C A P Í T U L O VI

APLICATIVO

6.1 Algoritmos de Generación de Firmas Digitales

6.2 Utilización, manejo e implementación

6.3 Estudio de Alternativas

6.4 Desarrollo e implementación

6.5 Comparación entre Algoritmos

6.6 Pruebas y mejoras

6.1 Algoritmos de generación de firmas Digitales

Las siguientes son las primitivas criptográficas que se han tomado en cuenta y que se pueden implementar en .NET Framework. De las cuales para el Aplicativo se han analizado las correspondientes al Cifrado de Clave Pública.

Cifrado de clave secreta (criptografía simétrica).- Realiza la transformación de los datos, impidiendo que terceros los lean. Este tipo de cifrado utiliza una clave secreta compartida para cifrar y descifrar los datos.

- DES DESCriptoServiceProvider
- RC2 RC2CriptoServiceProvider
- Rijndael RijndaelManaged
- TripleDES TripleDESCriptoServiceProvider

Cifrado de clave pública (criptografía asimétrica).- Realiza la transformación de los datos, impidiendo que terceros los lean. Este tipo de cifrado utiliza un par de claves pública y privada para cifrar y descifrar los datos.

- DSA DSACriptoServiceProvider
- RSA RSACriptoServiceProvider
- ECC No soportado en .NET Framework, se aplica Dll's con funciones que proporcionen los campos especificados para las claves.

Estos algoritmos utilizan las clases auxiliares: AsymmetricKeyExchangeFormatter y AsymmetricSignatureFormatter.

Firmas criptográficas.- Garantiza que los datos se originen en una parte específica mediante la creación de una firma digital única para esa parte. En este proceso también se usan funciones hash.

.NET Framework proporciona las siguientes clases que implementan algoritmos de firma digital:

DSACryptoServiceProvider

RSACryptoServiceProvider

Valores hash criptográficos.- Asigna datos de cualquier longitud a una secuencia de bytes de longitud fija. Los valores hash son únicos estadísticamente; el valor hash de una secuencia de dos bytes distinta no será el mismo.

- MD5 MD5CriptoServiceProvider
- SHA1 SHA1CriptoServiceProvider
  SHA1Managed
- SHA256 SHA256Managed
- SHA384 SHA384Managed
- SHA512 SHA512Managed

6.2 Utilización, manejo e implementación

Una vez establecido los algoritmos a utilizar, es necesario analizar su funcionamiento y determinar las condiciones bajo las cuales se basará su utilización.

Básicamente el propósito es Generar un par de Claves asociadas a un Usuario, y con ellas obtener un Certificado Digital. Este certificado debe ser respaldado por la firma digital de una Autoridad Certificante quien da Fe Pública de la validez del certificado, con este certificado el usuario podrá demostrar que es él realmente y realizar las transacciones sin

dificultad. Visual Basic .NET, ofrece características de manejo criptográficas muy fáciles de implementar, proveyendo de las correspondientes clases y subclases con los respectivos espacios de nombres que las almacenan, con lo cual su uso es bastante fácil.

6.3 Estudio de Alternativas

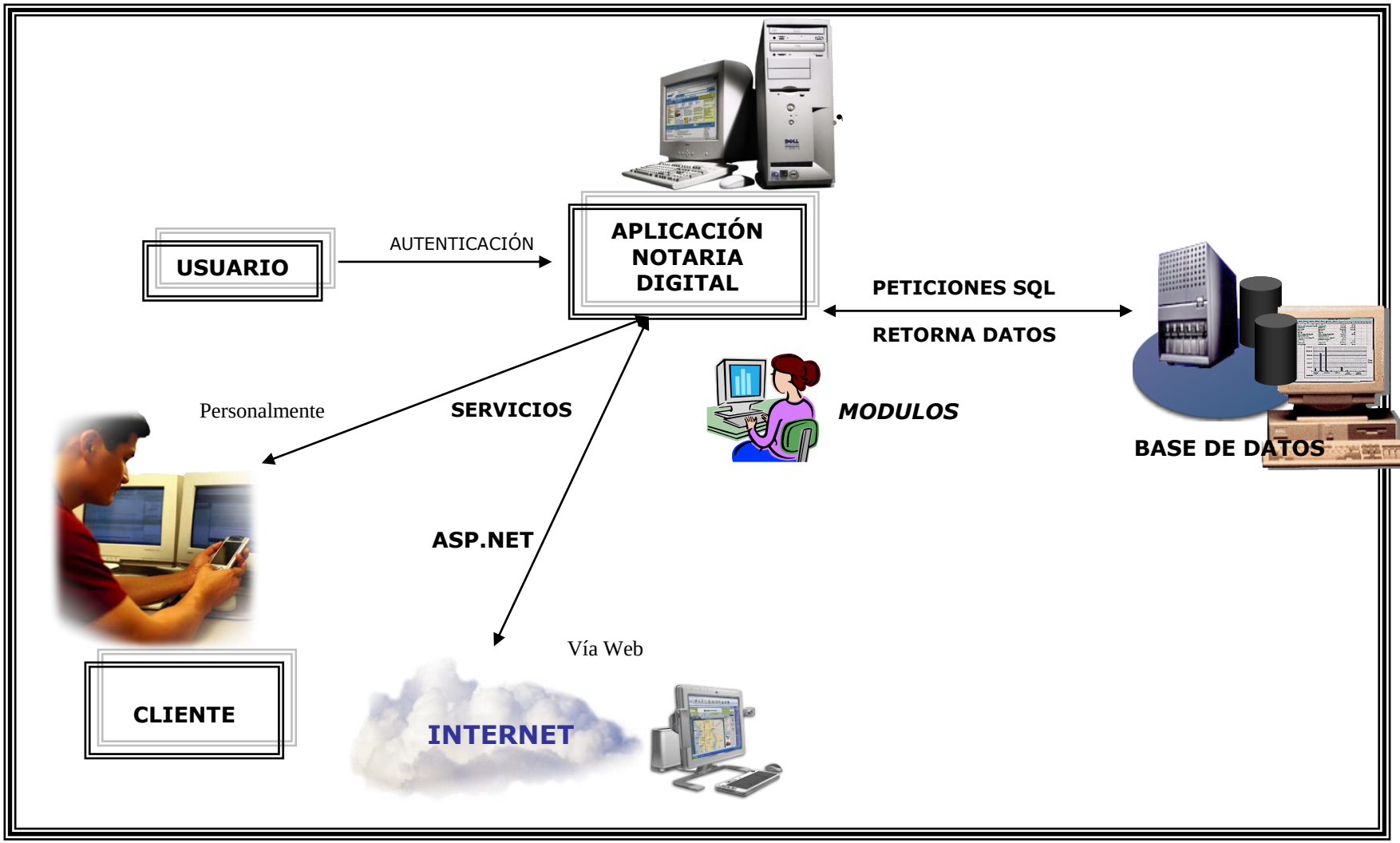
De acuerdo a los estudios y análisis previos, se ha considerado utilizar la Infraestructura de Clave Pública que alberga a los algoritmos Asimétricos, y en especial Algoritmo de Curvas Elípticas y el RSA para el cifrado, y SHA1, y MD5 para generar Digest y firmas digitales.

Dependiendo del algoritmo y de las necesidades de seguridad, se puede escoger e implementar determinado algoritmo criptográfico, tomando en cuenta el tamaño de claves que generan cada uno, así para que RSA sea funcionalmente idóneo se debe manejar una clave de 1024 bits como mínimo, pudiendo generar claves de hasta 2048 bits, esto depende en gran medida del funcionamiento del algoritmo. ECC por el contrario basa su funcionamiento con claves de 163 bits, que serían el equivalente de RSA de 1024 bits, y claves de 210 bits equivalentes a 2048 bits en RSA, y sin embargo la seguridad será similar, con esto se puede decir que no importa en gran medida el tamaño de claves sino el funcionamiento mismo del algoritmo.

Para los algoritmos de generación de hash son algoritmos de facto usados en la gran mayoría de países, SHA1 que produce un hash de 160 bits codificado en Base64 y MD5 que genera un Digest de 128 bits.

6.4 Desarrollo e implementación

ARQUITECTURA DE NOTARIA DIGITAL



MODELADO DEL APLICATIVO

La parte inicial del proyecto consiste en diseñar los diferentes diagramas de modelado de la aplicación, que comprenden entre otros el diagrama de casos de uso, diagrama de secuencia, modelo conceptual de datos y modelo físico de datos, los que a continuación se muestran:

- **Diagrama de Casos de Uso.-** este diagrama es un documento que describe la secuencia de los eventos de un Actor que utiliza la Aplicación para completar un proceso, representa la forma en que interactúa el Cliente y la Aplicación, esto va en un orden adecuado empezando por la forma de autenticación de usuarios, administración y gestión de la aplicación, además de la forma, tipo y orden en como los diferentes elementos interactúan.

Actores de Notaría Digital

a) **Cliente.-** persona, institución o empresa que solicita el servicio, ya sea personalmente o a través de la página Web, y puede acceder a información y descargas de certificados.

b) **Administrador.-** administrador de la Aplicación que está facultado de acuerdo a sus privilegios a gestionar Clientes, control de usuarios, generar y administrar Claves, Certificados Digitales, etc.

c) **Usuario.-** aquel que puede acceder al sitio Web sin ninguna restricción, pero sin interactuar con la aplicación.

- **Diagrama de Secuencia.-** en este diagrama se detallan gráficamente los eventos que originan los actores y se ven reflejados en la aplicación, esto en gran medida depende de la formulación de los casos de uso lo que ocasiona que se inicie una operación en la aplicación.
- **Modelo conceptual.-** en este modelo se muestra gráficamente las clases de objetos o entidades y atributos más importantes. Representa la estructura lógica de la base de datos, Diagrama Entidad-Relación. Este modelo representa "cosas del mundo real", y no se asocia con elementos de software, explicando las entidades que intervienen dentro de la aplicación y su relación entre ellas.
- **Diagrama de clases.-** en este diagrama, se visualiza la interacción entre las diferentes clases u objetos que forman parte de la aplicación, las cuales pueden ser asociativas, de herencia, de uso y de contenido.
- **Modelo físico de Datos.-** en este modelo se esquematiza el diseñó de la base de datos, indicando la manera en que se relacionan lógicamente las tablas y si éstas mantienen una integridad referencial.

DIAGRAMA DE CASOS DE USO

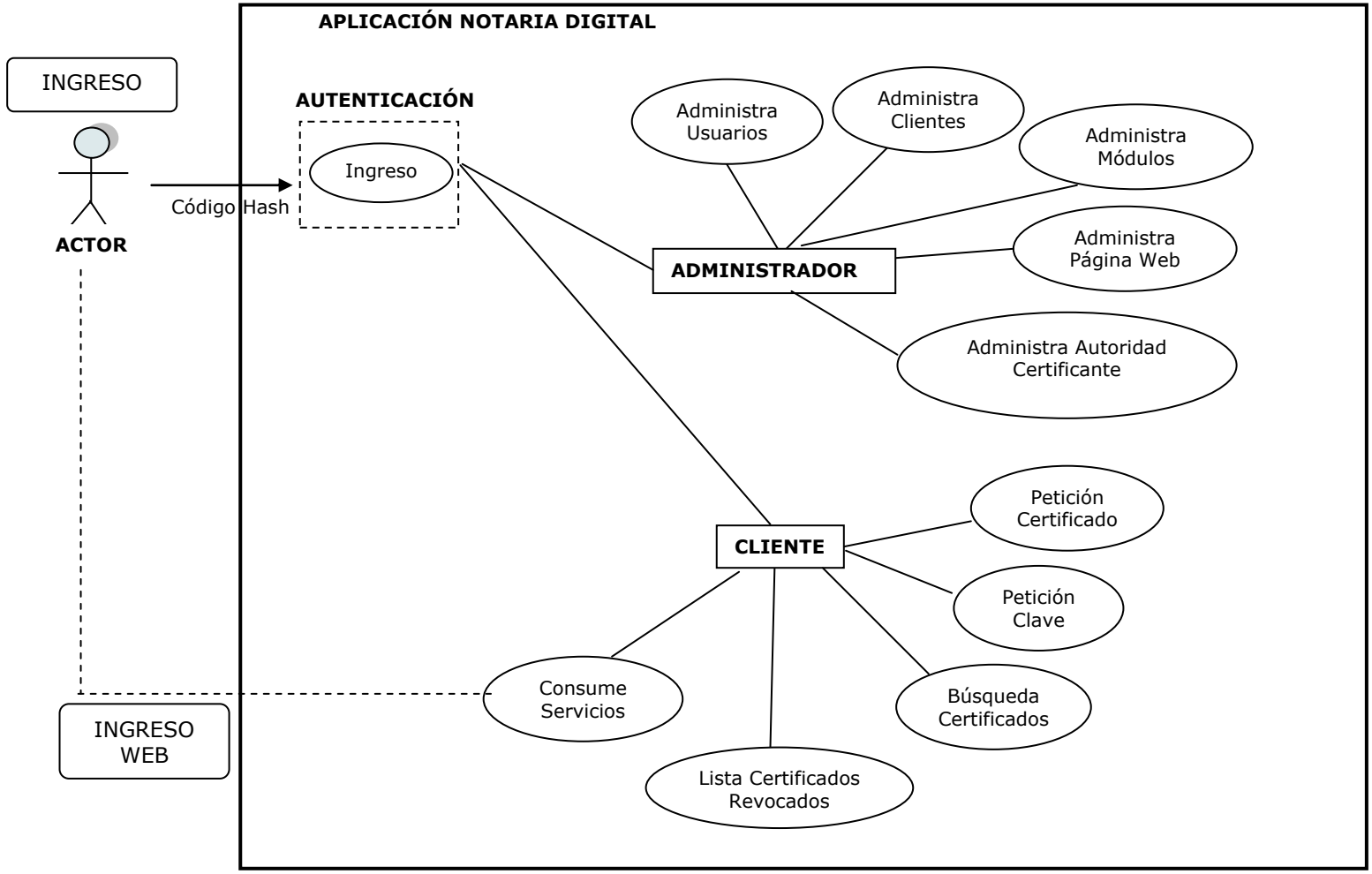
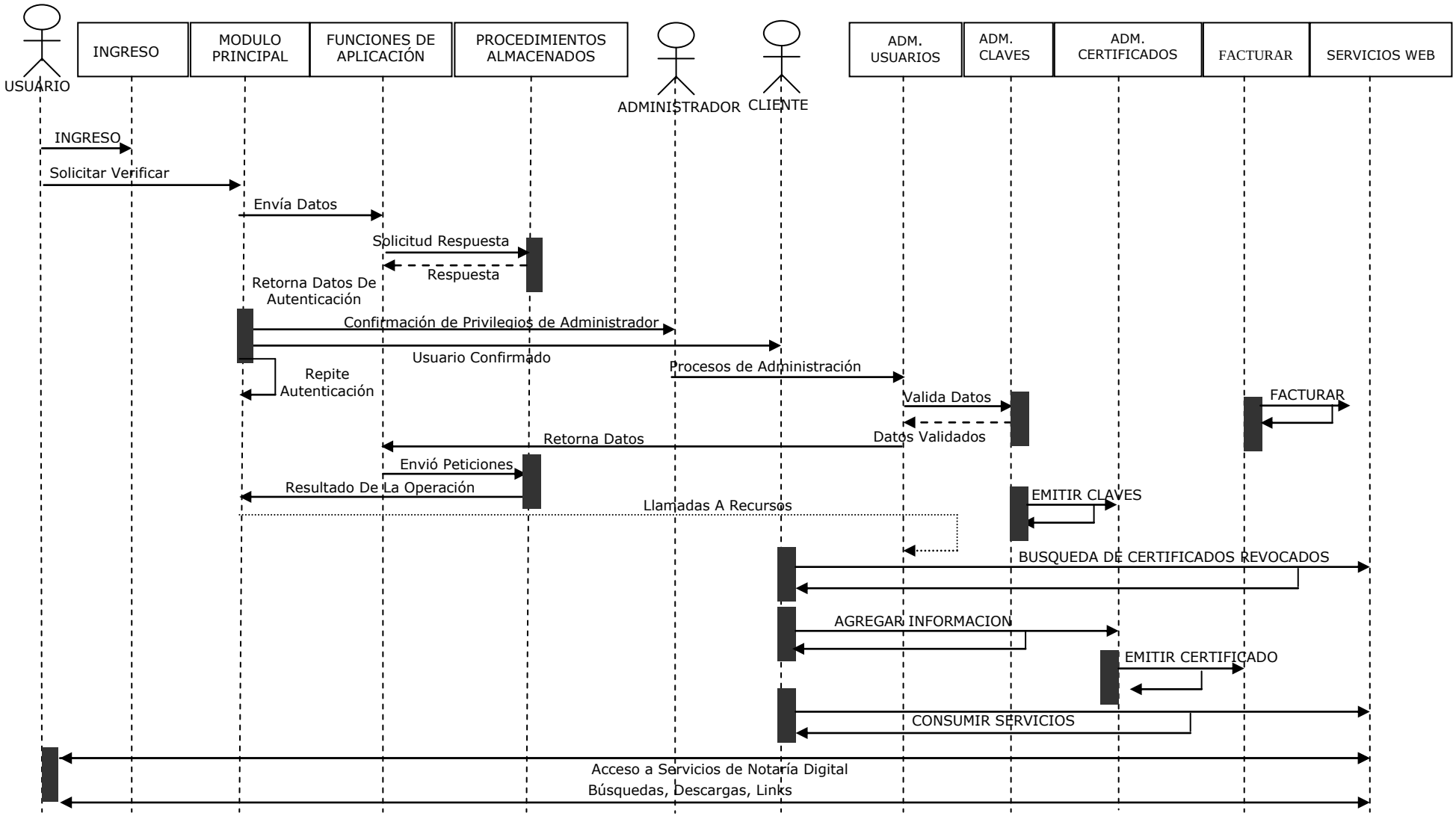
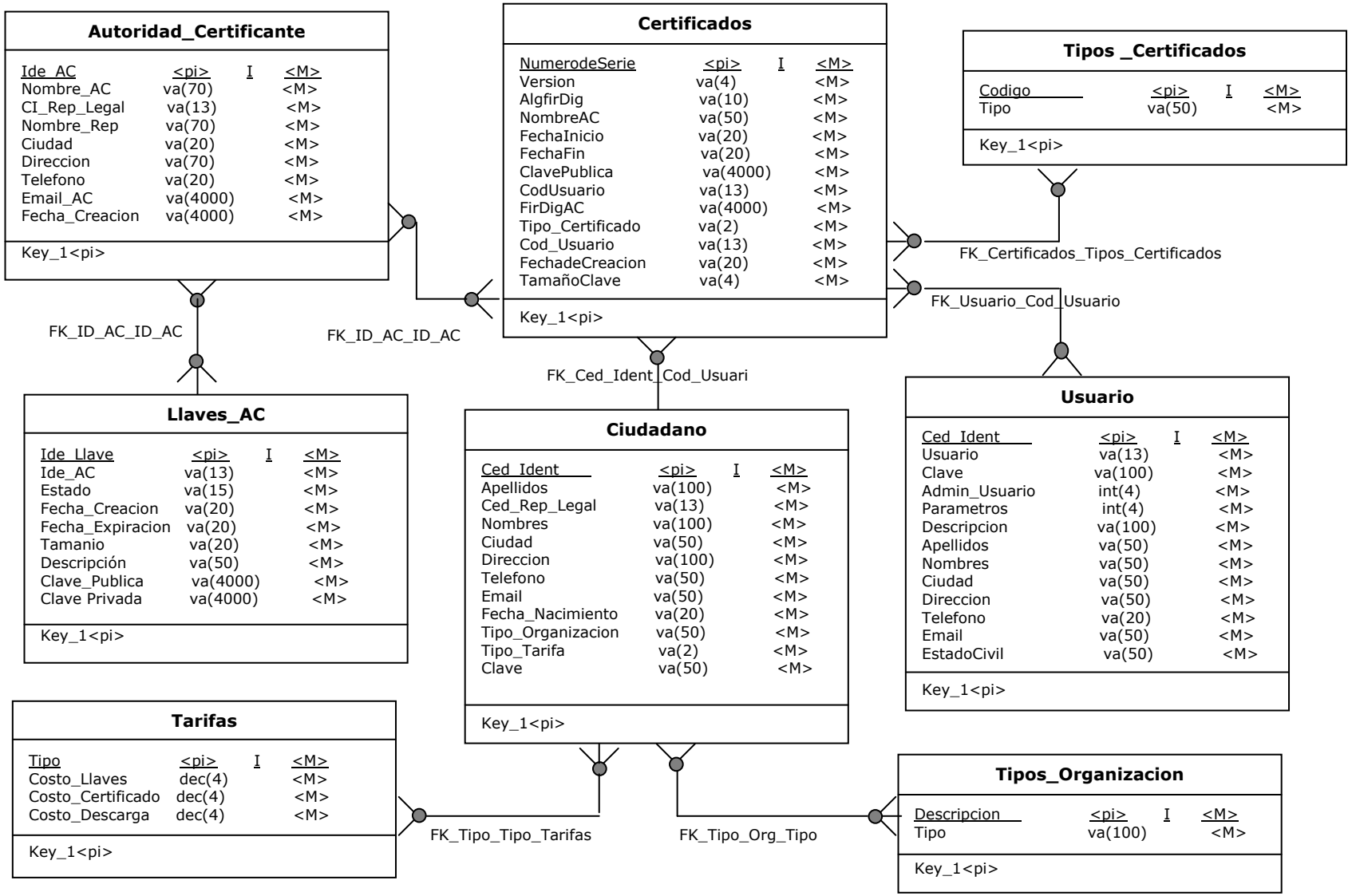


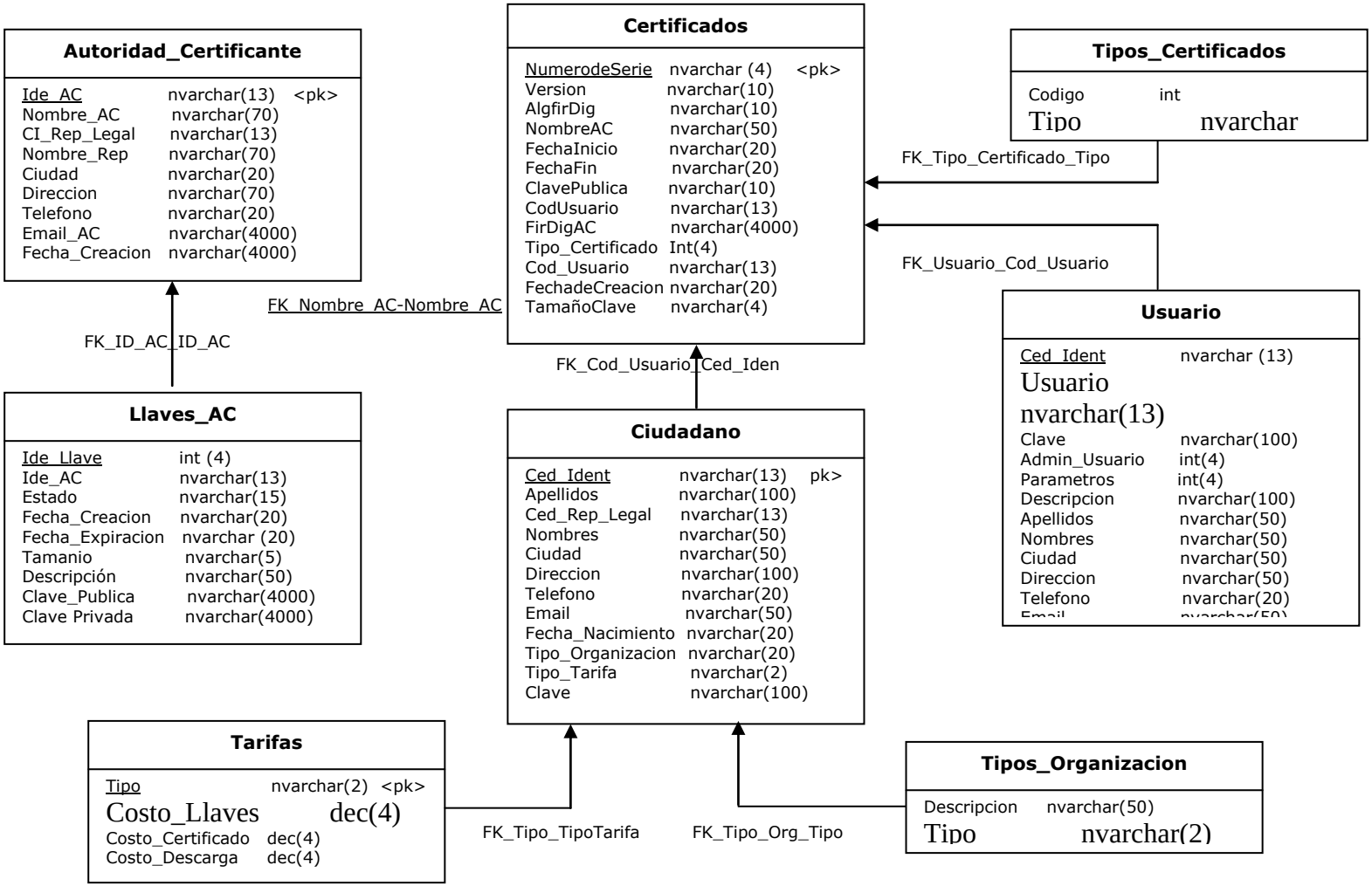
DIAGRAMA DE SECUENCIA



MODELO CONCEPTUAL DE DATOS



MODELO FÍSICO DE DATOS



Plataforma:

Windows 2000 Server, bajo un Controlador de Dominio

www.notariadigital.com

Sistema operativo:

- ✓ Windows 2000 Server como entrono de desarrollo
- ✓ Windows XP Profesional, corriendo Internet Explorer 6.0 como Cliente. Obteniendo del sistema la mejor respuesta en cuanto a funcionamiento y rendimiento.

Base de Datos:

SQL Server 2000

Lenguaje de Programación

Visual Basic .NET V. 2003 Español

REQUISITOS DEL SISTEMA

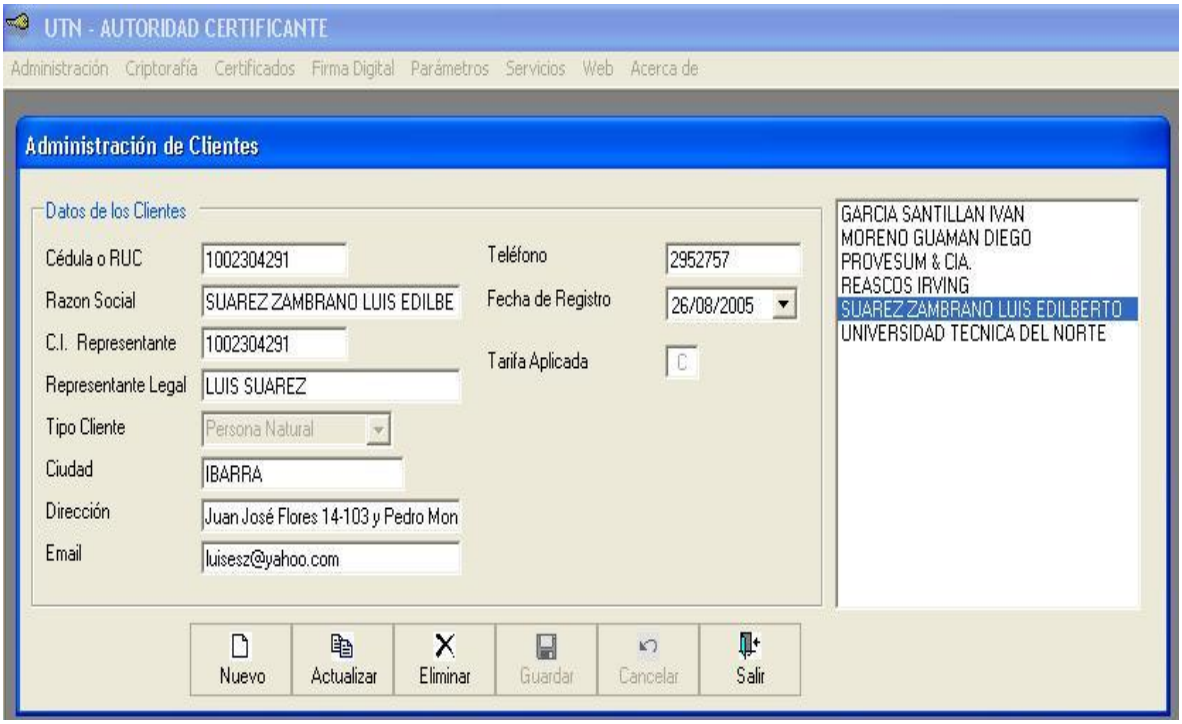
- ✓ **Procesador**: de 266 MHZ mínimo, recomendado Procesador de 800 MHZ o superior
- ✓ **Memoria:** 256 MB mínimo, recomendado 512 MB o superior
- ✓ **Espacio en Disco:** mínimo 3 GB para instalación de la Plataforma .NET
- ✓ **Sistema Operativo:** Windows NT 4.0 o superior, recomendado Windows 2000 Server, o Windows XP

Notaría Digital, es una aplicación, capaz de gestionar claves y certificados digitales para clientes de diversas clases, como empresas, personas naturales, instituciones, etc. Que incluye:

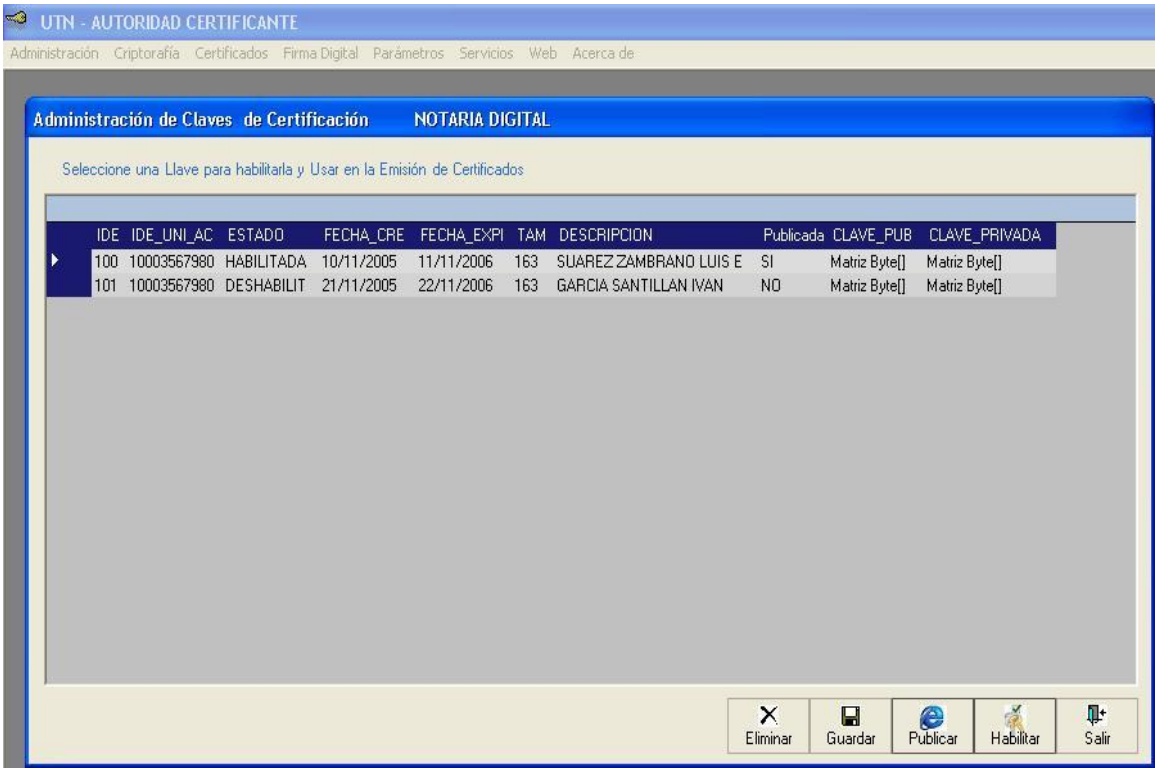
MÓDULOS DE LA APLICACIÓN

Módulo de Ingreso: módulo inicial de autenticación de usuarios basado en códigos Hash, que no permitan la captura de la contraseña del usuario conectado al sistema, dependiendo del privilegio del usuario, éste tendrá acceso o restricción a las opciones del sistema.

Módulo de Administración: en el cual se realizan procesos como Administración de Usuarios, Administración de Clientes, Cambio de Usuario, Cambio de Clave del usuario conectado.

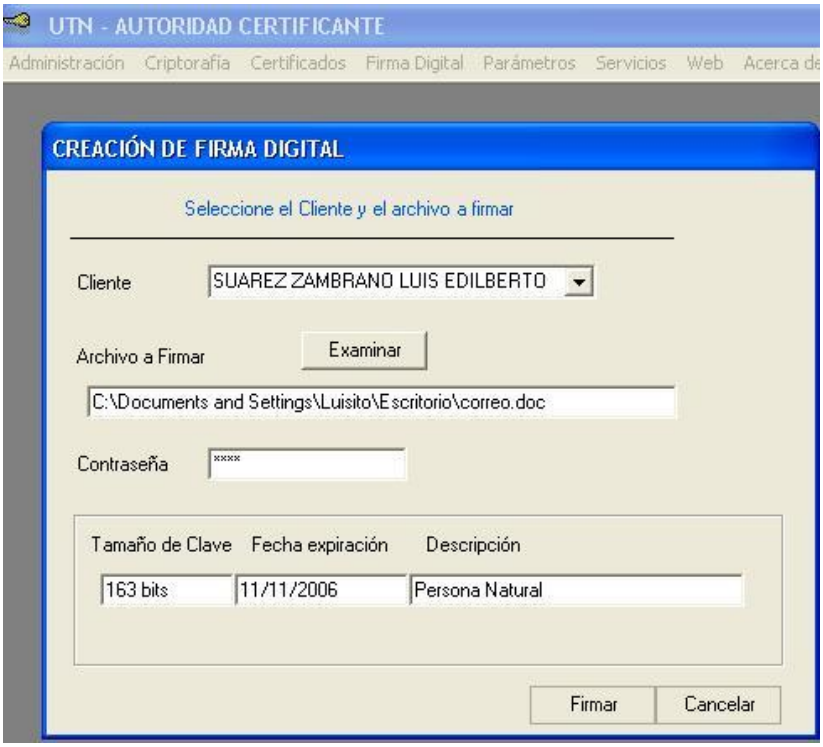


Módulo de Generación y Administración de Claves: en donde se tiene las opciones para generar nuevas llaves para un Cliente y administrar éstas llaves, además de la opción de cifrado Asimétrico para encriptar archivos que luego podrán ser Firmados Digitalmente.

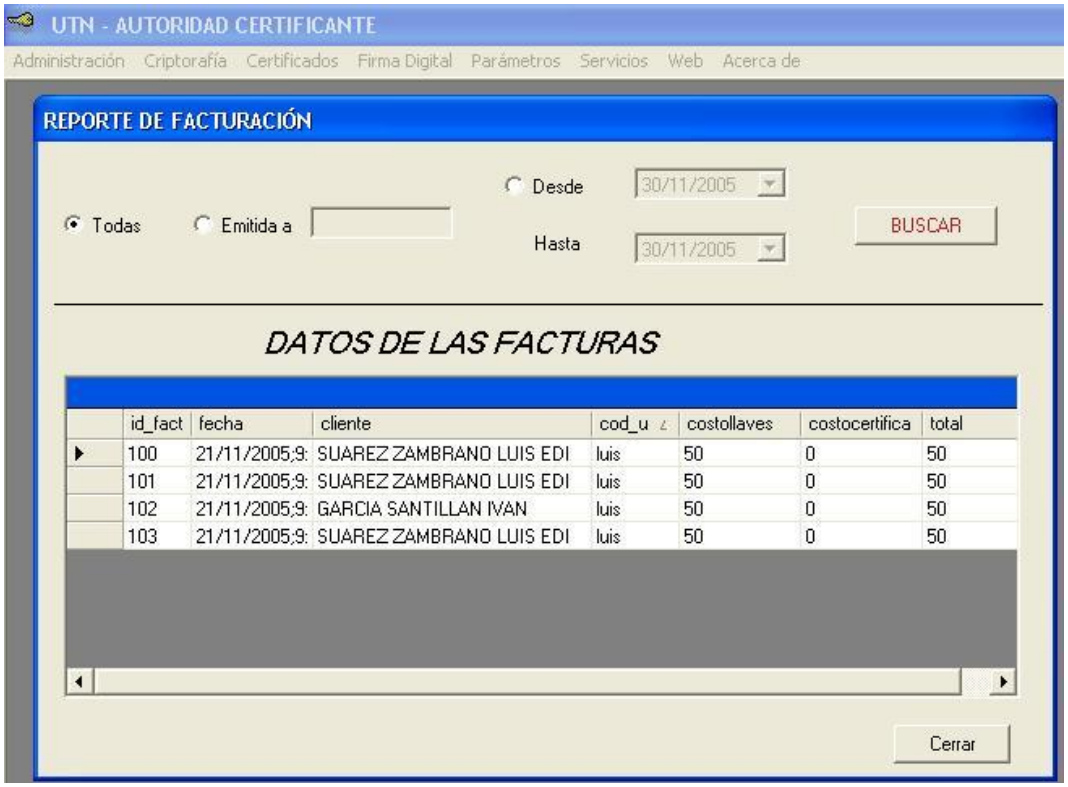


Módulo de Generación y Administración de Certificados: en este módulo se podrán realizar las tareas de Generación y Administración de Certificados Digitales para los clientes. Se tiene opciones de Emitir, Revocar, Suspender y Caducar Certificados por parte del Administrador para cada Cliente. Así como también se tiene los reportes de las Listas de Certificados: Emitidos, Revocados, suspendidos y Caducados para ser dadas a conocer al público en general.

Módulo de Generación y Verificación de Firma Digital: se tiene opciones de Firmado Digital, además de la opción de verificación de la firma.



Módulo de Parámetros: en el cual se tiene las opciones de administración de tipos de clientes, costos por servicios, reporte de facturas emitidas a los clientes.



El Cliente: con una página Web principal que brinda acceso a opciones de búsquedas, descargas de certificados, publicación de Certificados Revocados, Certificados Válidos, Servicios prestados y Base Legal referente a Firmas Digitales y Comercio Electrónico, que acceden a través de ASP.NET hacia la Base de Datos, en donde se almacena toda la información.

6.5 Comparación entre algoritmos

Algoritmo	¿Qué es?	Protocolo que Soporta	¿Qué Proporciona?	Año de Creación	Tamaño de Clave
ALGORITMOS SIMÉTRICOS					
DES	Algoritmo de Encripción de Datos	TLS (Transport Layer Security), S-HTTP	Cifrado Simétrico resistente a criptoanálisis, en bloques de 64 bits	1976	56 bits
3DES	Algoritmo de Encripción de Datos	TLS, S-HTTP	Cifrado Simétrico con 3 claves distintas en relación a DES	1977	192 bits
RC2	Algoritmo de Cifrado Simétrico	SSL(Secure Socket Layer), PCT(Private Communications Technology)	Cifrado Simétrico con claves de 40 bits en bloques	Ronald Rivest 1993	1-2048 impor, 40 bits, expor.
RC4	Algoritmo de Cifrado Simétrico	SSL,, PCT(Private Communications Technology), TLS	Cifrado deFlujo, adoptado por RSA	Ronald Rivest 1994	1-2048 impor, 40 bits, expor
RC5	Algoritmo de Cifrado Simétrico	SSL(Secure Socket Layer, PCT(Private Communications Technology)	Cifrado deFlujo, adoptado por RSA	Ronald Rivest 1994	1-2048 impor, 40 bits, expor
RIJNDAEL	Algoritmo de Cifrado y Firma Digital	SSL	Cifrado en bloque	NITS, J. Daemen, V. Rijmen	128, 192, 256 bits
ALGORITMOS ASIMÉTRICOS					
DSA	Algoritmo de Cifrado y Firma Digital, PKI	SSL	Autenticación basada en firmas digitales	Instituto Nacional de Tecnología y Estándares (NIST) 1994	56 bits
RSA	Algoritmo de Cifrado y Firma Digital, PKI	SSL, S-HTTP, PCT	Encripción de Daos y Firma Digital	Ronald Rivest Adi Shamir 1977	1024 uso corporativo, 2048 claves valuables
DIFFIE HELMAN	Algoritmo de Cifrado y Firma Digital, PKI	SSL, VPN	Proporciona claves basadas en logaritmos discretos	1976	1536 bits
ECC	Algoritmo de Cifrado y Firma Digital, PKI	SSL	Proporciona claves basado en el Logaritmo Discreto Elíptico	Millar, 1985	163,210 bits

ALGORITMOS DE HASH					
MD5	Algoritmo de Hash	SSL, PCT, TSL, S-HTTP	Proporciona Message Digest	Ron Rivest, 1992	128 bits
SHA1	Algoritmo de Hash	SSL, S-HTTP, TSL	Hash para Firma Digital	NSA(National Security Agency)	128, 286, 384, 512 bits

6.6 Pruebas y mejoras

En lo que respecta a las pruebas del Aplicativo, éstas se las realizó con datos reales, tomando en cuenta las normas reglamentarias que para Ecuador, de acuerdo a la Ley de Comercio Electrónico rigen desde el año 2002.

Por ser un prototipo de Notaría Digital, la aplicación puede tener las correspondientes mejoras de acuerdo a las necesidades existentes.