Proyecto de Grado

Ingeniería en Sistemas – IUA

Tema:

Firma Digital

Alejandro Anghillantte

Luciana Romero

Asesor: Eduardo Casanovas

Declaración de Derechos de Autor

Dedicatoria

A mi esposa, Jorgelina Maurino. Mi más grande reconocimiento pues gracias a su comprensión y apoyo fue posible este trabajo.

A mis padres Alberto Luis Anghillantte y Adriana Fino, quienes infundieron en mí el gusto por el aprendizaje, y me hicieron comprender que la mejor forma de crecer, es manteniendo en alto el espíritu y el coraje para enfrentar las dificultades y para disfrutar los buenos momentos.

A mi hermano Augusto Alberto Anghillantte, con quien siempre hemos estado unidos en la cultura de estudio y superación.

Alejandro Anghillantte

A mi familia, porque desde pequeña siempre me enseñaron a luchar para alcanzar mis metas, y este logro es de ustedes también. Gracias!

A mi pareja, mi compañero de vida, que siempre me brindó su apoyo, paciencia, motivación para seguir adelante y poder terminar este trabajo. Gracias!

Luciana Romero.

Abstract

El presente trabajo es un Proyecto Final de Grado de la carrera Ingeniería en Sistemas en el Instituto Universitario Aeronáutico (IUA). El problema observado es la necesidad de implantar un esquema de firma digital que agilice algunos procesos existentes, garantizando la autenticidad del firmante e integridad de los datos.

Para poder lograr cubrir con esta necesidad, el alumno considera necesaria la implementación de Firma Digital en el Instituto Universitario Aeronáutico, tomando como objetivo primordial y centrando la atención en verificar la posibilidad de ser una entidad emisora y certificante de claves, analizando sus costos asociados y requisitos legales exigidos por las leyes vigentes.

Para desarrollar el trabajo se ha realizado una investigación en base a diversas fuentes bibliográficas analizando el concepto de Firma Digital, algoritmos y estándares vigentes, e infraestructura de firma digital (conjunto de leyes, normativa legal complementaria, obligaciones legales, estándares tecnológicos, procedimientos de seguridad).

Posteriormente se aplica un proceso en cascada para el desarrollo de la solución, el cual permite clarificar el modelo. Finalmente se realiza el despliegue mediante la simulación de la generación de claves.

El resultado final del proyecto en su marco teórico es comprender el funcionamiento de las entidades certificantes, explicar las ventajas y desventajas de la implementación de la misma y defender la idea de que la tendencia hacia la implementación de firma digital existe en la actualidad y de que es 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.

Índice de Contenidos

Índice de Figuras

Índice de Tablas

1. Introducción

1.1. Antecedentes

Las iniciativas relacionadas con la firma digital en el ámbito de la Secretaría de Gabinete y Gestión Pública (SGP) se iniciaron en Marzo de 1997. En esa fecha, la entonces Secretaría de la Función Pública (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.

Posteriormente, en Abril de 1998, el Poder Ejecutivo Nacional dictó el Decreto N° 427, que autorizó 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 una Infraestructura de Firma Digital para el Sector Público Nacional.

La SFP era 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 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 en la implementación de la firma digital en las aplicaciones internas de distintos organismos.

Con el fin de difundir el uso de la tecnología, se crea 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 inicia 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.

Hacia inicios de 2001 se comienza 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 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 hace necesario avanzar en el desarrollo de la Autoridad Certificante 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 establece 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 comienza 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 son veinticuatro los organismos que utilizan esta operatoria.

En los últimos años, se han aprobado en todo el mundo nuevas leyes que soportan las firmas digitales y electrónicas como medio de autenticar datos y transacciones electrónicas.

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 ha

adolecido y sigue adoleciendo 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 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 la presencia de un notario que garantice la validez de ésta, lo cual hace lenta y costosa una transacción entre organizaciones ubicadas en diferentes partes del mundo. 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, consientes 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 mas 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 observado es la necesidad de implantar un esquema de firma digital que agilice algunos procesos existentes, garantizando la autenticidad del firmante e integridad de los datos.

1.4. Objeto de Estudio

El estudio se basa en la investigación de requisitos necesarios para la implementación de firma digital en el Instituto Universitario Aeronáutico (IUA), como así también la posibilidad de implementar una Autoridad Certificante que permita generar al IUA sus propios certificados.

Para lograr el objetivo propuesto, será necesario reconocer quienes son los participantes del problema y realizar un análisis costo beneficio para el Instituto Universitario Aeronáutico.

Va a ser necesario comprender el concepto de Firma Digital y su conjunto de leyes y normativas legales, como así también la tecnología disponible en el mercado que se deberán utilizar para llevar a cabo el proyecto.

1.5. Campo de Acción

El proyecto plantea la implementación de Firma Digital en el Instituto Universitario Aeronáutico (IUA), tomando como objetivo primordial y centrando la atención en verificar la posibilidad de ser una entidad emisora y certificante de claves, analizando sus costos asociados y requisitos legales exigidos por las leyes vigentes.

En base al estudio y comprensión del objeto de estudio, se buscará la manera de implementar una solución al problema planteado.

1.6. Objetivos

1.6.1. Objetivo General

Desarrollar un esquema de Firma Digital de manera que el Instituto Universitario Aeronáutico (IUA) pueda generar sus propios certificados.

1.6.2. Objetivos Específicos

Con el desarrollo del proyecto de fin de carrera se pretende lograr los siguientes

objetivos específicos:

- ✓ Analizar los algoritmos y estándares vigentes

- ✓ 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).
- ✓ Implementar un módulo que permita demostrar el proceso de generación y validación de licencias.
- ✓ Analizar la posibilidad de implementar una Autoridad Certificante que permita generar al IUA sus propios certificados

1.7. Idea a Defender / Propuesta Justificar / Solución a Comprobar

Se buscará defender la idea de que la tendencia hacia la implementación de firma digital existe en la actualidad y de que es 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.

Se propone por lo tanto, la implementación de un esquema de firma digital que agilice algunos procesos existentes, garantizando la autenticidad del firmante e integridad de los datos.

La implementación parcial del proyecto demostrará el proceso de creación de una entidad certificadora y la emisión de certificados propios.

1.8. Delimitación del Proyecto

La implementación de un esquema de firma digital cubre un amplio concepto, por lo que es necesario limitar el alcance del proyecto, centrándose en los objetivos específicos detallados y descartando los siguientes conceptos:

- ✓ Emisión de certificados para otras personas físicas o jurídicas
- ✓ Pago de licencias del software requerido
- ✓ Implementación en hardware definitivo

- ✓ No se generaran manuales de utilización para usuarios
- ✓ No se implementará en ningún área operativa

1.9. Aporte Teórico

Su creciente evolución en los últimos años de la tecnología en herramientas tecnológicas que permiten garantizar la autoría e integridad de los documentos digitales, y su alto interés por parte de las empresas, universidades, entes gubernamentales y otros, hace aún mas interesante a la implementación del proyecto y brinda conocimientos sobre las nuevas tecnologías y tendencias del mercado.

Por lo tanto, los resultados de este trabajo, podrán ser generalizados y aplicados a otros proyectos con características similares, con posibilidad de expansión dentro del mismo dominio en estudio.

1.10. Aporte Práctico

Según lo expresado en la situación problemática, el impacto que el proyecto tiene es en materia de reducción de costos, transparencia, publicidad y seguridad en la gestión, además de los efectos indirectos de tipo económico.

Entre los beneficios que permite la aplicación de la Firma Digital se destacan: la significativa contribución al proceso de "despapelización" de ciertas tareas administrativas, equiparando la firma de documentos electrónicos con los rubricados en forma manuscrita; la garantía de autoría e integridad de los documentos digitales; la 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. Por métodos empíricos nos referimos a modelos de investigación basados en la experiencia y pruebas sobre el objeto de estudio, el cual nos permite reconocer características y relaciones esenciales de los elementos considerados en este, lo que brinda las bases para estudios descriptivos.

1.11.1. Métodos Empíricos

En este proyecto se utiliza un método empírico para la utilización de la tecnología de claves y de la certificación digital en procesos de digitalización. Este método está pensado para ayudar en el suministro de soluciones óptimas de implementación con una pérdida en el trayecto mínimo con diversos tipos de obstáculos. El método empírico es validado por una herramienta de simulación. La comparación de los resultados obtenidos con el simulador en contra de los resultados experimentales demuestran que están en buen acuerdo.

1.11.2. Métodos Lógicos

Basándose en la aplicación del pensamiento deductivo, el análisis y la síntesis, se aplican métodos lógicos para:

- ✓ análisis de la situación problemática y definición del problema
- ✓ realización de un diagnóstico final
- ✓ para el análisis y diseño de generador de claves y sus elementos relacionados
- ✓ implementación de la solución teniendo en cuenta la teoría planteada y las herramientas disponibles.

1.12. Enfoque Metodológico

1.12.1. Paradigma

Como se denota de las consideraciones anteriores, el paradigma a ser utilizado será el deducido de la posibilidad de ser una entidad emisora y certificante de claves, y de los patrones a seguir para el análisis de la misma.

Tal como se planteó en el marco teórico, 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, por lo tanto se buscará su comprensión y aplicación.

1.12.2. Proceso

Para lograr los objetivos planteados, es necesario seguir secuencialmente un proceso. En primer lugar se va a hacer una aproximación al objeto de estudio, analizando el concepto de Firma Digital, su funcionamiento, algoritmos de encriptación, claves públicas y privadas, certificados digitales, leyes vigentes y el valor legal que tiene la firma digital.

A posteriori, se aplicara un desarrollo en cascada para el desarrollo de la solución, el cual permite clarificar el modelo:

- ✓ **Identificar requerimientos**: en base a las necesidades ya descriptas y patrones de diseño, se definirán los requerimientos como primera etapa del desarrollo los que van a servir 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**: con el análisis obtenido se procede al diseño de la solución, seleccionando las herramientas, tecnologías, algoritmos, leyes y estándares necesarios para la implementación, así como también la herramienta necesaria para la simulación.
- ✓ **Despliegue**: se genera la simulación del ente certificante, considerando lo desarrollado.

1.12.3. Métodos

Como se mencionó anteriormente, la metodología a aplicar es en cascada, considerando en cada etapa el alcance del proyecto. Se tendrá en cuenta el marco normativo vigente de la República Argentina (leyes y decretos), algoritmos y tecnologías disponibles en el mercado, como también su análisis costo-beneficio.

1.12.4. Técnicas

Las técnicas a aplicarse se pueden separar en los siguientes grupos:

- ✓ Recopilación de requerimientos: se pretende generar un listado de los requerimientos del sistema y por consecuente de las tecnologías de hardware y

software disponibles en el mercado, el marco normativo, los costos asociados, entre otros.

- ✓ Análisis, diseño y modelado: aquí se genera un modelo del sistema, un plano general del objeto en estudio, el cual refleje como van a interactuar los usuarios con el sistema, a quienes afecta y como les afecta.
- ✓ 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 2007: 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 2000: esta aplicación es utilizada para el desarrollo de la planificación del proyecto mediante diagramas de Gantt.
  - Ubuntu Server: este Sistema Operativo nos permite correr una aplicación que demuestre efectiva y económicamente la generación y manipulación de certificados.
  - OpenSSL y Servidor Apache: El software OpenSSL es un proyecto de software desarrollado por lo miembros de la comunidad Open Source. Es un robusto juego de herramientas que le ayudan al sistema a implementar el Secure Sockets Layer (SSL), así como otros protocolos relacionados con la seguridad , tales como el Transport Layer Security (TLS). También incluye una librería de criptografía. Estas herramientas nos van a permitir crear en primer lugar nuestra autoridad certificadora para expedir certificados digitales, luego generar y revocar certificados.

2. Marco Contextual

2.1. Entorno del Objeto de Estudio

Previamente se definió el objeto de estudio al desarrollar la introducción del proyecto, observándose que se presenta como un contexto amplio y complejo.

Las firmas digitales se muestran en un entorno donde las personas desarrollan cada vez más sus actividades diarias y que día a día crece más aceleradamente. Se notó un crecimiento más notorio en los últimos años con la aparición de nuevos métodos de manipulación de documentación en formato digital y con un gran potencial de uso, reemplazando a la metodología de manipulación manuscrita y por ende necesitando que dichos conjunto de datos tengan un respaldo legal y una metodología que garantice la identidad del firmante y la integridad del mensaje.

Por otra parte, se ha decidido enfocar además el estudio a los protocolos existentes como medios de seguridad, ya que han ido evolucionando constantemente logrando un nivel de seguridad aceptable en el mercado.

No podemos dejar de lado el estudio de la infraestructura de firma digital que no es mas que el conjunto de leyes, normativa legal complementaria, obligaciones legales, estándares tecnológicos y procedimientos de seguridad.

2.2. Relación Tesista y Objeto de Estudio

El autor de este trabajo se ve afectado directamente con los problemas planteados en la situación problemática. Por una parte, como alumno, es parte de la sociedad que hace uso de las nuevas metodologías de tratamiento de documentos, observando una estrecha relación entre las necesidades de inversión y los resultados que se obtienen al aplicar dicha tecnología.

Por otra parte se encuentra vinculado a un mundo donde es necesario estar permanentemente conectado con la sociedad y utilizando lo más reciente en avance tecnológico.

En los últimos años, Argentina ha demostrado un amplio crecimiento en este tipo de tratamiento de documentos que reemplaza al tratamiento tradicional manuscrito y es inevitable, como institución, no aprovechar ese potencial.

Por lo tanto el problema planteado anteriormente requiere el desarrollo de este trabajo para lograr comprender el concepto y aplicación de firma digital a una institución.

2.3. Análisis de Problemas Observados

Como se mencionó anteriormente, existe la necesidad en el Instituto Universitario Aeronáutico de implantar un esquema de firma digital que agilice algunos procesos existentes, garantizando la autenticidad del firmante e integridad de los datos.

Recordemos cuales son los puntos claves que representan dicha tecnología:

- Autentificación: la firma digital es equivalente a la firma física de un documento.
- Integridad: el mensaje y/o transacciones no pueden ser modificados.
- No repudio en origen: el emisor no puede negar haber enviado el mensaje o haber realizado una determinada transacción.

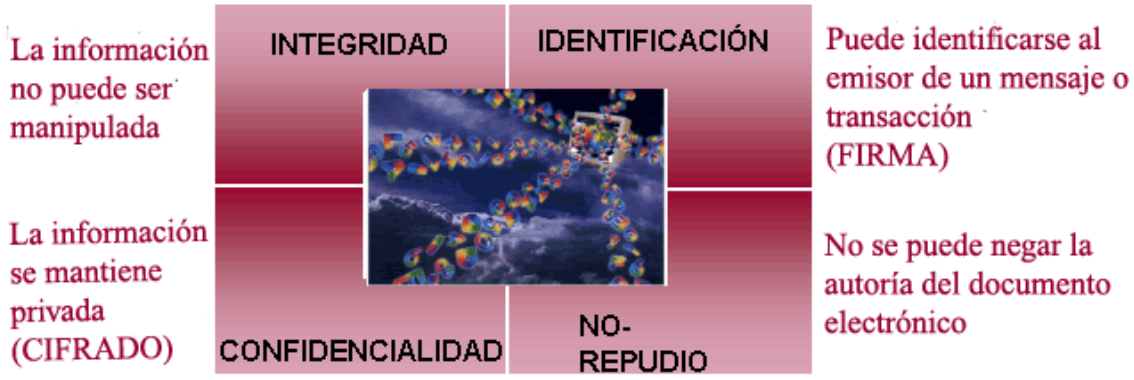


Figura 1: Características importantes en Firma Digital

A la fecha del comienzo de este proyecto, no existe implementado en el Instituto Universitario Aeronáutico un esquema de firma digital, por lo tanto se encuentra la

necesidad de generar una solución para abordar dicho problema y se ha analizado que el proyecto propuesto es el medio más aproximado para cubrir dicha necesidad.

El desarrollo del marco teórico necesario para este proyecto implicará el análisis de diversos proyectos que podrían ser considerados como similares, pero que se encuentran en otros entornos.

2.4. Antecedentes de Proyectos Similares

Existen numerosos casos de proyectos similares en los cuales se ha desarrollado o aplicado Firma digital, aunque en su gran mayoría son implementados en otros países.

Las leyes varían de acuerdo al País donde es implementado, y aunque son muy similares, deben tratarse por separado y con la importancia que estas se merecen.

Para citar algunos ejemplos de casos similares, se puede consultar en http://www.pki.gov.ar proyectos implementados en AFIP (Administración Federal de Ingresos Públicos) y ANSES (Administración Nacional de la Seguridad Social)

3. Marco Teórico

3.1. Introducción

El desarrollo del marco teórico buscara comprender los elementos que componen al concepto de Firma Digital, entendiendo sus formas, tecnologías y tendencias, lo que será la base para el futuro desarrollo de un modelo teórico y la concreción de dicho modelo.

En esta sección buscaremos cumplimentar con las siguientes funciones:

- 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.

Para poder abarcar dichos puntos es necesario una ardua investigación y consultas a diversas fuentes. De esta manera al alcanzar dicho objetivo, el autor podrá volcar los conocimientos adquiridos al documento y utilizarlos para concretar un modelo adecuado que satisfaga con los requerimientos del proyecto.

3.2. 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 nos 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 adquirido en 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.

A continuación se detallan algunos puntos claves que representa 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, compuesto 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. Marco Legal de la Firma Digital en Argentina

3.3.1. Introducción

Los avances técnicos, 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.

Con la promulgación de la Ley 25506 - Ley de Firma Digital, publicada en el Boletín Oficial el 14/12/2001 (Anexo 1: Ley de Firma Digital), se continua en forma específica, el desarrollo legislativo, con la aprobación del decreto Nº 2628/2002 (Anexo 2: Decreto 2628/2002).

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.

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.

3.3.3. 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).

3.3.4. 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 aquí 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 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.

3.3.5. 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 como 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 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, y 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, está acreditando 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, otorgando la 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 u acto con consecuencias jurídicas que ha sido firmado por particulares sin intervención de un funcionario público competente, que no tiene otro requisito que la firma.

Un documento electrónico no podría considerarse un instrumento privado si no existe una ley que de 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.

3.3.6. 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.

3.3.7. La Firma Digital en la Argentina

Toda la información relacionada a la firma digital, su infraestructura, y contenido de la ley de firma digital en la Argentina, puede consultarse en el Anexo 1.

3.4. Criptografía

3.4.1. Introducción

La Criptografía es el estudio de técnicas matemáticas relacionadas con aspectos de seguridad de la información, tales como la confidencialidad, integridad de datos, autenticación de entidades, y la autenticación del origen de datos.

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

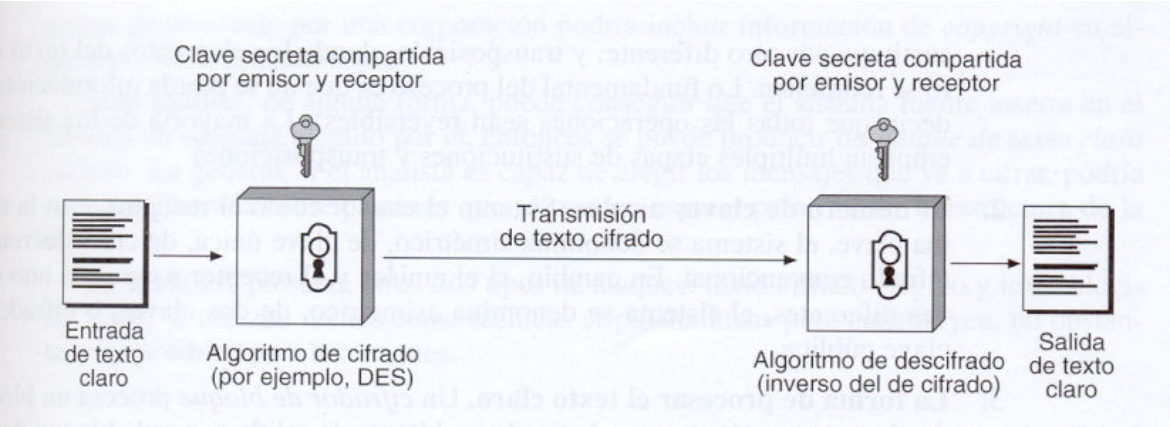


Figura 2: Proceso de criptografía simétrica.

Un esquema de cifrado simétrico tiene cinco componentes (Figura 2):

- Texto claro: es el mensaje que se introduce en el algoritmo como entrada
- Algoritmo de cifrado: realiza sustituciones y transformaciones en el texto claro.
- Clave secreta: es una entrada del algoritmo. Las sustituciones y transformaciones del algoritmo dependen de ella.
- Texto cifrado: es el mensaje ilegible que se produce como salida.
- Algoritmo de descifrado: es el algoritmo de cifrado ejecutado a la inversa.

La criptografía moderna usa las mismas ideas básicas que la criptografía tradicional (la transposición y la sustitución), pero su orientación es diferente. Tradicionalmente, los criptógrafos han usado algoritmos. Hoy el objetivo es hacer el algoritmo de encriptación tan complicado y rebuscado que incluso el criptoanalista obtiene cantidades enormes de texto cifrado a su gusto, no será capaz de entender nada en absoluto sin contar con la clave.

Se entiende como *Algoritmo de clave simétrica* porque utilizan la misma clave para encriptar y desencriptar.

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.

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 llave (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 sume 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.

3.4.2. Criptografía de Clave Pública

En los últimos años, el crecimiento vertiginoso de las redes de comunicaciones y el aumento de usuarios, está conllevando nuevos problemas a los cuales no les sirven las soluciones obtenidas hasta el momento. Un ejemplo claro lo encontramos en la seguridad. Cuando las redes de comunicaciones informáticas eran privilegio de unos pocos, estos podían intercambiar información entre ellos de un modo seguro utilizando lo que hoy conocemos como sistemas de clave simétrica. Para ello cuando dos usuarios quieren mantener una comunicación segura estos deben compartir una clave secreta que tan solo ambos conocen. Esta clave se utiliza tanto para cifrar la información como para descifrarla luego, permitiendo de este modo obtener un canal de comunicación seguro. El precio que se paga es el hecho que para cada par de usuarios que se quiera establecer una comunicación segura se requiere una clave distinta. Si hacemos cuentas, vemos que de este modo un usuario de una red debe almacenar tantas claves como personas con las que desee mantener una comunicación segura.

En dirección a la solución de estos problemas nace lo que se conoce como criptografía de clave pública. La idea general es proveer a cada usuario de un solo par de claves (una pública y una privada) independientemente del número de usuarios con los que desee comunicarse. Estas claves tienen la propiedad 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. De este modo se puede definir un método de cifrado que es el que se denomina cifrado de clave pública, que consiste en fijar una de las dos claves de cada usuario como pública y la

otra como privada. 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 este 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.

Hoy en día, en toda red de información es necesario cumplir con los principios de la seguridad computacional que se resumen en los siguientes servicios:

- **Integridad:** Se garantiza que los mensajes se reciben tal y como son enviados, sin duplicidad, inserción, modificación, reordenación ni repeticiones. La destrucción de datos también queda cubierta con este servicio.

- **Autentificación:** Es la encargada de determinar con quién se está comunicando antes de revelar información delicada, es decir verificar y asegurar la identidad de las partes.

- **Confidencialidad:** La confidencialidad consiste en mantener la información fuera del alcance de usuarios no autorizados.

- **Disponibilidad:** Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

- **No repudio:** El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje. Así cuando se envía un mensaje el receptor puede comprobar que efectivamente, el supuesto emisor envió el mensaje. De forma similar, cuando se recibe el mensaje, el emisor puede verificar que, de hecho, el supuesto receptor recibió el mensaje.

En el siguiente punto se ofrece una introducción en los conceptos de criptografía, para luego poder abordar lo relacionado a la criptografía de clave publica, donde se analizan los esquemas de Criptografía de Curvas Elípticas y RSA.

3.4.3. Algoritmo 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 la clave al tener que distribuirse 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 cirptosistema 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 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. Consistentemente nos referimos a estas claves como claves *públicas* y *privadas* y se distinguen de las claves *secretas* usadas en la criptografía convencional de clave simétrica.

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 publica. 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.

3.4.3.1. Intercambio de clave 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 computar 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, 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 $K= (Y_A)^{XB} \bmod q$.

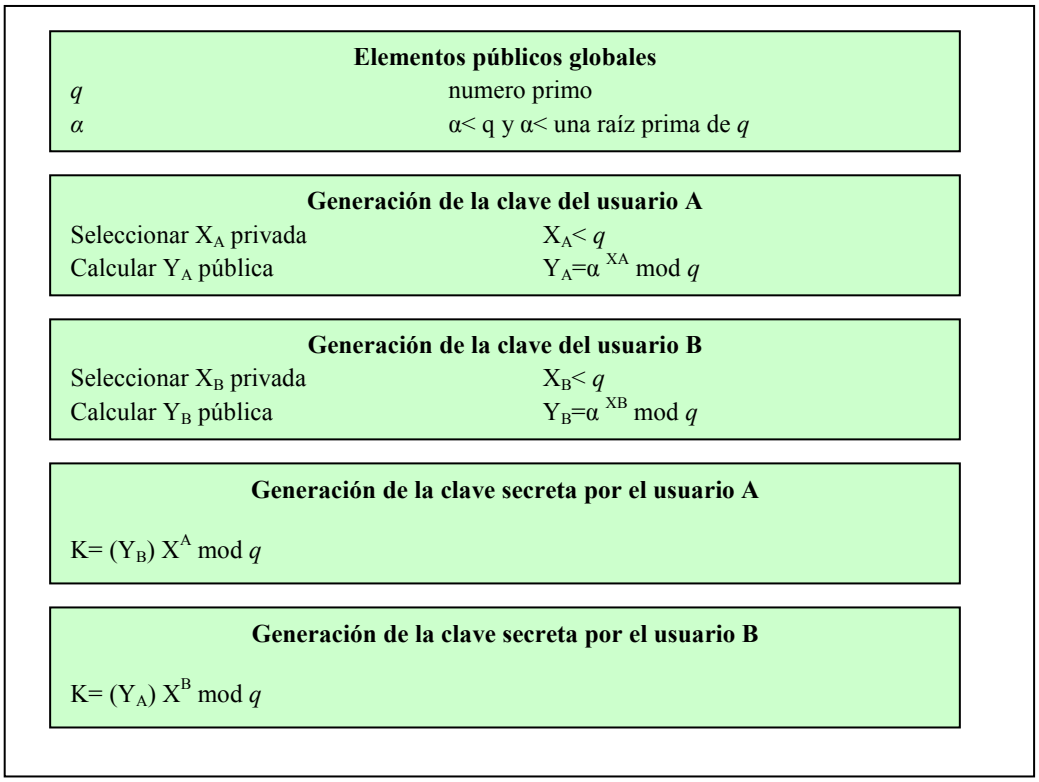


Figura 3: Algoritmo de intercambio de claves Diffie-Hellman

3.4.3.2. El Algoritmo RSA

Debido a las ventajas potenciales de la criptografía de clave pública, se están desarrollando nuevos algoritmos. Un buen método fue el desarrollado por un grupo del M.I.T (Riverst y cols., 1978). Es conocido por las iniciales de sus descubridores (Rivest, Shamir, Adleman): **RSA.** Ha sobrevivido a todos los intentos para romperlo por más de un cuarto de siglo y se le considera muy robusto. Mucha de la seguridad práctica se basa en él. Su mayor desventaja es que requiere claves de por lo menos 1024 bits para una buena seguridad (en comparación de los 128 bits de los algoritmos de clave simétrica), por lo cual es más lento.

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 de del RSA como lo hemos descrito 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.

3.4.3.3. Criptografía de Curva Elíptica

Las primeras propuestas de uso de curvas elípticas en la criptografía fueron hechas por Neal Koblitz y Victor Millar, de manera independiente, en 1985. 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.

3.4.4. La necesidad de autenticación en los sistemas de clave pública

El criptoanálisis de clave pública es un sistema ideal, que no requiere un canal seguro para transferir la clave de cifrado. Esto implicaría que dos entidades pueden comunicarse a través de un canal sin garantía, sin haber conocido a las claves cambiadas.

Desgraciadamente, esto no es el caso. Se observa como un adversario activo puede derrotar el sistema (descifrar el mensaje destinado a una segunda entidad) sin romper el sistema de encriptación. Esto se trata de un tipo de suplantación de identidad y es un ejemplo de falla de protocolo. En este escenario, el adversario se hace pasar por la entidad B mediante el envío de la clave pública '*e'* a la entidad A, donde éste supone (incorrectamente) que es la clave pública de B. El adversario intercepta los mensajes cifrados de A a B, descifra con su clave privada *d,* vuelve a cifrar el mensaje con la clave pública de B *e,* y lo envía a B. Esto pone de relieve la necesidad de autenticar las claves públicas para lograr datos de autenticación de origen de las claves públicas. Se debe estar convencido de que es cifrado bajo la clave pública legítima de B.

3.4.5. Clave simétrica vs. Criptografía de clave pública

Los esquemas de cifrado de clave simétrica y clave pública tienen ventajas y desventajas, alguno de los cuales son comunes a ambos. A continuación se destacan algunas de estas características.

I. Ventajas de la criptografía de clave simétrica

- Los sistemas de cifrado de clave simétrica pueden ser diseñados para tener altas tasas de transferencia de datos. Algunas implementaciones de hardware logran tasas de cifrado de cientos de megabytes por segundo, mientras que las implementaciones de software pueden alcanzar tasas de rendimientos en los megabytes de segundo rango.

- Las claves para los sistemas de cifrado de clave simétrica son relativamente cortas.

- Los sistemas de cifrado de clave simétrica pueden ser empleados como primitivas para la construcción de varios mecanismos criptográficos,

incluidos los generadores de números pseudoaleatorios, funciones hash, esquemas de firma digital computacionalmente eficientes, por nombrar algunos.

- Los sistemas de cifrado de clave simétrica pueden producir sistemas de cifrado más fuertes. A partir de transformaciones simples, facilidad de analizar su propia debilidad, pueden ser usados para construir fuertes sistemas de cifrado.

- El cifrado de clave simétrica que se percibe, tiene una larga historia, aunque se debe reconocer que, antes de la invención de las máquinas de rotor, muchos de los conocimientos en esta área han sido adquiridos con posterioridad a la invención de la computadora digital, y en particular al diseño de DES (Data Encryption Standard).

II. Desventajas de la criptografía de clave simétrica.

- En una comunicación de dos partes, la clave debe ser secreta en ambos extremos.

- En una red grande, hay varios pares de claves que deben gestionarse. En consecuencia, la gestión de claves requiere el uso incondicional de confianza TTP [1].

- En una comunicación de dos partes entre las entidades A y B el cifrado dicta que la clave puede cambiar con frecuencia, y tal vez por cada periodo de sesiones de comunicación.

- Los mecanismos de firma digital derivados del cifrado de clave simétrica típica, requieren claves grandes para la función pública de verificación o el uso de un TTP.

III. Las ventajas de la criptografía de clave pública.

- Solo la clave privada debe mantenerse en secreto (la autenticidad de las claves públicas deben garantizarse)

[1] TTP : Siglas en inglés Trusted Third Party, traducido como Tercero de confianza.

- La administración de claves en una red, requiere la presencia de un TTP funcionalmente de confianza en comparación con una confianza incondicional TTP. Dependiendo el modo de uso, el TTP solo podría ser necesario de manera "off-line" en lugar de en tiempo real.

- Dependiendo el modo de uso, una clave privada / par de claves publicas pueden permanecer sin cambios durante un periodo prolongado de tiempo, por ejemplo, muchas sesiones (incluso varios años).

- Muchos sistemas de clave pública, tienen un rendimiento relativamente eficiente de los mecanismos de firma digital. La clave usada para describir la función de verificación pública, suele ser mucho menor que la contraparte de clave simétrica.

- En una red grande, el número de claves necesarias puede ser considerablemente más pequeño que el escenario de clave simétrica.

IV. Desventajas de la criptografía de clave pública.

- Las tasas de rendimiento para los métodos de encriptación más populares de clave pública son de varios órdenes y de magnitudes mucho más lento que los mejores regímenes conocidos de clave simétrica.

- Los tamaños de clave son normalmente mayores que las requeridas para el cifrado de clave simétrica y el tamaño de las firmas de clave pública es más grande que el de las etiquetas que proporcionan autenticación del origen de datos de las técnicas de clave simétrica.

- Ningún esquema de clave pública ha demostrado ser seguro (lo mismo puede decirse para el bloque de sistemas de cifrado). Los sistemas de encriptación más eficaces de clave pública que se encuentran al día, tienen su seguridad basada en la dificultad pretendida de un pequeño conjunto de problemas teóricos de números.

- La criptografía de clave pública no tiene un historial extenso como el cifrado de clave simétrica, siendo descubierto a mediados de la década de 1970.

3.5. Firma digital

La autenticidad de documentos legales, financieros y de cualquier otro tipo se determina por la presencia o ausencia de una firma manuscrita 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:

1. El receptor pueda verificar la identidad del transmisor: Propiedad de autenticidad
2. El transmisor no pueda repudiar (negar) después el contenido del mensaje: Propiedad de no repudio
3. 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.

El proceso de firma dentro de los esquemas de llave pública se puede ver como el proceso de cifrado con la llave privada y el proceso de verificación se puede ver como el proceso de descifrado con la llave pública. El esquema general de firma digital se muestra en la figura 4. Como se observa, al mensaje se le aplica una función hash2 cuyo resultado será firmado con la llave 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* [2] al mensaje obteniendo el valor v1 y a la firma la verifica con la llave 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.

[2] Una función hash toma un mensaje como entrada de longitud arbitraria, lo digiere y produce una salida conocida como digestión de longitud fija. Los tipos de funciones hash como MD5 y SHA1 se describen en la sección 3.6.2 y 3.6.3.

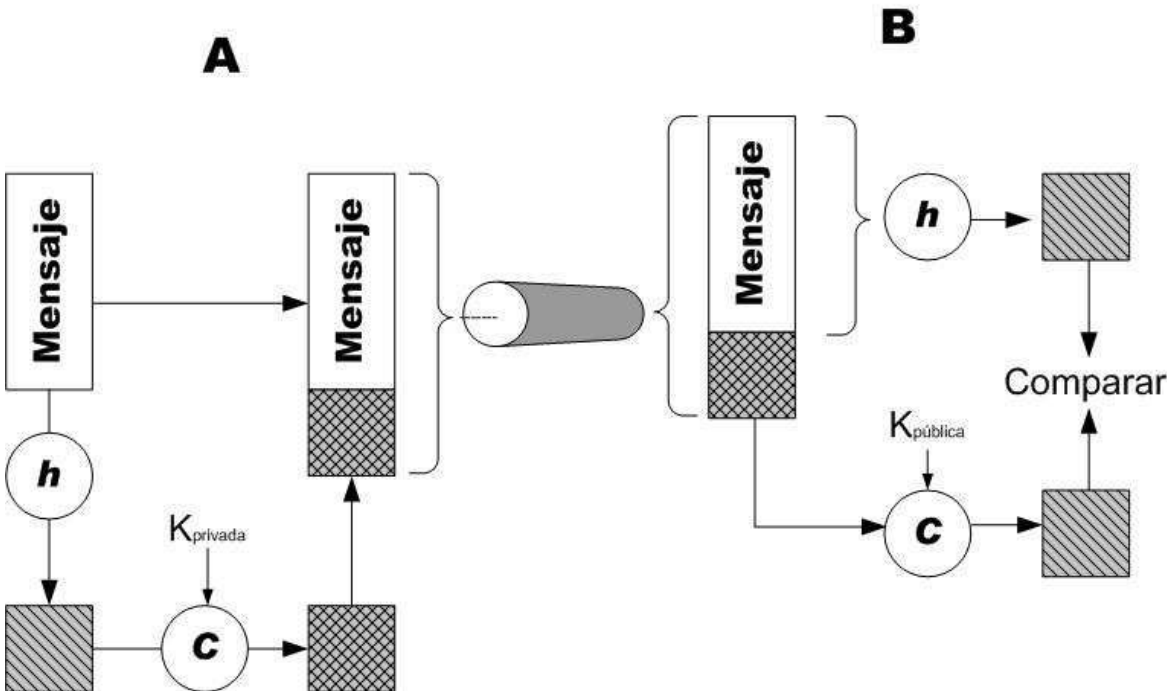


Figura 4: Esquema de firma digital.

3.5.1. 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 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 verifique 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.

3.5.2. 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 $mcd(e_A; \phi(n)) = 1$, 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 arriba 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, esta 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.

Las figuras 5 y 6 indican el procedimiento de la firma y verificación para RSA en este estándar. Para cifrar el mensaje m, se digiere con una función *hash* dando como resultado una digestión que es codificada 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, representado en la figura 5 por el paso 3, 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).

Figura 5: Firma con RSA

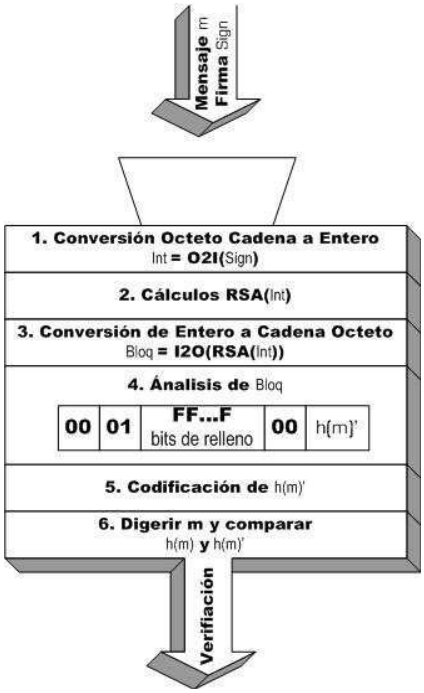


Figura 6: Verificación en RSA

3.6. Autentificación

La principal meta de la criptografía es garantizar que se cumplan los cinco servicios de la seguridad computacional: la Confidencialidad, la Integridad de los datos, la 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 “intruso en 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 si.

En la primera sección se señalarán los diferentes tipos de autentificación que existen.

Luego se introduce a la infraestructura de clave, todo lo referente a certificados, que es un elemento de la autentificación.

3.6.1. 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, momento en que un documento fue enviado y/o firmado, la identidad de una computadora o usuario, etc.

Los métodos se clasifican en cinco tipos:

- Autentificación del origen de datos: es un tipo de autenticación 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: Esta autentificación 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).

- Autentificación de clave: La 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.

3.6.2. MD5

Se ha propuesto una variedad de funciones para el compendio de mensajes. Las de mayor uso son MD5 (Rivest, 1992) y SHA-1 (NIST, 1993). **MD5** es la quinta de una serie de compendios de mensaje diseñados por Ronald Rivest. 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[3]. 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.

3.6.3 SHA -1

La otra función principal para el compendio de mensajes es **SHA-1** (**Algoritmo Seguro de *Hash* 1**)**,** desarrollado por NSA y aprobado por el NIST en FIPS 180-1. Al igual que MD5,

[3] 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.

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 7 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. Para los mensajes cuya integridad es importante pero cuyo contenido no es secreto, se utiliza ampliamente el esquema de la figura 8-21. 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.

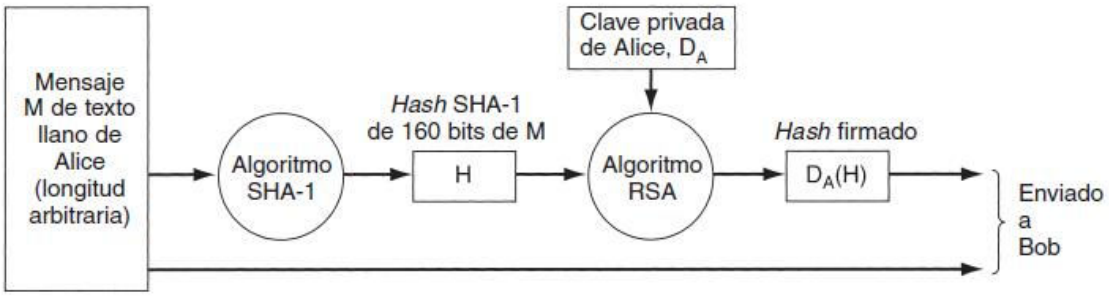


Figura 7: Uso de SHA-1 y RSA para firmar mensajes no secretos.

3.7. Administración de Clave Pública.

La criptografía de clave pública nos da la posibilidad que las personas que no comparten una clave común se comuniquen con seguridad, que se pueda firmar mensajes sin la presencia de un tercero confiable y además los compendios de mensajes firmados hacen que sea fácil verificar la integridad de los mensajes recibidos. Sin embargo, existe un problema que se basa en cómo las dos personas que quieren comunicarse obtienen cada una la clave pública del otro, sin necesidad de conocerse. Una solución obvia puede ser que se coloque su clave pública en su sitio Web, pero esto no funciona por la siguiente

razón. Si el primer usuario quiere buscar la clave pública de otro usuario con el que quiere comunicarse en el sitio Web de éste, empieza ingresando a la URL del receptor del mensaje. A continuación su navegador busca la dirección DNS de la página de inicio del receptor y le envía una solicitud *GET*, como se muestra en la figura 5. Pero si se presenta un tercero que intercepta la solicitud y responde con una página de inicio falsa, excepto por el reemplazo de la clave pública del receptor con la del tercer usuario. Cuando el emisor encripta su primer mensaje con *ET*, el intruso lo desencripta, lo lee, lo vuelve a encriptar con la clave pública del receptor del mensaje y lo envía a éste, quien no tiene la menor idea de que el intruso está leyendo los mensajes que le llegan. Peor aún, el tercer usuario puede modificar los mensajes antes de volverlos a encriptar para el receptor real. Como vemos, se necesita un mecanismo para asegurar que las claves públicas puedan intercambiarse de manera segura.

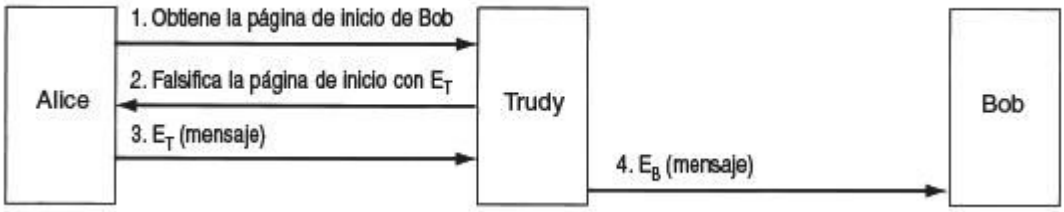


Figura 8: Forma mediante un intruso (Trudy) puede subvertir la encriptación de clave pública

3.7.1. Certificados

Como un primer intento para distribuir claves públicas de manera segura, podemos definir un centro de distribución de claves disponible que proporciona claves públicas a petición. Uno de los muchos problemas con esta solución es que no es escalable, y además que estaríamos presente a otro problema a presentarse rápidamente como es un cuello de botella. Además, si alguna vez fallara, la seguridad en Internet podría reducirse a nada. Por estas razones, se ha desarrollado una solución diferente, en donde lo que hace es certificar las claves públicas que pertenecen a las personas, empresas y otras organizaciones. Una organización que certifica claves públicas se conoce como **CA** (**autoridad de certificación**)**.** Como un ejemplo, suponga que un usuario A desea permitir que otras personas se comuniquen con él de manera segura. Él puede ir con la CA con su clave pública junto con su pasaporte o licencia de conducir para pedir su certificación. A continuación, la CA emite un certificado similar al que se muestra en la figura 6 y firma su

hash SHA-1 con la clave privada de la CA. El usuario A paga la cuota de la CA y obtiene un disco flexible que contiene el certificado y su *hash* firmado.

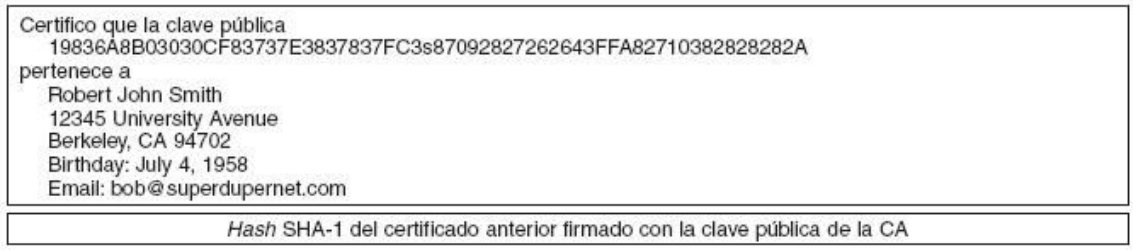


Figura 9: Ejemplo de posible certificado y su *hash* firmado.

La idea principal de la utilización de un certificado es enlazar una clave pública con el nombre de un personaje principal (individual, empresa, etcétera). Los certificados mismos no son secretos ni protegidos. Por ejemplo, este usuario podría decidir colocar su nuevo certificado por ejemplo en su sitio Web.

Ahora si volvemos a analizar la figura 8. Cuando el intruso intercepta la solicitud que realiza el usuario primero para obtener la página de inicio del usuario receptor, ¿qué puede hacer ese intruso? Puede poner su propio certificado y bloque de firma en la página falsificada, pero cuando el usuario lea el certificado, verá inmediatamente que no está hablando con el que desea ser el receptor de su mensaje porque el nombre de éste no se encuentra en dicho certificado. El intruso puede modificar la página de inicio del usuario final, reemplazando la clave privada de éste con la suya. Sin embargo, cuando usuario que envía el mensaje ejecute el algoritmo SHA-1 en el certificado, obtendrá un *hash* que no corresponde con el que obtuvo cuando aplicó la clave privada bien conocida de la CA al bloque de firma. Como el tercer usuario no tiene la clave privada de la CA, no tiene forma de generar un bloque de firma que contenga el *hash* de la página Web modificada con su clave pública en él. De esta manera, el usuario emisor puede estar seguro de que tiene la clave pública del que quiere que sea el receptor y no la de un intruso o la de alguien más. Este esquema no requiere que la CA esté en línea para la verificación, por lo tanto se elimina un cuello de botella potencial.

La función estándar de un certificado es enlazar una clave pública a un personaje principal, pero también se puede utilizar para enlazar una clave pública a un **atributo.** Por ejemplo, un certificado podría decir: Esta clave pública pertenece a alguien mayor de 18 años. Podría utilizarse para probar que el dueño de la clave privada no es una persona menor de

edad y, por lo tanto, se le permitió acceder material no apto para niños, entre otras cosas, pero sin revelar la identidad del dueño. Por lo general, la persona que tiene el certificado podría enviarlo al sitio Web, al personaje principal o al proceso que se preocupa por la edad. El sitio, el personaje principal o el proceso podrían generar a continuación un número aleatorio y encriptarlo con la clave pública del certificado. Si el dueño pudiera desencriptarlo y regresarlo, ésa sería una prueba de que el dueño tenía el atributo establecido en el certificado. De manera alternativa, el número aleatorio podría utilizarse para generar una clave de sesión para la conversación resultante.

Otro ejemplo en el que un certificado podría contener un atributo es un sistema distribuido orientado a objetos. Cada objeto normalmente tiene múltiples métodos. El dueño del objeto podría proporcionar a cada cliente un certificado que dé un mapa de bits de cuáles métodos puede invocar y que enlace dicho mapa de bits a una clave pública mediante un certificado firmado. Nuevamente, si el dueño del certificado puede probar la posesión de la clave privada correspondiente, se le permitirá realizar los métodos en el mapa de bits. Tiene la propiedad de que la identidad del dueño no necesita conocerse, lo cual es útil en las situaciones en las que la privacidad es importante.

El sistema de autenticación debe tener:

- Una política de certificación
- Un certificado de la C.A
- Los certificados de los usuarios (X.509)
- Los protocolos de autenticación, gestión y obtención de certificados:

  -Se obtienen de base de datos (directorio X.509)

  -O bien directamente del usuario en tiempo de conexión (www con SSL).

3.7.2. Estándar X.509

Si todas las personas que desean algo firmado fueran a la CA 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** y se utiliza ampliamente en Internet en su

versión V3. El X.509 ha recibido una enorme influencia del mundo de OSI (por ejemplo, la asignación de nombres y la codificación). 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 7. Las descripciones dadas ahí deben proporcionar una idea general de lo que hacen 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 10: 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 su 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.

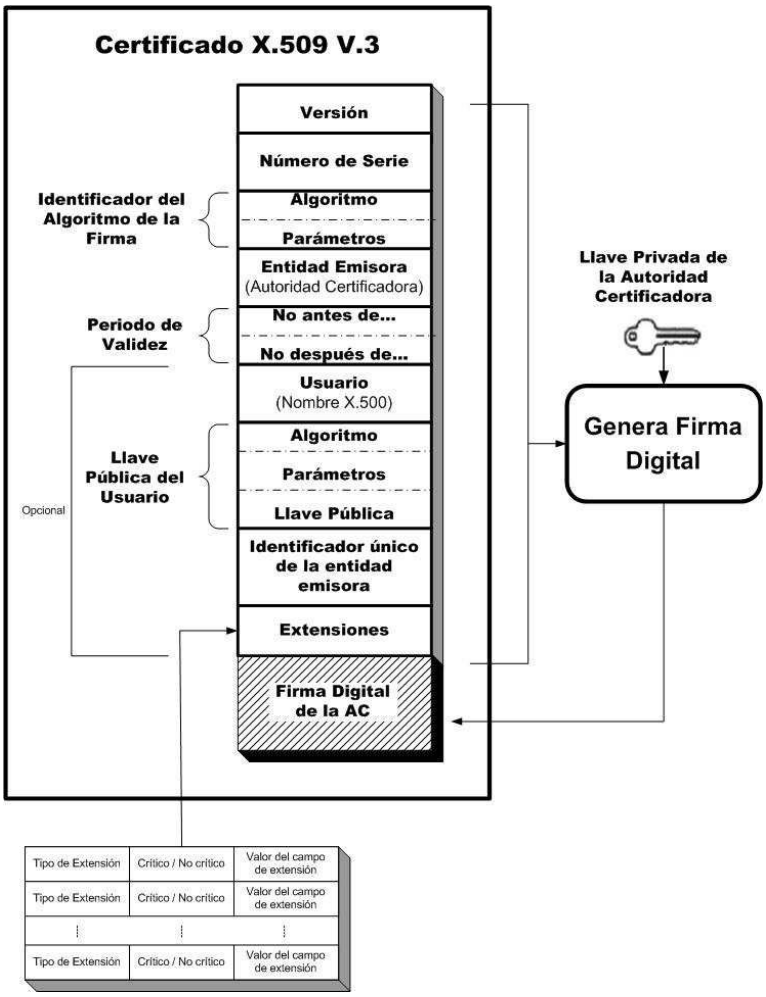


Figura 11: Formato certificado X.509

3.7.3. Infraestructura de clave pública

El hecho de que una sola CA emita todos los certificados del mundo obviamente no funciona. Podría derrumbarse por la carga y también podría ser un punto central de fallas. Otro interrogante que se plantea es ¿qué organización podría operar la CA? Es difícil imaginar cualquier autoridad que podría ser aceptada mundialmente como legítima y digna de confianza. Por estas razones, se ha desarrollado una forma diferente para certificar claves públicas. Tiene el nombre general **PKI (Infraestructura de Clave Pública).**

Una infraestructura de llave pública o PKI por sus siglas en inglés (*Public Key Infrastructure*) es el término utilizado para referirse a la infraestructura de seguridad, basada en criptografía de clave pública, que permite la gestión de certificados digitales. La meta de una infraestructura de llave 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, CAs, 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 CAs, como se muestra en la figura 12. La CA de nivel superior, la raíz, certifica a CAs 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 los Cas 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 CA, produce y firma un certificado que indica su aprobación y que contiene la clave pública de la CA.

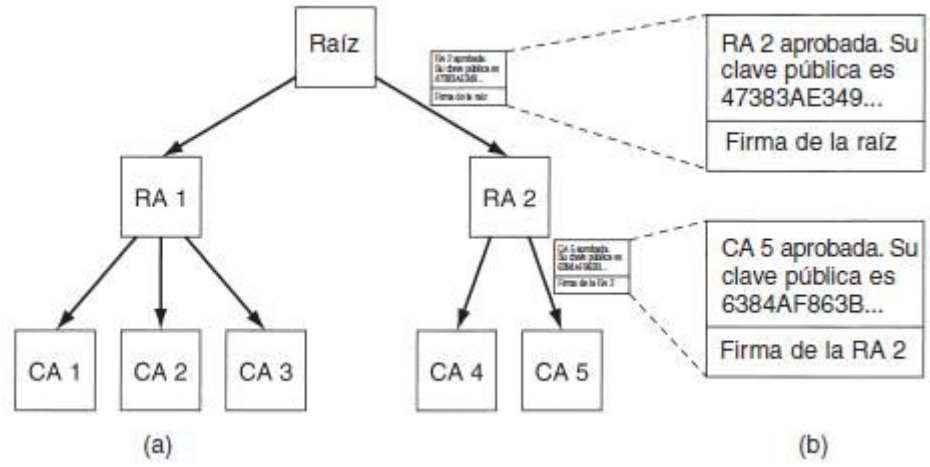


Figura 12: a) PKI jerárquica. b) Cadena de certificados.

Directorios

Un problema de cualquier PKI es en dónde están almacenados los certificados (y sus cadenas hacia un ancla de confianza [4]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

[4] 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.

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 CA 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 CA 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 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.

Otra complicación 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 CA.

¿Dónde deben almacenarse las CRLs? Un buen lugar sería el mismo en el que se almacenan los certificados. Una estrategia es que una CA 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, esa alteración 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

En base al desarrollo del marco teórico hemos logrado comprender el concepto de Firma Digital, entendiendo sus algoritmos, estándares vigentes e infraestructura de firma digital (conjunto de leyes, normativa legal complementaria, obligaciones legales, estándares tecnológicos).

Buscando alcanzar el objetivo del proyecto buscaremos ahora generar un modelo teórico apropiado.

En esta sección buscaremos cumplimentar los siguientes objetivos específicos:

- Definir los requerimientos para la implementación de firma digital en el Instituto Universitario Aeronáutico (IUA).
- Definir los requerimientos para implementar una Autoridad Certificante que permita al IUA generar sus propios certificados.
- Modelar un esquema de Firma Digital y Autoridad Certificante, considerando la infraestructura, leyes, normativas y estándares tecnológicos estudiados.

4.2. Planificación

Las actividades que se consideran a continuación le servirán al autor del trabajo para cumplimentar cada etapa del proyecto en un lapso de tiempo considerado óptimo.

4.2.1. Etapas, actividades y duración

	Nombre de tarea	Duración	Comienzo	Fin
1	**Proyecto de Grado**	**410 days**	**Mon 18/10/10**	**Thu 01/12/11**
2	**Introducción**	**20 days**	**Mon 18/10/10**	**Sat 06/11/10**
3	**Marco Contextual**	**10 days**	**Sun 07/11/10**	**Tue 16/11/10**
4	**Marco Teórico**	**90 days**	**Wed 17/11/10**	**Mon 14/02/11**
5	**Modelo Teórico**	**190 days**	**Tue 15/02/11**	**Tue 23/08/11**
6	Planificación	30 days	Tue 15/02/11	Wed 16/03/11
7	Requerimientos	40 days	Thu 17/03/11	Mon 25/04/11
8	Análisis	30 days	Tue 26/04/11	Wed 25/05/11
9	Diseño	90 days	Thu 26/05/11	Tue 23/08/11
10	**Concreción del modelo**	**50 days**	**Wed 24/08/11**	**Wed 12/10/11**
11	Simulación del proyecto	30 days	Wed 24/08/11	Thu 22/09/11
12	Revisión del modelo	20 days	Fri 23/09/11	Wed 12/10/11
13	**Revisión**	**50 days**	**Thu 13/10/11**	**Thu 01/12/11**
14	Revisión de documentación	20 days	Thu 13/10/11	Tue 01/11/11
15	Redacción de conclusiones	10 days	Wed 02/11/11	Fri 11/11/11
16	Corrección final	20 days	Sat 12/11/11	Thu 01/12/11

Tabla 1: Etapas, actividades y duración del proyecto

4.2.2. Diagrama Gantt

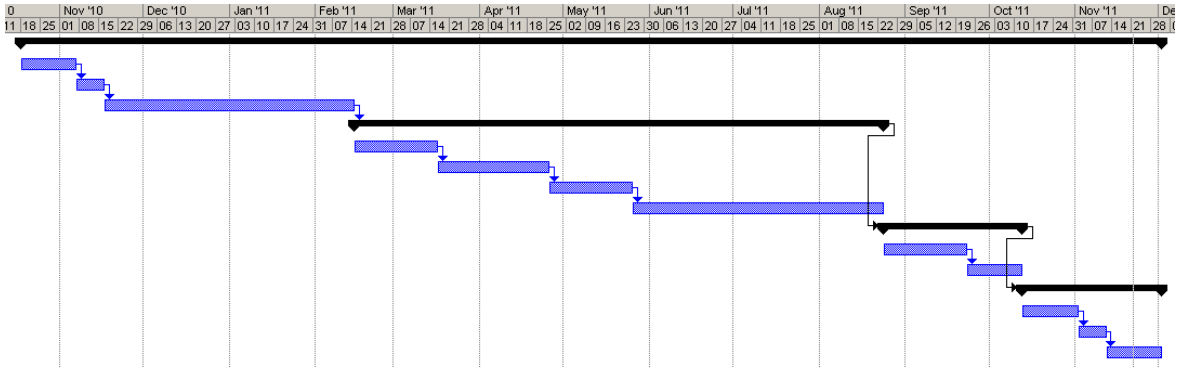


Figura 13: Diagrama Gantt del proyecto

4.3. Requerimientos

Los requerimientos para un sistema son la descripción de los servicios proporcionados por el sistema y sus restricciones operativas. Estos requerimientos reflejan las necesidades de los clientes de un sistema que ayuda a resolver un problema.

En nuestro caso, las necesidades de los clientes está dado por poder poseer un sistema de firma digital que brinde seguridad, autenticación en todos los documentos generados, pudiendo ahorrar tiempo, espacio en todos los archivos trabajados por los usuarios.

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 que es lo que se va a implementar, las funciones, servicios operativos.

En las secciones posteriores se realizará un análisis detallado sobre estos requerimientos mencionados para nuestro sistema.

4.3.1 Requerimientos funcionales y no funcionales

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

Requerimientos funcionales

Estos requerimientos describen lo que el sistema debe hacer. A continuación se presentan algunos de estos:

- 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 tendrá la posibilidad de buscar y/o seleccionar los documentos firmados.
- El sistema generará una clave privada que se asignará a cada usuario de manera única.
- El sistema deberá informar periódicamente una lista de certificados revocados.

Requerimientos no funcionales

Estos requerimientos son aquellos que no se refieren directamente a las funciones específicas que brinda el sistema, sino a las propiedades emergentes de éste como fiabilidad, tiempo de respuesta, almacenamiento, regulaciones legales, rendimiento, etc.

El cumplimiento de estos requerimientos hace que nuestro sistema entero sea útil para todo el usuario que así lo solicita.

Los tipos de requerimientos no funcionales son los siguientes:

- Requerimientos de fiabilidad: recuperación del sistema ante un eventual fallo. Se contará con un sistema de backup periódicos para resguardar toda la información.
- Requerimiento de eficiencia: desempeño correcto del sistema para cualquier requerimiento y transacción necesaria.
- Requerimientos de usabilidad: implica el grado de utilidad del sistema de firma, es decir, que tan fácil es para ser aplicado, utilizado reemplazando la firma manuscrita. Para ello, se realizará capacitaciones y se podrá consultar al manual de usuario.
- El sistema de firma no deberá revelar al personal que lo utilice ninguna información sobre las claves privadas de otros usuarios, ni transacciones realizadas, aparte 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 que debe cumplir un solicitante para obtener una licencia, deberán ajustarse a las normativas de Firma Digital de la República Argentina de acuerdo con el Artículo 30 de la ley 25506.
- El proceso de desarrollo de firma digital debe cumplir con los procedimientos, normativas de verificación y gestión de cada área, dispuestos por la Universidad.

4.3.2. Actores del Negocio

Los actores del negocio, son aquellos implicados con el sistema de firma digital.

Entre ellos, podemos 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.
- 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.
- 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 que conforme la **Infraestructura de Firma Digital Nacional** (IFDN), con el fin de poder utilizar esta tecnología en forma segura.

  Además es el encargado de elaborar todas las normativas que regula la actividad, establece las condiciones para otorgar y/o revocar licencias. Tiene el poder de designar un Ente licenciante.

4.3.3. Requerimientos Legales Generales

4.3.3.1. Obligación de Información

El certificador debe informar a los potenciales suscriptores, terceros usuarios y otros posibles interesados, las condiciones de utilización del certificado digital, su tramitación y revocación así como las condiciones de la Política de Certificación. Dicho mecanismo debe contar en la documentación presentada.

4.3.3.2. Garantías

Las entidades privadas que soliciten licencia de certificador deberán constituir un seguro de caución a fin de garantizar el cumplimiento de sus obligaciones.

4.3.3.3. Contratos de Servicios de Tercerización

El certificador debe tener claramente acordados los niveles de servicio que permitan garantizar la correcta prestación del servicio.

4.3.4. Instalaciones

4.3.4.1. Ubicación de las instalaciones

La ubicación de los sistemas de certificación de los certificados licenciados no debe estar públicamente identificada. No debe haber ambientes compartidos que permitan la visibilidad de las operaciones críticas de emisión o revocación de certificados y estar físicamente protegidos. En la Figura 14 se puede observar la ubicación de las instalaciones del Instituto Universitario Aeronáutico.

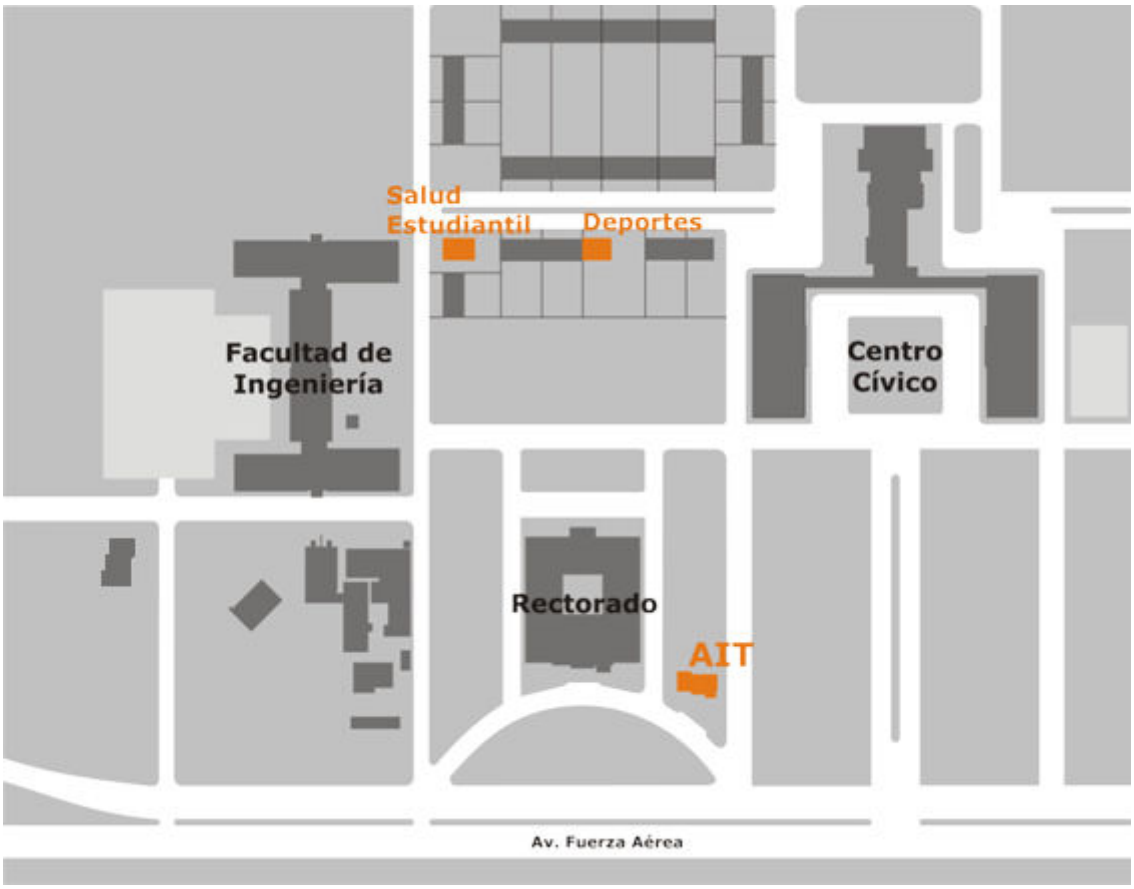


Figura 14: Instalaciones del IUA

De acuerdo a la disposición física observada en el Layout del campus y a los requisitos de instalaciones, se considera conveniente la ubicación física de los sistemas de certificación en el Edificio Principal (Rectorado – Figura 15).

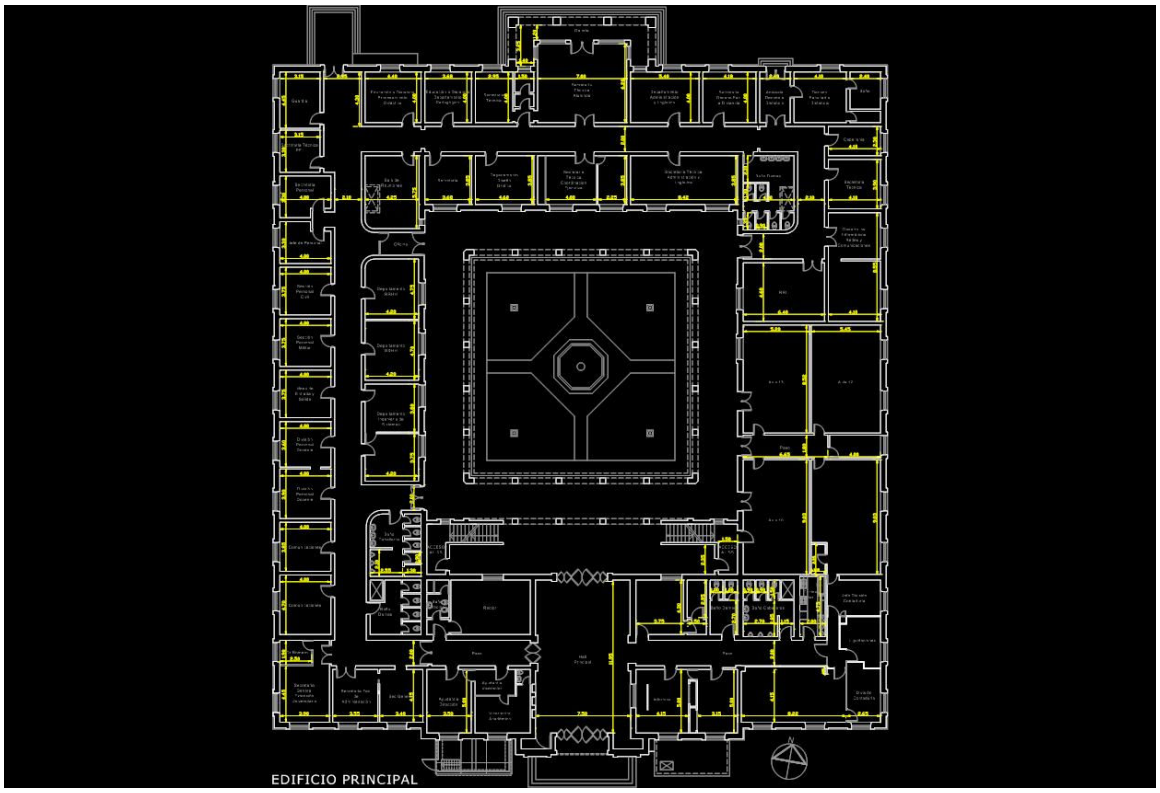


Figura 15: Layout Edificio Principal IUA

Dentro del mismo se encuentra un compartimento (aula 12) que es óptima para la instalación del cofre. El mismo ofrece dimensiones más que aceptables que se pueden observar en la figura 15. La estructura maciza de sus paredes incrementa la seguridad previa al acceso al cofre y evita que el mismo sea visualizado e identificado fácilmente desde el exterior.

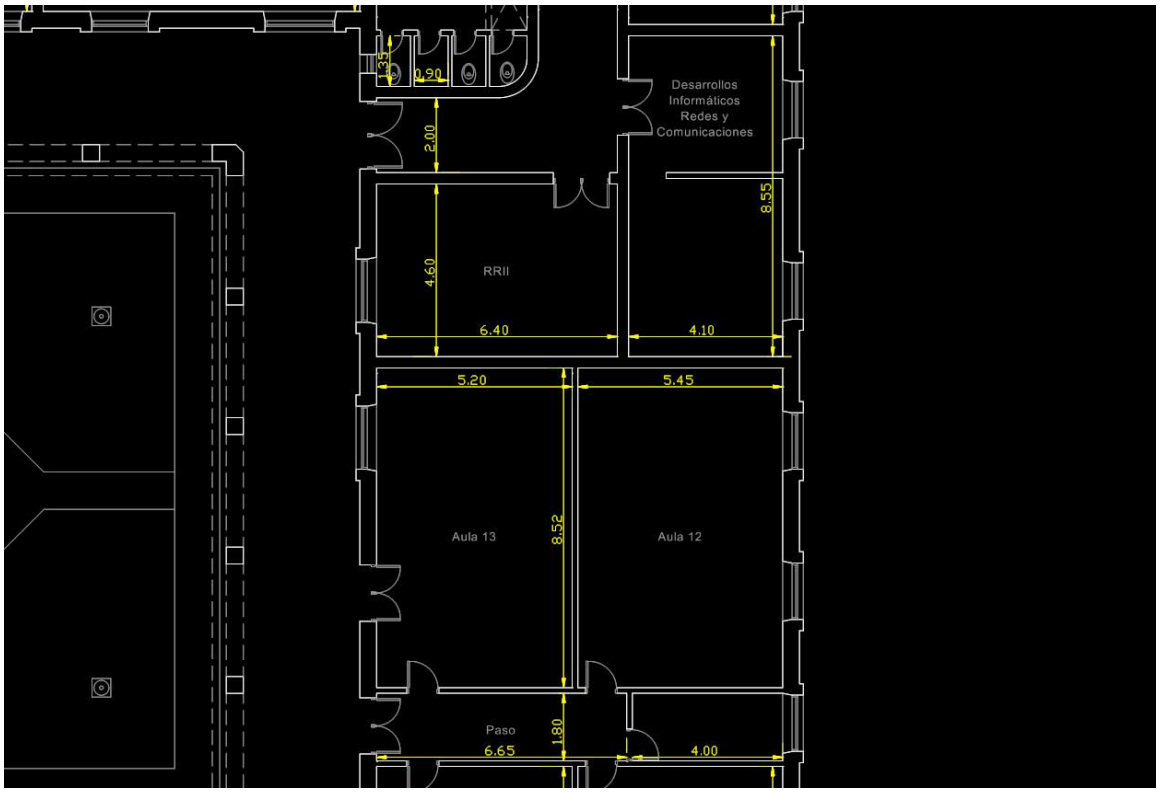


Figura 16: Layout actual Edificio Principal IUA (zoom aula 12)

Para poder acceder al aula 12 debe realizarse una antesala de manera de poder cumplir con los 4 niveles de seguridad establecidos en los requisitos de Infraestructura de Firma Digital Argentina Art.30 de la ley 25506, la cual va a ser accedida por la oficina que se encuentra en el pasillo principal haciendo una comunicación hacia la sala 12 y cerrando el actual ingreso. Dicha antesala se encuentra identificada como N2 (Nivel 2) como se muestra en la figura 16.

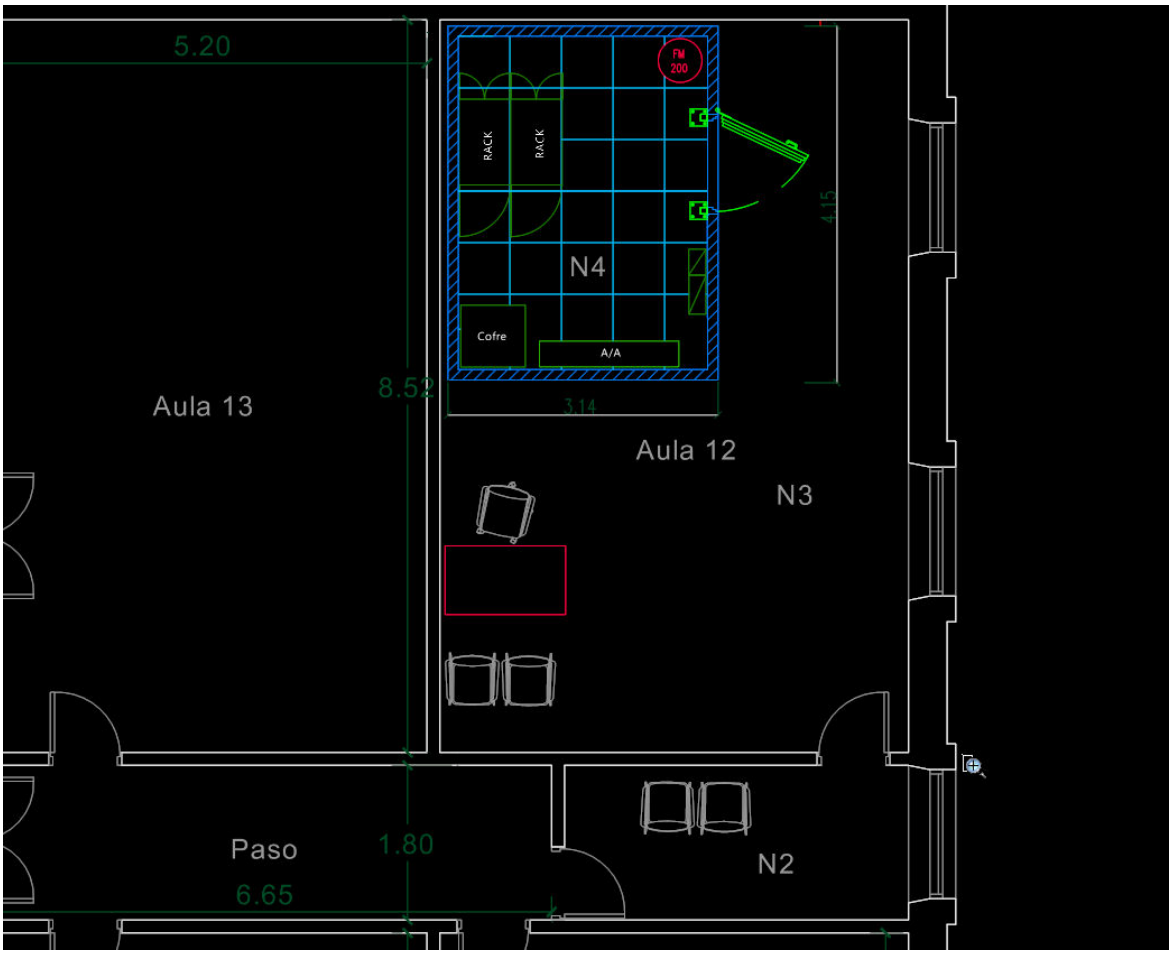


Figura 17: Layout modificado Edificio Principal IUA (zoom aula 12)

Se puede observar que se modificó la posición original de la puerta para poder generar los distintos niveles de acceso planteados en la reglamentación. La Sala Cofre es el Nivel 4 (N4).

Dentro de la sala se previó espacio para 2 racks, el cofre para las claves criptográficas, el sistema de extinción de incendio y equipos de aire acondicionado de precisión (Liebert). Los equipos de aire son 2 split que van colocados uno arriba de otro para tener redundancia.

En el diseño se dibujó piso técnico pero no es excluyente ya que no se insufla aire bajo el piso y el cableado se puede hacer con bandejas aéreas.

4.3.4.2. Acceso Físico a las Instalaciones

Se debe implementar un control de acceso físico que garantice la seguridad de las operaciones, debiendo contar con por lo menos cuatro niveles de acceso físico para llegar al ambiente donde residen los equipos de la Autoridad Certificante.

Para lograr cubrir dichas necesidades, se ofrece la instalación de la Sala Cofre Smart Shelter+ de AST.

Construida bajo los principios de una Sala IT de Alta Seguridad Certificada de acuerdo a ANSI/TIA 942, brinda la más alta protección de la industria para un centro de cómputos (CPD), contra fuego/calor manteniendo la temperatura interior por debajo de los límites establecidos por la normas EN 1047/2 , NBR 15247 en caso de incendio. Aún así, en situaciones extremas de 945º C de temperatura exterior, la interior no supera los 30º C y la humedad relativa es menor al 85% durante el lapso de ensayo que establece la norma (60 minutos).

La Sala Cofre Smart Shelter+ combina características de protección para Hardware y Medios Magnéticos (máxima. temperatura admisible 48.9º C de acuerdo a NFPA 75)

La Sala Cofre Smart Shelter+ provee ventajas únicas en términos de seguridad, rápida instalación y modularidad, asegurando las perfectas condiciones ambientales para ambientes de misión crítica.

La Sala Cofre Smart Shelter+ ha sido diseñada de acuerdo a los más exigentes standards. Sus componentes, ensamblado y control de calidad son ejecutados de acuerdo a procesos y normas internacionales (IEC, EN, ISO, DIN, etc).

La figura muestra la estructura externa de la Sala Cofre Smart Shelter+

Figura 18: Sala Cofre Smart Shelter+ de AST (vista externa)

Sus principales propiedades son:

- Certificado de conformidad ANSI / TIA 942: 2008: Cumplimiento de los requerimientos de protección al fuego para clasificación TIER III & TIER IV.
- Resistencia al Fuego: Paneles conformados como un sándwich de chapa de acero con clasificación RF 120 de acuerdo a EN 13501.
- Estabilidad Térmica: Los paneles de Sala Cofre Smart Shelter+, construidos en base a un corazón de compuestos aislantes, soportan 945º C de temperatura sin que la interior aumente más de 12º C.
- EN 1047-2: Ensayada como una sala completa bajo la curva de calentamiento de la norma EN 1047/2, posee la mayor estabilidad térmica del mercado. Ensayos certificados por SGS y TUV Rheinland.
- Test de Impacto: De acuerdo a EN 1047/2 es ensayada mediante una carga pendular de 200 kg.

- NFPA: Conforme con NFPA 75 de acuerdo a las definiciones de: Fire-Resistant Rated Construction. Conforme NFPA 232 de acuerdo a la definición de Fire-resistive Records Vault. La temperatura interior no supera los 48.9º C establecidos por NFPA 75.

- Estructura Sólida de Bóveda: Conformada por elementos de pared, piso y techo, su sistema de acero estructural soporta más que una construcción tradicional. Los paneles están revestidos por una chapa de acero galvanizado con un acabado lacado en ambos lados. En su interior poseen material termoaislante e ignífugo.

- Puertas: Sistema de puerta única con cerramiento automático y barral anti pánico. La puerta está diseñada para brindar protección a la intrusión de acuerdo a EN 1628 y clasificada como WK4 (EN 1627). Ensayo Certificado por Cidemco.

- Pasaje de cables: Sistema multidiámetro FireStop de pasaje de cables y tubulaciones conforme a NFPA 75.

- Aislación Electro-Magnética: Su conformación protege de campos electromagnéticos de alta y baja frecuencia que dañan los medios porta datos. Jaula de Faraday de acuerdo a TIA-942 y EN 61000-4-3 y EN 61000-4-8.

- Estanqueidad: Posee resistencia al polvo y agua de incendio de acuerdo a la norma EN 60529 con clasificación IP65. Posee ensayo de Inundación por columna de agua perimetral. Ensayos Certificados por SGS y TUV.

- Barrera de Vapor: cumplimenta las exigencias de NFPA 75.

- Monitoreo ambiental: monitoreo de temperatura, humedad, iluminación, ruido, flujo de aire, polvo, corriente, polución, etc.

- Detección y combate de Incendio: Sistema de supresión de incendio no contaminante para personas ni medio ambiente por medio de agente limpio conforme NFPA 2001.

- Diseño flexible : La Sala Cofre Smart Shelter+ es la mas liviana del mercado siendo apta para instalarse en pisos superiores y adaptable para poder ser

relocalizable. Puede instalarse en interiores (room in a room) o en el exterior (outdoor) sin protección adicional.

- Construcción Modular : Construida en base a paneles de 1000/1200 mm de ancho y de hasta 5 m de alto pueden ser customizadas de acuerdo a las necesidades y expandidas en el futuro.

4.3.4.3. Resguardo Físico de Elementos Sensibles

Está constituido por una caja de seguridad o gabinete reforzado con cerradura antirrobo.

La línea Polaris de Rosengrens ofrece una nueva generación de cofres ignífugos para medios magnéticos testeados y certificados para soportar dos horas de fuego.

Este tipo de cofres ofrecen el máximo de capacidad en el mínimo de espacio con una extensa variedad de accesorios internos para acomodar distintos tipos de medios magnéticos (CD / DAT / DLT / 3480). Están testeados y aprobados de acuerdo a normas y estándares de Calidad ISO 9001 y los estándares de protección del medio ambiente ISO 14000. Además de ofrecer protección anti robo, poseen protección antimagnética.

Los cofres están disponibles en 5 tamaños diferentes:

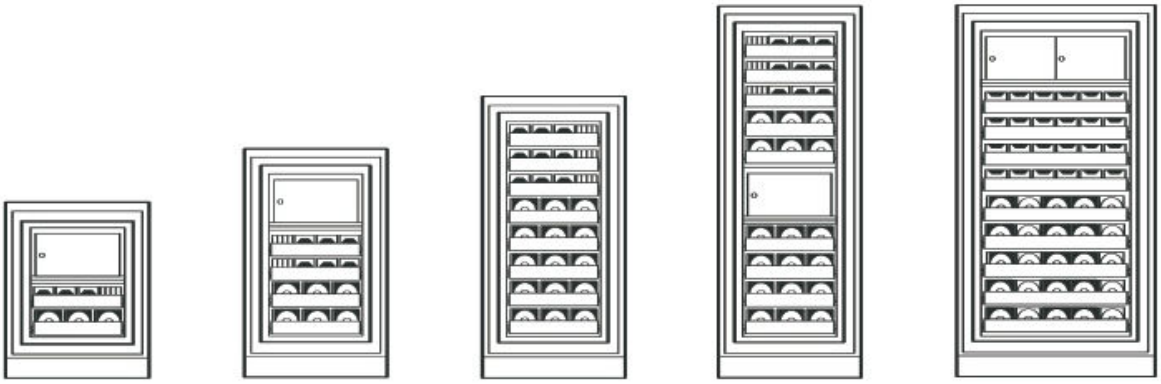


Figura 19: Modelos de cofres ignífugos

En el siguiente cuadro se pueden observar las especificaciones de cada uno de los 5 productos que ofrece la línea Polaris:

Product Data

Modelo	Dimensiones Externas (mm) Alto	Ancho	Prof.*	Dimensiones Internas (mm) Alto	Ancho	Prof	Peso**(Kg)	Vol (l).
D120	920	750	720	570	490	400	318	115
D170	1200	750	720	850	490	400	395	171
D230	1480	750	720	1130	490	400	495	227
D320	1950	750	720	1580 (1600)	490	400	645 (635)	316 (321)
D570	1950	1040	770	1580 (1600)	780	460	865 (840)	577 (587)

Dimensiones entre () son válidas para D320 y D570 aprobadas bajo UL Clase 125 2Horas. El resto de medidas son válidas para las dos certificaciones.
* No contemplan 61 mm para manipuleo. ** Peso vacío y sin packing.

Capacidad de Almacenamiento

Tipo de Medio Mag.	Tamaño En mm	Medios x Estante D120 - D320	D570	No Total de Medios Mag. / No de Estantes D120	D170	D230	D320	D570
CD/DVD	142x124x10	117	225	468/4	702/6	936/8	1404/12	2700/12
Zip drives	103x104x12	128	250	640/5	896/7	1280/10	1742/14	3500/14
DLT tapes	110x112x30	48	94	192/4	336/7	432/9	624/13	1222/13
DAT cassettes	80x60x15	134	260	1072/8	1608/12	2144/16	3216/24	6240/24
LTO tapes	102x105x22	68	120	272/4	476/7	612/9	884/13	1560/13

Figura 20: Capacidad de almacenamiento de cofres ignífugos

El modelo D120 contempla la capacidad de almacenamiento necesaria, y ofrece un tiempo más que aceptable de protección ignífuga.

4.3.4.4. Prevención y Protección contra Incendios

En el punto 4.3.5.2. (Acceso Físico a las Instalaciones) fueron descriptas las principales propiedades ofrecidas por la Sala Cofre Smart Shelter+ en donde se destacan como prevención y protección contra incendios:

- Cumplimiento de los requerimientos de protección al fuego para clasificación TIER III & TIER IV.
- Paneles conformados como un sándwich de chapa de acero con clasificación RF 120de acuerdo a EN 13501.
- Los paneles están construidos en base a un corazón de compuestos aislantes que soportan 945º C de temperatura sin que la interior aumente más de 12º C.
- Posee la mayor estabilidad térmica del mercado. Ensayos certificados por SGS y TUV Rheinland.

- La temperatura interior no supera los 48.9º C establecidos por NFPA 75.
- La estructura sólida de la bóveda, conformada por su sistema de acero estructural soporta más que una construcción tradicional. Los paneles están revestidos por una chapa de acero galvanizado con un acabado lacado en ambos lados. En su interior poseen material termoaislante e ignífugo.
- Posee monitoreo ambiental (temperatura, humedad, iluminación, ruido, flujo de aire, polvo, corriente, polución, etc.)
- Posee un sistema de supresión de incendio no contaminante para personas ni medio ambiente por medio de agente limpio conforme NFPA 2001.

4.3.4.5. Acondicionamiento Ambiental

Dentro de la Sala Cofre Smart Shelter+ se previó espacio para instalar equipos de aire acondicionado de precisión. Los mismos son 2 Split que van colocados uno arriba de otro para obtener redundancia.

De acuerdo a las dimensiones de la Sala Cofre, se realiza el cálculo correspondiente para saber las frigorías necesarias para mantener un ambiente óptimo. El resultado de la misma es de 2200 Kcal aproximadamente como se muestra en la figura 20.

Figura 21: Cálculo de frigorías para acondicionamiento ambiental

Según los valores obtenidos en el cálculo térmico, y considerando redundancia para aumentar la confiabilidad y disponibilidad de la Sala Nivel 4 (N4), se decide instalar 2 equipos de aire acondicionado uno arriba de otro con las siguientes características:

Marca / Modelo: AIRE ACONDICIONADO SAMSUNG AS09UG

Refrigeración: 2700 Kcal

Dimensiones: 54,8 alto x 72 ancho x 26,5 de profundidad

Origen: Argentina

4.3.5. Plataforma Tecnológica

Ajustándose a los Estándares Tecnológicos vigentes requeridos por el proceso de certificación se definen las necesidades de la Plataforma Tecnológica del Proyecto.

4.3.5.1. Servidores

Para Empresas y Corporaciones con grandes necesidades podemos encontrar el modelo de HP Proliant DL580 G7 (figura 22). El mismo tiene grandes capacidades de desempeño y rendimiento, con un agregado de hasta un 70% de ahorro energético respecto a otros modelos.

Figura 22: Servidor HP Proliant DL 580 G7

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

  - 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 (Listo): esta función amplía la capacidad de resistencia ante fallos en dos x4 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 2: Especificaciones técnicas - Servidor HP Proliant DL 580 G7

4.3.5.2. Almacenamiento, Respaldo y Recuperación

El certificador debe:

- Mantener el control exclusivo sobre las claves criptográficas durante su almacenamiento y sobre sus copias de respaldo.
- Implementar procedimientos para realizar la recuperación de sus claves a partir de copias de respaldo.

A fin de cumplimentar con los requisitos legales descriptos en el Artículo 30 de la ley 25506, no está permitida la custodia de claves criptográficas por parte de terceros.

Para cumplir con los requisitos descriptos se diseña el siguiente esquema de almacenamiento que se aplica a todos los documentos y datos en soporte magnético y/o digital de valor para el Sistema 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 es necesario preservar por formar parte de los procesos que integran el Sistema 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:

Unidad de Cinta SDLT 600 Quantum

Figura 23: Unidad de cinta SDLT 600 Quantum

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

4.3.5.3. 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 (http://www.apc.com).

La elección de esta marca es debido 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 elegido es APC Smart-UPS y sus características son las siguientes:

APC Smart-UPS RT 1000VA 230V

Figura 24: UPS (suministro de energía ininterrumpible)

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.

4.3.6. Software y Licencias

Hay muchas razones por las que se consideró usar Linux como Sistema Operativo de los Servidores y Workstation.

La principal razón es que es un Sistema Operativo libre, es decir, no necesitamos adquirir licencias a un determinado costo para utilizarlo. La mayoría del software para Linux es también gratuito.

También existen otras razones secundarias pero no menores por la cual se decidió utilizar Linux:

- 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

4.3.7. Publicación Oficial

De acuerdo al artículo 21 (punto I) del Capítulo I de la Ley de Firma Digital, es obligación por parte del certificador licenciado publicar en el boletín oficial aquellos datos que la autoridad de aplicación determine.

Por tal motivo, se publicarán dichos actos en el formato exigido para la publicación de edictos (Resolución Nº 01/09) que son:

a) El documento deberá ser presentado en soporte papel por duplicado en hoja A4, letra Arial 12, interlineado 1,5 cm., margen derecho 2 cm., izquierdo 4,5 cm., superior 4 cm. e inferior 2,5 cm., con firma, sello y aclaración del interesado y/o profesional interviniente.

b) Una vez ingresada la/s publicación/es deberán remitirse por correo electrónico el/los textos como archivo adjunto a la siguiente dirección: boletinoficialcba@cba.gov.ar o boletinoficialweb@cba.gov.ar.
En el asunto del mail se deberá colocar el número de aviso asignado.

4.3.8. Aranceles y Garantías

Los trámites que se realicen ante el ente licenciante están sujetos al pago de los siguientes aranceles a saber:

CONCEPTO	IMPORTE
Por solicitúd de licencia única y supervisión del proceso de licenciamiento:	$ 30.000
Por obtención de licencias adicionales en caso de infraestructura previamente inspeccionada por el ente licenciante, cuyo nivel de seguridad y prestaciones sean adecuados para las necesidades de las nuevas políticas a licenciar:	$ 15.000
Por renovación de licencia:	$ 15.000
Monto mínmo a integrarse en concepto de garantía o seguro de caución:	$ 500.000

4.3.9. Algoritmo Criptográfico

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 Infraestructura de Firma Digital de la República Argentina (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**.

En nuestro caso para la generación de claves se utilizará el algoritmo criptográfico asimétrico RSA debido a las siguientes ventajas de utilizar el mismo:

- No requiere claves secretas.
- Permite Encriptar y Firmar digitalmente.
- Utilizado conjuntamente con DES otorga una mayor velocidad de operación.
- La clave DES, empleada por RSA, es válida para un único mensaje, en el peor de los casos en que se logre 'quebrar' la clave, ésta no se puede aplicar para otro mensaje o documento.
- Permite además la detección de:
    - Alteraciones en los documentos.
    - Errores en la transmisión de documentos.
- Es un estándar internacional.

4.4. Conclusión

Podemos considerar que hemos logrado cumplir los objetivos planteados para esta etapa del proyecto:

- Definir los requerimientos para la implementación de Firma Digital en el Instituto Universitario Aeronáutico
- Definir los requerimientos para implementar una Autoridad Certificante que permita al IUA generar sus propios certificados
- Modelar un esquema de Firma Digital y Autoridad Certificante, en base a la aplicación de los patrones de diseño, considerando las tecnologías y estándares estudiados.

El análisis teórico realizado anteriormente y la aplicación de los patrones de diseño a la situación problemática nos han brindado requerimientos para el desarrollo de una Infraestructura de Firma Digital que se ajusta al objetivo principal del trabajo.

Las decisiones tomadas y los detalles brindados nos dan la base para el desarrollo de la última etapa del proyecto, donde abarcaremos la concreción del modelo teórico.

5. Concreción del Modelo

5.1. Introducción

Ingresamos a la parte final del Proyecto, en la cual buscaremos lograr la ultima parte del objetivo general concretando la implementación de Firma Digital, en base a lo desarrollado en el modelo teórico y el marco teórico. En esta sección buscaremos cumplimentar el siguiente objetivo específico:

Realizar la simulación del ente certificante en base a la aplicación de los patrones de diseño, utilizando como base OpenSSL 0.9.8o y Apache Server 2.2.17 ejecutándose sobre un Sistema Operativo Linux distribución Ubuntu Server 11.04.

En busca de este objetivo analizaremos cada uno de ellos, realizaremos una descripción e indicaremos como obtener una información más detallada de cada uno.

Además podremos observar interfaces de la generación de certificados.

Por último, analizaremos la puesta en marcha considerando las necesidades técnicas que presenta el modelo elegido, así como 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, por ejemplo Apache.

Sitio principal del proyecto: http://www.openssl.org

La distribución puede ser obtenida en: http://www.openssl.org/source/openssl-0.9.8o.tar.gz

5.2.2. Apache Server

Apache es un servidor web gratuito, potente y que nos ofrece un servicio estable y sencillo de mantener y configurar. Es indiscutiblemente uno de los mayores logros del Software Libre.
Destacaremos las siguientes características:

- Es multiplataforma, aunque idealmente está preparado para funcionar bajo linux.
- Muy sencillo de configurar.
- Es Open-source.
- Muy útil para proveedores de Servicios de Internet que requieran miles de sitios pequeños con páginas estáticas.
- Amplias librerías de PHP y Perl a disposición de los programadores.
- Posee diversos módulos que permiten incorporarle nuevas funcionalidades, estos son muy simples de cargar.
- Es capaz de utilizar lenguajes como PHP, TCL, Python, etc.

Sitio principal del proyecto: http://www.apache.org

La última distribución puede ser obtenida en: http://apache.xmundo.com.ar//httpd/httpd-2.2.19.tar.gz

5.2.3. Arquitectura del Sistema

Este proyecto como la mayoría de las aplicaciones que utilizan las Firmas Digitales tienen arquitectura cliente-servidor.

Del lado del cliente hemos utilizado un programa para realizar conexiones con servidores remotos por línea de comandos llamado PuTTY release 0.61. 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, en el que nos conectamos a otra máquina a través de la red, aunque en este caso se realizan las conexiones cifradas, lo que aumenta la seguridad, pues evitamos que otras personas puedan ver las comunicaciones entre el ordenador origen y destino.

Del lado del servidor hemos trabajado sobre un sistema operativo Linux distribución Ubuntu Server 11.04. En el mismo se instaló OpenSSL 0.9.8o y Apache Server 2.2.17 provisto en el paquete LAMP (Linux,Apache,MySQL,PHP) de Ubuntu Server.

El servidor Ubuntu está montado sobre una máquina virtual VMWare 1.0.10 a través de técnicas de virtualización.

La virtualización simplemente 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 maquina host) para emular o imitar el comportamiento de algún sistema o de una misma pc, esto se lleva a cabo mediante una maquina virtual.

El concepto de maquina 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, un poco abstracto el concepto pero podría resumirse como una PC nueva con otro sistema operativo, disco duro, memoria y procesador (todo virtual) dentro de una PC física.

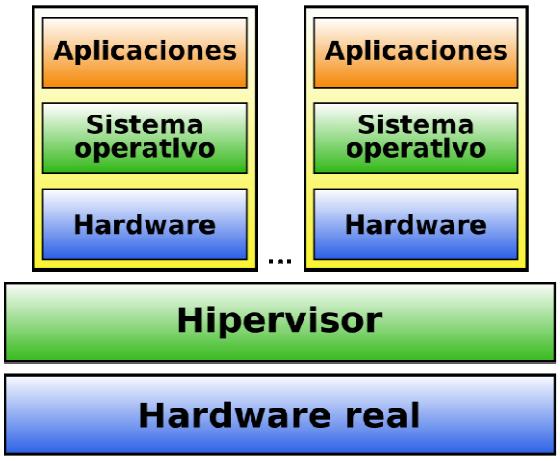


Figura 25: Virtualización

5.3. Pruebas

Para acercarnos un poco más a los temas desarrollados en este proyecto, vamos a ejecutar y analizar el proceso de creación de una Entidad Certificadora y la generación de certificados digitales.

El objetivo es demostrar, a través de elementos de entrada, cuales son los resultados obtenidos.

Para poder llevar adelante las pruebas, es necesario cumplir con ciertos requisitos. Uno de ellos es tener instalado Openssl que vamos a corroborar de la siguiente manera:

```
anghilla@NBUbuntu:~$ openssl version
OpenSSL 0.9.8o 01 Jun 2010
```

Podemos ver que tenemos instalada la versión 0.9.8o que es del 01 de Junio del 2010.

Otro requisito es tener el servidor Apache, ya que el certificado a crear será para ser utilizado en una aplicación web, y que posea el módulo ModSSL.

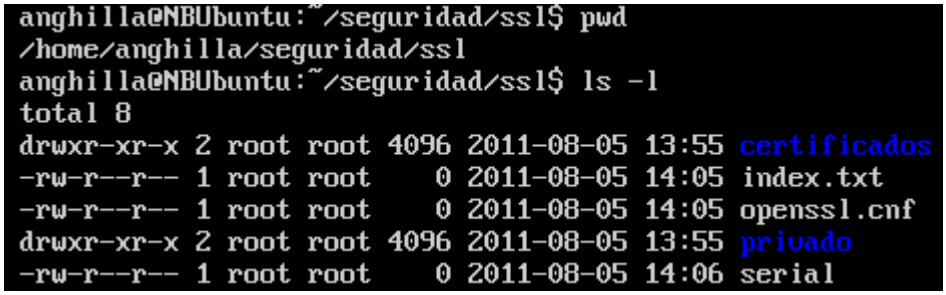
```
anghilla@NBUbuntu:~$ apache2 -v
Server version: Apache/2.2.17 (Ubuntu)
Server built:   Feb 22 2011 18:33:02
```

```
anghilla@NBUbuntu:/etc/apache2/conf.d$ sudo a2enmod ssl
[sudo] password for anghilla:
Enabling module ssl.
See /usr/share/doc/apache2.2-common/README.Debian.gz on how to configure SSL and
 create self-signed certificates.
Run '/etc/init.d/apache2 restart' to activate new configuration!
```

De esta manera hemos corroborado que tenemos instalado OpenSSL y el servidor Apache por lo que tenemos todo como para empezar sin mayores inconvenientes.

5.3.1. Estructura de Directorios

Para comenzar vamos a crear distintos archivos y directorios que sirven para crear los certificados y mantener un cierto orden, así es como tenemos el siguiente esquema:



La utilización de cada uno de ellos es para:

- certificados: directorio donde se guardan las copias de los certificados creados
- privado: directorio contenedor de la llave privada
- serial: contenedor del número de serie del siguiente certificado a crear, inicialmente en 01.
- index.txt: inicialmente vacío, se utilizará como una base de datos en base al número de serie.
- openssl.cnf: configuración a importar al realizar los certificados.

Cabe aclarar que para que el comando que se va a ejecutar a continuación funcione correctamente es necesario que el archivo openssl.cnf esté completo como se detalla a continuación:

```
dir     = .
default_ca = CA_default
[CA_default]
serial  = $dir/serial
database        = $dir/index.txt
new_certs_dir   = $dir/certificados
certificate     = $dir/cacert.pem
private_key     = $dir/privado/cakey.pem
default_md      = md5
preserve        = no
nameopt         = default_ca
certopt         = default_ca
policy          = policy_match
[policy_match]
countryName     = match
stateOrProvinceName     = match
organizationName        = match
organizationalUnitName  = optional
commonName      = supplied
emailAddress    = optional
[req]
default_bits    = 1024
default_keyfile = key.pem
default_md      = md5
string_mask     = nombstr
distinguished_name      = req_distinguished_name
req_extensions  = v3_req
[req_distinguished_name]
0.organizationName      = Nombre de la organizacion
```

```
0.organizationName_default      = IUA
organizationalUnitName  = Ingenieria en Sistemas
emailAddress    = Correo electronico
emailAddress_max        = 40
localityName    = Ciudad
localityName_default    = Cordoba
stateOrProvinceName     = Provincia
stateOrProvinceName_default     =       Cordoba
countryName     = Codigo del pais (dos letras)
countryName_default     = AR
countryName_min = 2
countryName_max = 2
commonName      = Nombre comun (hostname o IP)
commonName_max  = 64
[v3_ca]
basicConstraints        = CA:TRUE
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always,issuer:always
[v3_req]
basicConstraints        = CA:FALSE
subjectKeyIdentifier    = hash
```

5.3.2. Crear la Entidad Certificadora

Lo primero que hay que hacer es crear un certificado que nos validará como autoridad certificadora CA. La clave que nos pedirá será la clave privada de dicha CA y quedará guardada en el directorio "privado" como se había estipulado. Finalmente obtendremos dos archivos, el certificado raíz, cacert.pem, (que servirá para firmar certificados para las aplicaciones web y luego ser validados por el navegador) y la clave privada, cakey.pem. (PEM, Privacy Enhanced Message).

```
anghilla@NBUbuntu:~/seguridad/ssl$ sudo openssl req -new -x509 -extensions v3_ca
 -keyout privado/cakey.pem -out cacert.pem -days 3650 -config ./openssl.cnf
Generating a 1024 bit RSA private key
..++++++
.........++++++
writing new private key to 'privado/cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Nombre de la organizacion [IUA]:IUA
Departamento o division []:Ingenieria en Sistemas
Correo electronico []:anghilla@gmail.com
Ciudad [Cordoba]:Cordoba
Provincia [Cordoba]:Cordoba
Codigo del pais (dos letras) [AR]:AR
Nombre comun (hostname o IP) []:NBUbuntu
anghilla@NBUbuntu:~/seguridad/ssl$
```

Las opciones utilizadas tienen el siguiente propósito:

- req –new –x509. Crea un certificado nuevo autofirmado.
- -extensions v3_ca. Crea un certificado raíz CA.
- -keyout. Nombre y donde guardará la llave.
- -out. Nombre del certificado raíz CA.
- -days. Cantidad de días que el certificado tendrá validez.
- -config. Archivo de configuración a utilizar.

Podemos hacer consultas al certificado de la CA, por ejemplo, el tiempo de validez del mismo.

```
anghilla@NBUbuntu:~/seguridad/ssl$ openssl x509 -in cacert.pem -noout -dates
notBefore=Aug  8 15:24:37 2011 GMT
notAfter=Aug  5 15:24:37 2021 GMT
```

5.3.3. Crear un Certificate Signing Request (CSR) (Solicitud de firmado de certificado)

Ya tenemos un certificado Raíz que nos valida como CA. A continuación lo que necesitamos es tener un certificado firmado por una CA, que somos nosotros mismos en este caso, para utilizar en el servicio a prestar y brindar la seguridad deseada. Por lo tanto se generará una solicitud de firmado de certificado con el comando openssl para lograr lo anterior. Casi todo será igual a lo anterior. Solo que en la solicitud de firmado no es necesario especificar una contraseña, aunque si se generará una clave privada para la solicitud.

```
anghilla@NBUbuntu:~/seguridad/ssl$ sudo openssl req -new -nodes -out iua-cert.pe
m -config ./openssl.cnf
[sudo] password for anghilla:
Generating a 1024 bit RSA private key
..................++++++
.....................................................................................
...++++++
writing new private key to 'key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Nombre de la organizacion [IUA]:IUA
Departamento o division []:Departamento Sistemas
Correo electronico []:anghilla@gmail.com
Ciudad [Cordoba]:Cordoba
Provincia [Cordoba]:Cordoba
Codigo del pais (dos letras) [AR]:AR
Nombre comun (hostname o IP) []:iua.edu.ar
```

Ahora hemos obtenido dos nuevos archivos:

- iua-cert.pem: solicitud de firmado de certificado
- key.pem: la clave privada

Las opciones utilizadas tienen el siguiente propósito:

- req. Requerimiento de solicitud de nuevo certificado
- -out. Nombre del certificado que deseamos firmar.
- -config. Archivo de configuración a utilizar.
- -nodes: llave privada sin contraseña

La solicitud que acabamos de realizar debe ser firmada por una CA, que en este caso somos nosotros mismos. Con el comando siguiente se puede verificar que se trata de un requerimiento de certificado.

```
anghilla@NBUbuntu:~/seguridad/ssl$ openssl req -in iua-cert.pem -text -verify -n
oout
```

5.3.4. Firmar el Certificado

Por último firmaremos la solicitud que hicimos en el paso previo, para firmarlo necesitaremos indicar la contraseña que autentifique que somos la CA y que por serlo tenemos la autoridad de autorizar (firmar) certificados. (Para nuestro propio uso).

Al final se realizan dos preguntas a las que responderemos afirmativamente, ellas son para confirmar el tiempo de validez del certificado y para guardarlo en la base de datos (archivo index.txt).

```
anghilla@NBUbuntu:~/seguridad/ssl$ sudo openssl ca -out certificado-iua.pem -con
fig ./openssl.cnf -days 3650 -infiles iua-cert.pem
Using configuration from ./openssl.cnf
Enter pass phrase for ./privado/cakey.pem:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
organizationName      :PRINTABLE:'IUA'
organizationalUnitName:PRINTABLE:'Departamento Sistemas'
emailAddress          :IA5STRING:'anghilla@gmail.com'
localityName          :PRINTABLE:'Cordoba'
stateOrProvinceName   :PRINTABLE:'Cordoba'
countryName           :PRINTABLE:'AR'
commonName            :PRINTABLE:'iua.edu.ar'
Certificate is to be certified until Aug  5 16:25:58 2021 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Las opciones utilizadas tienen el siguiente propósito:

- ca. Se firmará el certificado como CA.
- -out. Nombre del certificado firmado.
- -config. Archivo de configuración a utilizar.
- -infiles: archivo de donde toma la solicitud de firmado

Luego se puede comprobar cómo se incrementa el número de serie y el registro que queda guardado en la base de datos. También se almacena en el directorio "certificados" un certificado con el correspondiente número de serie, el cual complementa la base de datos.

```
anghilla@NBUbuntu:~/seguridad/ssl$ more serial
02
anghilla@NBUbuntu:~/seguridad/ssl$ more index.txt
V       2108051625582           01      unknown /C=AR/ST=Cordoba/O=IUA/OU=Depart
amento Sistemas/CN=iua.edu.ar/emailAddress=anghilla@gmail.com
anghilla@NBUbuntu:~/seguridad/ssl$ ls -l certificado-iua.pem
-rw-r--r-- 1 root root 2699 2011-08-08 13:26 certificado-iua.pem
```

5.3.5. Configuración del Servidor Web

Tenemos entonces dos elementos ya generados que necesitaremos para Apache:

- key.pem (la llave privada)
- certificado-iua.pem (certificado autofirmado)

Teniendo asegurado que se ha habilitado el módulo SSL en apache, como se mostró al inicio del documento, se procede a cambiar la configuración del servicio.

El archivo en cuestión se llama "default" ubicado en el directorio sites-available del apache, generalmente ubicado en /etc/apache2 para Ubuntu, o /etc/httpd para sistemas basados en Debian.

La configuración a realizar es la detallada a continuación:

```
NameVirtualHost *:443
<VirtualHost *:443>
        ServerName iuatesting.edu.ar
        DocumentRoot /var/www/ejemplo
        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/certificado-iua.pem
        SSLCertificateKeyFile /etc/apache2/ssl/key.pem
</VirtualHost>
```

Donde:

- ServerName. Es el nombre del sitio a utilizar el certificado
- DocumentRoot. Directorio donde se aloja el sitio
- SSLEngine. Habilitación del módulo SSL

- SSLCertificateFile: certificado firmado por la CA a utilizar
- SSLCertificateKeyFile: archivo de clave privada del certificado

Aclaración: iuatesting.edu.ar se ha agregado a /etc/hosts para que sea resuelto por el servicio de dominio nombres y su valor es 127.0.0.1.

Finalmente debemos reiniciar el servicio web para que los cambios surjan efecto.

```
anghilla@NBUbuntu:/etc/apache2/sites-available$ sudo /etc/init.d/apache2 restart
```

5.3.6. Ingreso al Sitio desde un Navegador Web

Desde un navegador ingresamos en el url https://iuatesting

Obtendremos un error sec_error_unknown_issuer, ya que el certificado no será confiable para el navegador porque el emisor del certificado es desconocido.

De esta manera será el usuario el que debe decidir si continuar o no en el sitio, de querer seguir adelante, debe agregar el certificado como conocido o excepción de seguridad y podrá ingresar de esa forma al sitio.

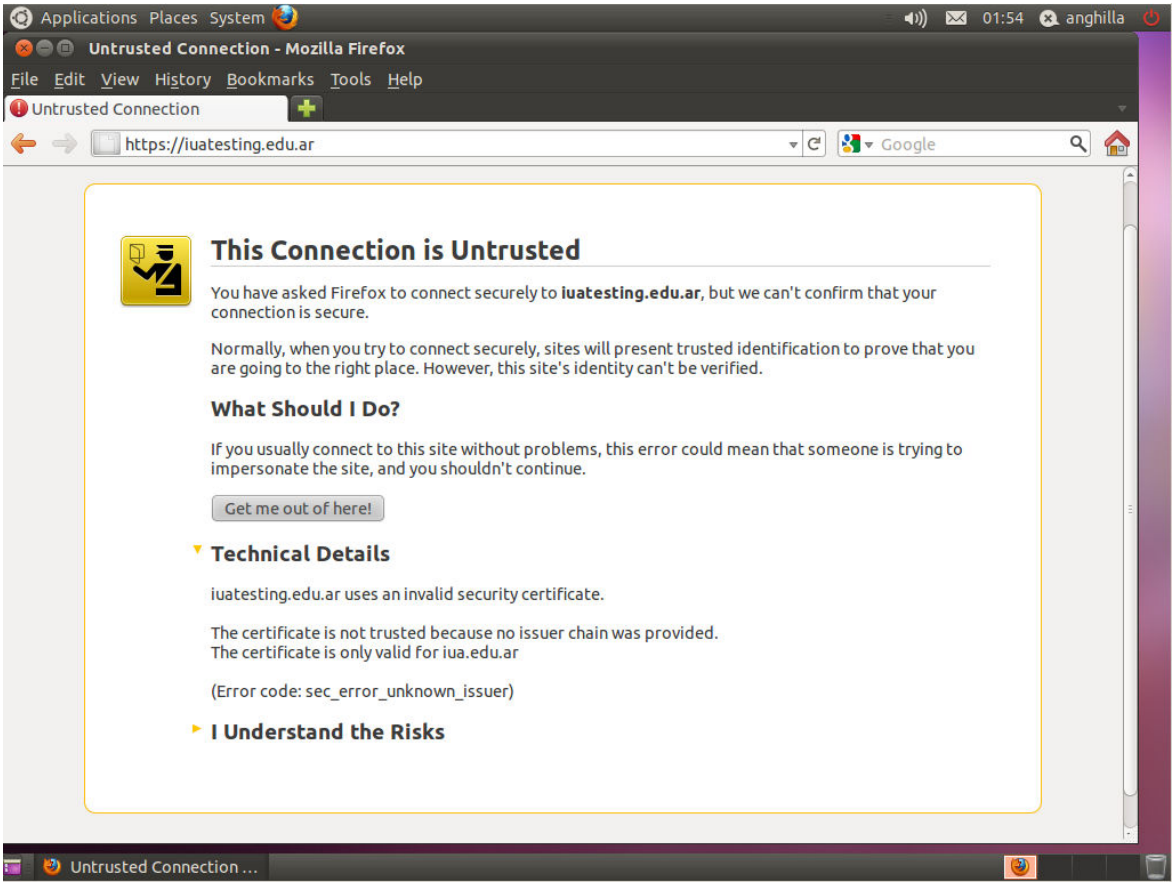


Figura 26: Pruebas - Ingreso al sitio desde un navegador web

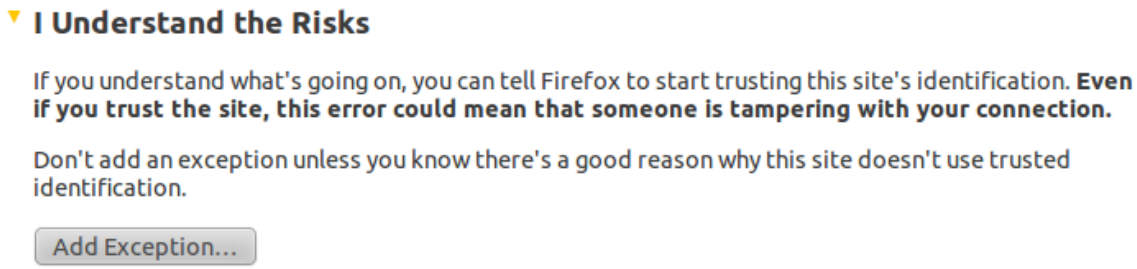


Figura 27: Pruebas – Mensaje de reconocimiento de sitio web riesgoso

Figura 28: Pruebas – Agregando una excepción de seguridad

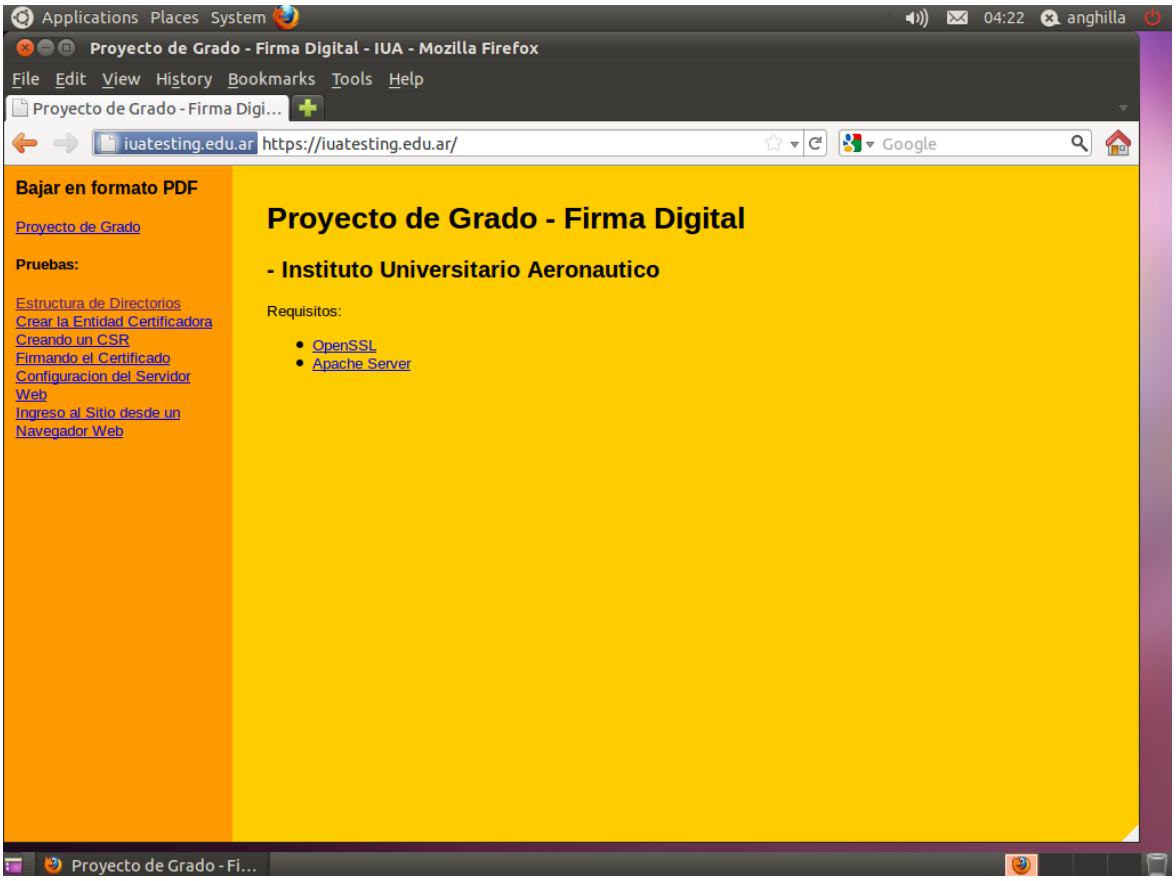


Figura 29: Pruebas – Sitio web seguro (HTTPS)

5.4. Puesta en Marcha

Especificamos a continuación las principales acciones a realizar para que el modelo sea aplicado a la realidad.

5.4.1. Infraestructura necesaria

Nuestra entidad certificadora utiliza como base OpenSSL 0.9.8o y Apache Server 2.2.17 ejecutándose sobre un Sistema Operativo Linux distribución Ubuntu Server 11.04.

Por tanto los requerimientos de hardware dependen directamente del Sistema Operativo a utilizar. En nuestro 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. Dependiendo de sus necesidades, podría arreglarse con menos que eso, sin embargo, no es aconsejable.

En el punto 5.2.1 y 5.2.2 se encuentran las referencias a los sitios donde se pueden obtener OpenSSL y Apache Server en sus variadas versiones, en tanto que Ubuntu Server puede obtenerse desde su sitio oficial http://www.ubuntu.com/download/server/download

Como se comentó en la etapa de requerimientos, la sala cofre Smart Shelter+ es una solución que se adapta perfectamente a nuestras necesidades, ya que está pensado para ser utilizado en proyectos de firma digital y es ofrecido por una empresa de gran envergadura como lo es Area Data.

Se puede consultar el producto en un catalogo virtual, como también otros productos de gran importancia para nuestro proyecto en http://www.areadata.com.ar

5.4.2. Capacitación a usuarios

Los usuarios tendrán una inducción general a cerca de la nueva implementación de firma, en donde se podrá visualizar el proceso y como utilizar el nuevo mecanismo.

Además se informará y se capacitará sobre el buen uso de claves públicas y privadas y el valor importante que tiene cada uno de estos datos para el usuario.

Se desea lograr el menor impacto de cambios, logrando así que el usuario pueda interactuar y adaptarse de manera correcta a la nueva plataforma de firma digital.

5.5. Prefactibilidad

Luego de realizar el desarrollo del proyecto propuesto y de establecer las causas que merecen de implementar un sistema de firma digital, es necesario realizar un análisis de la prefactibilidad del proyecto valorada en los siguientes aspectos: técnico, operacional y económico, para satisfacer con los objetivos de la organización.

5.5.1. Prefactibilidad Técnica

Se ha dispuesto una evaluación a cerca de los recursos técnicos disponibles actuales en la Universidad, para poseer información sobre la tecnología que se posee, si éstos pueden ser

útiles para la implementación del proyecto y también si es necesario adquirir otras tecnologías para poder llevar a cabo la puesta en marcha del sistema de firma digital.

Además del equipamiento que se encuentra en la Universidad, destacamos la necesidad de adquirir otras tecnologías para el correcto desarrollo, funcionamiento y cumplimiento de las normativas para el proyecto.

Cantidad	Descripción
1	Servidor HP Proliant DL580 G7
1	Unidad de Cintas de Backup SDLT 600 Quantum
1	UPS APC Smart-UPS RT 1000VA 230V
1	Cofre Ignífugo Polaris D120
1	Sala Cofre Smart Shelter+ de AST
2	Unidad de Aire Acondicionado Samsung

Tabla 3: Insumos requeridos

En lo que respecta al software, las estaciones de trabajo de los usuarios operan bajo ambiente de Windows, y en lo que respecta al servidor se requerirá el sistema operativo Linux. Para el uso general de las actividades, solo basta contar con las herramientas de escritorio y office utilizadas actualmente.

En base a los análisis y estudios realizados, el proyecto es factible en el marco de lo técnico.

Luego analizaremos el aspecto de la factibilidad económica, para lograr y alcanzar los requerimientos propuestos anteriormente.

5.5.2. Prefactibilidad Operativa

Mediante el estudio de la prefactibilidad operativa, podemos estimar que el proyecto será utilizado y operado de manera correcta por los usuarios involucrados, aprovechando así las ventajas que este nuevo sistema genera en las actividades que se desarrollan diariamente.

Existe una necesidad de mejoras y actualización en los procesos que hoy se llevan a cabo, por los mismos avances tecnológicos, que permita reemplazar la firma manuscrita por firma digital y utilizar el formato electrónico en todo el proceso del circuito de actas de exámenes generados. El usuario se ve beneficiado con las características de garantía de autoría e integridad de los documentos digitales; la validez legal a la documentación electrónica, y con un novedoso mecanismo de seguridad técnica.

Además, de contribuir con el proceso de "despapelización" y reducir así la cantidad de archivos, ganando espacios y disponibilidad de cada documento cuando se requiera, el personal colabora con el medio ambiente, minimizando el costo del papel.

Para poder garantizar el efectivo funcionamiento de este nuevo sistema de firma digital y además que sea aceptado positivamente por el usuario, se realizaron capacitaciones para conocer el nuevo mecanismo y generar una herramienta útil y amigable al usuario.

5.5.3. Prefactibilidad Económica

De acuerdo al estudio realizado a cerca de la prefactibilidad económica para implementar el proyecto, se presentan a continuación el análisis de costos y beneficios. Se determinan los recursos necesarios para desarrollar, implementar y mantener el proyecto presentado, evaluando los costos requeridos pero atendiendo a su vez, los beneficios que se derivarán con su ejecución.

5.5.3.1 Análisis costo beneficio del sistema propuesto

El sistema propuesto de implementación de firma digital, involucra los siguientes costos:

- **Costos generales**

Al implementar el proyecto propuesto, se logran optimizar varios procesos, mejorando los tiempos de respuesta, de entrega de documentos (actas, notas, etc.) y aumenta la seguridad de la información. Reduce la cantidad de tareas, procesos que deben seguirse, logrando así alcanzar los resultados esperados.

Se puede estimar que el uso de planillas, actas e impresión de cada solicitud se reduciría en un 50%, permitiendo así ahorrar en el uso de papel y material de oficina, tóner de impresora, archivadores, etc. Además que los archivos al encontrarse automatizados,

pueden ser consultados en cualquier momento, lo que mejora los tiempos y recursos de oficina en el momento de disponer con la información requerida en tiempo oportuno y óptimo.

Además de permitir que las planillas y documentos puedan ser firmados y enviados por mail por el usuario desde cualquier punto geográfico, sin la obligación de presentar la hoja física firmada en la secretaría, mejora los tiempos de respuesta y comodidad para el usuario.

- **Costos de hardware, software e infraestructura**

De acuerdo a lo mencionado en la prefactibilidad técnica, se necesita de una inversión en equipamientos necesarios para la puesta en marcha del proyecto.

En los siguientes cuadros se detallan los costos en dólares[5].

Cantidad	Descripción	Precio (U$S)
1	Servidor HP Proliant DL580 G7	U$S 7617
1	Unidad de Cintas de Backup SDLT 600 Quantum	U$S 2450
5	Cintas de Backups	U$S 250
1	UPS APC Smart-UPS RT 1000VA 230V	U$S 913
1	Cofre Ignífugo Polaris D120	U$S 6252
1	Sala Cofre Smart Shelter+ de AST	U$S 195000
2	Unidad de Aire acondicionado Samsung as09ug	U$S 1250
1	Sistemas de Seguridad Externa	U$S 1000
1	Reforma Edilicia	U$S 200
	TOTAL	**U$S 214932**

Tabla 4: Costos de Hardware e infraestructura

[5] Se toma como base cotización a $4.17 ARS

Licencia	Costo de Licencias (U$S)
Linux S.O	Gratuita – open source
Solicitud de licencia única (Licencia CA)	U$S 4500
Garantía o Seguro de Caución	U$S 120000
Renovación de licencia (cada 5 años). No aplicable en el costo inicial.	U$S 3750 (dentro de 5 años)
TOTAL	**U$S 124500**

Tabla 5: Costos de Software y licencias

- **Costo de personal**

En lo que respecta al costo de personal, para poder desarrollar el sistema propuesto se necesitó de personal capacitado por lo que se generan los costos que a continuación se detallan en la tabla 6.

Estos costos se definen: personal por hora para realizar el modelo teórico y concreción de modelo. El cálculo está basado en 4 hs 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, teniendo en cuenta los honorarios publicados por el Consejo Profesional de Ciencias Informáticas de la Provincia de Córdoba (CPCIPC)[6].

[6] La información de los costos mensuales se pueden consultar en la página www.cpcipc.org

Actividad	Tipo personal	Costo(U$$)/hs	Horas	Total (U$$)
Planificación	Analista de Proyectos	10,80	100	U$$ 1080
Análisis requerimientos	Analista	21,58	40	U$$ 863
Análisis de sistema	Analista	21,60	60	U$$ 1295
Diseño de sistemas	Analista	21,60	80	U$$ 1727
Implementación	Desarrollador	33,57	100	U$$ 3357
Capacitación de usuarios	Instructor	19,2	5	U$$ 96
		Total		**U$$ 8418**

Tabla 6: Costo de personal

- **Resumen de Costos (U$$)**

Resumen de Costos	U$$
Costos de Hardware e Infraestructura	U$$ 214932
Costo de Software y Licencias	U$$ 124500
Costo de Personal	U$$ 8418
Total	**U$$ 347850**

Tabla 7: Resumen de Costos

Se puede deducir entonces, que el costo total del sistema es de **U$$ 347850.**

5.5.3.2 Análisis costo-beneficios

En el siguiente cuadro se observa los costos anuales y beneficios en 9 años de la aplicación del proyecto (U$$).

Período en años	0 Año 0	1 Año 1	2 Año 2	3 Año 3	4 Año 4	5 Año 5	6 Año 6	7 Año 7	8 Año 8	9 Año 9
Inversion										
Servidor HP Proliant	-7617									
Unidad de Cinta de Backups	-2450									
Cintas de Backups	-250									
UPS APC Smart-UPS	-913									
Cofre Ignífugo Polaris D120	-6252									
Sala Cofre Smart Shelter+	-195000									
Aire Acondicionado x 2 unid.	-1250									
Reforma Edilicia	-200									
Sistemas de Seguridad externa	-1000									
Planificación	-1080									
Análisis de Requerimientos	-863									
Análisis de Sistemas	-1295									
Diseño de Sistemas	-1727									
Implementación	-3357									
Capacitación a Usuarios	-96									
total inversion	-223350	0	0	0	0	0	0	0	0	0
Beneficios										
Posicionamiento del IUA										
Responsabilidad social empresarial										
Ahorro de Papel		1200	1224	1248	1273	1298	1324	1351	1378	1406
Ahorro en mantenim. de Impresoras		250	250	250	250	250	250	250	250	250
Ahorro en insumos de impresión		200	204	208	212	216	220	225	229	234
Generar certificados propios		84000								
Renovar certificados propios			84000	84000	84000	84000	84000	84000	84000	84000
Vender certificados externos al IUA										
total	0	85650	85678	85706	85735	85764	85794	85826	85857	85890
Costos										
Linux S.O.										
Garantía o seguro de caución	-120000									
Licencia única	-4500									
Renovación de licencia						-3750				
Analista de seguridad		-16000	-16000	-16000	-16000	-16000	-16000	-16000	-16000	-16000
total	-124500	-16000	-16000	-16000	-16000	-19750	-16000	-16000	-16000	-16000
Flujo de fondos	-347850	69650	69678	69706	69735	66014	69794	69826	69857	69890
Tasa de descuento		11%								
Flujo descontado	-347850	62747,7	56552,2	50968,4	45936,6	39176,1	37314,7	33632,3	30312,8	27321,7
VAN		36.112,64 USD								
TIR		14%								

flujo acumulado	-347850	-278200	-208522	-138816	-69081	-3067	66727	136553	206410	276300
flujo acumulado descontado	-347850	-285102	-228550	-177582	-131645	-92469	-55154	-21522	8790,91	36112,6

Tabla 8: Análisis costos-beneficios

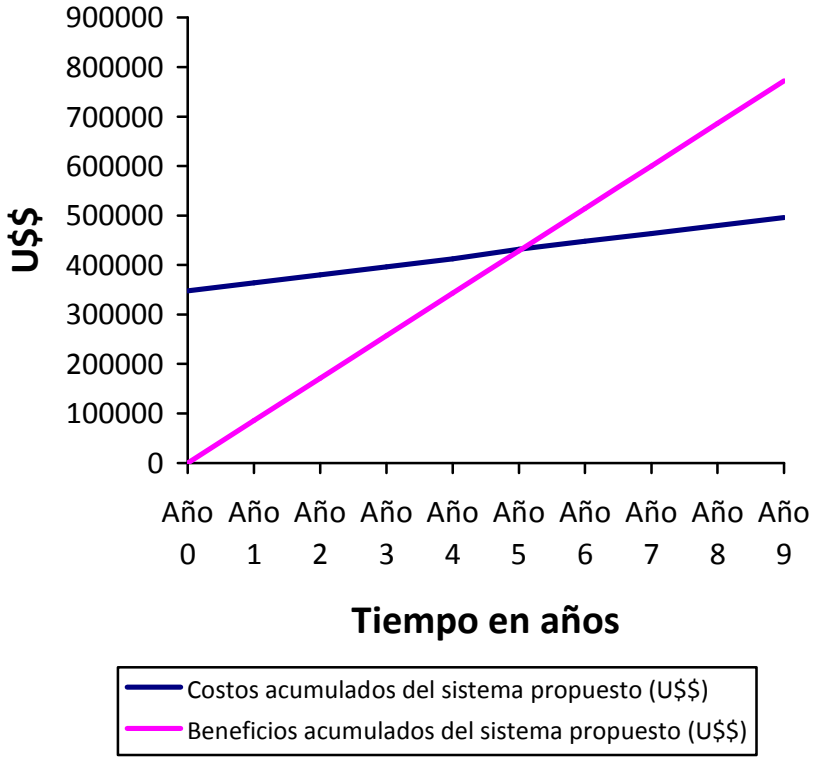


Figura 25: Análisis de recuperación

El gráfico nos muestra que en 5 años se recuperarán los costos iniciales de la implementación del proyecto. Inicialmente se observa un costo alto, por la inversión del nuevo proyecto. A medida que transcurre los años estos costos se reducen, sin embargo los beneficios del sistema propuesto, están enfocados en mejorar los tiempos de respuesta, el control de las actividades, seguridad en la información, que será a futuro un gran beneficio para la Institución.

- Beneficios tangibles

Los beneficios tangibles que se obtienen a través del nuevo sistema son:

-Reducción de costos de papelería e insumos de librería.

-Mejora en los tiempos de respuesta y procesamiento de datos en las actas de examen.

-Seguridad y privacidad en la información con la que se trabaja.

-Aumento en la velocidad de consulta, búsqueda de información de forma más oportuna.

-Reducción de archivadores, generando así ganancia de espacios.

- Beneficios intangibles

Se pueden destacar los siguientes beneficios intangibles:

- Brinda una mayor flexibilidad y rapidez para gestionar la información, lo que ofrece a su vez una mejora en las herramientas de trabajo del usuario.
- Genera información con mayor alto de confiabilidad y seguridad, lo que ayuda a la toma de decisiones.
- Aumentar la reputación e imagen de la Universidad al contar con una herramienta de firma digital y ser certificador propio.
- Ayudar al medio ambiente, evitando malgastar papelería y archivos.

En relación a los costos-beneficios, la aplicación del nuevo proyecto brinda grandes ventajas para la Universidad en todos sus aspectos.

Con esta implementación, la información tendrá gran valor al ser más segura, confiable y oportuna cuando se requiera. De esta manera, será un gran apoyo para la toma de decisiones y el éxito de la Universidad.

Además, impacta positivamente en optimizar las tareas administrativas diarias de los usuarios, reduciendo los tiempos de procesamiento y gestión de la información; mejora las relaciones humanas, evitando demoras, pérdida de tiempo en presentar personalmente cada documento firmado. Todas estas características mejoran el clima laboral, disminuyen las cargas de trabajo ociosas, ya que la información puede encontrarse de manera oportuna, confiable y segura.

5.6. Conclusión

Al llegar al final de la etapa de concreción del modelo, es posible considerar que se ha alcanzado el objetivo específico planteado:

Analizar la posibilidad de implementar una Autoridad Certificante que permita generar al IUA sus propios certificados

Este es el último de los objetivos específicos que este trabajo de grado persigue, por lo cual podemos dar por finalizado el desarrollo de las etapas de documentación del proyecto. Se ha alcanzado una implementación de un esquema de firma digital que debería ser la solución planteada al problema analizado en un primer momento. Es importante destacar que ésta implementación es solo parcial, de manera de demostrar que es factible la misma y que puede utilizarse como patrón para un proyecto a mayor escala.

6. Conclusiones

Se ha llegado a la conclusión de este trabajo final de grado. Es posible considerar que se ha alcanzado tanto el objetivo general como los objetivos particulares planteados en la introducción del proyecto, destacándose los siguientes resultados:
Se tiene una solida base teórica sobre infraestructura de Firma Digital, conociendo de manera general los diferentes tipos de algoritmos y estándares vigentes en los cuales se manifiesta dicha infraestructura. A su vez conocemos la forma en que los usuarios de Firma Digital se relacionan actualmente con esta tecnología, y la infraestructura necesaria para llevar a cabo el proyecto con éxito.

Hemos logrado obtener un fuerte análisis sobre el 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.

Para canalizar estos conocimientos, el autor de este trabajo ha analizado patrones de diseño que surgen de la observación de diversos trabajos implementados con éxito en todo el mundo, obteniendo un conocimiento más profundo de las prácticas que permiten aprovechar el potencial de Firma Digital como base para el desarrollo de soluciones a una gran variedad de situaciones.

Posteriormente, se han considerado los aspectos tecnológicos y metodológicos necesarios para llevar a cabo el desarrollo de dicho tipo de proyectos completando así la investigación teórica del proyecto de grado, y contando el tesista con los conocimientos necesarios para desarrollar una solución al problema planteado.

Como implementación práctica se ha instalado un servidor de Firma Digital en base a los requerimientos, considerando la situación problemática y siguiendo un patrón de diseño, el cual nos permite demostrar el proceso de generación y validación de licencias.

El mencionado servidor se encuentra funcional en la actualidad ejecutándose sobre una maquina virtual VMWARE, con la posibilidad de ser exportada dicha imagen sobre otro servidor VMWARE, donde pueda ser utilizado para el desarrollo y crecimiento futuro de la comunidad.

Finalizando el proyecto se ha realizado un análisis de factibilidad para verificar la posibilidad de implementar una Autoridad Certificante que permita al IUA generar sus propios certificados.

Este trabajo demuestra el potencial del uso de Firma Digital, habiendo pasado de ser una revolución tecnológica teórica a una herramienta para facilitar y agilizar diversos tipos de actividades de uso cotidiano y con una validez legal.

7. Bibliografía

[1] Kenneth E. Kendall, Julie E. Kendall. Análisis y diseño de sistemas. 6ª ed. México: Pearson Educación; 2005.

[2] Menezes, Alfred J., Van Oorschot, Paul C. y Vanstone, Scott A. Handbook of Applied Cryptography.CRC Press; 1996.

[3] Stallings William. Fundamentos de Seguridad en redes. Aplicaciones y estándares. 2ª ed. Madrid: Pearson Educación; 2004.

[4] Tanenbaum Andrew. Redes de computadoras. 4ª ed. México: Pearson Educación; 2003.

[5] Infraestructura de Firma Digital para el Sector Público Nacional, a que alude el Decreto N° 427/98. Secretaría de la Función Pública de la Jefatura de Gabinete de Ministros. Administración Pública Nacional. Resolución 194/98.Buenos Aires, (27-11-1998). Disponible en: http://infoleg.mecon.gov.ar/infolegInternet/anexos/50000-54999/54714/norma.htm

[6] Ley de firma digital. Ley 25.506. Senado y Cámara de Diputados de la Nación Argentina. Buenos Aires. Sancionada: Noviembre 14 de 2001. Boletín Oficial. Promulgada de Hecho: Diciembre 11 de 2001. Disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

[7] Política de Certificación. Criterios para el licenciamiento de las Autoridades Certificantes de la Administración Pública Nacional. Organismo Licenciante. Secretaría de la Función Pública. Resolución 212/98. Buenos Aires, (30-12-1998). Disponible en: http://infoleg.mecon.gov.ar/infolegInternet/anexos/55000-59999/55346/norma.htm

[8] Régimen al que se ajustará el empleo de la firma digital en la instrumentación de los actos internos. Administración Pública Nacional. Decreto 427/98. Buenos Aires, (16-04-1998). Disponible en: http://infoleg.mecon.gov.ar/infolegInternet/anexos/50000-54999/50410/norma.htm

[9] Firma Digital Argentina – Firma Digital – Evolución (en línea) – http://www.pki.gov.ar

[10] Sala Cofre Smart Shelter – AreaData S.A. – Evolución (en línea) – http://areadata.com.ar

[11] Gabinetes Polaris – AreaData S.A. – Evolución (en línea) – http://areadata.com.ar

[12] Servidores HP Proliant – Hewlett Packard – Evolución (en línea) – http://www.hp.com

8. Anexos

Anexo 1 - Ley Nº 25.506 - 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 Infraestructura de Firma Digital 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.

Decreto N° 2628/2002 - Reglamentario de la Ley de Firma Digital (Boletín Oficial del 20/12/2002)

El Decreto N° 2628/2002 reglamenta la LFD 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.

Otras normas específicas sobre Firma Digital

Disposición Nº 5 AC-ONTI

Documentación técnica de la Autoridad Certificante de la ONTI (Oficina Nacional de Tecnología Informática).

Resolución JGM Nº 176/2002

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

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 Nº 1023/2001

En su artículo 21 permite la realización de las contrataciones comprendidas en el Régimen en formato digital firmado digitalmente.

Decreto Nº 889/2001

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 Nº 677/2001

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 Nº 673/2001

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 Infraestructura de Firma Digital para el Sector Público Nacional y para la aplicación de nuevas tecnologías informáticas en la Administración Pública Nacional.

Ley Nº 25.237

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

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

Establece los estándares sobre tecnología de Firma Digital para la Administración Pública Nacional.

Decreto Nº 427/98

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 Infraestructura de Firma Digital para el Sector Público Nacional.

Resolución SFP Nº 45/97

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

Reglamenta los archivos digitales. Establece como órgano rector a la Contaduría Gral. de la Nación.

Ley Nº 24.624 Artículo 30

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 2 - 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 Infraestructura de Firma Digital 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 3 – Buen uso de Certificados Digitales

Almacenamiento de claves privadas

Es importante destacar la necesidad de proteger las claves criptográficas privadas y la contraseña, para resguardarlas contra posibles accesos no autorizados. Esto también lo podemos definir como privacidad.

Se recomienda por lo tanto, que el perfil del usuario con las claves privadas se almacene en una tarjeta inteligente. El uso de tarjetas inteligentes, en comparación con otros medios, por ejemplo, memory stick (MS), secure digital (SD), pendrive, entre otras, reduce las posibilidades de uso indebido.

Para el buen uso de certificados digitales en el IUA, ver las Políticas y las instrucciones que se describen en el ***Capítulo 1 Anexo 3 (Almacenamiento de claves privadas en una tarjeta inteligente).***

En el caso que el usuario no vaya a utilizar una tarjeta inteligente, ver las instrucciones descritas en el ***Capítulo 2 Anexo 3 (Almacenamiento de claves privadas con otros medios).***

Para el uso seguro de las contraseñas, seguir las instrucciones en el ***Capítulo 3 Anexo 3 (Uso de contraseñas).***

Capítulo 1 Anexo 3: Almacenamiento de claves privadas en una tarjeta inteligente

Seguridad

El uso de tarjetas inteligentes para el almacenamiento de claves privadas y los perfiles asegura que las claves privadas no se transfieran a la memoria de la computadora o en un medio de almacenamiento donde podría ser accedido por personas no autorizadas.

Las Claves se almacenan en una tarjeta inteligente, por lo cual, el usuario debe asegurarse de no revelar su contraseña o código PIN para impedir que otras personas puedan utilizar

su certificado digital y claves privadas.

Los datos en una tarjeta inteligente deben ser almacenados de tal manera que solo las personas autorizadas tengan acceso a ella, por lo tanto, se deben seguir las instrucciones descritas en el ***Capítulo 3 Anexo 3 (Uso de contraseñas)*** cuando se utilice una contraseña para resguardar los datos en una tarjeta inteligente.

Uso

El usuario debe instalar el lector de tarjetas inteligentes, es decir, un dispositivo que se conecta a un ordenador. Cuando se desea utilizar un certificado digital, se debe introducir la tarjeta inteligente en el dispositivo. Para ello, es necesario instalar el software de la tarjeta inteligente. Es importante seguir las instrucciones del fabricante de la tarjeta inteligente

Copia de respaldo

La tecnología de tarjetas inteligentes desactiva la realización de copias de seguridad.

Capítulo 2 Anexo 3: Almacenamiento de claves privadas con otros medios

Seguridad

En la situación de que el usuario no vaya a utilizar la tarjeta inteligente, se puede brindar otros medios alternativos de almacenamiento (memory stick (MS), secure digital (SD), pendrive, etc) para guardar el perfil y clave privada. Sin embargo, esto podría aumentar la posibilidad de uso indebido de las claves privadas en comparación con el uso de las tarjetas inteligentes.

Es importante resguardar el dispositivo de almacenamiento para que no sea posible el acceso de personal no autorizado. El perfil del usuario debe ser asegurado con una contraseña adecuada. Para esto, seguir las instrucciones en el ***Capítulo 3 Anexo 3 (Uso de contraseñas).***

Uso de otros medios de almacenamiento

Utilizar los medios de almacenamiento alternativos como se indica en las recomendaciones del fabricante y las instrucciones.

Copia de respaldo

Recomendamos la realización de copias de seguridad en un CD ROM, siempre y cuando tenga los medios. Se debe utilizar el CD-ROM como se indica en las instrucciones del fabricante de CD-ROM.

En el caso de que el usuario no tenga la posibilidad de almacenar una copia de seguridad de su perfil en el CD-ROM, existe la posibilidad de hacer una copia de seguridad en otro medio de almacenamiento alternativo, sin embargo, ofrecerá un medio menos confiable y menos duradero para el almacenamiento de copias de seguridad de las claves privadas. Siempre utilizar los medios de almacenamiento alternativos de acuerdo con las instrucciones del fabricante.

Cuando se realice un cambio de claves, es fundamental actualizar la copia. La copia de seguridad de las claves, en CD ROM u otros medios de almacenamiento, se debe resguardar en un lugar seguro para evitar la utilización de manera indebida por personas no autorizadas.

Capítulo 3 Anexo 3: Uso de las contraseñas

Al generar un certificado digital, el software nos instruye acerca de la elección de contraseñas adecuadas, a saber:

- Uso variado de las letras mayúsculas y minúsculas, números y caracteres especiales
- Contraseña compuesta por al menos 8 caracteres,
- Evitar el uso de palabras que se escriben en el diccionario.

Se recomienda que el usuario memorice su contraseña y no la escriba. En el caso de que

desee el usuario escribir contraseña, es primordial guardarla en un lugar conocido solo por el usuario.

Software

Es fundamental utilizar solamente software licenciado y certificado y de manera adecuada. Para instalar el software, seguir las instrucciones para su instalación provista por el proveedor del mismo.

Para la instalación de software para el uso de tarjetas inteligentes, ver las instrucciones del ***Capítulo 1 Anexo 1 (Almacenamiento de claves privadas en una tarjeta inteligente)*** y las instrucciones del fabricante.

En casos de mal uso

Si se producen cambios que están relacionados con los certificados digitales, mal uso o probabilidades de mal uso, el usuario debe informar inmediatamente a la Entidad Certificadora. En los casos de mal uso o probabilidad de mal uso, debe presentar un formulario de solicitud de revocación de certificados, en persona o por correo electrónico, o llamar al número de servicio de revocación de certificados propios de la Entidad Certificadora.

Anexo 4 – Glosario Técnico

CA: en criptografía una autoridad de certificación, certificadora o certificante (AC o CA por sus siglas en inglés Certification Authority) es una entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública

Criptosistema: es un sistema que toma información, legible, intelegible para convertirlo en información no legible, inintelegible, o no entendible.

FTP: (siglas en inglés de File Transfer Protocol, "Protocolo de Transferencia de Archivos") es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

HTTPS: Hyper Text Transfer Protocol Secure (en español "Protocolo seguro de transferencia de hipertexto"), más conocido por sus siglas HTTPS, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hiper Texto, es decir, es la versión segura de HTTP.

Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas.

Plug and Play: (en español "enchufar y usar") es la tecnología que permite a un dispositivo informático ser conectado a una computadora sin tener que configurar, mediante jumpers o software específico (no controladores) proporcionado por el fabricante, ni proporcionar parámetros a sus controladores. Para que sea posible, el sistema operativo con el que funciona el ordenador debe tener soporte para dicho dispositivo.

SSL: Siglas de Secure Socket Layer. Es un protocolo desarrollado por Netscape Communications Corporation para dar seguridad a la transmisión de datos en transacciones comerciales en Internet. Utilizando la criptografía de llave pública, SSL provee autentificación del servidor, encriptar de datos, e integridad de los datos en las comunicaciones cliente/servidor.

TLS: Transport Layer Security (en español "Seguridad de la Capa de Transporte") es un protocolo criptográfico que proporcionan comunicaciones seguras por una red.

UPS: fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica. Los UPS son llamados en español SAI (Sistema de alimentación ininterrumpida). UPS significa en inglés Uninterruptible Power Supply.