad. Recuperar y restaurar un sistema completamente, a un cierto punto en el tiempo, requiere localizar una copia de seguridad full y todas las incrementales posteriores realizadas hasta el instante que se desea restaurar. Los inconvenientes son tener que tratar con grandes series de copias incrementales y contar con un gran espacio de almacenaje.

Cabe aclarar que los documentos y datos de valor, son todos aquellos cuya integridad y disponibilidad será necesario preservar por formar parte de los procesos que integran el esquema de Firma Digital.

Una solución óptima para el respaldo y recuperación de esta información es el producto de unidades de cintas (DLT) de la firma CPU Inc.

Adaptándose a las necesidades del proyecto se detalla el siguiente producto:

Con una cifra de 72 MB / s de velocidad de transferencia comprimida y un colosal de 600 GB de almacenamiento comprimido.

Velocidad de transferencia sostenida	
Original:	36 MB / segundo
Comprimida (2:1):	72 MB / segundo
Velocidad de transferencia	
Ultra 160:	160 MB / segundo (máximo)
Canal de Fibra:	200 MB / segundo (máximo)
Capacidad formateada	
Original:	300 GB
Comprimido:	600 GB

Tabla 4: Especificaciones técnicas - Unidades de cintas (DLT) - CPU Inc.

4.4.6.3. Suministro de Energía Ininterrumpible

Para garantizar el suministro de energía ininterrumpible, en aquellos equipos considerados de alta criticidad, como lo son los servidores de almacenamiento de claves criptográficas, es necesario implementar uno de los productos como los que ofrece APC de la Firma Schneider Electric.

La elección de esta marca responde a la garantía y soporte que brinda la firma y su reconocimiento mundial como una de las mejores soluciones para este tipo de necesidad.

El producto definido es APC Smart-UPS y sus características son las siguientes:

Disponibilidad

- Bypass interno automático
- Proporciona potencia de línea a las cargas conectadas en caso de que la unidad UPS sufra una sobrecarga o falla.
- Autonomía escalable
- Permite incrementar la autonomía rápidamente cuando se lo necesita.
- Manejo inteligente de la batería
- Maximiza el rendimiento, la vida útil y la confiabilidad de las baterías a través de la carga inteligente y de precisión.
- Baterías reemplazables en caliente
- Garantiza que llegue un suministro puro e ininterrumpido a los equipos protegidos durante el recambio de baterías.
- Restablecimiento automático de cargas tras el cierre del sistema UPS
- Pone en marcha automáticamente los equipos conectados cuando se reconecta la red.
- Carga de baterías con compensación de temperatura
- Prolonga la vida útil de las baterías al regular la tensión de carga según la temperatura real de las baterías.

Manejabilidad

- Administrable a través de una red
- Proporciona administración remota de las unidades UPS a través de la red.
- Permite la administración centralizada a través del InfraStruXure Manager de APC.
- Personalice las funcionalidades de la UPS mediante placas de gestión.
- Indicadores de estado LED
- Comprenda rápidamente el estado de la unidad y del suministro de energía con los indicadores visuales.
- Conectividad serial
  Proporciona administración de la unidad UPS por medio de un puerto serial.

Adaptabilidad

- Baterías externas "Plug-and-Play"
- Garantiza que llegue un suministro puro e ininterrumpido a las cargas cuando se agrega tiempo de autonomía a la UPS.
- Convertible para torre o rack
- Protege la inversión inicial en sistemas UPS cuando se migra de un entorno en torre a otro de montaje en rack.
- Firmware de actualización veloz
  Es posible instalar versiones de mantenimiento del firmware en forma remota mediante FTP.

Funcionabilidad

- Baterías que puede reemplazar el usuario
- Permite actualizar y reemplazar las baterías en forma sencilla.
- Autodiagnóstico automático
- Garantiza la detección anticipada de posibles problemas mediante la realización de diagnósticos periódicos de los componentes de las unidades UPS.
- Notificación predictiva de fallas

• Analiza el sistema a fin de advertir anticipadamente en caso de fallas posibles, lo que garantiza el reemplazo proactivo de componentes.
• Notificación de desconexión de baterías • Advierte cuando una batería no se encuentra disponible para ofrecer suministro de respaldo.
• Alarmas sonoras Ofrece notificaciones sobre cambios en las condiciones de las unidades UPS y de la compañía eléctrica.
Protección
• Regulación de tensión y frecuencia • Ofrece mayor disponibilidad para sus aplicaciones al corregir niveles de frecuencia y tensión inadecuados sin emplear las baterías.
• Acondicionamiento de energía • Protege la carga conectada contra sobretensiones breves o prolongadas, rayos y otras irregularidades energéticas.
• Corrección del factor de alimentación de entrada • Minimiza los costos de instalación al posibilitar el uso de sistemas de cableado y generadores más pequeños.
• Compatible con generador • Garantiza que llegue un suministro puro e ininterrumpido a los equipos protegidos cuando se recurre a la alimentación con generadores.
• Capacidad de arranque en frío • Proporciona alimentación temporaria a través de la batería cuando se interrumpe el suministro de la red.
• Interruptor de circuito reiniciable • Recuperación rápida luego de una sobrecarga, sin necesidad de reemplazar fusibles.

Tabla 5: Especificaciones técnicas - APC Smart-UPS

4.4.6.4. Dispositivos Criptográficos Token USB

Para el almacenamiento de las claves privadas de los usuarios, se utilizarán dispositivos Token USB, lo cuales se emplean para la autenticación de usuarios y portabilidad de certificados digitales. Son ligeros, portátiles y proveen la mejor seguridad al menor costo conectándose al puerto USB de cualquier PC.

Soportan el procedimiento de autenticación a través de dos factores: el dispositivo criptográfico, algo que el usuario tiene; y la password, algo que el usuario conoce y necesita para tener acceso a cualquier aplicación, certificado digital o sistema que este validando a través del dispositivo.

El dispositivo a utilizar es el Token USB MS-ID Protect, (la aplicación PKI on-card de Athena), el cual brinda una solución completa de autenticación multi-factor en la forma de un práctico dispositivo USB.

El token criptográfico USB de Macroseguridad IDProtect está basado en la tarjeta inteligente Java card IDProtect, diseñado de total conformidad con la arquitectura de Microsoft smartcard logon y con aplicaciones de terceras partes que soporten MiniDriver de Microsoft (smartbase csp), CAPI y/o PKCS#11.

El token USB MS-IDProtect soporta en su totalidad la solución para Windows Smartcard Logon y Terminal Server; y su arquitectura avanzada de alta seguridad, su sofisticado manejo de la memoria y algoritmos eficientes, son la gran fortaleza detrás de la alta performance que ofrece esta solución.

Una interfase USB 2.0 de alta velocidad, una arquitectura de chip único, certificaciones ISO IP58 / IP68 y de seguridad de la industria, como FIPS y Common Criteria, hacen de MSIDProtect Token USB la plataforma ideal para implementar una solución de seguridad digital realmente portátil.

Especificaciones Técnicas:

Interfaz	USB 2.0 tipo A - Plug and Play
Memoria para Certificados	72KB (EEPROM)
Plataformas soportadas	Java Card™ 2.2.2 GlobalPlatform™ 2.1.1
Transmisión de datos	ISO7816 - Protocolos T=1 y T=0
Seguridad Física	Tamper Evident
Algoritmos Criptográficos Soportados	RSA2048, RSA1024, RSA512, 3-DES, DES, AES128, AES192, AES256, GOST 28147-89, GOST 3411, Elliptic Curves (EC_FP, EC_F2M)
Algoritmos de Hashing	SHA-1 - SHA-256 - SHA-384 - SHA-512
Criptografía	Random Number Generator (RNG) Generación de algoritmos "On Board"
FIPS	FIPS 140-2 Level 3 (certificado)
Compatibilidad PKI	Microsoft Crypto API (CAPI) Microsoft Crypto API : Next Generation (CNG) PKCS#11 2.20 (2.01, 2.10 y 2.11) PKCS#1, PKCS#7, PKCS#10 PKCS#15 (opcional)
Soporte Resistencia al polvo y al agua	VPN y SSLVPN Certificación IP58 Certificación IP68

Tabla 6: Especificaciones técnicas - Token USB MS-ID Protect

Soporte para:

- Microsoft ILM/FIM.
- Windows Smartcard Logon.
- Terminal Server.
- Firma y encriptación de mails en Outlook, Outlook Express y Mozzilla Thunderbird.
- VPN Microsoft.
- SSLv3.
- Almacenamiento de certificados raíz de Microsoft CA.
- Adobe Acrobat.
- VPN CheckPoint.
- VPN Cisco.
- OpenVPN.
- Citrix.
- Lotus Notes.
- Novell.
- MAC OS.
- GNU/Linux.
- PGP.
- Netscape.
- SSH.
- Windows Live Mail.
- Mozilla Thunderbird.
- Mozilla Firefox

4.4.7. Software y Licencias

Como sistema operativo del Servidor se utilizará Linux, debido a que es un sistema libre, es decir, que no se necesitan adquirir licencias a un determinado costo para utilizarlo. Además, la mayoría del software para Linux es también gratuito.

Otras características que valen la pena destacar son las siguientes:

- Es seguro: Linux fue construido para ser un sistema multiusuario, por tanto existen ciertas restricciones con el fin de mantener seguro al sistema. Los usuarios no siempre ejecutan aplicaciones como administrador, por lo que las acciones que puedan afectar el sistema deben ser ejecutadas explícitamente. El software no puede ser instalado a menos que se posean privilegios de administrador, y se permita explícitamente hacer esto, así que los virus no pueden auto-instalarse.

- Es fácil: Esto es nuevo. Solía ser bastante difícil para un usuario nuevo probar Linux, sobre todo porque la instalación era difícil. Eso es parte del pasado, ahora instalar Linux es bastante fácil gracias a los asistentes de instalación. Una vez que el sistema esté configurado, sólo se detiene por algún fallo en el hardware

4.4.8. Algoritmo Criptográfico y Formato de los Certificados

Frente a cualquier transacción que involucre el uso de una Firma Digital o de un certificado digital, la adopción de estándares tecnológicos internacionalmente aceptados permite asegurar un proceso efectivo de verificación de dichas firmas, otorgando seguridad técnica y legal a las transacciones electrónicas.

En este marco, la IFDRA ha adoptado los siguientes estándares tecnológicos:

- Para el formato de los certificados y de las listas de certificados revocados: **ITU–T X509**.

- Para la generación de las claves: **RSA, DSA o ECDSA**.

- Para la protección de las claves privadas de certificadores y suscriptores: **FIPS 140**.

- Para las políticas de certificación: **RFC 5280 y 3739**.

A los fines del presente proyecto, para el caso de la generación de claves se utilizará el algoritmo criptográfico asimétrico RSA, debido a las siguientes ventajas que brinda el mismo:

- No requiere claves secretas.

- Permite Encriptar y Firmar digitalmente.

- Utilizado conjuntamente con AES otorga una mayor velocidad de operación.
- Permite además la detección de:
    - Alteraciones en los documentos.
    - Errores en la transmisión de documentos.
- Es un estándar internacional.

Para el caso de del formato de los certificados, se utilizará OpenPGP, el cual trabaja con una estructura que se denomina anillo de confianza. El mismo consiste en tener claves de gente firmada por otra gente, que la han firmado y que, con su firma, aseguran que esa clave es realmente de quien dice ser y no ha sido alterada. Si por ejemplo se tiene dos personas: A y B. Las personas A y B son amigas y se intercambian entre ellas las claves públicas, verifican sus huellas digitales para ver que las claves son las correctas y quedan para ver las claves que se han pasado son correctas. Entonces, una vez verificado que todo es correcto, cada uno firma la clave de su amigo. Ahora, si por ejemplo un usuario C obtiene la clave de B y está firmada por A (que es una persona que C conoce y en la que confía) entonces, C confía de que esa clave es la clave correcta de B y es posible usar. Ahora, solo le queda a C ponerse en contacto con B para verificar las claves a fin de firmarlas y establecer la confianza.

Por lo tanto, OpenPGP ofrece la posibilidad de intercambiar datos cifrados y correos electrónicos sin necesidad de autenticación por un organismo de rango superior. Es suficiente, si confía en la dirección de correo electrónico y en el certificado correspondiente de la persona que se está comunicando. Por tal motivo, y dado que aún no se encuentra implementada en el IUA una autoridad certificante, que funcione como tercera parte de confianza y que permita brindar un esquema de confianza jerárquico, se ha decidido utilizar OpenPGP para diseñar e implementar un esquema de Firma Digital en la Institución.

4.4.9. Uso y Conservación de la clave privada

La clave privada podrá ser utilizada por autoridades competentes de la Institución IUA para firmar digitalmente los siguientes documentos:

- Certificado de Alumno Regular.
- Certificado Parcial de Estudios.
- Constancia de Titulo en Trámite.
- Programas de Estudio.
- Pedido de Análisis de Excepción.
- Solicitud de Equivalencias.
- Transferencia de Legajos de Alumnos Egresados.
- Libre deuda.

En cuanto a la conservación y protección de la clave privada, existen varias categorías de tipos de seguridad. En la Institución se adoptará la categoría "Seguridad Alta", que se basa en algo que el usuario tiene y en algo que el usuario sabe o conoce; para ello se utilizarán dispositivos Token USB para su almacenamiento, los cuales cumplen con estos requisitos de seguridad.

Para poder llevar a cabo esta implementación se establecerán una serie de requisitos a cumplimentar por parte de las distintas personas involucradas en el proceso de Firma Digital:

- Sólo se concederá la utilización de Firma Digital a las autoridades responsables de cada área de la Institución.
- Dichas autoridades serán las únicas personas autorizadas a la tenencia de su clave privada correspondiente, no siendo posible la delegación de esta responsabilidad a terceros.
- Los mecanismos de conservación y guarda adoptados, deberán estar basados en algo que sólo el usuario sepa. La clave privada deberá encontrarse cifrada y para poder tener acceso a ella, previamente, se la deberá descifrar mediante una contraseña que sólo conocerá el usuario.
- Los mecanismos de conservación y guarda adoptados deberán estar basados en algo que sólo el usuario posea. La clave privada deberá encontrarse en un dispositivo físico al que sólo tendrá acceso el usuario.
- Ante cualquier anormalidad ocurrida sobre la seguridad de la clave privada, se deberá solicitar inmediatamente la revocación del certificado.

5. Concreción del Modelo

5.1. Introducción

Esta etapa corresponde a la parte final del presente proyecto, cuyo objetivo general es cumplimentar la implementación de Firma Digital en el IUA, en base a lo expuesto en el Modelo Teórico y el Marco Teórico. En tal sentido, se procederá a realizar una simulación de los procesos a los cuales se les aplicará Firma Digital; analizando la puesta en marcha y considerando las necesidades técnicas que presenta el modelo elegido, como así también la capacitación de los usuarios y la prefactibilidad del proyecto.

5.2. Implementación

5.2.1. OpenSSL

OpenSSL es un proyecto de software desarrollado por los miembros de la comunidad Open Source para libre descarga.

Consiste en un robusto paquete de herramientas de administración y librerías relacionadas con la criptografía, que suministran funciones criptográficas a otros paquetes como OpenSSH y navegadores web (para acceso seguro a sitios HTTPS).

Estas herramientas ayudan al sistema a implementar el Secure Sockets Layer (SSL), así como otros protocolos relacionados con la seguridad, como el Transport Layer Security (TLS). Este paquete de software es importante para cualquiera que esté planeando usar cierto nivel de seguridad en su máquina, con un sistema operativo libre basado en GNU/Linux. OpenSSL también permite crear certificados digitales que pueden aplicarse a un servidor.

5.2.2. Public Key Server

Un servidor de claves es un servidor en el que se almacenan claves públicas. Es posible buscar la clave pública de una persona en el servidor a través del nombre o bien exportar claves para almacenarlas allí. Una vez obtenida la clave, se puede utilizar para enviar

mensajes cifrados al dueño de la clave pública o bien para comprobar la Firma Digital de un mensaje enviado por el dueño de la clave pública.

Para configurar el servidor se trabajará sobre un sistema operativo Linux distribución Ubuntu Server 12.04.3. A su vez, el servidor Ubuntu está montado sobre una máquina virtual Virtual Box 4.2.18 a través de técnicas de virtualización.

La virtualización es el proceso mediante el cual se comparten recursos de hardware y software de un ordenador, mediante un software en un sistema operativo que se encuentra ya instalado en dicho ordenador (conocida como máquina host); a fin de emular o imitar el comportamiento de algún sistema o de una misma pc, esto se lleva a cabo mediante una máquina virtual.

El concepto de máquina virtual puede ser un poco amplio, pero se define en este caso como un software que crea prácticamente una PC con los recursos de software y hardware de nuestra PC; en resumen: como una PC nueva con otro sistema operativo, disco duro, memoria y procesador (todo virtual) dentro de una PC física.

Por otra parte, del lado del cliente se utilizará PuTTY release 0.61, la cual es una aplicación que permite realizar conexiones con servidores remotos por línea de comandos. Es un programa sencillo, pero potente y posiblemente la opción más recomendable para conectarse por SSH a otros ordenadores en red.

SSH es un protocolo de red muy similar a Telnet, que posibilita la interacción con otra máquina a través de la red, pero mediante una conexión que se encuentra cifrada; lo que aumenta la seguridad, pues evita que otras personas puedan ver las comunicaciones entre el ordenador origen y destino.

5.2.3. Gpg4win

Es un proyecto Open Source que permite a los usuarios enviar con seguridad correos electrónicos y archivos con la ayuda de cifrado y firmas digitales. Es la distribución oficial de GNU Privacy Guard para Windows. Gpg4win, es apoyado por la Oficina Federal Alemana para seguridad de la información (BSI). Su objetivo es proporcionar a un instalador de Windows con un número de aplicaciones gratuitas para ayudar a los usuarios a mantener sus datos seguros.

El instalador incluye los siguientes componentes:

- GnuPG, la herramienta de cifrado de núcleo compatible con OpenPGP y S/MIME (x.509) estándares de criptografía.
- Administrador de certificados de Kleopatra.
- GNU Privacy Assistant (GPA), también un administrador de certificados.
- GpgOL, un plug-in para Microsoft Outlook para cifrar mensajes de correo electrónico.
- GpxEX, un complemento para el explorador de Windows para el cifrado de archivo rápido.
- Claws Mail, un cliente de correo electrónico con soporte de cifrado.
- Gpg4win compendio, documentación exhaustiva de las herramientas.

GnuPG es el motor detrás del paquete Gpg4win, este crea y administra certificados OpenPGP y X.509 con una longitud de clave predeterminada de 2048 bits. Utiliza RSA para firmar y cifrar de forma predeterminada, (se pueden configurar tanto estos factores). El motor también tiene compatibilidad integrada para tarjetas inteligentes para OpenPGP y S/MIME. Kleopatra y el GPA ofrecen características similares para gestión de certificados basada en GUI.

Es posible utilizar estas herramientas para crear, editar, firmar, certificar, eliminar, importar y exportar las claves almacenadas y certificados de búsqueda desde un servidor de certificados. La interfaz muestra detalles acerca de cada uno de los certificados locales, así como los certificados de confianza, incluyendo el nombre, dirección de correo electrónico asociada, validez tipo y id de clave de cada uno. Kleopatra y el GPA también proporcionan funciones de cifrado, descifrado, firma y verificación de archivos.

5.2.4. Mozzilla Thunderbird

Es un cliente de correo electrónico y lector de noticias gratuito, de código abierto y multiplataforma para la mayoría de sistemas operativos modernos, incluyendo -pero no limitado- a Windows, GNU/Linux y Macintosh. Está basado en la base de código Mozilla. Es un cliente robusto y fácil de usar.

Algunas de sus características principales son:

- Gestiona múltiples cuentas POP, IMAP, SMTP, NNTP y canales web desde una sola interfaz, mejorada con las carpetas inteligentes y el uso de pestañas.

- Potentes filtros de detección de correo basura y correo fraudulento (*phishing*).
- Un sistema de búsquedas basado en base de datos que localiza en segundos todos los resultados relevantes entre decenas de miles de mensajes, con avanzadas herramientas de análisis.
- Filtros de mensajes para organizar el correo fácilmente.
- Capacidad de redactar y visualizar mensajes HTML.
- Libreta de direcciones con posibilidad de varias libretas separadas y conexión LDAP.
- Etiquetas y vistas de correo personalizables.
- Potente sistema de extensiones, permite añadir características adicionales a medida de las necesidades del usuario; donde Thunderbird no llegue quizá lo haga una extensión.
- Proporciona características de seguridad necesarias en gobiernos y empresas como S/MIME, Firma Digital, cifrado de mensajes, soporte de certificados y dispositivos de seguridad.

Además, se utilizará Enigmail, el cual es un complemento o extensión de Mozilla Thunderbird, que permite proteger la privacidad de las comunicaciones por correo electrónico. La interfaz Engimail está representada como una *OpenPGP*, en la barra de herramientas del panel de control de Thunderbird, y permite utilizar las opciones de cifrado que brinda GnuPG.

Engimail está basado en criptografía de clave pública o criptografía asimétrica donde, como ya ha sido mencionado, cada usuario dispone de su propio par de claves, una clave pública y una privada.

La clave pública, entonces, será conocida y podrá ser compartida con sus contactos. Además, una vez que el usuario disponga de la clave pública de los demás, podrá empezar a enviar correos electrónicos cifrados a dichas personas. Así, sólo el destinatario será capaz de descifrar y leer los correos electrónicos, debido a que es la única persona que tiene acceso a la clave privada que se empareja con la pública.

Finalmente, el Enigmail también permite adjuntar firmas digitales a los mensajes. Así, el destinatario del mensaje que cuenta con copia de la clave pública del emisor, será capaz de

verificar que el correo electrónico proviene del mismo y que su contenido no fue manipulado en el camino.

5.3. Pruebas

Para reflejar los temas analizados y desarrollados en el presente proyecto, se procede a realizar una serie de pruebas que permiten representar de forma más apropiada cómo se realizará la implementación y puesta en marcha del mismo.

5.3.1. Configuración del Servidor de Claves

Para comenzar a trabajar, es necesario realizar la configuración del servidor de claves.

1. Lo primero que se debe realizar es bajar el paquete pks-0.9.6.tar.gz para ejecutar la instalación del servidor.
2. Se debe crear un directorio dentro de /etc para trabajar con todo lo relacionado con el servidor:

   ```
   #mkdir pks
   ```
3. Se debe posicionar en el directorio que se acaba de crear y copiar el paquete que se descargó en el primer paso:

   ```
   #cd pks
   #cp /media/datos/PKS/pks-0.9.6.tar.gz /etc/pks
   ```
4. Se debe descomprimir el paquete en el directorio:

   ```
   #tar -zxf nano.tar.gz
   ```
5. Se/ comienza con la instalación:

   ```
   # apt-get install build-essential
   ```

   ```
   # apt-get install gcc-4.6-base cpp-4.6 libgomp1 libquadmath0 libc6-dev
   ```

   Ejecutar el comando ./configure y se comenzará a configurar el paquete:

   ```
   #./configure
   ```
6. Se instala el paquete make para terminar la instalación:

   ```
   #apt-get install make
   ```

   Ejecutar el comando make install para que el sistema reconozca los comandos y demás características del servidor:

   ```
   #make install
   ```
7. El servidor necesita una base de datos donde almacenará las claves públicas de los usuarios, la cual se crea con el siguiente comando:

```
#/usr/local/bin/pksclient /usr/local/var/db créate
```

8. Se debe copiar el archivo de configuración del servidor a /etc/pks. A continuación, se ingresa al directorio:

```
#cp pksd.conf /etc/pks/
#cd..
```

9. Se debe editar el archivo de configuración para que el servidor pueda funcionar correctamente:

```
#nano pksd.conf
```

Dejándolo de la siguiente forma:

```
pks_bin_dir /usr/local/bin
db_dir /usr/local/var/db
www_dir /usr/local/var
### Set www_port to the port on which HTTP requests should be
accepted.
### If you do not want to process HTTP requests, set this to 0.
www_port 82
### Set www_readonly to 0 if you want to allow ADD requests over HTTP
www_readonly 0
socket_name /usr/local/var/pksd_socket
### Specify the envelope sender address as the -f argument to
### sendmail. This is the address which will receive any bounces.
### If you don't use sendmail, then change this to an equivalent
command.
### If you do not want to process mail requests, leave this unset.
mail_delivery_client /usr/sbin/sendmail -t -oi -fmailer-daemon
### Set this to the address which should be displayed as the From:
### address in all outgoing email, and as the maintainer in the body
### of each message.
maintainer_email PGP Key Server Administrator <nobody>
mail_intro_file /usr/local/share/mail_intro
help_dir /usr/local/share
mail_dir /usr/local/var/incoming
### If you change this, make sure to put a corresponding help file in
### the help_dir named above
default_language EN
### This is the email address of this site. It will be inserted in all
### outgoing incremental messages, so it should match whatever the
### downstream sites use as syncsite in their pksd.conf files.
# this_site pgp-public-keys@your-site
```

5. Concreción del Modelo

```
### Include a syncsite line for each site with which you are exchanging
### incremental requests.
# syncsite pgp-public-keys@pgp-server-1
# syncsite pgp-public-keys@pgp-server-2
### Set this to 0 to disable mailserver LAST requests completely, to a
### positive integer to limit LAST requests to that many days, or -1
### to allow any argument to LAST.
max_last -1
### Set this to the maximum number of keys to return in the reply to
### a last query. Setting it to -1 will allow any size reply.
max_last_reply_keys -1
### Set this to the maximum number of keys to return in the reply to
### an index, verbose index, or get query. Setting it to -1
### will allow any size reply.
max_reply_keys -1
```

10. Se iniciará el servidor de claves públicas con el siguiente comando y luego se trabajará desde otra terminal:

```
# pksd /etc/pks/pksd.conf
```

11. Una vez iniciado el servidor se ingresa al navegador web para ingresar a su interfaz web: http://ubuntuserver:11371/

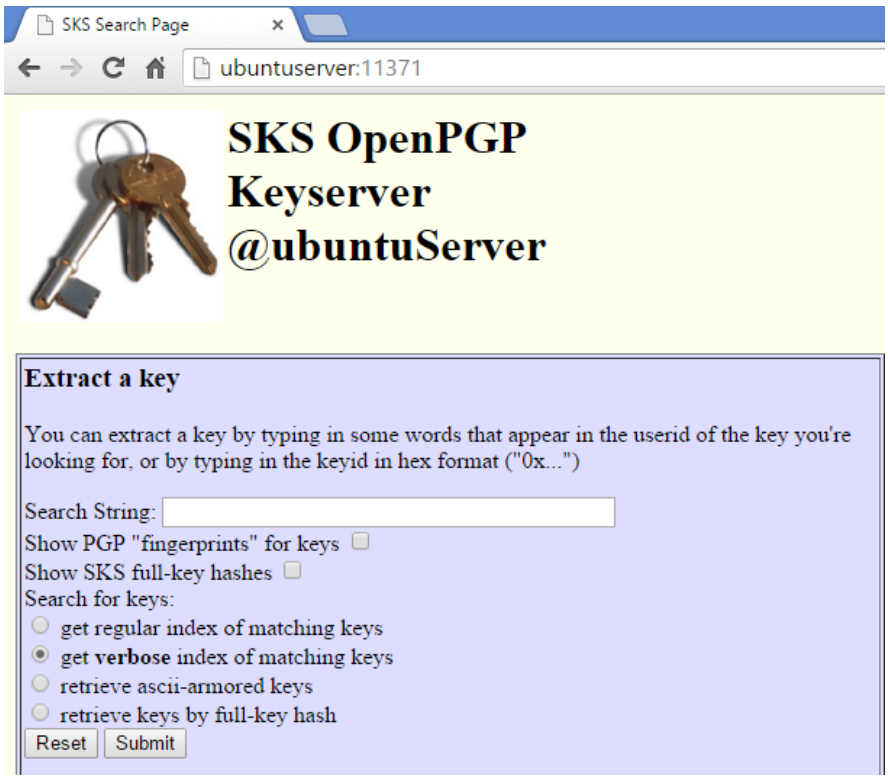


Figura 12: Key Server

5. Concreción del Modelo

5.3.2. Creación de Certificados

Una vez configurado e iniciado el servidor, se procede a la creación de certificados, lo cual permite determinar si el servidor recibe las claves públicas de los usuarios y los certificados de revocación de claves correctamente.

Para ello, es necesario implementar pgp:

```
# apt-get install pgp
```

1. Para generar una clave se debe ejecutar el siguiente comando:

```
#gpg --gen-key
```

```
root@(none):/home/laura# gpg --gen-key
gpg (GnuPG) 1.4.11; Copyright (C) 2010 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 2048
Requested keysize is 2048 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 12m
Key expires at miÃ© 08 oct 2014 16:32:01 ART
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: AIT
Name must be at least 5 characters long
Real name: AITIUA
Email address: iua.ait@gmail.com
Comment: AITIUA
You selected this USER-ID:
    "AITIUA (AITIUA) <iua.ait@gmail.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
```

Figura 13: Generación de claves.

A continuación, se solicita ingresar la contraseña para comenzar la generación de las claves, lo cual puede demorar varios minutos.

Finalmente, una vez generada las claves, se muestra lo siguiente:

```
gpg: key 2313F46F marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   4  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 4u
gpg: next trustdb check due at 2014-10-08
pub   2048R/2313F46F 2013-10-13 [expires: 2014-10-08]
      Key fingerprint = 7F72 2FAF 4373 BA29 1738  CB73 F932 2D78 2313 F46F
uid                  AITIUA (AITIUA) <iua.ait@gmail.com>
sub   2048R/BB074840 2013-10-13 [expires: 2014-10-08]
```

Figura 14: Claves generadas.

2. Terminado el proceso de generación de claves, se verifica que se hayan creado correctamente:

```
#gpg --list-keys
```

```
pub   2048R/2313F46F 2013-10-13 [expires: 2014-10-08]
uid                  AITIUA (AITIUA) <iua.ait@gmail.com>
sub   2048R/BB074840 2013-10-13 [expires: 2014-10-08]
```

Figura 15: Lista de claves.

3. Ahora, se exporta la clave para poder subirla al servidor:

```
#gpg -a -o /home/laura/clave-AITIUA --export
```

4. Se visualiza la clave para luego copiarla e ingresarla en la interfaz del servidor en el navegador web:

```
# more /home/laura/ clave-AITIUA --export
```

Figura 16: Exportar clave.

5. Después de copiar la clave, es necesario dirigirse al navegador donde se encuentra el servidor de llaves y se ingresa en el campo *Enter ASCII-armored PGP key here*:

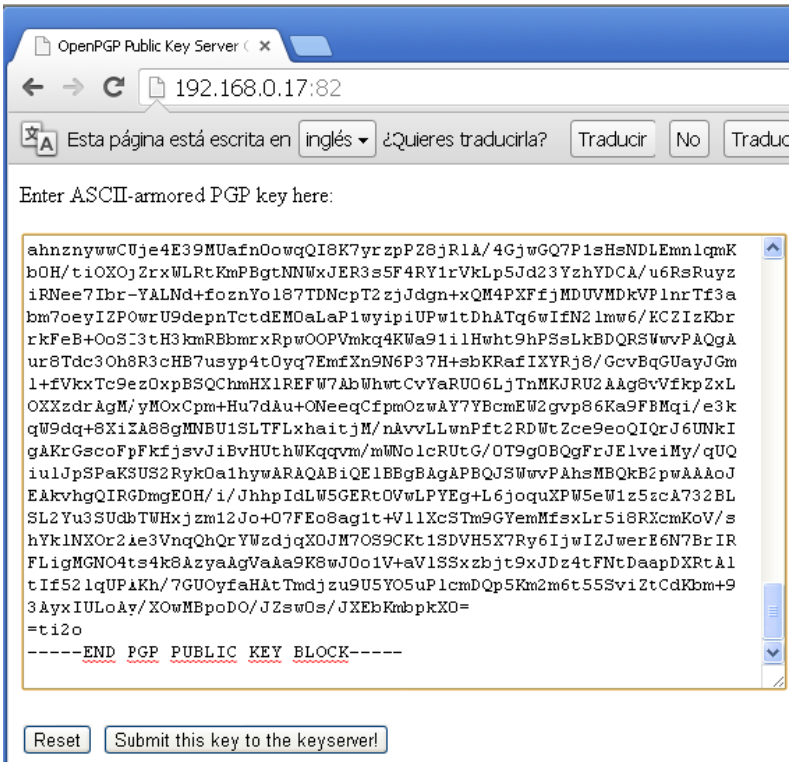


Figura 17: Exportar clave al servidor.

6. Se visualiza en el servidor que se agregó la clave:

Figura 18: Clave exportada al servidor.

7. Se buscara en el servidor la clave que se acaba de subir en la opción *Search String*:

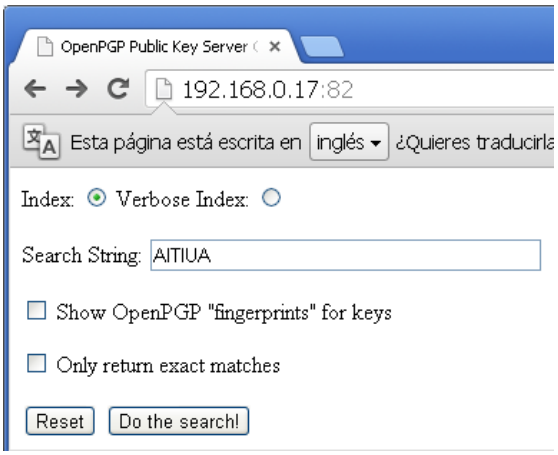


Figura 19: Búsqueda de clave en el servidor.

8. Se visualiza la clave encontrada:

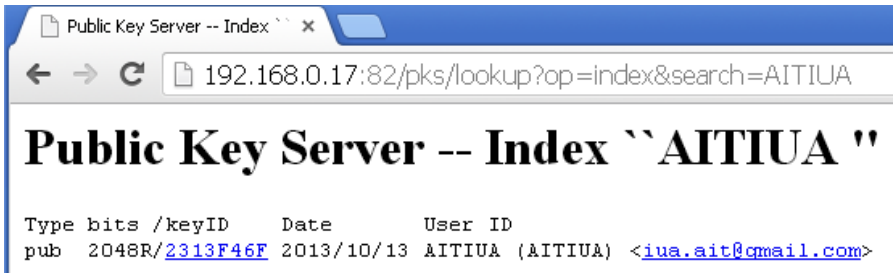


Figura 20: Clave encontrada en el servidor.

5.3.3. Creación de Certificados de Revocación

A continuación, se procede a crear el certificado de revocación, el cual es necesario cuando la clave deja de estar en uso por algún motivo o ha sido comprometida:

1. `#gpg --output Secretaria.asc --gen-revoke 726DA648` *`(id de la clave del usuario)`*

   `#cp Secretaria.asc /media/datos`

```
laura@(none):~$ gpg -o rev-Secretaria.asc --gen-revoke -a 726DA648

sec  2048R/726DA648 2013-10-14 Secretaria (Secretaria IUA) <iua.secretaria@gmail
.com>

Create a revocation certificate for this key? (y/N) Y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision? La clave ya no estará en uso
Invalid selection.
Your decision? s
Invalid selection.
Your decision? 3
Enter an optional description; end it with an empty line:
> La clave ya no estará en uso
>
Reason for revocation: Key is no longer used
La clave ya no estará en uso
Is this okay? (y/N) y

You need a passphrase to unlock the secret key for
user: "Secretaria (Secretaria IUA) <iua.secretaria@gmail.com>"
2048-bit RSA key, ID 726DA648, created 2013-10-14

gpg: gpg-agent is not available in this session
Revocation certificate created.
```

Figura 21: Creación de certificado de revocación.

2. Una vez creado el certificado de revocación, se procede a importarlo:

```
#gpg --import Secretaria.asc
```

```
laura@(none):~$ gpg --import rev-Secretaria.asc
gpg: key 726DA648: "Secretaria (Secretaria IUA) <iua.secretaria@gmail.com>" revo
cation certificate imported
gpg: Total number processed: 1
gpg:     new key revocations: 1
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2014-10-09
laura@(none):~$
```

Figura 22: Importar certificado de revocación.

3. Se verifica que la clave se encuentra revocada:

```
#gpg --list-keys
```

```
laura@(none):~$ gpg --list-keys
/home/laura/.gnupg/pubring.gpg
------------------------------
pub   2048R/726DA648 2013-10-14 [revoked: 2013-10-14]
uid                  Secretaria (Secretaria IUA) <iua.secretaria@gmail.com>
```

Figura 23: Clave revocada.

4. A continuación, se exporta la clave revocada:

```
#gpg -a -o /home/laura/rev-Secretaria.asc --export
```

5. Se visualiza la clave para luego copiarla e ingresarla en la interfaz del servidor en el navegador web:

```
#more /home/laura/rev- Secretaria.asc
```

Figura 24: Exportar clave.

6. Después de copiar la clave, es necesario dirigirse al navegador donde se encuentra el servidor de llaves e ingresar en el campo *Enter ASCII-armored PGP key here*:

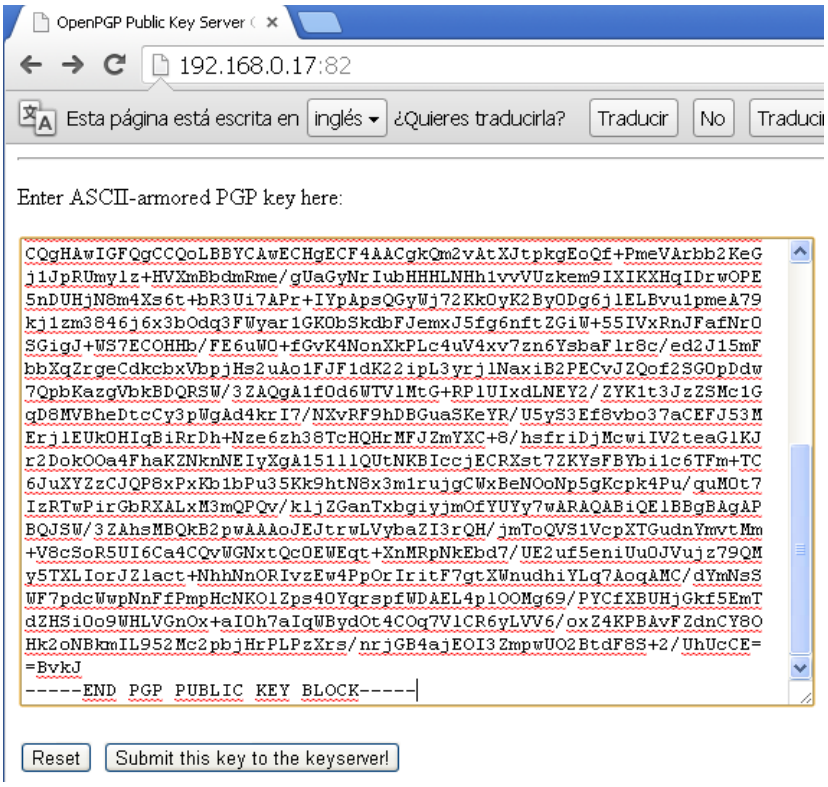


Figura 25: Exportar clave al servidor.

7. Se visualiza en el servidor que se agregó la clave:

Figura 26: Clave exportada al servidor.

8. Se busca en el servidor la clave que se acaba de subir en la opción *Search String* y se visualiza la clave encontrada:

Figura 27: Clave encontrada en el servidor.

5.3.4. Creación del anillo de confianza

Una vez creadas las claves, se procede a crear el anillo de confianza. Crear un anillo de confianza consiste en tener claves de gente firmada por otra gente que la han firmado y que con su firma aseguran que esa clave es realmente de quién dice ser y no ha sido alterada.

Para crear nuestro anillo de confianza, las claves serán firmadas por el Rector según se muestra a continuación:

```
1. #gpg --sign-key AITIUA
```

```
root@(none):/home/laura# gpg --sign-key AITIUA

pub  2048R/2313F46F  created: 2013-10-13  expires: 2014-10-08  usage: SC
                     trust: ultimate      validity: ultimate
sub  2048R/BB074840  created: 2013-10-13  expires: 2014-10-08  usage: E
[ultimate] (1). AITIUA (AITIUA) <iua.ait@gmail.com>


pub  2048R/2313F46F  created: 2013-10-13  expires: 2014-10-08  usage: SC
                     trust: ultimate      validity: ultimate
 Primary key fingerprint: 7F72 2FAF 4373 BA29 1738  CB73 F932 2D78 2313 F46F

     AITIUA (AITIUA) <iua.ait@gmail.com>

This key is due to expire on 2014-10-08.
Are you sure that you want to sign this key with your
key "Rector IUA (Rector) <iua.rector@gmail.com>" (D357BE7B)

Really sign? (y/N) y

You need a passphrase to unlock the secret key for
user: "Rector IUA (Rector) <iua.rector@gmail.com>"
2048-bit RSA key, ID D357BE7B, created 2013-10-13
```

Figura 28: Creación del anillo de confianza.

2. Se verificara la firma de la clave:

```
#gpg --list-sigs
```

```
pub   2048R/2313F46F 2013-10-13 [expires: 2014-10-08]
uid                  AITIUA (AITIUA) <iua.ait@gmail.com>
sig 3        2313F46F 2013-10-13  AITIUA (AITIUA) <iua.ait@gmail.com>
sig          D357BE7B 2013-10-14  Rector IUA (Rector) <iua.rector@gmail.com>
sub   2048R/BB074840 2013-10-13 [expires: 2014-10-08]
sig          2313F46F 2013-10-13  AITIUA (AITIUA) <iua.ait@gmail.com>
```

Figura 29: Clave firmada.

5.3.5. Distribución de Certificados

Para poder comenzar a hacer uso de los certificados y realizar la correspondiente distribución de los mismos, es necesario exportarlos a archivos, separando la clave privada de la clave pública.

1. Para exportar la clave pública se procede de la siguiente forma:

```
#gpg --armor --output clavepublicaAIT.asc --export iua.ait@gmail.com
#more clavepublicaAIT.asc
```

```
root@(none):/home/laura# more clavepublicaAIT.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.11 (GNU/Linux)

mQENBFJa9iABCAC3w1Km/xyv9JBEsApjUEF9ce1OAwyn1vJuI1dV8L/T5f4j9kC2
USvnqsG6bzQKWzKx7ABsKektvMb3/Ez15osvntdDg62tYPPZRSA3SJPOxcOinhPa
K41BSsrfOzH94P2mQ+fZuTCFmWTKDpO+VTSFWLt2q8AGOnbL/rVDUZu73XTh/kbX
dPTvWi9ZtCAWFf3wQOcCO9afJtGANkfBsDj8TWyUp2pEIKTAVffUUViOGbQRZOyB
mn77UWK7+syMFt1BWc+FIrTZAepnujLh3wSFLb27kG7pDtOPINGUeI1Ec39yQY1L
usOTlOMdwKYb5M6+prknuzeG8ECYhfVgEMZLABEBAAGOIOFJVE1VQSAoQU1USVVB
KSA8aXVhLmFpdEBnbWFpbC5jb20+iQE+BBMBAgAoBQJSWvYgAhsDBQkB2pwABgsJ
CAcDAgYVCAIJCgsEFgIDAQIeAQIXgAAKCRD5Mi14IxPOb0CmB/4qjuky6Fs6SBOx
```

Figura 30: Exportar clave pública.

Se copia entonces la clave pública en un archivo .asc.

2. Para exportar la clave privada se procede de la siguiente forma:

```
#gpg --output claveprivadaAIT.asc --armor --export-secret-key iua.ait@gmail.com
#more claveprivadaAIT.asc
```

```
root@(none):/home/laura# more  claveprivadaait.asc
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: GnuPG v1.4.11 (GNU/Linux)

lQO+BFJa9iABCAC3w1Km/xyv9JBEsApjUEF9ce1OAwyn1vJuI1dV8L/T5f4j9kC2
USvnqsG6bzQKWzKx7ABsKektvMb3/Ez15osvntdDg62tYPPZRSA3SJPOxcOinhPa
K41BSsrfOzH94P2mQ+fZuTCFmWTKDpO+VTSFWLt2q8AGOnbL/rVDUZu73XTh/kbX
dPTvWi9ZtCAWFf3wQOcCO9afJtGANkfBsDj8TWyUp2pEIKTAVffUUViOGbQRZOyB
mn77UWK7+syMFt1BWc+FIrTZAepnujLh3wSFLb27kG7pDtOPINGUeI1Ec39yQY1L
usOTlOMdwKYb5M6+prknuzeG8ECYhfVgEMZLABEBAAH+AwMCGq/z7bcf7y9gK6CR
oVYq+mSsGxHzs4PcQDzeOg9Zod3su3PAbKl/OjDz3rZGb/Y2OPUkgpX4T8yB+fFR
ObuP7qkQZIKnBwCj49cJTV3IrOPbHgNmMOx4BI5vIi1ODZjsL+lQKDg8NwsffcN9
zOPOtR47aaRPFF2O6AEfW/PnBOoUJgetdm3qaAOnTk7qpw9KU95rtAkcvtjukFrC
```

Figura 31: Exportar clave privada.

Se copia entonces la clave privada en un archivo .asc.

Cabe aclarar que, en la etapa inicial se instalarán en todas las máquinas correspondientes, las claves públicas que se encuentran en el servidor; por tal motivo, copiando los archivos pubring.gpg en el directorio GnuPG será suficiente. Para el caso de nuevos certificados creados posteriormente se procede como en el punto 1.

A continuación, las claves deben ser importadas desde las aplicaciones para que puedan ser utilizadas posteriormente. Desde la interfaz Kleopatra, que se utiliza para administrar los certificados, se pueden importar directamente desde el servidor utilizando la opción *Lookup Certificates on Server* o bien desde archivo procediendo de la siguiente forma:

1. Se debe seleccionar el botón *Import Certificates* y luego se selecciona la clave pública a importar:

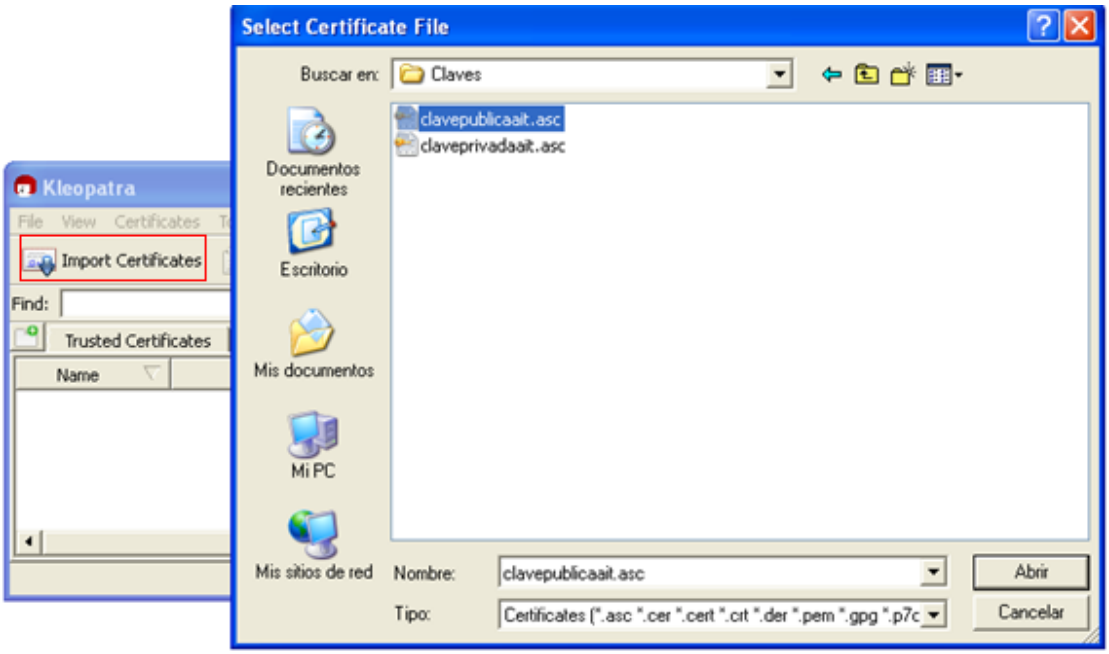


Figura 32: Importar certificado en Kleopatra.

2. Se importa el certificado:

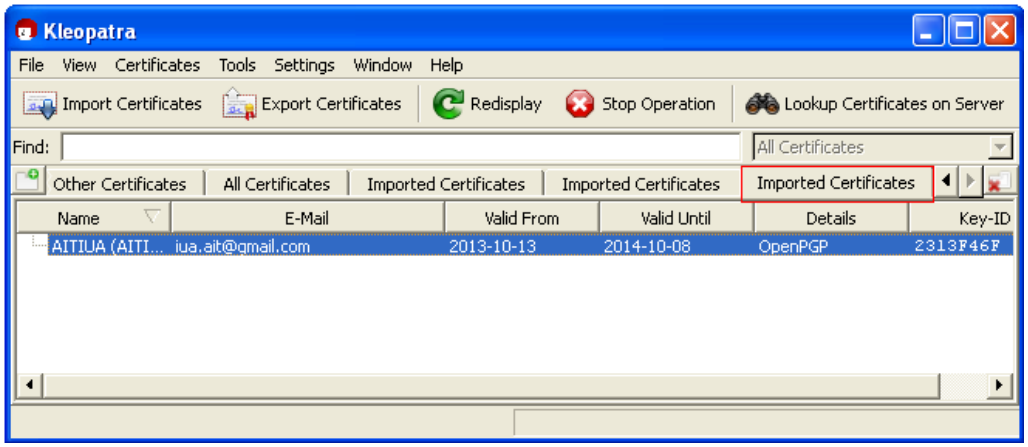


Figura 33: Certificado importado en Kleopatra.

3. Realizando click derecho sobre el certificado y la opción *Certificate Details*, se podrá visualizar los detalles del certificado importado:

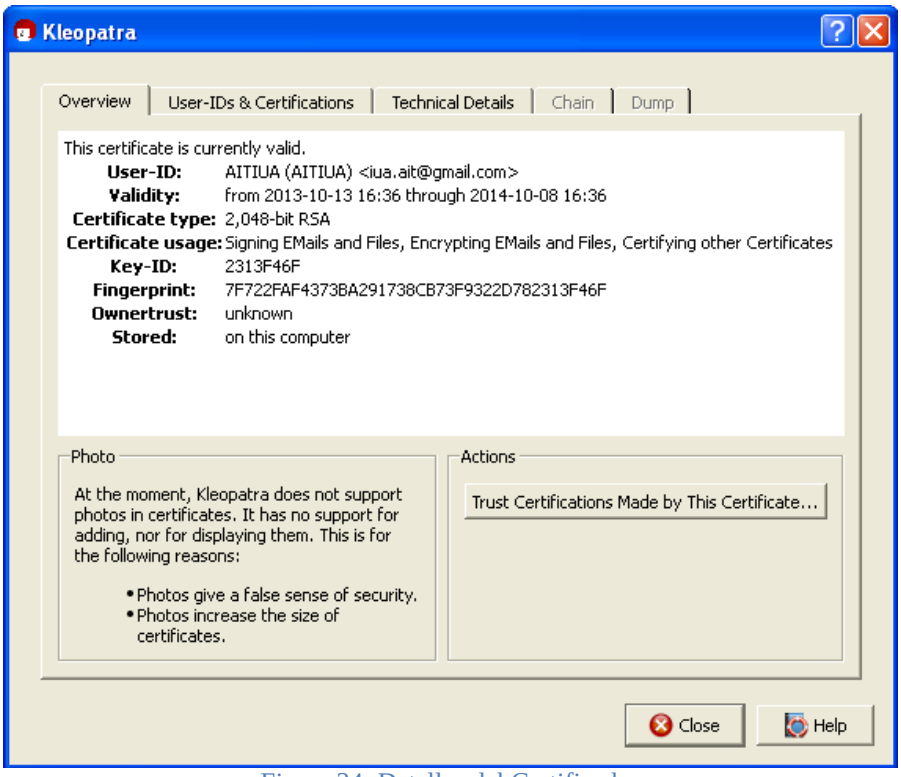


Figura 34: Detalles del Certificado.

Finalmente, es importante destacar que las claves privadas están disponibles y son utilizadas solo por el propietario de la misma.

5.3.6. Firma Digital de Documentos

Una vez creadas las claves públicas y privadas es posible comenzar a firmar archivos y documentos.

Cabe destacar que los pasos a seguir, que a continuación se describen, aplican cada vez que se desee firmar un documento en la Institución a través de los procedimientos administrativos descriptos en la etapa de diseño.

Razones de la Firma Digital de archivos y documentos:

- Indicar que se ha leído o aprobado el documento (por ejemplo, la aprobación de solicitudes).
- Proteger la integridad de los datos, mediante el uso y verificación de la firma, es posible asegurarse y saber si el documento recibido ha sufrido alteraciones o no.

Requisitos previos:

- Para crear una Firma Digital, se debe poseer una clave pública y otra privada.
- Se necesita un documento digital para firmar.

Flujo del proceso

El usuario indica que desea firmar un documento. El sistema solicita la clave privada del firmante, antes de proceder. El sistema procede a firmar el documento.

El siguiente esquema muestra lo que sucede cuando se Firma Digitalmente un documento:

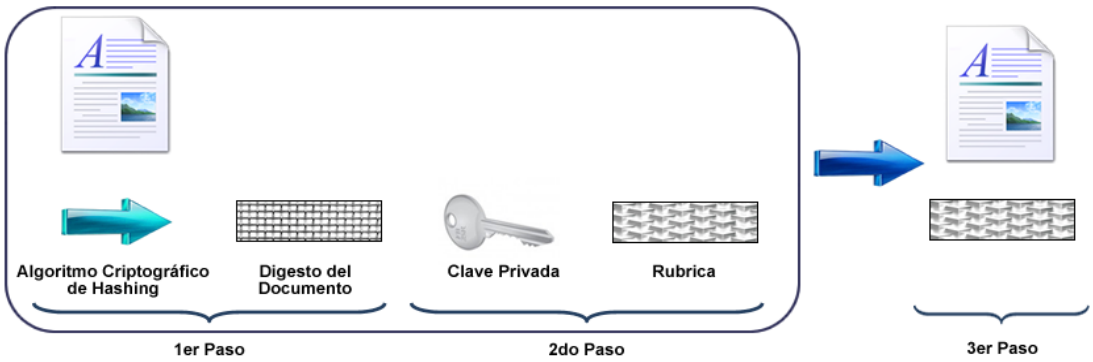


Figura 35: Proceso de Firma Digital.

1. Se aplica documento un algoritmo de hash, para crear un digesto del mismo. El resultado es un resumen del archivo. Este resumen, representa una huella digital única para el documento. El cual es imposible de reproducir a partir de otro archivo.

2. Se aplica la clave privada del firmante al resumen del archivo para encriptarlo y de esta forma, crear una firma del documento.

3. La firma se adjunta con el documento, o lo acompaña, para indicar que el archivo está firmado digitalmente.

El resultado es un documento firmado digitalmente que se puede procesar de igual forma que cualquier otro documento. Al verificar la Firma Digital, será posible probar quién es el firmante del documento, así como la integridad del mismo.

A continuación, se demuestra cómo se debe proceder para firmar un archivo mediante la herramienta:

1. La firma es muy fácil de realizar mediante GpgEX. Para realizarlo, se debe seleccionar el documento que se desea firmar y realizar un click sobre el mismo con el botón derecho:

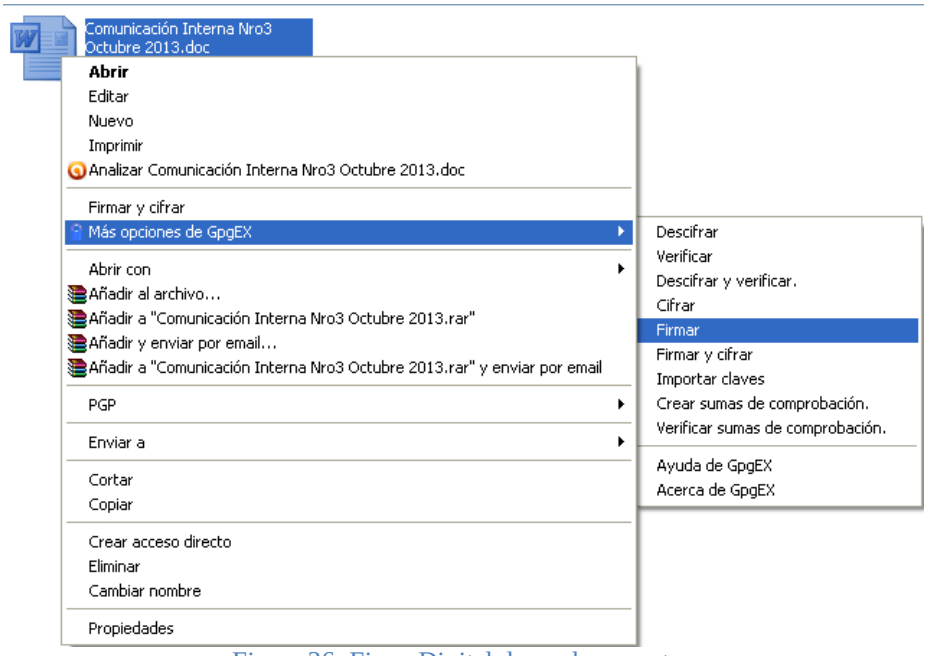


Figura 36: Firma Digital de un documento.

2. En la siguiente ventana se selecciona la acción que se desea realizar, en este caso *Sign:*

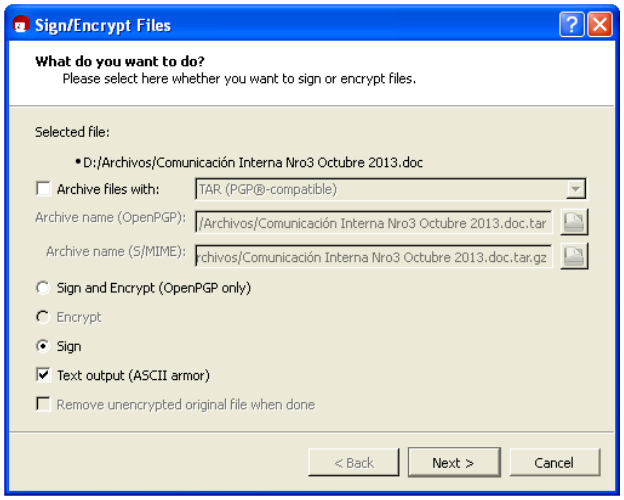


Figura 37: Firma Digital de un documento mediante GpgEX.

Se genera el archivo de la firma con extensión .asc (OpenPGP) o .pem (S / MIME), si se ha seleccionado la opción *Text Outpout(ASCII armor).* Estos tipos de archivos se pueden abrir

con cualquier editor de texto, aunque sólo se podrán ver los números y letras. De lo contario, si no se selecciona esta opción, la firma se creará con la extensión .sig (OpenPGP) o .p7s (S / MIME). Estos archivos son archivos binarios, y no se pueden ver en un editor de texto.

1. En la siguiente ventana, si no está seleccionado de forma predeterminada, se debe seleccionar el certificado privado (OpenPGP o S / MIME) con el que desea firmar el documento:

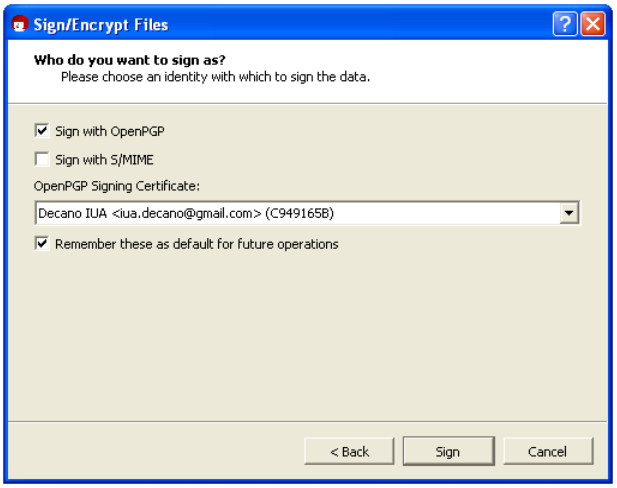


Figura 38: Firma Digital de un documento con OpenPGP.

2. A continuación, se solicita una contraseña para desbloquear la clave secreta que es la que se utiliza para firmar:

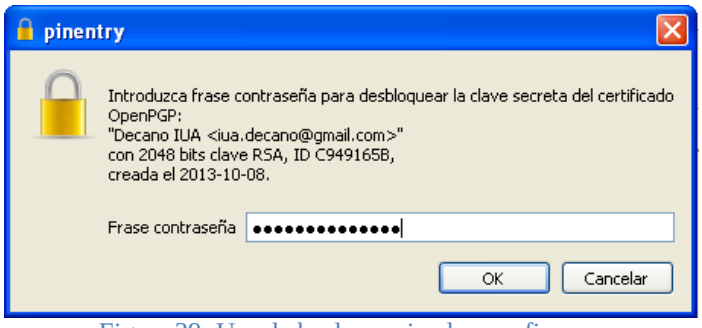


Figura 39: Uso de la clave privada para firmar.

3. Una vez que el proceso de firma se ha completado con éxito, aparece la siguiente ventana:

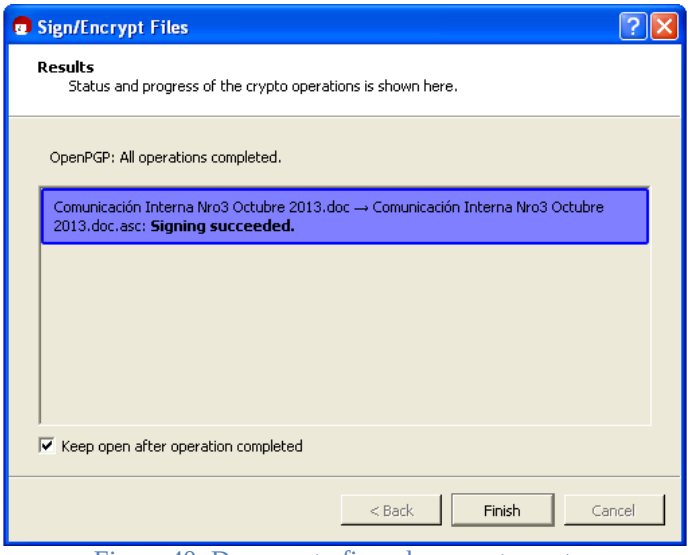


Figura 40: Documento firmado correctamente.

Ahora, se ha firmado correctamente el documento.

Una firma 'independiente' siempre se utiliza para firmar un archivo o documento, esto significa que el archivo que se va a firmar no se modificará y se creará un segundo archivo con la firma real. Para verificar la firma más adelante, habrá entonces dos archivos. En este caso al firmar con OpenPGP se ha generado un archivo .asc:

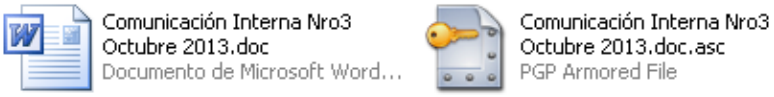


Figura 41: Documento original y documento firmado digitalmente.

5.3.6.1 Comprobación de la firma:

Ahora, se procede a comprobar el archivo o documento que se ha sido firmado. Para ello, es necesario comparar los dos digestos para validar la igualdad.

Requisitos previos:

- Contar con un documento firmado para verificar.
- También se debe contar con el certificado con clave pública del firmante para conocer el algoritmo de hash y encriptación que el firmante utiliza para su firma.

Flujo del proceso

El usuario, debe indicar que desea verificar una Firma Digital, lo cual se realiza mediante el certificado y la rúbrica. El sistema se encarga de realizar la verificación.

El siguiente diagrama muestra lo que sucede cuando se verifica una Firma Digital.

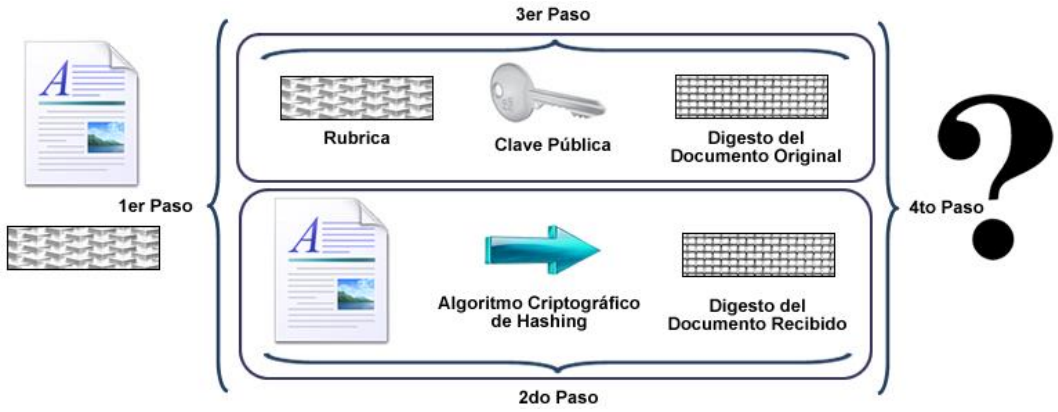


Figura 42: Proceso de verificación de Firma Digital.

1. El documento firmado digitalmente se divide en sus componentes: La Firma Digital y el propio documento.

2. El mismo algoritmo hash que se utilizó en el proceso de firma se aplica al documento a verificar, usando el algoritmo de hash solicitado por el certificado. Se obtiene un hash del documento actual.

3. La clave pública se aplica a la firma con el algoritmo solicitado en el certificado, para obtener el hash del documento original del firmante.

El resultado de esta validación es la aceptación o denegación del archivo recibido, en base a las siguientes conclusiones:

- Si los digestos comparados son idénticos, entonces:
  - El firmante es quién dice ser, es decir, el firmante es el único propietario de la clave privada que se corresponde a la clave pública que se utiliza para verificar la firma).
  - El documento no ha sido alterado después de haber sido firmado.
- Si los digestos no son idénticos, entonces:
  - El documento puedo haber sido alterado.

- El firmante puede no ser quién uno piensa, es decir, el archivo ha sido firmado con una certificado distinto, por lo tanto la clave privada y/o algoritmos del certificado no se corresponden a los usados durante la verificación.

A continuación, se siguen los pasos necesarios para realizar la comprobación de la firma mediante la herramienta:

1. Para verificar la firma, es decir el archivo o documento con la terminación .asc en este caso, el documento firmado y documento original deberán estar en la misma carpeta. Así, se debe seleccionar el documento firmado y la opción *Verificar*:

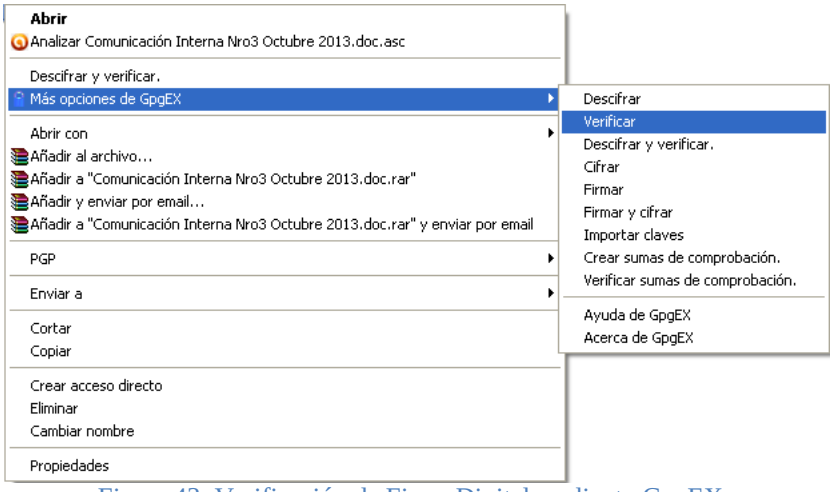


Figura 43: Verificación de Firma Digital mediante GpgEX.

2. Aparece la siguiente ventana:

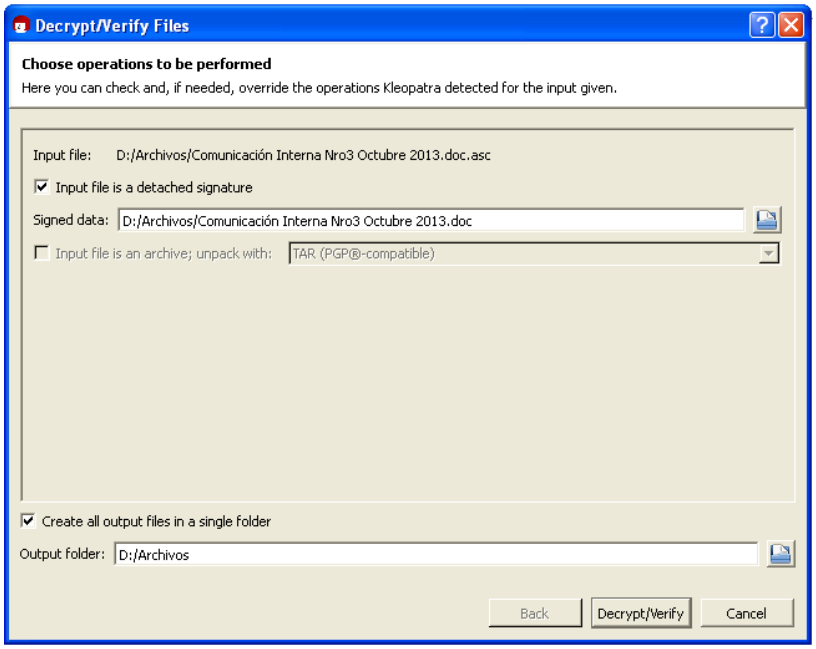


Figura 44: Verificación de Firma Digital con OpenPGP.

En *Input file* se muestra la ruta del archivo de firma .asc. Por otro lado, en *Signed data*, se refleja el archivo original.

3. A continuación, se procede verificar el documento. Tras una verificación exitosa, aparece la siguiente ventana:

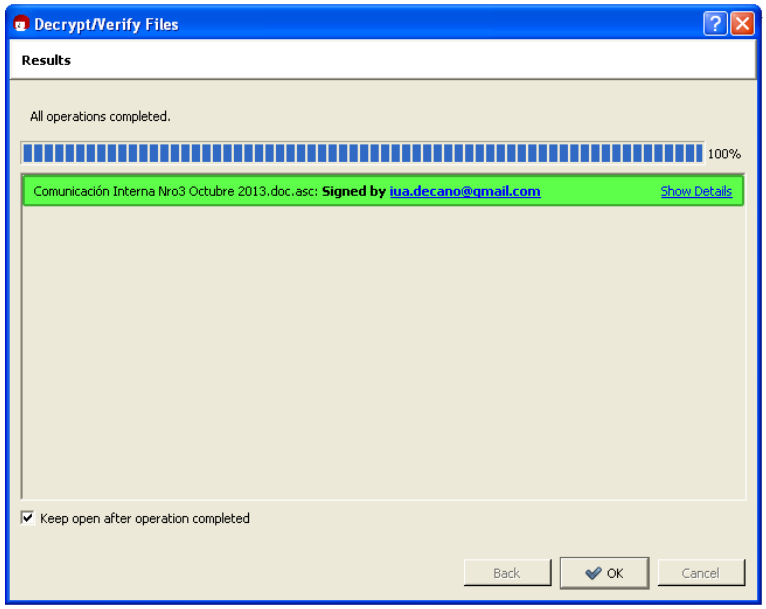


Figura 45: Firma Digital verificada correctamente.

5. Concreción del Modelo

El resultado muestra que la firma es correcta, por lo cual, es posible estar seguro de que la integridad del documento se ha conservado, es decir que el documento no ha sido modificado.

Por otro lado, en caso de que el documento original haya sido modificado, apenas en un solo carácter, o se elimina o modifica, la firma se mostrará como si hubieran sido rota:

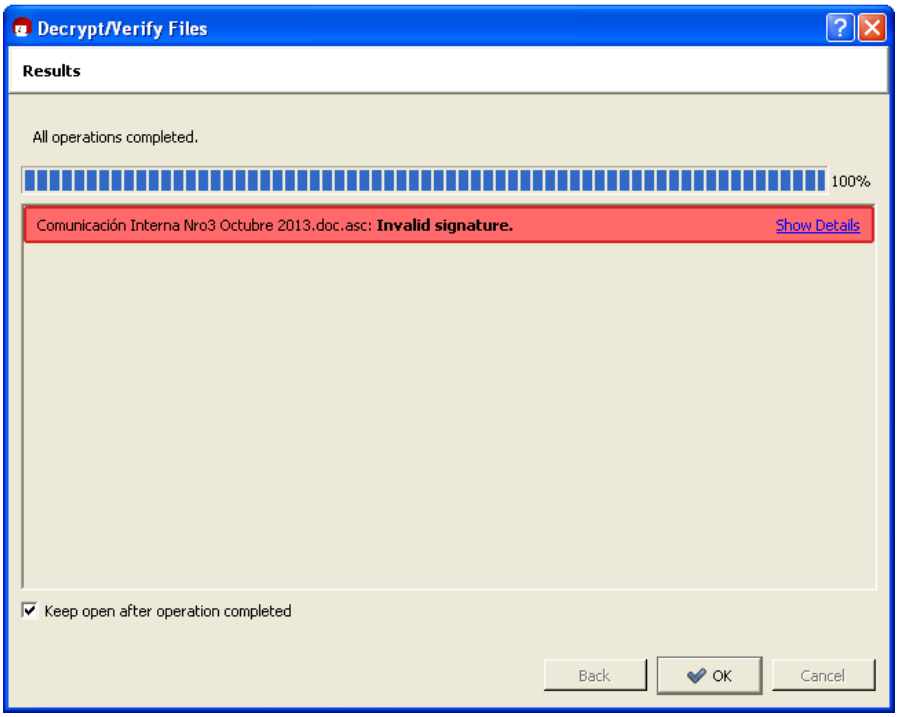


Figura 46: Firma Digital verificada erróneamente.

5.3.7. Cifrado de Archivos

Además de firmar digitalmente un archivo o documento, también es posible cifrarlo. A continuación se muestran los pasos necesarios para poder realizarlo:

1. Se debe seleccionar el archivo que se desea cifrar y realizar un click sobre el mismo con el botón derecho:

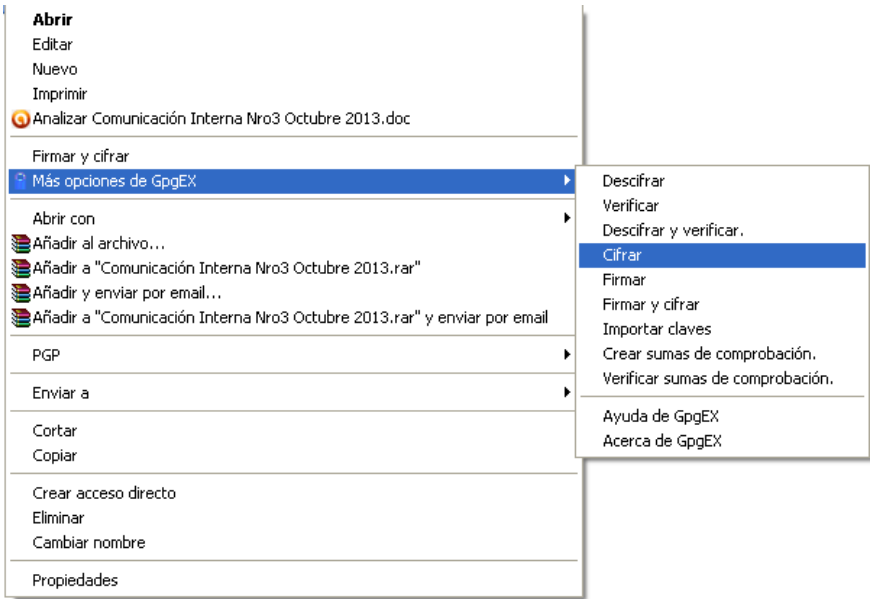


Figura 47: Cifrado de un documento mediante GpgEX.

2. En la siguiente ventana se selecciona la acción que se desea realizar, en este caso *Encrypt:*

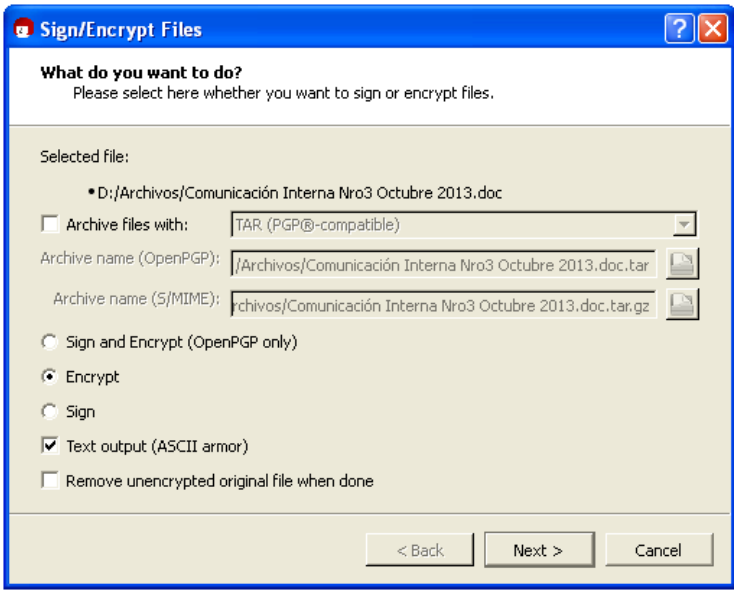


Figura 48: Cifrado de un documento con OpenPGP.

Se genera el archivo cifrado con extensión .asc (OpenPGP) o .pem (S / MIME), si se ha seleccionado la opción *Text Outpout(ASCII armor).* De lo contario, si no se selecciona esta opción, la firma se creará con la extensión .gpg (OpenPGP) o .p7m (S / MIME). Estos archivos son archivos binarios, y no se pueden ver en un editor de texto.

5. Concreción del Modelo

3. En la siguiente ventana, se debe seleccionar uno o más certificados públicos de él o los receptores:

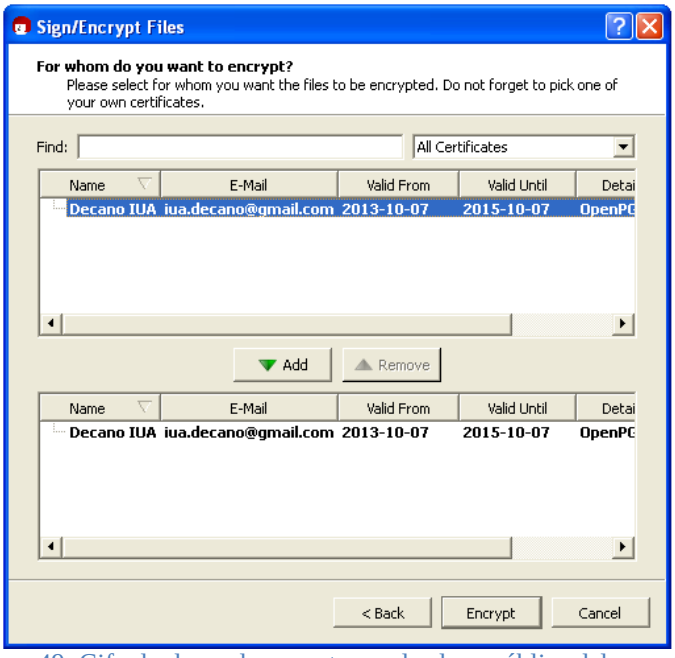


Figura 49: Cifrado de un documento con la clave pública del receptor.

4. Según el certificado de destinatario seleccionado y su tipo (OpenPGP o S/MIME), el archivo se cifra usando OpenPGP y /o S/MIME. Así, si se ha seleccionado un certificado OpenPGP *y* un certificado S / MIME, se reciben dos archivos cifrados. En este caso, se seleccionó un certificado OpenPGP se recibe un archivo .asc:

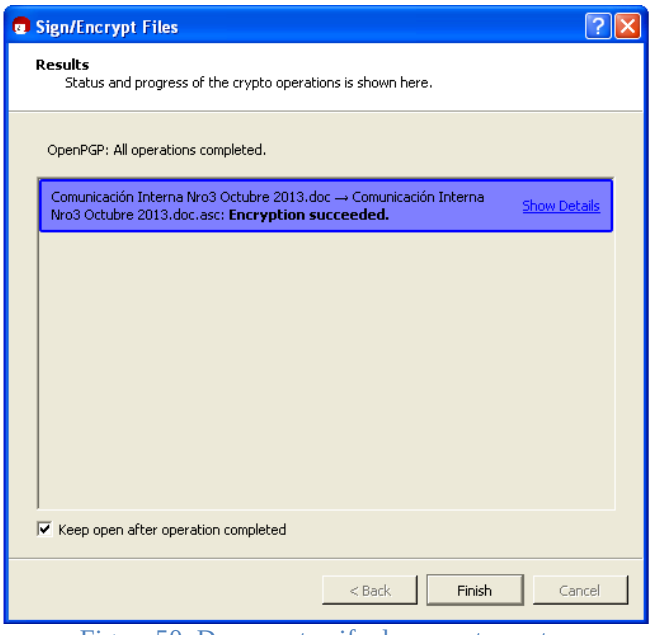


Figura 50: Documento cifrado correctamente.

5. Concreción del Modelo

Ahora, se ha cifrado correctamente el documento.

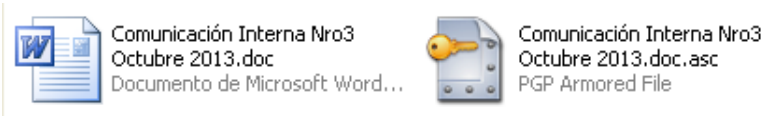


Figura 51: Documento original y documento cifrado.

5.3.7.1 Descifrar un archivo:

A continuación, se procede a descifrar el archivo o documento que se acaba de cifrar:

1. Se selecciona el documento cifrado y la opción *Descifrar*:

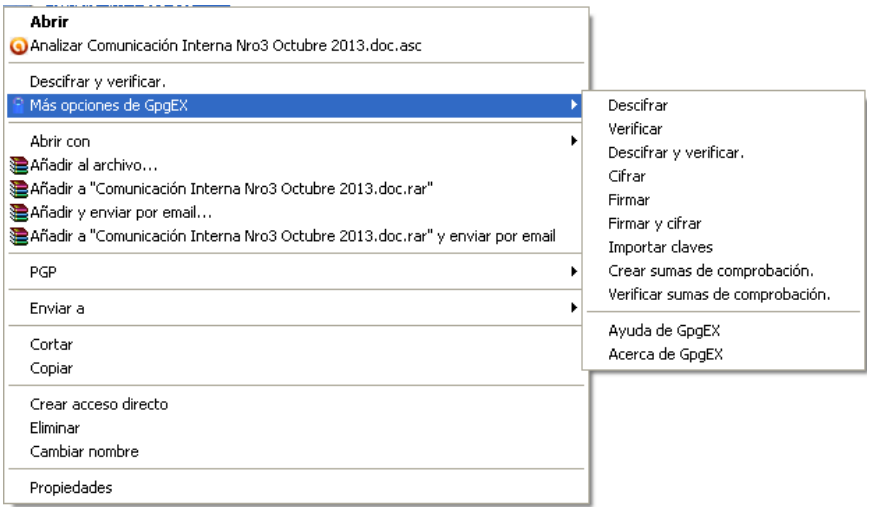


Figura 52: Verificación de cifrado mediante GpgEX.

2. Aparece la siguiente ventana:

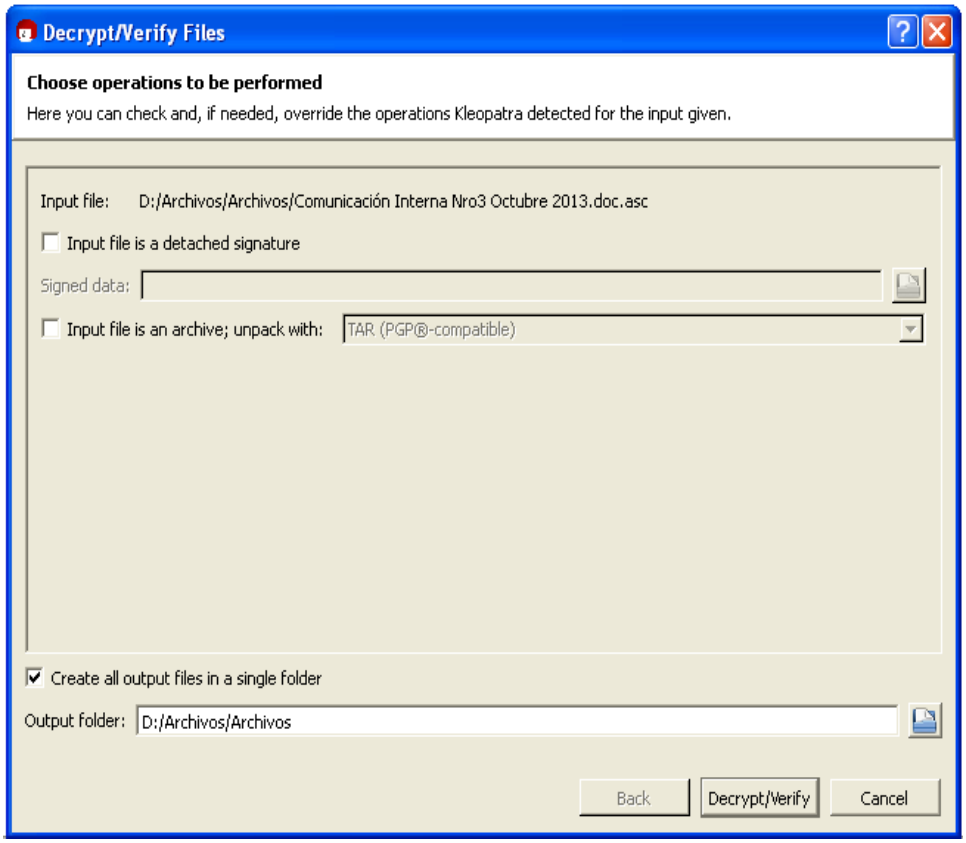


Figura 53: Verificación de cifrado con OpenPGP.

3. A continuación, se le solicita una contraseña para desbloquear la clave secreta:

Figura 54: Uso de la clave privada para descifrar.

4. Si el descifrado se ha realizado con éxito se muestra la siguiente pantalla:

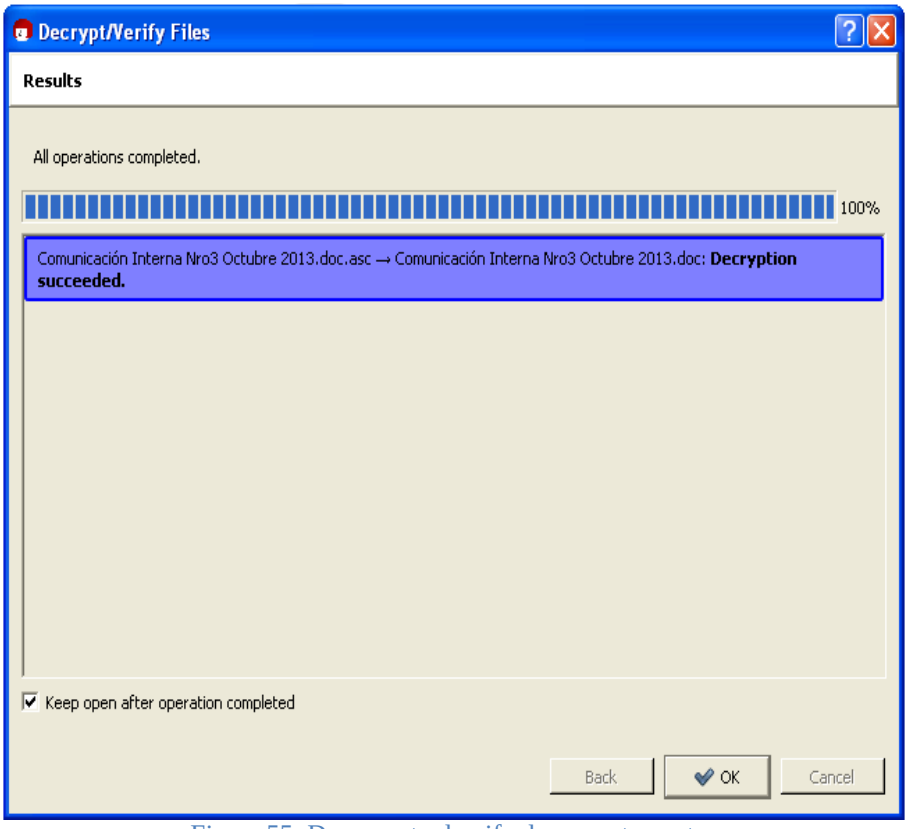


Figura 55: Documento descifrado correctamente.

Finalmente, también es posible firmar y cifrar un archivo al mismo tiempo, siguiendo pasos similares a los ya mencionados.

5.3.8. Firma Digital de correos electrónicos

Es posible también enviar correos electrónicos firmados, para ello se utilizará el cliente de correo Mozilla Thunderbird junto con el complemento Enigmail.

Cabe destacar, que los pasos a seguir que a continuación se describen aplican cada vez que se desee firmar un correo electrónico en la Institución a través de los procedimientos administrativos descriptos en la etapa de diseño.

5.3.8.1 Configurar Enigmail en las Cuentas de Correo Electrónico

Una vez configurada la cuenta de correo que desea utilizar, es necesario verificar si Enigmail ha sido instalado correctamente, por lo cual se debe dirigir en el menú a *OpenPGP/Preferencias:*

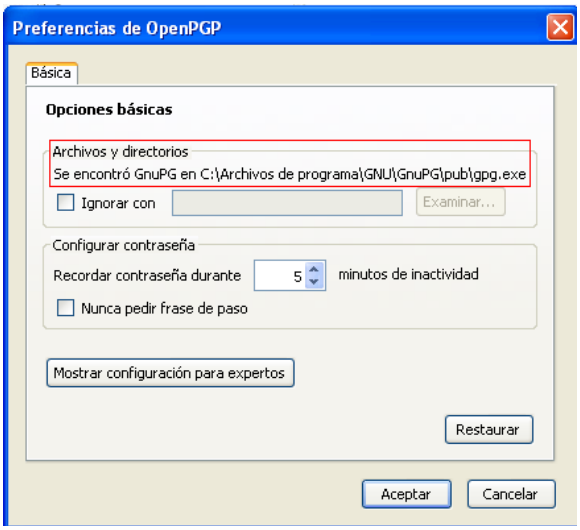


Figura 56: Configuración de preferencias OpenPGP.

Aquí se puede ver que GnuPG fue instalado exitosamente verificado que la sección *Archivos y directorios* se indica que *Se encontró GNUPG en C:\Archivos de Programa\GNU\GnuPG\pub\gpg.exe.*

Para habilitar el uso de Enigmail con una cuenta específica de correo electrónico, se ejecutan los siguientes pasos:

1. Seleccionar *Herramientas/Configuración de la Cuenta*.

2. Seleccionar la opción del menú *Seguridad OpenPGP* de la barra lateral como sigue:

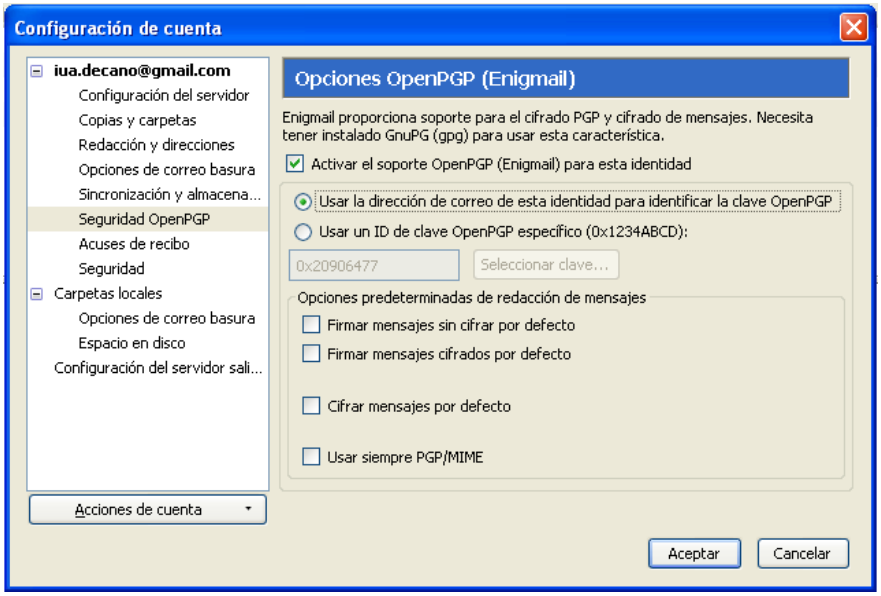


Figura 57: Configuración de Enigmail en la cuenta de correo electrónico.

3. Habilitar la opción *Activar el soporte OpenPGP* y seleccionar la opción *Usar la dirección de correo de esta identidad para identificar la clave OpenPGP*.

4. *Aceptar* para regresar al panel de control de Thunderbird

Una vez que confirmado que Enigmail y GnuPG están trabajando adecuadamente, se puede comenzar a trabajar.

5.3.8.2. Importar claves públicas

Es posible además desde Kleopatra, como ya se ha visto, importar claves públicas en Thunderbird. La importación puede realizarse desde el Servidor de claves o desde un archivo. Cabe aclarar, que si las claves ya han sido importadas previamente desde Kleopatra, ya se encontraran disponibles y para hacer utilizadas desde Thunderbird, por lo cual no será necesario realizarlo desde aquí.

Importar desde el Servidor

Para ello, se procede de la siguiente forma:

1. Se debe ingresar a *OpenPGP/Administración de claves*:

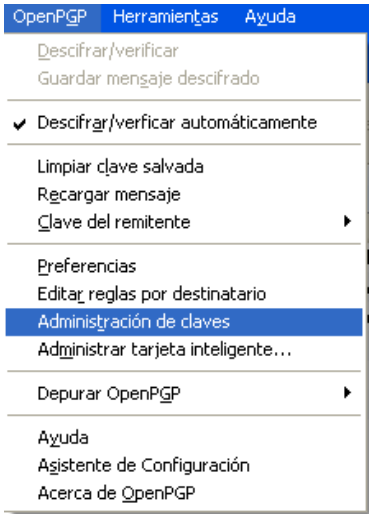


Figura 58: OpenPGP/Administración de claves en Thunderbird.

2. Se ingresa al Administrador de claves y allí se debe seleccionar la opción *Servidor de Claves/Buscar claves* para importar una clave desde el servidor:

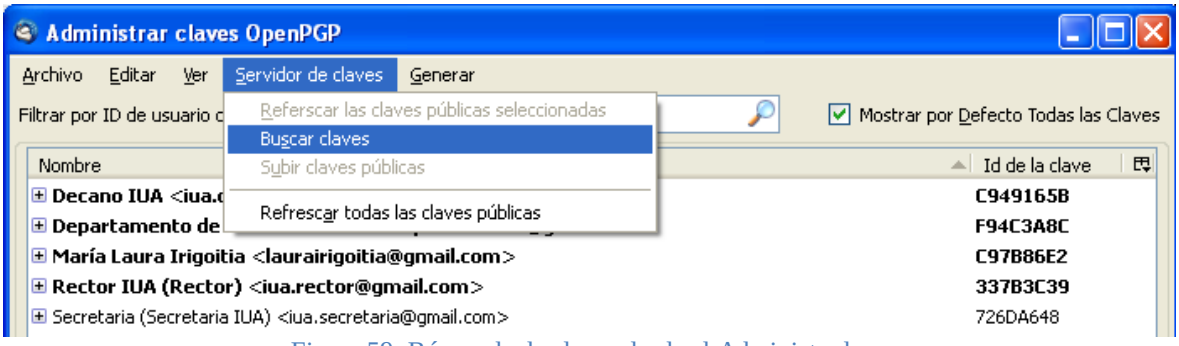


Figura 59: Búsqueda de claves desde el Administrador.

3. Se solicitara el nombre de la clave a buscar:

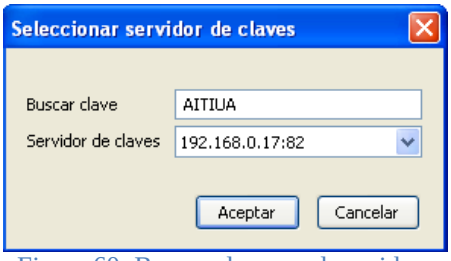


Figura 60: Buscar clave en el servidor.

4. Se muestra la clave encontrada:

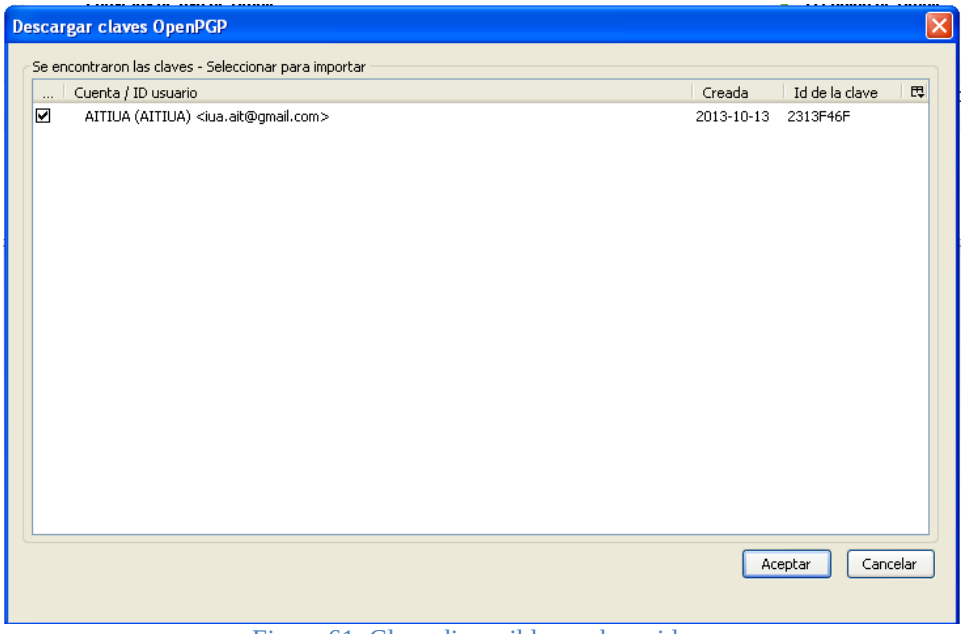


Figura 61: Clave disponible en el servidor.

5. Concreción del Modelo

5. Al *Aceptar* se importa la clave:

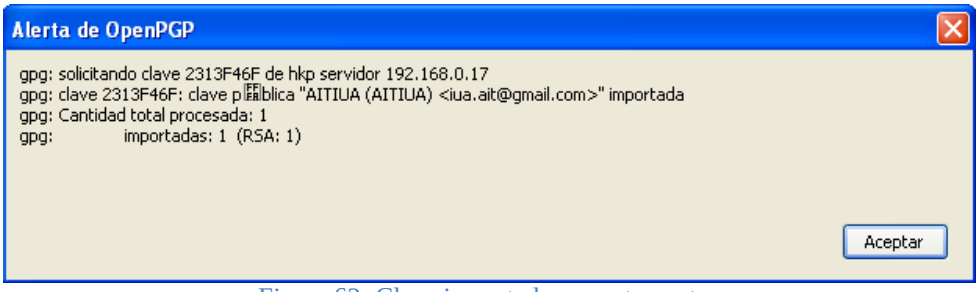


Figura 62: Clave importada correctamente.

Importar desde Achivo

Para ello, se procede de la siguiente forma:

1. Desde el Administrador de claves se debe ir a la opción *Archivo/Importar Fichero* y seleccionar la clave desde la ubicación correspondiente:

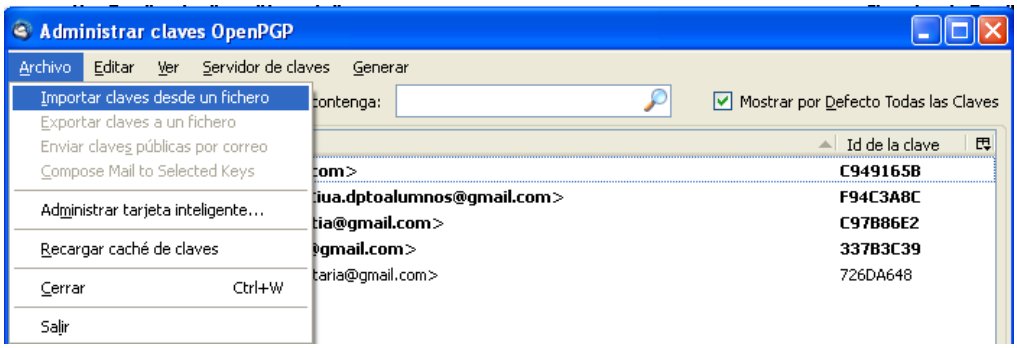


Figura 63: Importar clave dese un archivo.

2. Se informa que la clave ha sido importada:

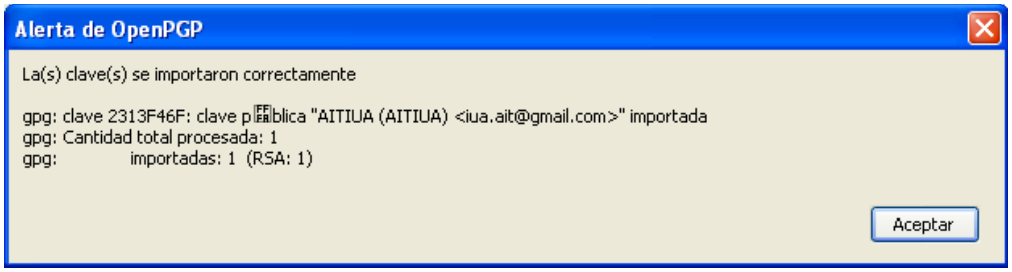


Figura 64: Clave importada correctamente.

Se visualiza en el Administrador la clave que ha sido importada junto a las demás:

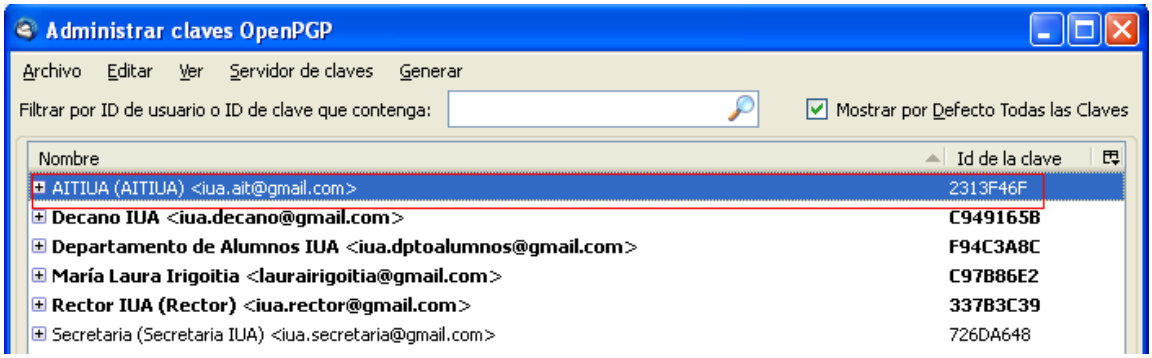


Figura 65: Vista de las claves disponibles en el Administrador de claves.

5.3.8.3. Intercambiar claves públicas

Es posible también, intercambiar las claves a través del correo electrónico, para ellos se procede de la siguiente forma:

1. Ejecutar *Redactar.*

2. Seleccionar la opción del menú *OpenPGP /Adjuntar Mi Clave Pública*

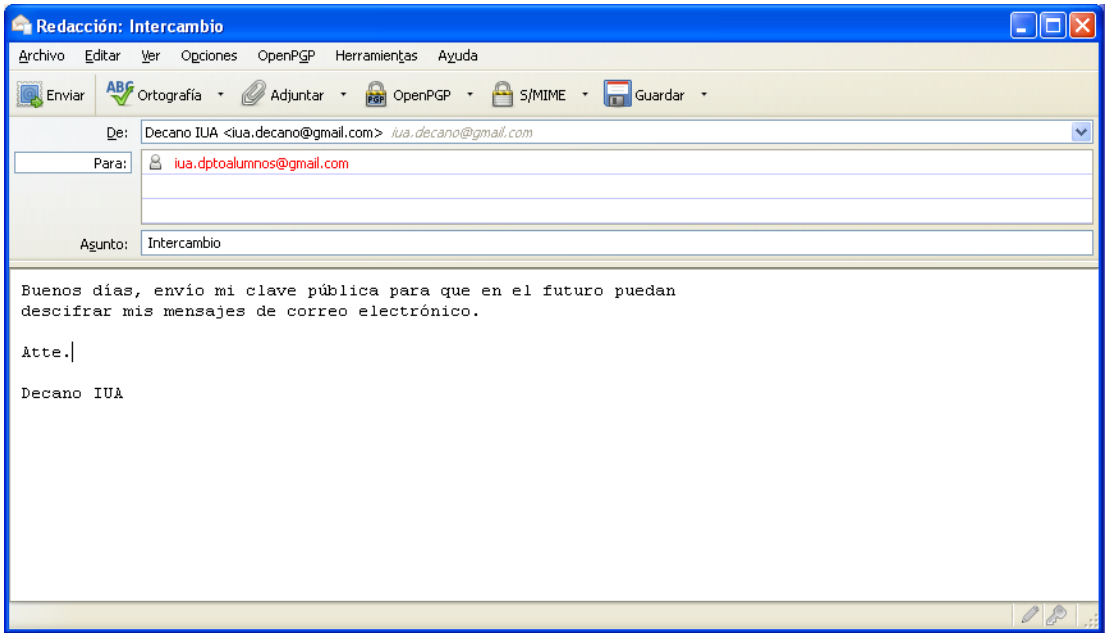


Figura 66: Enviar correo electrónico con la clave pública.

3. Al presionar *Enviar*, es posible ver el adjunto:

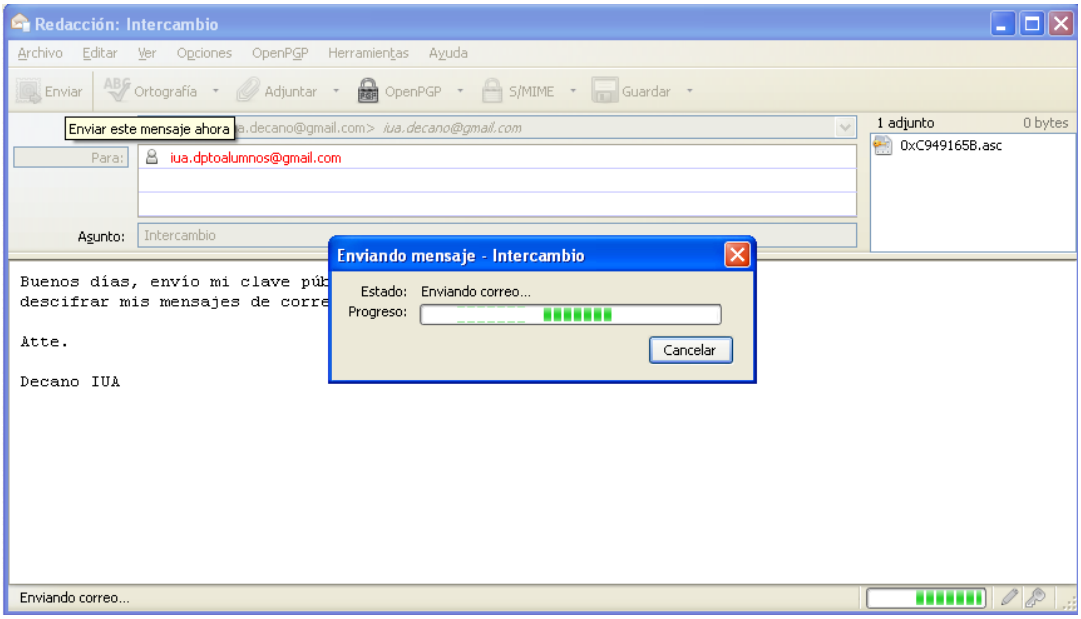


Figura 67: Correo electrónico enviado con la clave pública.

A continuación, se procede a importar la clave pública.

4. Abrir el mensaje

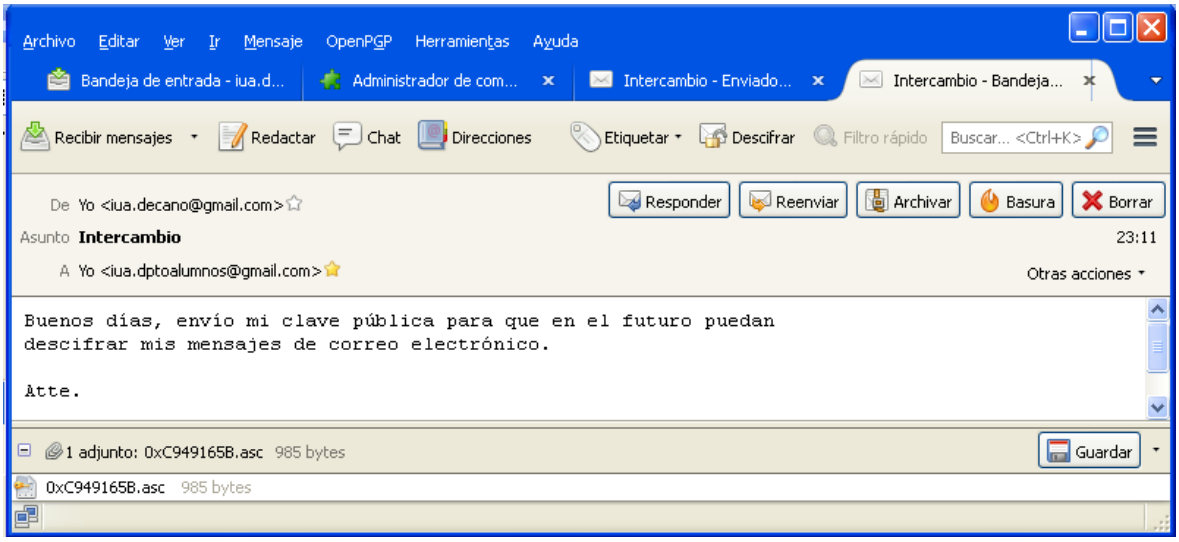


Figura 68: Correo electrónico recibido con una clave pública.

5. Concreción del Modelo

5. Presionar *Descifrar*, aparece la advertencia:

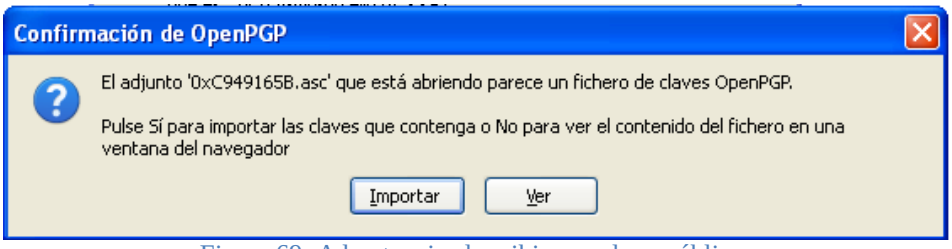


Figura 69: Advertencia al recibir una clave pública.

6. *Importar*. Si se ha importado con éxito la clave pública, un mensaje similar al siguiente aparece:

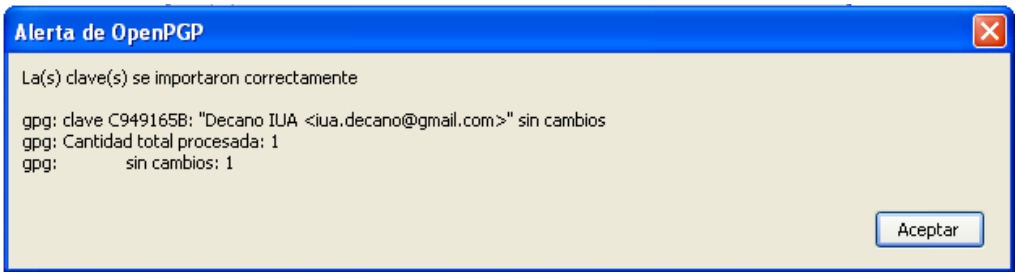


Figura 70: Clave pública importada correctamente.

5.3.8.4. Validar y Firmar un par de claves

Un paso importante a seguir es verificar que la clave pública importada verdaderamente pertenece a la persona que supuestamente lo envió, entonces, se debe confirmar su 'validez'.

En primer lugar, resultará conveniente ponerse en contactos con los demás contactos de correo electrónico a través de medios de comunicación diferentes. Es necesario, tener absoluta certeza que realmente se está comunicado con la persona correcta.

Tanto el emisor como el receptor deben verificar las 'huellas digital' de las claves públicas que han intercambiado. Una huella digital es una serie única de números y letras que identifica a cada clave. Es posible utilizar la pantalla de *OpenPGP/Administrar Claves* para ver la huella digital de los pares de claves que se han creado y de las claves públicas que se han importado.

Para ver la huella digital de un par de claves particular, se ejecutan los siguientes pasos:

Seleccionar *OpenPGP/Administrar Claves* y luego pulsar con el botón derecho sobre una clave particular para activar el menú emergente:

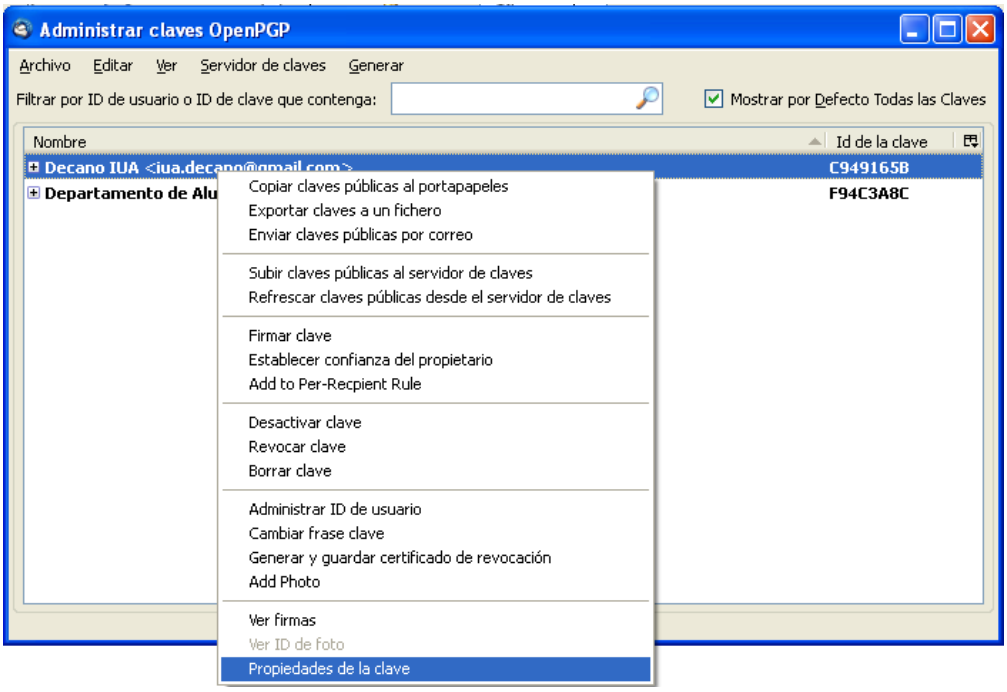


Figura 71: Verificar una clave desde el Administrador.

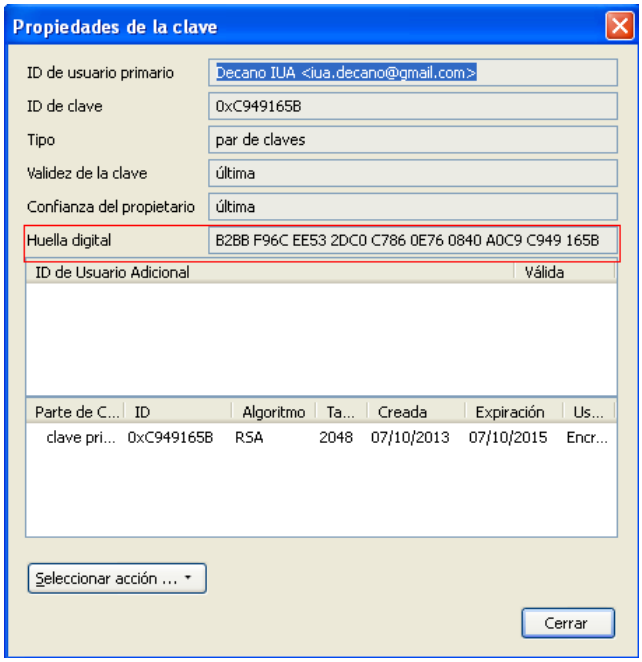


Figura 72: Verificar la huella digital de una clave.

5. Concreción del Modelo

A continuación, deben confirmar entre ambos si la huella digital para la clave que todos han intercambiado coincide con la original del remitente. Si no coinciden, será necesario intercambiar nuevamente sus claves públicas y repetir el proceso de validación.

5.3.8.5. Firmar una clave pública válida

Después de que se ha establecido que la clave de un contacto concuerda exactamente, es posible *firmarla o* bien utilizar la opción *Establecer confianza del propietario de la clave del remitente*, para confirmar que se considera válida esta clave.

Para firmar una clave pública adecuadamente validada, se ejecutan los siguientes pasos:

1. Ir a *OpenPGP/Administración de Claves* y click con el botón sobre la clave pública recibida y a continuación, seleccionar la opción del menú *Firmar Clave* para activar la siguiente pantalla:

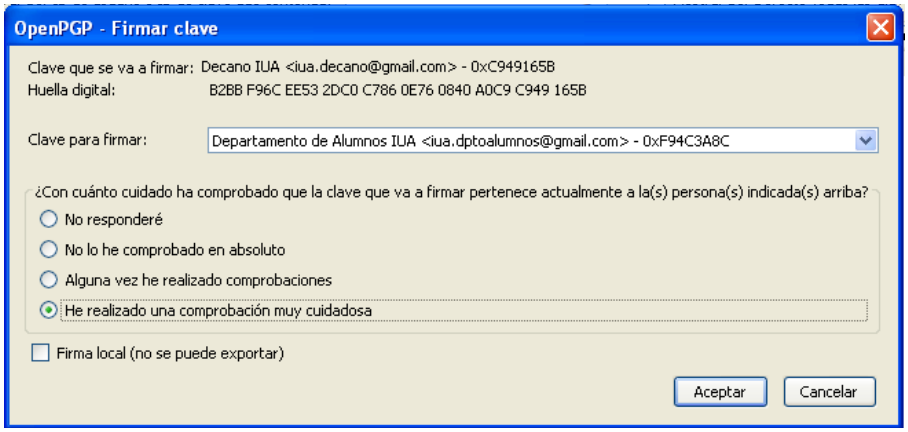


Figura 73: Firmar una clave pública.

2. *Aceptar* para completar la firma de la clave pública y se le solicita la contraseña para completar el proceso:

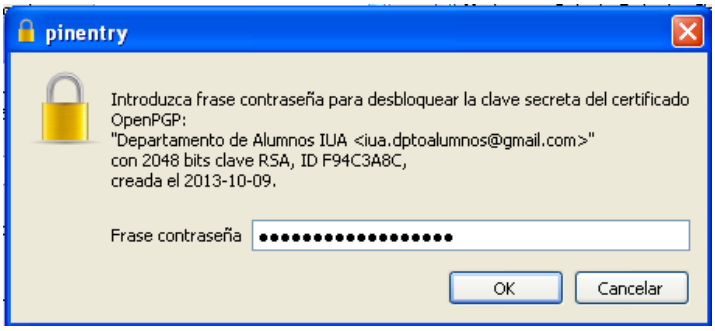


Figura 74: Uso de la clave privada para firmar una clave pública.

5.3.8.6 Firmar y cifrar mensajes de correo electrónico

Una vez que todos los contactos hayan importado y validado las claves públicas de los demás, es posible comenzar a enviar mensajes firmados y/o cifrados y descifrar los recibidos.

Es necesario tener en cuenta que el encabezado de cualquier mensaje de correo electrónico, es decir, el *Asunto* y los destinatarios (incluyendo cualquier información en los campos *De*, *CC* y *BCC*) no pueden ser cifrados y serán enviados en texto claro. Para garantizar la privacidad y la seguridad del intercambio de correo electrónico, el asunto o título del correo electrónico debe mantenerse sin descripción para no revelar información sensible. Además, se recomienda colocar todas las direcciones en el campo *BCC* cuando se envían correos electrónicos a un grupo de personas.

Cuando se cifran mensajes de correo electrónico con archivos adjuntos, se recomienda utilizar la opción PGP/MIME, pues este extenderá el cifrado para incluir cualquier archivo adjunto al correo electrónico.

1. Para comenzar, ejecutar *Redactar* para redactar el mensaje y a continuación el botón OpenPGP de la barra de menú para activar la siguiente ventana:

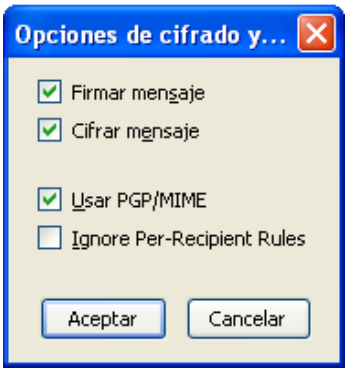
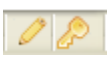


Figura 75: Opciones de cifrado y Firma.

Habilitando estas opciones, es posible comenzar enviar correo firmado y/o cifrado según se requiera.

2. Para validar que el mensaje es tanto cifrado como firmado, se verifica que los siguientes dos íconos aparezcan en la esquina inferior derecha del panel del mensaje como se muestra a continuación: 

3. Pulsar *Enviar* para enviar el mensaje. Se le solicita una contraseña para utilizar la clave privada para firmar el mensaje:

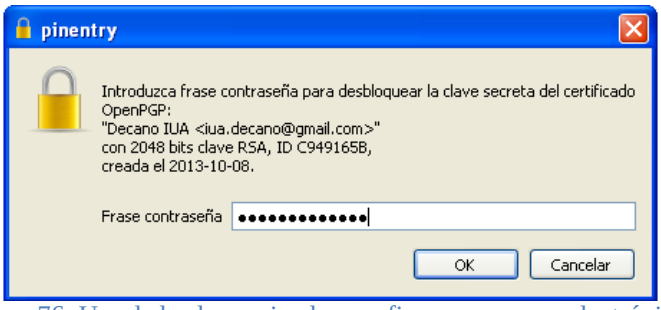


Figura 76: Uso de la clave privada para firmar un correo electrónico.

4. A su vez, al recibir y abrir un mensaje cifrado, automáticamente se intenta descifrarlo y se solicita la clave privada, en este caso la de receptor:

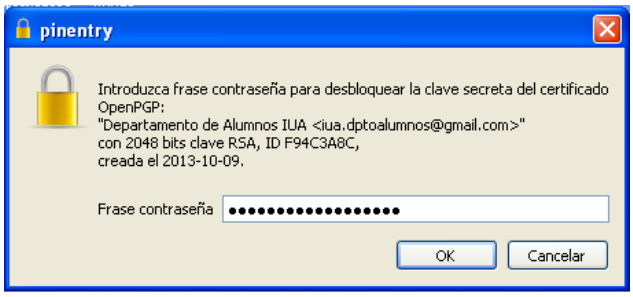


Figura 77: Uso de la clave privada para descifrar un correo electrónico.

5. Una vez ingresada la clave, el mensaje se descifra como se muestra a continuación:

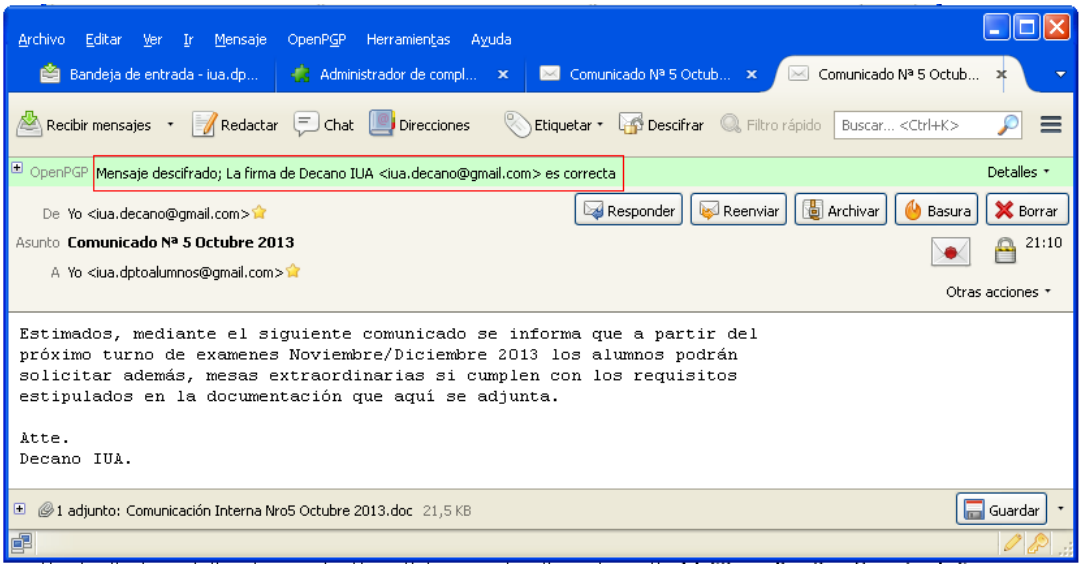


Figura 78: Correo electrónico descifrado correctamente con Firma Digital verificada.

Como se podrá visualizar en la parte superior se indica que el mensaje ha sido descifrado y que la firma del emisor es correcta, es decir, que ha sido validada con éxito.

5. Concreción del Modelo

6. Al realizar click en el icono del sobre a la izquierda se informa lo siguiente:

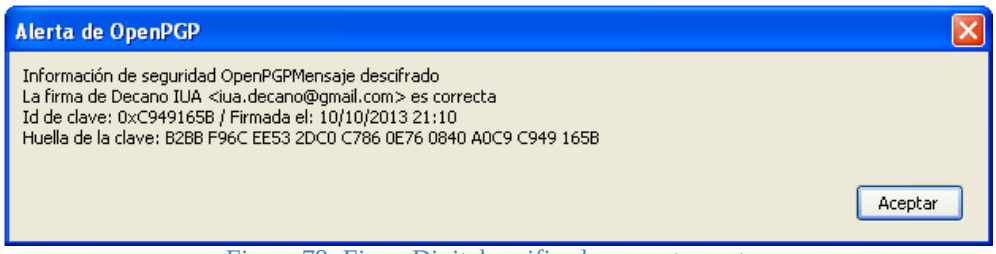


Figura 79: Firma Digital verificada correctamente.

De este modo, cada vez que se intercambian mensajes de correo electrónico, será posible mantener un canal de comunicación privado, autenticado, independientemente de quien podría estar intentando vigilar el intercambio de mensajes.

Finalmente, es posible recibir un mensaje firmado por ejemplo cuya firma no se haya comprobado como se muestra a continuación:

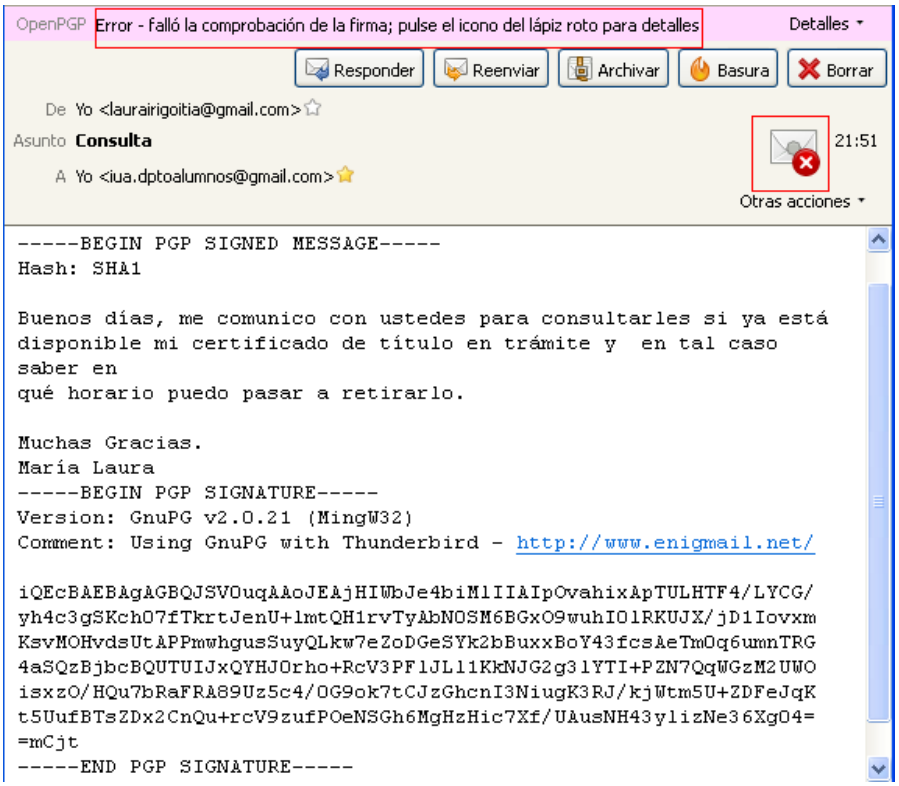


Figura 80: Error al verificar la Firma Digital.

Al hacer click en el icono con el mensaje roto, se muestra el siguiente mensaje indicando que en este caso la comprobación de la firma ha fallado:

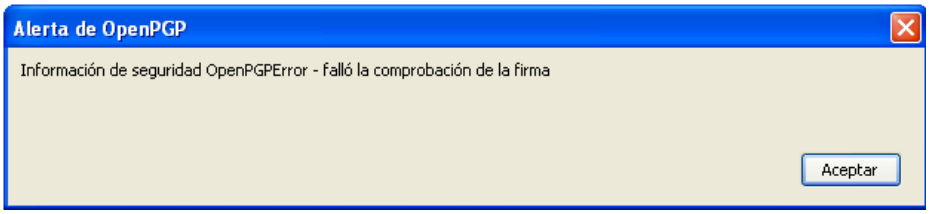


Figura 81: Información de Seguridad: fallo en la comprobación de la firma.

Este fallo en la comprobación sucederá cuando se reciban mensajes de un emisor del cual no se dispone su clave pública.

5.4. Puesta en Marcha

Se desarrollarán a continuación, las principales acciones a realizar para que el modelo propuesto sea aplicado a la realidad.

5.4.1. Infraestructura necesaria

Para configurar el servidor de claves públicas se utilizará el Sistema Operativo Linux distribución Ubuntu Server 12.04.3.

Por lo tanto, los requerimientos de hardware dependen directamente del Sistema Operativo a utilizar. En este caso, Ubuntu Server Edition está pensado para funcionar en cualquier procesador Intel o AMD x86, AMD_64, EM_64T. Se requiere un mínimo de 192 MB de RAM y 1 GB de espacio en disco.

Los requerimientos necesarios para la utilización de Gpg4win son los siguientes:

- Sistema operativo Windows 2000, XP, 7 y 10. Funciona en sistemas de 32 y 64 bits.
- El plugin para Outlook GpgOL con compatible con Microsoft Outlook .
- En la actualidad, el plugin para Explorer GpgEX sólo funciona con la versión de 32 bits.

Los requerimientos necesarios para la utilización de Mozzilla Thunderbird son los siguientes:

- Procesador: Pentium 233 MHz (Pentium 500 MHz o más rápido).
- Para Windows 10/7/Vista/XP 768MB RAM.
- Para Windows 2000 256 MB de RAM.
- Disco duro: 52 MB de espacio libre en disco duro.
- El plugin Enigmail.

5.4.2. Capacitación a usuarios

Los usuarios recibirán una capacitación acerca de la implementación de Firma Digital, en donde podrán visualizar el proceso y así comprender cómo utilizar el nuevo mecanismo.

Además, se informará y se capacitará sobre la correcta utilización de claves públicas y privadas y la importancia de uso adecuado.

Se buscará lograr el menor impacto posible en las tareas de los usuarios, en pos de lograr que los mismos puedan interactuar y adaptarse de forma efectiva a la nueva plataforma de Firma Digital.

5.5. Prefactibilidad

Una vez planteado el desarrollo del proyecto, resulta necesario un análisis de prefactibilidad, teniendo en cuenta los siguientes aspectos: técnico, operacional y económico.

5.5.1. Prefactibilidad Técnica

Se realizó un análisis y una evaluación de los recursos tecnológicos disponibles actualmente en la organización, a fin de definir si estos son suficientes y determinar la necesidad de adquirir nuevas tecnologías para poder llevar adelante la implementación y puesta en marcha del proyecto.

En relación al software, las estaciones de trabajo de los usuarios operan bajo el sistema operativo Windows las cuales cuentan con las herramientas de escritorio necesarias para la adecuada realización de las actividades diarias. Para el caso del servidor se requerirá el sistema operativo Linux.

En lo referente al hardware, además del equipamiento que se encuentra en la Institución, será necesario adquirir otras tecnologías para el correcto desarrollo, puesta en marcha y funcionamiento del proyecto.

Cantidad	Descripción
1	HP Proliant DL580 G7
1	Unidad de Cinta SDLT 600 Quantum
1	APC Smart-UPS RT 1000VA 230V
10	Token USB MS-ID Protect

Tabla 7: Insumos requeridos.

De este modo, en base al análisis realizado se determina que el proyecto es factible desde el punto de vista de lo tecnológico.

5.5.2. Prefactibilidad Operativa

Resulta necesario realizar un estudio de prefactibilidad operativa a fin de definir la posibilidad de éxito que tendrá el proyecto al momento de ser implementado y operado por el personal de la organización.

Así, a partir de este estudio, es posible prever que el sistema será utilizado y operado correctamente por los usuarios involucrados, los cuales aprovecharán las mejoras y los beneficios que el mismo generará en el desarrollo de sus actividades cotidianas.

Se refleja una necesidad evidente de actualización y mejora en los procesos surgida a partir de los avances tecnológicos, que actualmente permiten reemplazar la firma hológrafa por la Firma Digital, brindando la posibilidad de utilizar el formato electrónico en los procesos administrativos de la Institución. A partir de lo cual, los usuarios harán uso y dispondrán de los consiguientes beneficios que se desprenden de las características de garantía de

autoría e integridad de los documentos digitales, el sustento legal de los mismos y de un conveniente mecanismo de seguridad informática.

Vale destacar que, la implementación de este proyecto permitirá contribuir con el proceso de "despapelización", reduciendo así la cantidad de archivos, ganando espacios y facilitando disponibilidad de cada documento cuando se requiera; a la vez de contribuir con el medio ambiente, minimizando el costo del uso del papel.

Finalmente, para poder garantizar el efectivo funcionamiento de este sistema de Firma Digital, de modo tal que sea aceptado por los usuarios finales, se realizarán capacitaciones para dar conocer el nuevo mecanismo y generar una herramienta de trabajo útil y amigable al usuario.

5.5.3. Prefactibilidad Económica

Conforme al estudio realizado acerca de la prefactibilidad económica para implementar el proyecto, se expone a continuación el análisis de costos y beneficios, donde se determinan los recursos necesarios para desarrollar, implementar y mantener el proyecto; evaluando los costos requeridos pero atendiendo, a su vez, a los beneficios derivados de su ejecución.

5.5.3.1. Análisis costo beneficio del sistema propuesto

El proyecto propuesto involucra los siguientes costos:

- **Costos generales**

La reformulación de los procesos, en base a esta nueva tecnología, supone una optimización de los mismos, mejorando los tiempos de respuesta de entrega de documentos, reduciendo la cantidad de tareas realizadas, mejorando de este modo las condiciones de trabajo y aumentando la eficiencia en el tratamiento de los procesos. Permitiendo, así mismo, el ahorro de recursos, aprovechando las ventajas de perdurabilidad de los documentos en soporte digital y la consiguiente disminución de la necesidad de espacio y/o volumen físico requerido; además de la preservación del medio ambiente derivada del menor consumo de papel y el consumo eléctrico producto del menor uso de fotocopiadoras e impresoras.

Se puede estimar así que, el uso de la documentación en papel se reduciría de forma significativa, brindando los beneficios ya mencionados, a la vez de posibilitar las ventajas que se desprenden de trabajar con documentación electrónica, la cual puede ser consultada de forma confiable, optima y oportuna, cada vez que el personal lo requiera. Permitiendo, además, que dichos documentos puedan ser firmados y enviados por mail desde cualquier punto geográfico, sin la obligación de presentar el documento físico firmado y, finalmente, brindando un mayor y mejor control del uso de los mismos.

- **Costos de hardware**

Acorde a lo expuesto en el estudio de prefactibilidad técnica, resulta necesario la realización de una inversión en equipamiento tecnológico para llevar adelante la puesta en marcha del proyecto.

A continuación, se detallan los costos en dólares:

Cantidad	Descripción	Precio US$
1	HP Proliant DL580 G7	**2649.99**
1	Unidad de Cinta SDLT 600 Quantum	**485**
1	APC Smart-UPS RT 1000VA 230V	**522.99**
10	Token USB MS-ID Protect	**350**
		TOTAL: US$4007.98

Tabla 8: Costos de Hardware.

- **Costo de personal**

Para llevar adelante las diferentes etapas del el presente proyecto, se requirió de personal capacitado, para lo cual se calcula a continuación los costos de personal en pesos argentinos.

Dichos costos hacen mención: al personal por hora para realización de las etapas referentes al modelo teórico y concreción de modelo. El cálculo está basado en 4 horas hombre por día, 5 días a la semana. Las estimaciones, tanto de costos como de tiempo, fueron realizadas en función de las horas hombre que se ocupa para cada tarea, tanto

incorporar software, hardware, desarrollar el sistema, como así también mantenerlo en funcionamiento.

Actividad	Profesional	Costo$/hs	Horas	Total AR$
Planificación	Analista de Proyectos	320	40	12800
Análisis de Requerimientos	Analista	250	40	10000
Análisis de Sistemas	Analista	250	80	20000
Diseño de Sistemas	Analista	250	140	35000
Implementación	Desarrollador	192	120	23040
Capacitación de usuarios	Instructor	170	8	1360
		TOTAL	**405 hs**	**$102200 US$7248.23**

Tabla 9: Costos de Personal.

A partir del mencionado análisis de costos, se deduce que el costo Total del sistema expresado en dólares es: **US$11256.21**, tomando como referencia el precio del dólar a $14.10.

5.5.3.2. Análisis costo-beneficios

A continuación se expone la evaluación económica del proyecto, la cual constituye un balance de las ventajas y desventajas asignadas al mismo, analizando los recursos definidos para su realización:

PERIODOS	**0**	**1**	**2**	**3**
INGRESOS				
Reducción de costos de papelería e insumos de librería		$ 154.088,00	$ 195.691,76	$ 248.527,78
Reducción del consumo eléctrico derivado del uso de impresoras y fotocopiadoras		$ 16.500,00	$ 20.955,00	$ 26.612,85
Reducción de mobiliario para almacenamiento		$ 55.479,90	$ 70.459,47	$ 89.483,53
Total Ingresos PESOS		$ 226.067,90	$ 287.106,23	$ 364.624,16
Total Ingresos Dólares		**U$s 16.033,18**	**U$s 20.362,14**	**U$s 25.859,87**
EGRESOS				
Recursos Humanos		$ 140.800,00	$ 178.816,00	$ 227.096,00
Total Egresos PESOS		$ 140.800,00	$ 178.816,00	$ 227.096,00
Total Egresos Dólares		**U$s 9.985,82**	**U$s 12.681,99**	**U$s 16.106,09**
INVERSION INICIAL				
Costos de Hardware	$ 4.007,98			
Costos de Personal	$ 7.248,23			
Total Costos Dólares	**U$s 11.256,21**			
Total Costos PESOS	$ 158.712,56			
FFN	-U$s 11.256,21	U$s 6.047,36	U$s 7.680,15	U$s 9.753,78

Cálculos del Proyecto:	
Tasa de Descuento (Incluye la inflación anual)	**37%**
Tasa de inflación anual promedio	**27%**

Tasa Interna de Retorno (TIR)	**43%**			
Valor Actual Neto (VAN)	**U$s 1.043,10**			
VAN Períodico	U$s 1.043,10	U$s 4.414,13	U$s 4.091,93	U$s 3.793,25
Periodo de Recupero Actualizado	-U$s 11.256,21	-U$s 6.842,08	-U$s 2.750,15	U$s 1.043,10
Periodo de Recupero Sin Actualizar	-U$s 11.256,21	-U$s 5.208,85	U$s 2.471,30	U$s 12.225,08
Periodo Recupero Inversión (PRI)	**2**			
Beneficios	U$s 0,00	U$s 11.703,05	U$s 10.848,81	U$s 10.056,91
Costos	U$s 11.256,21	U$s 7.288,92	U$s 6.756,88	U$s 6.263,66
Relación Beneficio/Costo (B/C)	**1,03**			
Rentabilidad Inmediata (RI)	**0,54**			

Tabla 10: Evaluación Económica.

La valoración económica se realizó teniendo en cuenta los distintos indicadores, aquí reflejados, que ayudan a determinar la viabilidad del proyecto.

A partir este análisis, se desprende que los costos iniciales se recuperarán en el segundo año de implementación del proyecto (Periodo de Recupero de la Inversión). Así mismo, teniendo en cuenta los valores arrojados por el VAN y la TIR, es posible afirmar que el proyecto es económicamente viable y conveniente. Por otro lado, dada la relación Beneficio/Costo, se deduce que los beneficios (ingresos) son mayores a los costos (egresos) y, en consecuencia, el proyecto es rentable y generará un beneficio para la Institución.

- Beneficios tangibles

Los beneficios tangibles que se obtienen mediante la implementación son los siguientes:

- Reducción de costos de papelería e insumos de librería.
- Mejora en los tiempos de respuesta y procesamiento de documentos.
- Seguridad y privacidad en la información con la que se trabaja.
- Aumento en la velocidad de consulta, búsqueda de información de forma más oportuna.
- Mejora en la productividad laboral; es posible realizar más actividades como consecuencia de la reducción de tareas que poseen un alto grado de consulta sobre papel y un alto consumo de tiempo. Esto posibilita a cada usuario el poder organizar su trabajo y automatizar las tareas que requieran manipular información.
- Reducción del uso de carpetas, archivadores y registros, generando así ganancia de espacios.
- Reducción del consumo eléctrico derivado del uso de impresoras y fotocopiadoras

- Beneficios intangibles

Se pueden destacar los siguientes beneficios intangibles:

- Brindar una mayor flexibilidad y rapidez para gestionar la información, lo que ofrece a su vez una mejora en las herramientas de trabajo del usuario.
- Permitir una administración más efectiva de la información, posibilitando trabajar con documentos más ordenados y almacenados de forma oportuna, confiable y segura.
- Generar información con mayor confiabilidad y seguridad, lo que ayuda a la toma de decisiones.
- Depurar la información en papel, eliminando duplicados, hojas no necesarias, etc.

5. Concreción del Modelo

- Aumentar la reputación e imagen de la Universidad al implementar el uso de la Firma Digital en sus procesos

- Ayudar al medio ambiente, reduciendo el uso de papel.

Analizando los costos-beneficios que se desprenden de la implementación del presente proyecto, es posible afirmar que la puesta en marcha del mismo supone un impacto positivo para esta Institución, brindando las importantes ventajas que han sido valoradas oportunamente durante el desarrollo de esta investigación.

6. Conclusiones

Concluida la etapa final del presente proyecto, es posible considerar y valorar el alcance de los objetivos planteados en la etapa inicial:

- La investigación, el análisis y la fundamentación en las bases teóricas, han servido de base para llevar adelante el desarrollo del proyecto, permitiendo conocer y profundizar en el concepto de Firma Digital, certificados digitales, su situación actual, usos y aplicaciones.
- La recopilación información basada en los avances tecnológicos, procedimientos vigentes, y la valoración de diversos trabajos implementados con éxito en distintos ámbitos, posibilitó obtener un conocimiento más profundo y acabado de las prácticas que permiten aprovechar y desarrollar el potencial de Firma Digital como base para el diseño de soluciones que satisfacen diversas necesidades, las cuales sirvieron como referentes para el presente proyecto.
- Mediante la investigación teórica y el análisis de la Infraestructura de Firma Digital, algoritmos y estándares tecnológicos, los requisitos legales exigidos por las leyes vigentes, procedimientos de seguridad y herramientas disponibles en el mercado, ha sido posible elaborar una estrategia de diseño e implantación de Firma Digital, como medida de seguridad para la autenticación de documentos electrónicos firmados por el personal y las autoridades del IUA.
- A partir de dicho diseño, se procedió a la concreción del modelo; realizando el despliegue, mediante la configuración de un servidor de claves para la generación y el almacenamiento de las mismas, su distribución y la simulación de los procesos que involucran la Firma Digital de documentos y correos electrónicos en el ámbito de la Institución. Permitiendo agilizar la burocracia de algunos procesos administrativos existentes, garantizando la autenticidad del firmante e integridad de los datos y replanteando la forma en el que se desarrollan las tareas.

De este modo, se ha cumplimentado con el objetivo principal de este proyecto, planteando un modelo teórico para la implantación de la Firma Digital en el IUA, considerando los beneficios a largo plazo, dado al elevado nivel de seguridad que otorga. Justificando de este modo la inversión y valorando así esta potente herramienta, como la vía más apropiada para garantizar la autoría e integridad de los documentos digitales, posibilitando que éstos gocen de una característica que únicamente era propia

de los documentos en papel, que es la garantía de identidad sobre la base de un sustento legal.

7. Bibliografía

- [1] William Stallings - Fundamentos de Seguridad en Redes, Aplicaciones y Estándares, Segunda Edición Año 2003, Editorial Prentice Hall.
- [2] William Stallings - Cryptography and Network Security Principles and Practices, Fifth Edition Año 2010, Editorial Prentice Hall.
- [3] Manuel J. Lucena López - Criptografía a y Seguridad en Computadores, Tercera Edición, Marzo de 2002.
- [4] A. Menezes, P. van Oorschot, and S. Vanstone - Handbook of Applied Cryptography, Editorial CRC Press, Año 1996.
- [5] ChristofPaar y Jan Pelzl - Understanding Cryptography: A Textbook for Students and Practitioners, First Edition Año 2010, Editorial Springer.
- 6] Jonathan Katz - Digital Signatures (Advances in Information Security), Second Edition Año 2010, Editorial Springer.
- [7] Joshua Davies - Implementing SSL / TLS Using Cryptography and PKI, First Edition Año 2011, Editorial WiLey Publishing Inc.
- [8] Firma Digital Argentina – Firma Digital - https://pki.jgm.gov.ar
- [9] Sistema Nacional de Certificación Digital - http://www.firmadigital.go.cr
- [10] ACraíz – Solicitud de Licenciamiento - https://www.acraiz.gob.ar/
- [11] InfoLEG – Información Legistativa - http://www.infoleg.gov.ar/
- [12] VeriSign – Funcionamiento de la firma de código:http://www.verisign.es/code-signing/information-center/how-code-signing-works/index.html

8. Anexos

Anexo 1: Ley Nacional Nº 25.506 – Leyes de Firma Digital Infraestructura de Firma Digital (Boletín Oficial del 14/12/2001)

La Ley Nº 25.506 establece una Infraestructura de Firma Digital de alcance federal. La norma deroga el Decreto Nº 427/98, por cuanto cubre sus objetivos y alcance. A partir de la puesta en vigencia de la Ley y su decreto reglamentario, corresponderá establecer la IFDRA para la Administración Pública Nacional, creada por el Decreto 427/98, dentro de los términos fijados por la nueva legislación.

La normativa establece la configuración de la siguiente estructura:

- **Autoridad de Aplicación:** es la Jefatura de Gabinete de Ministros, quien estará facultada a establecer las normas y procedimientos técnicos necesarios para la efectiva implementación de la Ley.
- **Comisión Asesora para la Infraestructura de Firma Digital:** funcionará en el ámbito de la Jefatura de Gabinete de Ministros, emitiendo recomendaciones sobre los aspectos técnicos referidos al funcionamiento de la Infraestructura de Firma Digital.
- **Ente Administrador de Firma Digital:** es el órgano técnico-administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad.
- **Certificadores licenciados:** son aquellas personas de existencia ideal, registro público de contratos u organismo público que obtengan una licencia emitida por el ente administrador para actuar como proveedores de servicios de certificación en los términos de la Ley Nº 25.506 y su decreto reglamentario.
- **Autoridades de Registro:** son entidades que tienen a su cargo las funciones de validación de la identidad y otros datos de los suscriptores de certificados. Dichas funciones son delegadas por el certificador licenciado.
- **Sistema de Auditoría:** será establecido por la autoridad de aplicación, a fin de evaluar la confiabilidad y calidad de los sistemas utilizados por los certificadores licenciados.

La Subsecretaría de la Gestión Pública pone a disposición pública una Autoridad Certificante gratuita a través de la cual se podrá obtener un certificado digital propio.

Utilizando este certificado el usuario podrá asegurar todas sus comunicaciones de correo electrónico, garantizando su autoría y la integridad del mensaje.

Para optimizar el proceso de difusión de la tecnología de Firma Digital, se ha implementado un Laboratorio de Firma Digital, donde el público en general, y particularmente los funcionarios y agentes de la Administración Pública Nacional, experimenten la generación de un par de claves, la gestión de su propio certificado y el envío de correo electrónico firmado, al tiempo de ofrecerse información diversa sobre esta tecnología.

Contenido de la Ley de Firma Digital

Consideraciones generales. Certificados digitales. Certificador licenciado. Titular de un certificado digital. Organización institucional. Autoridad de aplicación. Sistema de auditoría. Comisión Asesora para la Infraestructura de Firma Digital. Responsabilidad. Sanciones. Disposiciones Complementarias.

Sancionada: Noviembre 14 de 2001.

Promulgada de Hecho: Diciembre 11 de 2001.

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

LEY DE FIRMA DIGITAL

CAPITULO I

Consideraciones generales

ARTICULO 1º — Objeto. Se reconoce el empleo de la firma electrónica y de la Firma Digital y su eficacia jurídica en las condiciones que establece la presente Ley.

ARTICULO 2º — Firma Digital. Se entiende por Firma Digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La Firma Digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación

simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

ARTICULO 3º — Del requerimiento de firma. Cuando la Ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una Firma Digital. Este principio es aplicable a los casos en que la Ley establece la obligación de firmar o prescribe consecuencias para su ausencia.

ARTICULO 4º — Exclusiones. Las disposiciones de esta Ley no son aplicables:

a) A las disposiciones por causa de muerte;

b) A los actos jurídicos del derecho de familia;

c) A los actos personalísimos en general;

d) A los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la Firma Digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes.

ARTICULO 5º — Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada Firma Digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

ARTICULO 6º — Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.

ARTICULO 7º — Presunción de autoría. Se presume, salvo prueba en contrario, que toda Firma Digital pertenece al titular del certificado digital que permite la verificación de dicha firma.

ARTICULO 8º — Presunción de integridad. Si el resultado de un procedimiento de verificación de una Firma Digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.

ARTICULO 9º — Validez. Una Firma Digital es válida si cumple con los siguientes requisitos:

a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante;

b) Ser debidamente verificada por la referencia a los datos de verificación de Firma Digital indicados en dicho certificado según el procedimiento de verificación correspondiente;

c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado.

ARTICULO 10. — Remitente. Presunción. Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la Firma Digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente.

ARTICULO 11. — Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.

ARTICULO 12. — Conservación. La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.

CAPITULO II

De los certificados digitales

ARTICULO 13. — Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

ARTICULO 14. — Requisitos de validez de los certificados digitales. Los certificados digitales para ser válidos deben:

a) Ser emitidos por un certificador licenciado por el ente licenciante;

b) Responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación, y contener, como mínimo, los datos que permitan:

1. Identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;

2. Ser susceptible de verificación respecto de su estado de revocación;

3. Diferenciar claramente la información verificada de la no verificada incluidas en el certificado;

4. Contemplar la información necesaria para la verificación de la firma;

5. Identificar la política de certificación bajo la cual fue emitido.

ARTICULO 15. — Período de vigencia del certificado digital. A los efectos de esta Ley, el certificado digital es válido únicamente dentro del período de vigencia, que comienza en la fecha de inicio y finaliza en su fecha de vencimiento, debiendo ambas ser indicadas en el certificado digital, o su revocación si fuere revocado.

La fecha de vencimiento del certificado digital referido en el párrafo anterior en ningún caso puede ser posterior a la del vencimiento del certificado digital del certificador licenciado que lo emitió.

La Autoridad de Aplicación podrá establecer mayores exigencias respecto de la determinación exacta del momento de emisión, revocación y vencimiento de los certificados digitales.

ARTICULO 16. — Reconocimiento de certificados extranjeros. Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la Ley y sus normas reglamentarias cuando:

a) Reúnan las condiciones que establece la presente Ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o

b) Tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente Ley. A fin de tener efectos, este reconocimiento deberá ser validado por la autoridad de aplicación.

CAPITULO III

Del certificador licenciado

ARTICULO 17. — Del certificador licenciado. Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la Firma Digital y cuenta con una licencia para ello, otorgada por el ente licenciante.

La actividad de los certificadores licenciados no pertenecientes al sector público se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos.

ARTICULO 18. — Certificados por profesión. Las entidades que controlan la matrícula, en relación a la prestación de servicios profesionales, podrán emitir certificados digitales en lo referido a esta función, con igual validez y alcance jurídico que las firmas efectuadas en forma manuscrita. A ese efecto deberán cumplir los requisitos para ser certificador licenciado.

ARTICULO 19. — Funciones. El certificador licenciado tiene las siguientes funciones:

a) Recibir una solicitud de emisión de certificado digital, firmada digitalmente con los correspondientes datos de verificación de Firma Digital del solicitante;

b) Emitir certificados digitales de acuerdo a lo establecido en sus políticas de certificación, y a las condiciones que la autoridad de aplicación indique en la reglamentación de la presente Ley;

c) Identificar inequívocamente los certificados digitales emitidos;

d) Mantener copia de todos los certificados digitales emitidos, consignando su fecha de emisión y de vencimiento si correspondiere, y de sus correspondientes solicitudes de emisión;

e) Revocar los certificados digitales por él emitidos en los siguientes casos, entre otros que serán determinados por la reglamentación:

1) A solicitud del titular del certificado digital.

2) Si determinara que un certificado digital fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.

3) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.

4) Por condiciones especiales definidas en su política de certificación.

5) Por resolución judicial o de la autoridad de aplicación.

f) Informar públicamente el estado de los certificados digitales por él emitidos. Los certificados digitales revocados deben ser incluidos en una lista de certificados revocados indicando fecha y hora de la revocación. La validez y autoría de dicha lista de certificados revocados deben ser garantizadas.

ARTICULO 20. — Licencia. Para obtener una licencia el certificador debe cumplir con los requisitos establecidos por la Ley y tramitar la solicitud respectiva ante el ente licenciante, el que otorgará la licencia previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones. Estas licencias son intransferibles.

ARTICULO 21. — Obligaciones. Son obligaciones del certificador licenciado:

a) Informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus

características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorga el ente licenciante. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;

b) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de Firma Digital de los titulares de certificados digitales por él emitidos;

c) Mantener el control exclusivo de sus propios datos de creación de Firma Digital e impedir su divulgación;

d) Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación;

e) Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y las obligaciones que asume por el solo hecho de ser titular de un certificado digital;

f) Recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;

g) Mantener la confidencialidad de toda información que no figure en el certificado digital;

h) Poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación;

i) Mantener la documentación respaldatoria de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación;

j) Incorporar en su política de certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la autoridad de aplicación;

k) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados

digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación;

l) Publicar en el Boletín Oficial aquellos datos que la autoridad de aplicación determine;

m) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;

n) Informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular;

o) Verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales;

p) Solicitar inmediatamente al ente licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de Firma Digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de Firma Digital en él contenidos hayan dejado de ser seguros;

q) Informar inmediatamente al ente licenciante sobre cualquier cambio en los datos relativos a su licencia;

r) Permitir el ingreso de los funcionarios autorizados de la autoridad de aplicación, del ente licenciante o de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso;

s) Emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la Firma Digital y experiencia adecuada en los procedimientos de seguridad pertinentes;

t) Someter a aprobación del ente licenciante el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;

u) Constituir domicilio legal en la República Argentina;

v) Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente Ley y su reglamentación;

w) Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el ente licenciante.

ARTICULO 22. — Cese del certificador. El certificador licenciado cesa en tal calidad:

a) Por decisión unilateral comunicada al ente licenciante;

b) Por cancelación de su personería jurídica;

c) Por cancelación de su licencia dispuesta por el ente licenciante.

La autoridad de aplicación determinará los procedimientos de revocación aplicables en estos casos.

ARTICULO 23. — Desconocimiento de la validez de un certificado digital. Un certificado digital no es válido si es utilizado:

a) Para alguna finalidad diferente a los fines para los cuales fue extendido;

b) Para operaciones que superen el valor máximo autorizado cuando corresponda;

c) Una vez revocado.

CAPITULO IV

Del titular de un certificado digital

ARTICULO 24. — Derechos del titular de un certificado digital. El titular de un certificado digital tiene los siguientes derechos:

a) A ser informado por el certificador licenciado, con carácter previo a la emisión del certificado digital, y utilizando un medio de comunicación sobre las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de este sistema de licenciamiento y los procedimientos asociados. Esa información deberá darse

por escrito en un lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;

b) A que el certificador licenciado emplee los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por él, y a ser informado sobre ello;

c) A ser informado, previamente a la emisión del certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago;

d) A que el certificador licenciado le informe sobre su domicilio en la República Argentina, y sobre los medios a los que puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;

e) A que el certificador licenciado proporcione los servicios pactados, y a no recibir publicidad comercial de ningún tipo por intermedio del certificador licenciado.

ARTICULO 25. — Obligaciones del titular del certificado digital. Son obligaciones del titular de un certificado digital:

a) Mantener el control exclusivo de sus datos de creación de Firma Digital, no compartirlos, e impedir su divulgación;

b) Utilizar un dispositivo de creación de Firma Digital técnicamente confiable;

c) Solicitar la revocación de su certificado al certificador licenciado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;

d) Informar sin demora al certificador licenciado el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

CAPITULO V

De la organización institucional

ARTICULO 26. — Infraestructura de Firma Digital. Los certificados digitales regulados por esta Ley deben ser emitidos o reconocidos, según lo establecido por el artículo 16, por un certificador licenciado.

ARTICULO 27. — Sistema de Auditoría. La autoridad de aplicación, con el concurso de la Comisión Asesora para la Infraestructura de Firma Digital, diseñará un sistema de auditoría para evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el ente licenciante.

ARTICULO 28. — Comisión Asesora para la Infraestructura de Firma Digital. Créase en el ámbito jurisdiccional de la Autoridad de Aplicación, la Comisión Asesora para la Infraestructura de Firma Digital.

*(**Nota Infoleg**: Por art. 8° del Decreto N° 624/2003 B.O. 22/8/2003 se establece que la Comisión creada por el presente artículo actuará en la órbita de la SUBSECRETARIA DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS.)*

CAPITULO VI

De la autoridad de aplicación

ARTICULO 29. — Autoridad de Aplicación. La autoridad de aplicación de la presente Ley será la Jefatura de Gabinete de Ministros.

ARTICULO 30. — Funciones. La autoridad de aplicación tiene las siguientes funciones:

a) Dictar las normas reglamentarias y de aplicación de la presente;

b) Establecer, previa recomendación de la Comisión Asesora para la Infraestructura de la Firma Digital, los estándares tecnológicos y operativos de la Infraestructura de Firma Digital;

c) Determinar los efectos de la revocación de los certificados de los certificadores licenciados o del ente licenciante;

d) Instrumentar acuerdos nacionales e internacionales a fin de otorgar validez jurídica a las firmas digitales creadas sobre la base de certificados emitidos por certificadores de otros países;

e) Determinar las pautas de auditoría, incluyendo los dictámenes tipo que deban emitirse como conclusión de las revisiones;

f) Actualizar los valores monetarios previstos en el régimen de sanciones de la presente Ley;

g) Determinar los niveles de licenciamiento;

h) Otorgar o revocar las licencias a los certificadores licenciados y supervisar su actividad, según las exigencias instituidas por la reglamentación;

i) Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados;

j) Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la reglamentación;

k) Aplicar las sanciones previstas en la presente Ley.

ARTICULO 31. — Obligaciones. En su calidad de titular de certificado digital, la autoridad de aplicación tiene las mismas obligaciones que los titulares de certificados y que los certificadores licenciados. En especial y en particular debe:

a) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder, bajo ninguna circunstancia, a los datos utilizados para generar la Firma Digital de los certificadores licenciados;

b) Mantener el control exclusivo de los datos utilizados para generar su propia Firma Digital e impedir su divulgación;

c) Revocar su propio certificado frente al compromiso de la privacidad de los datos de creación de Firma Digital;

d) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos y direcciones de Internet tanto de los certificadores licenciados como los propios y su certificado digital;

e) Supervisar la ejecución del plan de cese de actividades de los certificadores licenciados que discontinúan sus funciones.

ARTICULO 32. — Arancelamiento. La autoridad de aplicación podrá cobrar un arancel de licenciamiento para cubrir su costo operativo y el de las auditorías realizadas por sí o por terceros contratados a tal efecto.

CAPITULO VII

Del sistema de auditoría

ARTICULO 33. — Sujetos a auditar. El ente licenciante y los certificadores licenciados, deben ser auditados periódicamente, de acuerdo al sistema de auditoría que diseñe y apruebe la autoridad de aplicación.

La autoridad de aplicación podrá implementar el sistema de auditoría por sí o por terceros habilitados a tal efecto. Las auditorías deben como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y, disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y, de contingencia aprobados por el ente licenciante.

ARTICULO 34. — Requisitos de habilitación. Podrán ser terceros habilitados para efectuar las auditorías las Universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales que acrediten experiencia profesional acorde en la materia.

CAPITULO VIII

De la Comisión Asesora para la Infraestructura de Firma Digital

ARTICULO 35.— Integración y funcionamiento. La Comisión Asesora para la IFDRA estará integrada multidisciplinariamente por un máximo de 7 (siete) profesionales de carreras afines a la actividad de reconocida trayectoria y experiencia, provenientes de Organismos del Estado nacional, Universidades Nacionales y Provinciales, Cámaras, Colegios u otros entes representativos de profesionales.

Los integrantes serán designados por el Poder Ejecutivo por un período de cinco (5) años renovables por única vez.

Se reunirá como mínimo trimestralmente. Deberá expedirse prontamente a solicitud de la autoridad de aplicación y sus recomendaciones y disidencias se incluirán en las actas de la Comisión.

Consultará periódicamente mediante audiencias públicas con las cámaras empresarias, los usuarios y las asociaciones de consumidores y mantendrá a la autoridad de aplicación regularmente informada de los resultados de dichas consultas.

ARTICULO 36. — Funciones. La Comisión debe emitir recomendaciones por iniciativa propia o a solicitud de la autoridad de aplicación, sobre los siguientes aspectos:

a) Estándares tecnológicos;

b) Sistema de registro de toda la información relativa a la emisión de certificados digitales;

c) Requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales de los términos de las políticas de certificación;

d) Metodología y requerimiento del resguardo físico de la información;

e) Otros que le sean requeridos por la autoridad de aplicación.

CAPITULO IX

Responsabilidad

ARTICULO 37. — Convenio de partes. La relación entre el certificador licenciado que emita un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la presente Ley, y demás legislación vigente.

ARTICULO 38. — Responsabilidad de los certificadores licenciados ante terceros.

El certificador que emita un certificado digital o lo reconozca en los términos del artículo 16 de la presente Ley, es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, por los errores u omisiones que presenten los

certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia.

ARTICULO 39. — Limitaciones de responsabilidad. Los certificadores licenciados no son responsables en los siguientes casos:

a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la Ley;

b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;

c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.

CAPITULO X

Sanciones

ARTICULO 40. — Procedimiento. La instrucción sumarial y la aplicación de sanciones por violación a disposiciones de la presente Ley serán realizadas por el ente licenciante. Es aplicable la Ley de Procedimientos Administrativos 19.549 y sus normas reglamentarias.

ARTICULO 41. — Sanciones. El incumplimiento de las obligaciones establecidas en la presente Ley para los certificadores licenciados dará lugar a la aplicación de las siguientes sanciones:

a) Apercibimiento;

b) Multa de pesos diez mil ($ 10.000) a pesos quinientos mil ($ 500.000);

c) Caducidad de la licencia.

Su gradación según reincidencia y/u oportunidad serán establecidas por la reglamentación.

El pago de la sanción que aplique el ente licenciante no relevará al certificador licenciado de eventuales reclamos por daños y perjuicios causados a terceros y/o bienes de propiedad de éstos, como consecuencia de la ejecución del contrato que celebren y/o por el incumplimiento de las obligaciones asumidas conforme al mismo y/o la prestación del servicio.

ARTICULO 42. — Apercibimiento. Podrá aplicarse sanción de apercibimiento en los siguientes casos:

a) Emisión de certificados sin contar con la totalidad de los datos requeridos, cuando su omisión no invalidare el certificado;

b) No facilitar los datos requeridos por el ente licenciante en ejercicio de sus funciones;

c) Cualquier otra infracción a la presente Ley que no tenga una sanción mayor.

ARTICULO 43. — Multa. Podrá aplicarse sanción de multa en los siguientes casos:

a) Incumplimiento de las obligaciones previstas en el artículo 21;

b) Si la emisión de certificados se realizare sin cumplimentar las políticas de certificación comprometida y causare perjuicios a los usuarios, signatarios o terceros, o se afectare gravemente la seguridad de los servicios de certificación;

c) Omisión de llevar el registro de los certificados expedidos;

d) Omisión de revocar en forma o tiempo oportuno un certificado cuando así correspondiere;

e) Cualquier impedimento u obstrucción a la realización de inspecciones o auditorías por parte de la autoridad de aplicación y del ente licenciante;

f) Incumplimiento de las normas dictadas por la autoridad de aplicación;

g) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de apercibimiento.

ARTICULO 44. — Caducidad. Podrá aplicarse la sanción de caducidad de la licencia en caso de:

a) No tomar los debidos recaudos de seguridad en los servicios de certificación;

b) Expedición de certificados falsos;

c) Transferencia no autorizada o fraude en la titularidad de la licencia;

d) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de multa;

e) Quiebra del titular.

La sanción de caducidad inhabilita a la titular sancionada y a los integrantes de órganos directivos por el término de 10 años para ser titular de licencias.

ARTICULO 45. — Recurribilidad. Las sanciones aplicadas podrán ser recurridas ante los Tribunales Federales con competencia en lo Contencioso Administrativo correspondientes al domicilio de la entidad, una vez agotada la vía administrativa pertinente.

La interposición de los recursos previstos en este capítulo tendrá efecto devolutivo.

ARTICULO 46. — Jurisdicción. En los conflictos entre particulares y certificadores licenciados es competente la Justicia en lo Civil y Comercial Federal. En los conflictos en que sea parte un organismo público certificador licenciado, es competente la Justicia en lo Contencioso-administrativo Federal.

CAPITULO XI

Disposiciones Complementarias

ARTICULO 47. — Utilización por el Estado Nacional. El Estado nacional utilizará las tecnologías y previsiones de la presente Ley en su ámbito interno y en relación con los administrados de acuerdo con las condiciones que se fijen reglamentariamente en cada uno de sus poderes.

ARTICULO 48. — Implementación. El Estado nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156, promoverá el uso masivo de la Firma Digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización.

En un plazo máximo de 5 (cinco) años contados a partir de la entrada en vigencia de la presente Ley, se aplicará la tecnología de Firma Digital a la totalidad de las Leyes, decretos, decisiones administrativas, resoluciones y sentencias emanados de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156.

ARTICULO 49. — Reglamentación. El Poder Ejecutivo deberá reglamentar esta Ley en un plazo no mayor a los 180 (ciento ochenta) días de su publicación en el Boletín Oficial de la Nación.

ARTICULO 50. — Invitación. Invítase a las jurisdicciones provinciales a dictar los instrumentos legales pertinentes para adherir a la presente Ley.

ARTICULO 51. — Equiparación a los efectos del derecho penal. Incorpórase el siguiente texto como artículo 78 (bis) del Código Penal:

Los términos firma y suscripción comprenden la Firma Digital, la creación de una Firma Digital o firmar digitalmente. Los términos documento, instrumento privado y certificado comprenden el documento digital firmado digitalmente.

ARTICULO 52. — Autorización al Poder Ejecutivo. Autorízase al Poder Ejecutivo para que por la vía del artículo 99, inciso 2, de la Constitución Nacional actualice los contenidos del Anexo de la presente Ley a fin de evitar su obsolescencia.

ARTICULO 53. — Comuníquese al Poder Ejecutivo.

DADA EN LA SALA DE SESIONES DEL CONGRESO ARGENTINO, EN BUENOS AIRES, A LOS CATORCE DIAS DEL MES DE NOVIEMBRE DEL AÑO DOS MIL UNO.

— REGISTRADA BAJO EL Nº 25.506 —

RAFAEL PASCUAL. — EDUARDO MENEM. — Guillermo Aramburu. — Juan C. Oyarzún.

ANEXO DE LA LEY

Información: conocimiento adquirido acerca de algo o alguien.

Procedimiento de verificación: proceso utilizado para determinar la validez de una Firma Digital. Dicho proceso debe considerar al menos:

a) que dicha Firma Digital ha sido creada durante el período de validez del certificado digital del firmante;

b) que dicha Firma Digital ha sido creada utilizando los datos de creación de Firma Digital correspondientes a los datos de verificación de Firma Digital indicados en el certificado del firmante;

c) la verificación de la autenticidad y la validez de los certificados involucrados.

Datos de creación de Firma Digital: datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear su Firma Digital.

Datos de verificación de Firma Digital: datos únicos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la Firma Digital, la integridad del documento digital y la identidad del firmante.

Dispositivo de creación de Firma Digital: dispositivo de hardware o software técnicamente confiable que permite firmar digitalmente.

Dispositivo de verificación de Firma Digital: dispositivo de hardware o software técnicamente confiable que permite verificar la integridad del documento digital y la identidad del firmante.

Políticas de certificación: reglas en las que se establecen los criterios de emisión y utilización de los certificados digitales.

Técnicamente confiable: cualidad del conjunto de equipos de computación, software, protocolos de comunicación y de seguridad y procedimientos administrativos relacionados que cumplan los siguientes requisitos:

1. Resguardar contra la posibilidad de intrusión y/o uso no autorizado;
2. Asegurar la disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento;
3. Ser apto para el desempeño de sus funciones específicas;
4. Cumplir las normas de seguridad apropiadas, acordes a estándares internacionales en la materia;
5. Cumplir con los estándares técnicos y de auditoría que establezca la Autoridad de Aplicación.

Clave criptográfica privada: En un criptosistema asimétrico es aquella que se utiliza para firmar digitalmente.

Clave criptográfica pública: En un criptosistema asimétrico es aquella que se utiliza para verificar una Firma Digital.

Integridad: Condición que permite verificar que una información no ha sido alterada por medios desconocidos o no autorizados.

Criptosistema asimétrico: Algoritmo que utiliza un par de claves, una clave privada para firmar digitalmente y su correspondiente clave pública para verificar dicha Firma Digital.

Anexo 2: Otras Normas y Decretos de interés

Decreto PEN Nº 901/2009 (16/07/2009)

Aprueba la nueva estructura organizativa de la Jefatura de Gabinete de Ministros y en particular, la de la Secretaría de la Gestión Pública. En su punto Nº 21 establece la competencia de la Secretaría para actuar como autoridad de aplicación del Régimen Normativo de la IFDRA (Ley Nº 25.506), como así también, en las funciones de ente licenciante de certificadores, supervisando su accionar. Entre los objetivos de la nueva Subsecretaría de Tecnologías de Gestión, establece su función de Autoridad Certificante de Firma Digital para el Sector Público Nacional.

Resolución JGM Nº 62/2008 (Boletín Oficial 14/11/2008)

Determina que la ONTI, con el concurso de la Dirección de Infraestructura y de Recursos Informáticos, emitirá el dictamen legal y técnico previo al licenciamiento de certificadores.

Resolución SGP N° 64/2007 (Boletín Oficial 20/11/2007)
Procedimientos operativos para la instalación y puesta en marcha de la Autoridad Certificante Raíz de la República Argentina.

Decisión Administrativa JGM Nº 06/2007 (Boletín Oficial12/02/2007)
Establece el marco normativo de Firma Digital aplicable al otorgamiento y revocación de las licencias a los certificadores que así lo soliciten.

Decreto PEN N° 724/2006 (13/06/2006)
Modifica el Decreto N° 2628/02 reglamentario de la Ley de Firma Digital.
Resolución JGM Nº 435/2004 (Boletín Oficial12/07/2004)
Aprueba el Reglamento de funcionamiento de la Comisión Asesora para la Infraestructura de Firma Digital, que fuera creada por la Ley N° 25.506 y cuyos miembros fueran designados por Decreto N° 160/04 del Poder Ejecutivo Nacional.

Decreto PEN Nº 160/2004 (06/02/2004)

Designa a los integrantes de la Comisión Asesora para la Infraestructura Nacional de Firma Digital, en cumplimiento de lo dispuesto en la Ley N° 25.506, los cargos duran, conforme al Artículo 35 de la Ley referida, 5 años y son renovables.

Resolución JGM Nº 20/2004 (Boletín Oficial 30/01/2004)

Asigna a la DIRECCIÓN DE APLICACIONES dependiente de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN la acción de asistir al Director de la Oficina en el cumplimiento de las obligaciones y funciones establecidas en los Artículos 13 y 14 del Decreto Nº 2628/2002, entre las cuales se encuentra la auditoría necesaria para el licenciamiento prevista en las normas técnicas de Firma Digital aprobadas por la Decisión Administrativa Nº 06/07. Esta norma está modificada por el Decreto 624/03.

Decreto PEN Nº 1028/2003 (10/11/2003)

Disuelve el Ente Administrador de Firma Digital, creado por el Artículo 11 del Decreto N° 2628/02, cuyo accionar será llevado a cabo por la Oficina Nacional de Tecnologías de Información de la Subsecretaría de la Gestión Pública. MODIFICATORIO del Decreto 624/03.

Decreto PEN Nº 624/2003 (22/08/2003)

Aprueba la estructura organizativa de primer nivel operativo de la Jefatura de Gabinete de Ministros.

Decreto PEN Nº 283/2003 (17/02/2003)

Autoriza con carácter transitorio a la Oficina Nacional de Tecnologías de Información a proveer certificados digitales para su utilización en aquellos circuitos de la Administración Pública Nacional que requieran Firma Digital, de acuerdo con la política de certificación vigente.

Decreto N° 2628/2002 - Reglamentario de la Ley de Firma Digital (Boletín Oficial del 20/12/2002)

El Decreto N° 2628/2002 reglamenta la Ley de Firma Digital y en su Anexo I define un importante Glosario:

- **Firma Electrónica:** Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizados

por el signatario como su medio de identificación, que carezca de algunos de los requisitos legales para ser considerada Firma Digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez (artículo 5°, Ley N° 25.506).

- **Firma Digital:** Se entiende por Firma Digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La Firma Digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital, posterior a su firma. Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes (artículo 2°, Ley N° 25.506).
- **Documento Digital o Electrónico:** Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte: utilizado para su fijación, almacenamiento archivo. Un documento digital también satisface el requerimiento de escritura (artículo 6°, Ley N° 25.506).
- **Certificado Digital:** Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (artículo 13, Ley N° 25.506).
- **Certificador Licenciado:** Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la Firma Digital y cuenta con una licencia para ello, otorgada por el ente licenciante. La actividad de los certificadores licenciados no pertenecientes al sector público se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos (artículo 17, Ley N° 25.506).
- **Política de Certificación:** Conjunto de criterios que indican la aplicabilidad de un certificado a un grupo de usuarios en particular o a un conjunto de aplicaciones con similares requerimientos de seguridad. En inglés Certification Policy (CP).

- **Manual de Procedimientos:** Conjunto de prácticas utilizadas por el certificador licenciado en la remisión y administración de los certificados. En inglés Certification Practice Statement (CPS).
- **Plan de Seguridad:** Conjunto de políticas, prácticas y procedimientos destinados a la protección; de los recursos del certificador licenciado.
- **Plan de Cese de Actividades:** conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios.
- **Plan de Contingencias:** Conjunto de procedimientos a seguir por el certificador licenciado ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones.
- **Lista de certificados revocados:** Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado, la cual ha sido firmada digitalmente y publicada por el mismo. En inglés Certificate Revocation List (CRL).
- **Certificación digital de fecha y hora:** Indicación de la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella.
- **Terceras partes confiables:** Entidades independientes que otorgan seguridad y confiabilidad al manejo de la información.
- **Proveedor de servicios de certificación digital:** Entidad que provee el servicio de emisión y administración de certificados digitales.
- **Homologación de dispositivos de creación y verificación de firmas digitales:** Proceso de comprobación efectuado para establecer la adecuación de los dispositivos a requerimientos mínimos establecidos.
- **Certificación de sistemas que utilizan Firma Digital:** Proceso de comprobación efectuado para establecer la adecuación de un sistema o aplicación a requerimientos mínimos establecidos.

Suscriptor o Titular de certificado digital: Persona a cuyo nombre se emite un certificado y posee una clave privada que se corresponde con la clave pública contenida en el mismo.

Disposición Nº 5/2002 AC-ONTI Documentación técnica de la Autoridad Certificante de la ONTI (26/4/2002).

Apruébense la "Política de Certificación: Criterios para el otorgamiento de certificados a favor de suscriptores", el "Manual de Procedimientos", el "Plan de Cese de Actividades" y la "Política de Seguridad" para la Autoridad Certificante de la Oficina Nacional de Tecnologías Informáticas.

Resolución JGM Nº 176/2002 (Boletín Oficial 15/4/2002)

Habilita en Mesa de Entradas de la Subsecretaría de la Gestión Pública el Sistema de Tramitación Electrónica para la recepción, emisión y archivo de documentación digital firmada digitalmente.

Resolución SGP Nº 17/2002 (Boletín Oficial 15/4/2002)

Establece el procedimiento para solicitar la certificación exigida al Registro del Personal acogido al Sistema de Retiro Voluntario, habilitando la modalidad de tramitación mediante el empleo de documentación digital firmada digitalmente.

Decreto PEN Nº 1023/2001 (16/08/2001)

En su artículo 21 permite la realización de las contrataciones comprendidas en el Régimen en formato digital firmado digitalmente.

Decreto PEN Nº 889/2001 (17/07/2001)

Aprueba la estructura organizativa de la Secretaría para la Modernización del Estado en el ámbito de la Subsecretaría de la Gestión Pública, creando la Oficina Nacional de Tecnologías de la Información y otorgándole competencias en materia de Firma Digital.

Decreto PEN Nº 677/2001 (28/05/2001)

Otorga a los documentos digitales firmados digitalmente remitidos a la Comisión Nacional de Valores de acuerdo a las reglamentaciones dictadas por ese organismo, similar validez y eficacia que los firmados en soporte papel.

Decreto PEN Nº 673/2001 (24/05/2001)

Crea la Secretaría para la Modernización del Estado en el ámbito de la Jefatura de Gabinete de Ministros, asignándole competencia para actuar como Autoridad de Aplicación del régimen normativo que establece la IFDRA para el Sector Público Nacional

y para la aplicación de nuevas tecnologías informáticas en la Administración Pública Nacional.

Ley Nº 25.237 (10/1/2000)

Establece en el artículo 61 que la SINDICATURA GENERAL DE LA NACION ejercerá las funciones de Organismo Auditante en el régimen de empleo de la Firma Digital en la instrumentación de los actos internos del Sector Público Nacional.

Resolución SFP Nº 212/98 (Boletín Oficial 06/01/1999)

Establece la Política de Certificación del Organismo Licenciante, en la cual se fijan los criterios para el licenciamiento de las Autoridades Certificantes de la Administración Pública Nacional.

Resolución SFP Nº 194/98 (Boletín Oficial 04/12/1998)

Establece los estándares sobre tecnología de Firma Digital para la Administración Pública Nacional.

Decreto PEN Nº 427/98 (21/04/1998)

Autoriza la utilización de la Firma Digital en la instrumentación de los actos internos del Sector Público Nacional, otorgándole los mismos efectos que la firma ológrafa y estableciendo las bases para la creación de la IFDRA para el Sector Público Nacional.

Resolución SFP Nº 45/97 (Boletín Oficial 24/03/1997)

Establece pautas técnicas para elaborar una normativa sobre Firma Digital que permita la difusión de esta tecnología en el ámbito de la Administración Pública Nacional.

Decisión JGM Nº 43/96 (Boletín Oficial 07/05/1996)

Reglamenta los archivos digitales. Establece como órgano rector a la Contaduría Gral. de la Nación.

Ley Nº 24.624 Artículo 30 (29/12/1995)

Autoriza el archivo y conservación en soporte electrónico u óptico indeleble de la documentación financiera, de personal y de control de la Administración Pública Nacional.

Anexo 3: Ley Provincial Nº 9401 Adhesión de la Provincia de Córdoba a la Ley Nacional Nº 25.506 sobre Firma Digital.

Fecha de Sanción: 04/07/2007.

Publicación: Boletín Oficial 19/07/2007.

Cantidad de Artículos: 04.

Cantidad de anexos: No posee.

La Legislatura de la Provincia de Córdoba sanciona con fuerza de Ley: 9401 Artículo 1º.- ADHIÉRESE la Provincia de Córdoba a la Ley Nacional Nº 25.506 "Ley de Firma Digital", en los términos del artículo 50 de dicho cuerpo legal. Artículo 2º.- EL Poder Ejecutivo determinará la Autoridad de Aplicación de la presente Ley dentro de la Administración Pública Provincial, la que tendrá a su cargo establecer los estándares tecnológicos y de seguridad correspondientes y la modalidad de obtención de los certificados digitales.

Artículo 3º.- AUTORÍZASE al Poder Ejecutivo Provincial a suscribir con los organismos correspondientes del Poder Ejecutivo Nacional los convenios y demás documentación necesaria a los fines de la implementación de la Firma Digital en el ámbito de la Provincia de Córdoba.

Artículo 4º.- COMUNÍQUESE al Poder Ejecutivo Provincial.

FORTUNA - ARIAS

TITULAR DEL PODER EJECUTIVO: DE LA SOTA.

DECRETO DE PROMULGACIÓN: Nº 1067/07.

Anexo 4: Aplicaciones en el Sector Público

A continuación se listan algunas aplicaciones de la tecnología de certificación digital en el ámbito público. Si bien algunas de ellas no constituyen una Firma Digital propiamente dicha, en los términos dispuestos por la normativa vigente, representan el aprovechamiento de las ventajas de esta herramienta, con las mismas seguridades desde la perspectiva técnica.

- **Registro de Reincidencias y Estadística Criminal del Ministerio de Justicia, Derechos Humanos y Seguridad** – Emisión del Certificado de Antecedentes Penales (para los casos en que no se registran antecedentes.).
- **Superior Tribunal de Justicia de Salta** - Digitalización de la remisión de planillas prontuariales de la Policía Provincial con una reducción de 7 a 3 días en el trámite
- **Oficina Nacional de Empleo Público** - Sistema de Retiro Voluntario – Se logró disminuir el tiempo promedio de respuesta: de 5 días a 2 horas.
- **PAMI** – A la fecha se ha logrado digitalizar y firmar usando certificados digitales más de 11.000 Resoluciones y 4.000 dictámenes.
- **Comisión Nacional de Valores –** Una de las experiencias más antiguas en el Estado, la Autopista de la Información Financiera lleva más de 35.000 documentos recibidos de empresas controladas por el organismo
- **Procuración General de la Nación –** Se la utiliza para la notificación de resoluciones a las 15 Fiscalías Generales del interior del país y a los Magistrados y Jefes de Área.
- **Superior Tribunal de Justicia de Córdoba –** Los Tribunales de Ejecución Fiscal de la Ciudad de Córdoba firman sus sentencias.
- **Ministerio de Economía y Finanzas:** altas de usuarios sistemas de administración financiera de la Administración Publica Nacional (SLU – UEPEX).
- **Sistemas de la SGGP –** Varios sistemas del organismo vienen utilizando esta tecnología. Entre ellos, el SIREPEVA (Sistema de Registro del Personal SINAPA), SECOP (Sistema Electrónico de Compras Públicas), Remisión de informes de Diagnóstico de Gobierno Electrónico, Informe sobre contratados, Acceso a las Bases de Datos confidenciales de ArCERT (Proyecto de Seguridad Informática de la ONTI).

- **AFIP** - A continuación se listan algunas de las aplicaciones para las cuales se aplicará la Firma Digital: Formulario Valor, Documentación para Desaduanamiento, Formulario multinota, Certificado de Origen digital, Notas internas y dictámenes jurídicos.
- **ANSES –** Se viene utilizando para las Disposiciones de la Gerencia de Sistemas y Telecomunicaciones, Expediente Electrónico, Formularios electrónicos firmados y Digitalización de documentación.