**INSTITUTO POLITÉCNICO NACIONAL**

**ESCUELA SUPERIOR DE CÓMPUTO**

**ESCOM**

*Trabajo Terminal*

**“Infraestructura de Identificación y**

**Autentificación Digital”**

*Que para cumplir con la opción de titulación curricular en la carrera de*

**“Ingeniería en Sistemas Computacionales**

**con especialidad en Sistemas”**

**Presentan:**

*Anízar González Sandra Andrea*

*Nogueda López Guiedani*

*Serrano Olea Sonia*

**Directores:**

*Chadwick Carreto Arellano*

*Mauricio Ramón García Gómez*





**INSTITUTO POLITÉCNICO NACIONAL**

**ESCUELA SUPERIOR DE CÓMPUTO**

No. Registro: TT 2010-0045 Serie: Amarilla Abril 2011-04-16

Documento técnico:

***“Infraestructura de Identificación y Autentificación Digital”***

Presentan:

**Anízar González Sandra Andrea¹**

**Nogueda López Guiedani**

**Serrano Olea Sonia**

Directores:

**Chadwick Carreto Arellano**

**Mauricio Ramón García Gómez**

**RESUMEN**

En el presente documento se describe de manera general el análisis, diseño, desarrollo, implementación, pruebas y resultados del Trabajo Terminal “Infraestructura de Identificación y Autentificación Digital” con el que se tiene como objetivo crear un perfil digital único del usuario, generado por medio de su información personal, pública y biométrica, permitiendo así realizar una identificación y autentificación del individuo que garantice seguridad recíproca entre él y las instancias externas de verificación que lo requieran.

**Palabras** **clave** –Identificación digital, Seguridad, Autentificación, Autentificación biométrica.

1 ttadndigital@gmail.com

**Advertencia**

*“Este informe contiene información desarrollada por la Escuela Superior de   
 Cómputo del Instituto Politécnico Nacional a partir de datos y documentos   
 con derecho de propiedad y por lo tanto su uso quedará restringido a las  
 aplicaciones que explícitamente se convengan.”*

La aplicación no convenida exime a la escuela su responsabilidad técnica  
 y da lugar a las consecuencias legales que para tal efecto se determinen.

Información adicional sobre este reporte técnico podrá obtenerse en:

En La Subdirección Académica de la Escuela Superior de Cómputo  
 del Instituto Politécnico Nacional, situada en Av. Juan de Dios   
 Bátiz s/n.

Teléfono: 57296000 Extensión 52000

**Agradecimientos**

Índice

[Índice 5](#_Toc291452614)

[Índice Tablas 7](#_Toc291452615)

[Índice Figuras 8](#_Toc291452616)

[Capítulo 1 Introducción 11](#_Toc291452617)

[1.1 Introducción 11](#_Toc291452618)

[1.2 Objetivos 12](#_Toc291452619)

[1.2.1 Objetivo General 12](#_Toc291452620)

[1.2.2 Objetivos Particulares 12](#_Toc291452621)

[1.3 Antecedentes y conceptos básicos 12](#_Toc291452622)

[1.3.1 El problema de la Identificación 12](#_Toc291452623)

[1.3.2 Medios de identificación 14](#_Toc291452624)

[1.3.3 Métodos de cifrado 24](#_Toc291452625)

[Capítulo 2 Estado del arte 32](#_Toc291452626)

[2.1 Planteamiento del problema 32](#_Toc291452627)

[2.2 Soluciones existentes 34](#_Toc291452628)

[2.3 Propuesta de solución 36](#_Toc291452629)

[Capítulo 3 Análisis 38](#_Toc291452630)

[3.1 Estudio de Factibilidad 38](#_Toc291452631)

[3.1.1 Factibilidad Operacional 38](#_Toc291452632)

[3.1.2 Factibilidad Técnica 38](#_Toc291452633)

[3.1.3 Estudio de Factibilidad Económica 38](#_Toc291452634)

[3.1.4 Estudio de Factibilidad Legal 47](#_Toc291452635)

[3.2 Análisis de requerimientos 47](#_Toc291452636)

[3.2.1 Requerimientos No Funcionales 47](#_Toc291452637)

[3.2.2 Requerimientos Funcionales 48](#_Toc291452638)

[Capítulo 4 Diseño 50](#_Toc291452639)

[4.1 Diagrama de Casos de Uso 50](#_Toc291452640)

[4.1.1 Definición de actores del sistema. 50](#_Toc291452641)

[4.1.2 Descripciones detalladas de cada Casos de Uso 52](#_Toc291452642)

[4.2 Diagramas de secuencia 58](#_Toc291452643)

[4.2.1Diagrama de secuencia Ingresar información privada 58](#_Toc291452644)

[4.2.2 Diagrama de secuencia Ingresar información pública 59](#_Toc291452645)

[4.2.3 Diagrama de secuencia Integrar datos 60](#_Toc291452646)

[4.2.4 Diagrama de secuencia Validar usuario 61](#_Toc291452647)

[4.2.5 Diagrama de secuencia Iniciar sesión 62](#_Toc291452648)

[4.2.6 Diagrama de secuencia Visualizar reportes 62](#_Toc291452650)

[4.2.7 Diagrama de secuencia Eliminar cuenta 63](#_Toc291452651)

[4.3 Diagrama de actividades 64](#_Toc291452652)

[4.3.1 Diagrama de actividades Primer Módulo 64](#_Toc291452653)

[4.3.1.1 Zoom del diagrama de actividades Primer Módulo-Ingresar información privada. 65](#_Toc291452654)

[4.3.1.2 Zoom del diagrama de actividades Primer Módulo-Ingresar información pública. 66](#_Toc291452656)

[4.3.1.3 Zoom del diagrama de actividades Primer Módulo-Integrar datos 67](#_Toc291452659)

[4.3.2 Diagrama de actividades Segundo Módulo 68](#_Toc291452661)

[4.3.2.1 Zoom del diagrama de actividades Segundo Módulo Parte de arriba 69](#_Toc291452664)

[4.3.2.2 Zoom del diagrama de actividades Segundo Módulo parte de abajo 70](#_Toc291452667)

[4.3.3 Diagrama de actividades Tercer Módulo 71](#_Toc291452670)

[4.4 Diagrama de clases 72](#_Toc291452673)

[4.5 Modelado de Base de Datos 74](#_Toc291452676)

[Capítulo 5 Desarrollo 76](#_Toc291452677)

[5.1 Módulo de registro y generación de ID 76](#_Toc291452678)

[5.2 Módulo de Validación 101](#_Toc291452679)

[5.3 Módulo de Administrador 107](#_Toc291452680)

[Capítulo 6 Trabajo a futuro 115](#_Toc291452681)

[Capítulo 7 Conclusiones 116](#_Toc291452682)

[Referencias 117](#_Toc291452683)

[Definición de términos 124](#_Toc291452684)

# Índice Tablas

##### **Tabla 1.1** Tecnologías biométricas.............................................................................................22

##### **Tabla 2.1** Descripción de sistemas semejantes..........................................................................35

##### **Tabla 3.1** Cálculo de la cuenta total............................................................................................40

##### **Tabla 3.2** Cálculo del valor de ajuste de la complejidad. ...........................................................41

##### **Tabla 3.3** Equivalencia de los Puntos de Función en Líneas de Código.....................................42

##### **Tabla 3.4** Coeficientes para los diferentes tipos de proyecto....................................................45

##### **Tabla 3.5** Elementos necesarios para sacar la FAE.....................................................................45

##### **Tabla 3.6** Estimación con COCOMO...........................................................................................46

##### **Tabla 3.7** Costo Total del Proyecto.............................................................................................46

##### **Tabla 4.1.2.1** Descripción de Caso de uso ingresar información privada...................................52

##### **Tabla 4.1.2.2** Descripción de Caso de uso ingresar información pública...................................53

##### **Tabla 4.1.2.3** Descripción de Caso de uso integrar datos .........................................................54

##### **Tabla 4.1.2.4** Descripción de Caso de uso validar usuario..........................................................55

##### **Tabla 4.1.2.5** Descripción de Caso de uso iniciar sesión.............................................................56

##### **Tabla 4.1.2.6** Descripción de Caso de uso visualizar reportes....................................................56

##### **Tabla 4.1.2.7** Descripción de Caso de uso eliminar cuenta........................................................57

# Índice Figuras

##### 

##### **Fig. 1.1** Cifrado Simétrico ...........................................................................................................28

##### **Fig. 1.2** Cifrado Asimétrico..........................................................................................................28

##### **Fig. 2.1** Tecnologías que apoyan el mecanismo de autentificación ...........................................33

##### **Fig. 2.2** Representación de la Infraestructura de Identificación y Autentificación digital. ........36

##### **Fig. 4.1** Diagrama de casos de uso de la Infraestructura.............................................................50

##### **Fig. 4.2.1** Diagrama de secuencia Ingresar información privada.................................................58

##### **Fig. 4.2.2** Diagrama de secuencia Ingresar información privada.................................................61

##### **Fig. 4.2.3** Diagrama de secuencia Integrar datos.........................................................................62

##### **Fig. 4.2.4** Diagrama de secuencia Validar usuario.......................................................................61

##### **Fig. 4.2.5** Diagrama de secuencia Iniciar sesión..........................................................................62

##### **Fig. 4.2.6** Diagrama de secuencia Visualizar reportes.................................................................62

##### **Fig. 4.2.7** Diagrama de secuencia Eliminar cuenta......................................................................63

##### **Fig. 4.3.1** Diagrama de actividades general Primer Módulo........................................................64

##### **Fig. 4.3.1.1** Zoom del diagrama de actividades Primer Módulo-Ingresar información privada...65

##### **Fig. 4.3.1.2** Zoom del diagrama de actividades Primer Módulo-Ingresar información pública...66

##### **Fig. 4.3.1.3** Zoom del diagrama de actividades Primer Módulo-Integrar datos...........................67

##### **Fig. 4.3.1** Diagrama de actividades Segundo Módulo...................................................................68

##### **Fig. 4.3.2.1** Zoom del diagrama de actividades Segundo Módulo arriba......................................69

##### **Fig. 4.3.2.2** Zoom del diagrama de actividades Segundo Módulo abajo.......................................70

##### **Fig. 4.3.3.1** Diagrama de actividades Tercer Módulo 71

##### **Fig. 4.4.1** Diagrama de clases del Módulo de registro y generación de ID 72

##### **Fig. 4.4.2** Diagrama de clases del Módulo de Validación 73

##### **Fig. 4.4.3** Diagrama de clases del Módulo de Administrador 73

##### **Fig. 4.5.1** Diagrama Entidad-Relación de la BD 74

##### **Fig. 4.5.2**Diagrama lógico de la BD 75

##### **Fig. 5.1** Pantalla de Bienvenida del Módulo de registro y creación de ID digital 77

##### **Fig. 5.2** Pantalla Datos Privados 77

##### **Fig. 5.3** Cuadro de diálogo Error al llenar campos 78

##### **Fig. 5.4**Fragmento de código para obtener Curp parte 1 80

##### **Fig. 5.5** Fragmento de código para obtener Curp parte 2 81

##### **Fig. 5.6** Cuadro de diálogo Error al obtener el Curp 81

##### **Fig. 5.7** Cuadro de diálogo Verificar información 82

##### **Fig. 5.8** Pantalla de Datos Públicos 82

##### **Fig. 5.9** Selector de archivos para elegir imagen del Curp 83

##### **Fig. 5.10** Cuadro de diálogo Error en selección de imagen 83

##### **Fig. 5.11** Cuadro de diálogo Error de conexión 89

##### **Fig. 5.12** Cuadro de diálogo Error al comparar Curp 90

##### **Fig. 5.13** Cuadro de diálogo Comparación exitosa 90

##### **Fig. 5.14** Pantalla módulo biométrico 91

##### **Fig. 5.15** Biometric Password Manager Biopod 91

##### **Fig. 5.16** Fragmento de código que genera el certificado 93

##### **Fig. 5.17** Fragmento de código método algoritmo hash 94

##### **Fig. 5.18** Fragmento de código Cifrar digital 95

##### **Fig. 5.19** Cuadro de diálogo Error al crear documentos 96

##### **Fig. 5.20** Pantalla Guardar información en Token 96

##### **Fig. 5.21** Selector de Token 97

##### **Fig. 5.22** Cuadro de diálogo Error al dar de alta en la BD 98

##### **Fig. 5.23** Cuadro de diálogo Error al guardar en Token 99

##### **Fig. 5.24** Fragmento de código Guardar reporte en BD 99

##### **Fig. 5.25** Pantalla Identificación lista 100

##### **Fig. 5.26** Archivos guardados en el token 100

##### **Fig. 5.27** Pantalla Bienvenida de Verificación 101

##### **Fig. 5.28** Cuadro de diálogo Campos vacíos 101

##### **Fig. 5.29** Cuadro de diálogo Curp mal escrito 102

##### **Fig. 5.30** Cuadro de diálogo Usuario inexistente en la BD 102

##### **Fig. 5.31** Seleccionar Token 102

##### **Fig. 5.32** Cuadro de diálogo No existe certificado en Token 103

##### **Fig. 5.33** Cuadro de diálogo Certificado expirado 103

##### **Fig. 5.34** Fragmento de código Verificar Firma 104

##### **Fig. 5.35** Pantalla Identificación y Autentificación exitosas 105

##### **Fig. 5.36** Cuadro de Diálogo Verificación Fallida 105

##### **Fig. 5.37** Pantalla Módulo biométrico 106

##### **Fig. 5.38** Cuadro de diálogo Solicitud de huella 106

##### **Fig. 5.39** Pantalla Error en identificación y autentificación 107

##### **Fig. 5.40** Pantalla Administrador 108

##### **Fig. 5.41** Cuadro de diálogo Contraseña inválida 108

##### **Fig. 5.42** Cuadro de diálogo Excedió intentos 108

##### **Fig. 5.43** Pantalla Menú del Administrador 109

##### **Fig. 5.44** Pantalla Visualizar Reportes 109

##### **Fig. 5.45** Cuadro de diálogo Curp mal escrito 110

##### **Fig. 5.46** Cuadro de Diálogo Campo del Curp vacío 110

##### **Fig. 5.47** Fragmento de código Verificar existencia en BD 110

##### **Fig. 5.48** Cuadro de diálogo Usuario no encontrado en BD 111

##### **Fig. 5.49** Reporte de usuario 111

##### **Fig. 5.50** Reporte.jrxml 112

##### **Fig. 5.51** Pantalla Eliminar usuario 113

##### **Fig. 5.52** Cuadro de diálogo El usuario no existe en la BD 113

##### **Fig. 5.53** Fragmento de código Eliminar usuario 114

##### **Fig. 5.54** Cuadro de diálogo Eliminación exitosa 114

# 

# Capítulo 1 Introducción

## 1.1 Introducción

En México la credencial para votar expedida por el IFE y la Cédula de Identidad Ciudadana son documentos con validez oficial que acreditan la identificación del individuo, al igual que otros documentos como el pasaporte y la cartilla militar (en el caso masculino) entre otros, pero todos ellos carecen de autenticación, lo cual no garantiza que el portador sea quien dice ser y hasta pueden ser falsificables, y por lo tanto, no certificar que los trámites que se realicen con ellos sean 100% confiables.

La identidad digital de un usuario, es la suma de datos únicos a su persona, como datos personales, académicos o financieros en un medio de transmisión digital. Con ella, la capacidad para conocer a actores que forman parte de distintas organizaciones para gestionar mejor los servicios, produce un resultado más satisfactorio para todos los implicados. [1]

El problema que se presenta en algunas de ellas, es el creado por la dispersión actual de las distintas partes que forman la identidad digital de un usuario, ya que actualmente el usuario es el responsable de mantener toda esa información de forma coherente y consistente, recordar el par usuario-contraseña para cada uno de los sistemas, y es el mismo quién debe administrarla para asegurarse de que cada sitio mantiene información actualizada.

Por todo lo anterior, la importancia de contar con un sistema de identidad digital confiable y robusto en cuanto a seguridad se refiere, se vuelve cada vez más necesario y sabiendo que la identificación de personas es y será un tema de investigación y desarrollo importante ligado a la constante evolución de las sociedades humanas, en este trabajo terminal se creara una Infraestructura de Identificación y Autentificación Digital de la que se obtendrá una identificación digital con la que se pretende lograr que los sistemas de seguridad sean más confiables, al combinar el análisis biométrico con un medio de identificación público y otro privado y así se pueda llegar a garantizar el no repudio.

## 1.2 Objetivos

### 1.2.1 Objetivo General

Desarrollar e implementar una infraestructura de identificación y autentificación de personas, que genere un perfil único integrando información pública, privada y biométrica, garantizando la validez de la información y permitiendo el acceso a un servicio de forma segura.

### 1.2.2 Objetivos Particulares

* Utilizar una interfaz amigable que elimine la complejidad de uso y sea apto para cualquier tipo de usuario.
* Manejar suficiente información al crear el perfil único con la seguridad adecuada para evitar la violación de datos.
* Ser almacenado en un dispositivo USB, obteniendo mayor portabilidad.
* Al instante de ser requerido por alguna institución o sistema para la solicitud de un servicio, garantizar seguridad recíproca entre el servidor y el usuario.
* Servir como base para nuevos métodos de identificación y autentificación.

## 1.3 Antecedentes y conceptos básicos

### 1.3.1 El problema de la Identificación

Como la acepción más común de la palabra identificación, se encuentra que es el acto de identificar, reconocer o establecer los datos e información principal sobre una persona, lo que la ha hecho crucial para la sociedad desde el comienzo de la civilización hasta nuestros días, usada en los sectores financieros, de salud, de transporte, de entretenimiento, cumplimiento de la ley, seguridad, control de acceso, control migratorio, gobierno, comunicación entra otros. [2]

Los principios básicos de la seguridad de la información son:

* Confidencialidad: propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.
* Integridad: propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información.
* Disponibilidad: cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. [3]

A estos principios también se les conoce como la Tríada CIA, del inglés: "Confidentiality, Integrity, Availability" y existen diversos tipos de personas maliciosas que buscan dañarlos como:

* El hacker [que es un usuario](http://www.mastermagazine.info/termino/5204.php) de ordenadores especializado en penetrar en las bases de datos de sistemas informáticos estatales con el fin de obtener [información](http://www.mastermagazine.info/termino/5204.php)  secreta. En la actualidad, el término se identifica con el de delincuente informático. [4]
* El cracker en realidad son hackers, pero con intenciones que van más allá de experimentar en casa y se dedican exclusivamente a [reventar sistemas](http://www.suite101.net/content/las-amenazas-a-la-seguridad-informtica-en-2011-a30485), ya sean estos electrónicos o informáticos. [5]
* El lammer personas deseosas de alcanzar el nivel de un hacker pero su poca formación y sus conocimientos les impiden realizar este sueño. Su trabajo se reduce a ejecutar programas creados por otros, a bajar, en forma indiscriminada, cualquier tipo de programa publicado en la red.
* El copyhacker Son una nueva generación de falsificadores dedicados al crackeo de Hardware, específicamente en el sector de tarjetas inteligentes, se interesan por poseer conocimientos de tecnología, son aficionados a las revistas técnicas y a leer todo lo que hay en la red. Su principal motivación es el dinero.
* PhreakerSe caracterizan por poseer vastos conocimientos en el área de telefonía terrestre y móvil, incluso más que los propios técnicos de las compañías telefónicas; recientemente con el auge de los celulares, han tenido que ingresar también al mundo de la informática y del procesamiento de datos.
* Newbie es el típico "novato" de red, sin proponérselo tropieza con una página de Hacking y descubre que en ella existen áreas de descarga de buenos programas de Hackeo, baja todo lo que puede y empieza a trabajar con ellos.
* Script kiddie denominados también “Skid kiddie”, son simples usuarios de Internet, sin conocimientos sobre Hack o Crack aunque aficionados a estos temas no los comprenden realmente, simplemente son internautas que se limitan a recopilar información de la red y a buscar programas que luego ejecutan sin los más mínimos conocimientos, infectando en algunos casos de virus a sus propios equipos. También podrían denominarse los “Pulsa Botones o Clickquiadores “de la red. [6]

### 1.3.2 Medios de identificación

#### Primeros medios de identificación

El lenguaje

El lenguaje se configura como aquella forma que tienen los seres humanos para comunicarse. Se trata de un conjunto de signos, tanto orales como escritos, que a través de su significado y su relación permiten la expresión y la comunicación humana, sin embargo desde principios de las civilizaciones, tanto sonidos como símbolos, y los lenguajes derivados de la evolución de estos son una forma de identificación.

El lenguaje como creación cultural, establece los principios constitutivos de la identidad del individuo y de los grupos sociales, mediante las formas particulares en que se desarrollan los dialectos y las lenguas, principalmente. Cuando la tecnología existente era prácticamente nula, los humanos se identificaban por sus rasgos físicos, y por el lenguaje que compartían como grupo social. [7]

Símbolos

El término símbolo hace referencia, a un signo de reconocimiento entre hospedador y huésped, que compartían las dos mitades de una misma cosa cuya reunión servía de legitimación y adquiría fuerza de prueba.

Por extensión, se aplicaba a las señales secretas de reconocimiento y de reunión de las que servían los iniciados en los misterios paganos y que adoptaron más tarde los primeros cristianos durante la era de las persecuciones. [8]

El “Diccionario de los Símbolos” de Chevalier-Cheerbrant (Herder, Barcelona 1991, p. 980) dice: “el tatuaje pertenece en suma a los símbolos de identificación”. [9]

Aunque un tatuaje no puede identificar de forma exclusiva a una persona, puede ayudar a las autoridades a reducir la lista de posibles identidades. También puede indicar la pertenencia a una pandilla, grupo social o religioso. [10]

#### Documentos

Los primeros documentos legales surgieron con el comienzo de la escritura y regulaba la compra-venta de tierras y sus obligaciones derivadas. Son contratos que dictaban las normas de funcionamiento de una legalidad, así como la identidad de los individuos participantes en los intereses plasmados en dichos documentos. [11]

Documentos con firmas

* Firmas Manuscritas

La firma es una palabra, o pequeño mensaje o dibujo, que tiene como fin identificar y asegurar o autentificar la identidad de un autor o remitente, o como una prueba del consentimiento y/o de verificación de la integridad y aprobación de la información contenida en un documento o similar. Surgió al realizarse los primeros documentos oficiales para identificar a las partes interesadas en dicho manuscrito. [12]

Por su parte la Real Academia Española la define como “el nombre y apellido o título de una persona que ésta pone con rúbrica al pié de un documento escrito de mano propia o ajena, para darle autenticidad, para expresar que se aprueba un contenido o para obligarse a lo que en él se dice”.

No obstante, esta definición está restringida a las firmas manuscritas pero en la interacción social cotidiana, la realidad es otra pues, además de dichas firmas, se utilizan medias firmas, firmas marcando una “x”, firmas con sellos, firmas mecánicas o impresas, firmas con huellas digitales, firmas utilizando tecnologías biométricas modernas y firmas digitales, entre otras.

Desde un punto de vista jurídico, no se pone tanto el acento en definir qué sea una firma pero sí en cuanto cuáles son los efectos que de la misma se derivan. La firma se ha convertido en un hecho previo o dato fáctico del cual se parte. Con la salvedad de algunos supuestos especiales del registro de firmas en relación con fedatarios públicos, la firma manuscrita no se somete a control ni requisitos. [13]

Es frecuente, por ejemplo que al entrar en algún lugar se exija la presentación de alguna tarjeta de identidad u otros certificados o constancias que usualmente contienen una foto, la firma, el nombre, posición etc. de la persona.

* Firmas Digitales

En las últimas décadas el desarrollo de las nuevas tecnologías ha provocado una profunda transformación, en los medios de comunicación y expresión de la voluntad. Inicialmente, los computadores, utilizados como máquinas de escribir desarrolladas, facilitaron la emisión de documentos sobre los que luego se estampaba una firma.

Actualmente, la intercomunicación de las computadoras posibilita no sólo la generación de documentos electrónicos, sino la transmisión de la información contenida en los mismos en tiempos mínimos, que permiten hablar, no ya de alta velocidad, sino de “tiempo real”, es decir, se accede a la “información distante justo al instante”. Se produce así el fenómeno que se ha dado en llamar “electronificación” o “digitalización”.

En los análisis técnicos jurídicos sobre las firmas electrónicas, el tema de las funciones de las firmas ha sido central pues los avances tecnológicos hasta los momentos no han logrado que la firma autógrafa u hológrafa pueda utilizarse en el medio electrónico. **[13]**

Aquello que tradicionalmente se ha entendido por firma autógrafa, pierde la capacidad para cumplir sus funciones en este medio. Si bien es posible crear una firma sobre un documento físico (no electrónico) y generar una imagen electrónica de la misma, es fácil que otra persona copie esa imagen electrónica y la coloque en cualquier documento electrónico, sin que el autor originario tenga la posibilidad de control sobre esto. Igualmente debido a la naturaleza de los documentos electrónicos, es muy fácil modificar su contenido sin que pueda detectarse alteración alguna.

En vista de estas circunstancias, desde finales de los años setenta, se han buscado alternativas para reproducir en el medio electrónico las funciones de la firma y con ello lograr un “equivalente funcional” entre la firma manuscrita y la firma electrónica . Sin embargo, esto no ha sido ni fácil ni uniforme pues las funciones que cumple una firma suelen ser muy variadas dependiendo de las circunstancias. **[14]**

Siguiendo a la Real Academia Española antes referida, son tres las posibles funciones:

* Autenticidad
* Aprobación del contenido
* Sujeción a las obligaciones contenidas en el documento.

Estas funciones están limitadas pues pueden no darse en ciertas circunstancias en las cuales se usen firmas. Si consideramos por ejemplo, la segunda de éstas, pudiera imaginarse el caso en que una firma no se coloque con el objeto de aprobar el contenido de un documento sino para dejar constancia de que se leyó el mismo. **[13]** Por tanto, resulta conveniente utilizar un concepto más amplio como los siguientes:

* Ayuda en la identificación del autor (Autenticidad)
* Ayuda en la demostración de la intención del autor
* Ayuda en asegurar la integridad de la información firmada (Integridad)

En definitiva, en Internet es prácticamente imposible verificar quien ha escrito la firma que presenta. Mientras que con la firma digital al receptor le basta comprobar si el certificado digital en donde está contenida la firma está en vigor y si ha sido incluido en el directorio de certificados revocados o suspendidos. Una vez comprobados ambos extremos, utiliza la clave pública del remitente para comprobar que la firma digital de éste es auténtica, todo ello confiere una ventaja a la Firma digital.  **[14]**

Esta es una función que pudiera ser subjetiva u objetiva según el documento de que se trate. En aquellos documentos en los cuales la ley otorga un significado específico a la firma (por ejemplo letras de cambio), generalmente no hay dudas con respecto a la intención del firmante y por ello puede decirse que la intención del autor está objetivada. Las variaciones son infinitas pero los mecanismos existentes funcionan debido a las costumbres, los convencionalismos, en el contexto en que se colocan las firmas y otros aspectos que han permitido cierta estabilidad y seguridad en cuanto a la intención. [13]

En el medio electrónico, la intención del autor es más difícil de comprender puesto que aún no existen prácticas generalizadas o costumbres con respecto a las tecnologías que se están utilizando para firmar electrónicamente ni con respecto los contextos de dicho medio. **[13]**

Otra función de la firma es contribuir a que la información en el documento firmado no sea alterada después de que la firma haya sido colocada, aunque no es una función exclusiva de la firma, pues las limitaciones físicas del papel u otro objeto físico, ayudan en tal sentido, la firma ayuda al ser colocada al pie del texto.

En el medio electrónico, las tecnologías de firmas electrónicas basadas en la criptografía han convertido a la firma en el método más confiable para determinar si un documento electrónico ha sido modificado desde que la firma en cuestión fue realizada. [15]

Y es que en un entorno tan vasto y potencialmente hostil como Internet, es muy difícil para el receptor de un documento advertir si éste ha sido manipulado, mientras que al incorporar el *hash* cualquier manipulación sería evidente de forma inmediata.

En este sentido deben aclararse algunos conceptos, por ejemplo criptografía, la criptografía es una rama de la criptología que consiste en mantener mensajes secretos, mientras que la criptología es la rama de las matemáticas compuesta por la criptografía y el criptoanálisis.

El criptoanálisis es la rama de la criptología que consiste en transgredir los sistemas criptográficos a fin de leer mensajes secretos. [16]

Por otra parte, en relación a la función hash, es necesario aclarar que los esquemas de firma digital suelen ser muy lentos en su transmisión y, en ocasiones, la longitud de la firma suele ser similar o mayor al mensaje mismo; por ende, en la práctica se utiliza la función *hash* antes de firmar un mensaje. Esta función consiste en aplicar a un mensaje de longitud variable, una representación de longitud fija del propio mensaje, que se denomina valor *hash* (este valor es siempre mucho menor que el mensaje, por ejemplo, un mensaje de 1 megabyte de longitud, puede reducirse a 64 o 128 bits de longitud). [17]

Bajo este contexto de seguridad algunos autores consideran con razón que el documento o mensaje encriptado se transforma en un documento que ninguna otra persona pudo haber generado y además, que la firma digital es más segura que la ológrafa, puesto que además de asegurar que el mensaje fue realmente generado por quien lo envía, garantiza que ninguna parte de él ha sido modificada.

Pero además se debe garantizar que quien recibe el mensaje es la persona que el emisor desea lo lea, ello implica seguridad y al mismo tiempo se busca garantizar que no se pueda negar la autoría de un mensaje enviado, así como no poder rechazar que un mensaje ha sido recibido, lo cual implica un No rechazo o No Repudio.

De lo anterior que la Firma Digital requiera lo siguiente:

* Estar vinculada al signatario de manera única
* Permitir la identificación del signatario
* Haber sido creada por medios que el signatario pueda mantener bajo su exclusivo control
* Estar vinculada a los datos relacionados de modo que se detecte cualquier modificación ulterior de los mismos.

Tales consideraciones ponen de manifiesto que estos métodos aportan la confiabilidad necesaria como para ser utilizados en el tráfico jurídico. Sin embargo, se debe resaltar que el proceso tecnológico de firmar digitalmente instrumentos no es suficiente por sí sólo, pues para que pueda cumplir adecuadamente con su objetivo requiere de un contexto determinado, usualmente denominado Infraestructura de clave pública o infraestructura de firma digital o Criptografía Asimétrica. [18]

Documentos con fotografía

Los medios de identificación que se ha utilizado comúnmente a partir de la democratización de la sociedades, son un conjunto de documentos con validez oficial que cuentan con fotografía y/o huella digital, sin embargo no todos los países emiten documentos de identidad, aunque la extensión de la práctica acompañó el establecimiento de sistemas nacionales de registro de la población y la elaboración de los medios de control administrativo del Estado. [19]

La posesión de un documento de identidad es obligatoria en la mayoría de los países en México se pueden presentar los siguientes:

* CURP.
* Acta de nacimiento.
* Credencial de elector.
* Certificado de estudios.
* Pasaporte
* Título y Cédula profesional
* Cartilla Militar.
* Visa
* Licencia de manejo.
* Credencial del IMSS
* Acta de defunción.
* Escrituras de tu casa.
* Credencia escolar.

#### Tarjetas Magnéticas

Las tarjetas magnéticas son tarjetas blancas normales con una bandamagnética que puede ser leída por un dispositivo electrónico. En dicha banda, aparece la [información](http://definicion.de/informacion) del usuario y se es posible leer e incluso volver a grabar este tipo de tarjetas todas las veces que sea necesario. [20]

Las tarjetas de crédito y débito se enmarcan dentro de este tipo de tarjetas, al igual que aquellas que, al ser pasadas por un cierto lector, posibilitan el acceso a determinados lugares.

El registro de datos sobre una pista magnética utiliza la propiedad que tienen algunos materiales de magnetizarse de manera duradera bajo la acción de un campo magnético. [21]

#### RFID

RFID es el acrónimo de Radio Frequency Identification por sus siglas en inglés, o Identificación por Radio Frecuencia. Pertenece a una amplia gama de tecnologías para adquisición de datos e identificación automática (AIDC) en la que también se incluyen los códigos de barras, la lectura de caracteres ópticos y los sistemas infrarrojos de identificación. [22]

Se trata de una tecnología basada en la utilización de un pequeño chip adherido a un producto, y a través del cual es posible mantener un rastreo de su localización. La distancia de rastreo varía mucho, dependiendo del tamaño, tipo y antena del chip, pero podría ser desde 2cm. a 13 metros en los sencillos, hasta incluso varios kilómetros en los más complejos.

Son realmente pequeños y tal y como van los avances, en poco tiempo podrían ser considerados virtualmente invisibles. [23]

#### SmartCard

Tarjetas con Chip integrado capaces de almacenar y en algunos casos procesar información de manera segura siendo utilizada en datos confidenciales.

Las tarjetas inteligentes se han utilizado también para identificar al personal de las empresas y actualmente en todos los teléfonos móviles (GSM). [24]

Por lo que están prevaleciendo más y más, por ejemplo en Malasia la Tarjeta Inteligente Multipropósito Mykad está siendo utilizada a escala nacional (18 Millones de Tarjetas) para manejar en una sola tarjeta: Identificación personal, licencia de conducir, tarjeta de seguro, pago (ePurse) para transporte público e información de viajero. [25]

#### Biometría

Del griego “bios” que es vida y “metron” que es medida, se define a la biometría como el estudio de los métodos automáticos y la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para “verificar” identidades o para “identificar” individuos. [26]

A continuación en la Tabla 1.3 se muestran las tecnologías biométricas más utilizadas en la actualidad e información relevante de cada una de ellas:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Tecnología*** | ***Ventajas/Desventajas*** | ***Como Trabaja*** | ***Fiabilidad*** | ***Costo*** |
| ***Huella digital*** | No puede perder sus huellas digitales como pierde una llave y no puede olvidar sus huellas digitales como puede olvidar un password. La exactitud varía en función del sexo, características raciales y residuos químicos presentes en los dedos, como el cloro de la piscina o los limpiadores domésticos. | Captura y compara patrones de la huella digital | Alta | Medio |
| ***Iris*** | Es única y permanece estable con el tiempo y en los ambientes, por lo que es altamente segura. Es bastante cara, solo para sitios de muy alta seguridad, los usuarios pueden desconfiar a poner el ojo cerca de una cámara. | Captura y compara los patrones del iris | Media | Muy alto |
| ***Voz*** | Es considerado uno de los sistemas biométricos más exactos, debido a su naturalidad, pues hasta en la vida diaria nos permite reconocer a personas con facilidad. Es un medio natural de interacción con el entorno y por tanto resulta muy aceptable para los usuarios pronunciar una palabra o frase ante un micrófono para identificarse.  La disponibilidad de dispositivos para tomar las muestras de voz, por ejemplo: la red telefónica y los micrófonos de las computadoras por lo que no será necesaria la compra de este dispositivo para el uso del sistema. [27] | Captura y compara cadencia y tono de la voz | Alta | Bajo |
| ***Geometría facial*** | Requiere de unas condiciones muy concretas, sobre todo de luz.  Consta normalmente de tres componentes. Por una parte, hace falta una cámara que registre una imagen. En segundo lugar, es necesario un software, es decir un programa informático que determine si en esa imagen aparece alguna cara localizando, entre otras cosas, la geometría del rostro: la disposición de los ojos, nariz, boca, entre otros. Y un sistema que sea capaz de clasificar todos esos elementos para diferenciar entre unas y otras personas. Por lo que lo hace muy caro. [28] | Captura y compara patrones faciales | Baja | Alto |

##### 

###### Tabla 1.1 Tecnologías biométricas

#### Autoridad de certificación

Una autoridad de certificación es un sistema informático dedicado a la emisión y gestión posterior de certificados digitales, incluyendo la renovación, expiración, suspensión, la habilitación y la revocación de certificados, a petición de la autoridad de registro. La emisión de certificados se hace de una forma automatizada y no sin la previa confirmación de la autoridad local de registro. La función básica de las autoridades de certificación: es verificar la identidad de los solicitantes de certificados.

El alcance de la responsabilidad de la Autoridad de Certificación se encuentra delimitado por su Política de Certificación, no siendo responsable en los siguientes casos:

* Por los casos que se excluyan en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos.
* Por los daños y perjuicios que resulten del uso no autorizado de un certificado, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización.
* Por los daños y perjuicios que excedan el valor límite por transacción, o por el total de transacciones, si tales valores límites constan en las correspondientes condiciones de emisión y utilización de sus certificados.
* Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en su manual de procedimientos, deba ser objeto de verificación, siempre que la Autoridad de Certificación (AC) pueda demostrar que ha tomado todas las medidas razonablemente practicables para verificar tal información, de acuerdo con las circunstancias y el tipo de certificado de que se trate. [29]

#### Certificados Digitales

Son documentos electrónicos de aproximadamente 1k de tamaño que asocian una clave pública con la identidad de su propietario. Tienen como objetivo principal permitir verificar la identidad del usuario, garantizando que únicamente él puede acceder a su información personal, evitando suplantaciones. También es el elemento usado para firmar electrónicamente solicitudes o documentos, ayudando a prevenir que alguien utilice una clave para hacerse pasar por otra persona.

Adicionalmente, además de la clave pública y la identidad de su propietario, un certificado digital puede contener otros atributos para, por ejemplo, concretar el ámbito de utilización de la clave pública, las fechas de inicio y fin de la validez del certificado, etc. El usuario que haga uso del certificado podrá, gracias a los distintos atributos que posee, conocer más detalles sobre las características del mismo y es válido únicamente dentro del período de vigencia, que comienza en la fecha de inicio indicada en el certificado y finaliza en su fecha de vencimiento, o con su revocación si fuere revocado. [30]

### 1.3.3 Métodos de cifrado

Es importante mencionar que el cifrado de datos es una herramienta de utilidad para la seguridad en sistemas de cómputo, ya que permite garantizar las propiedades de confidencialidad, integridad y disponibilidad de los recursos, lo importante a través de los años es mandar los mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entender el mensaje.

Por lo que se debe saber cómo utilizarla teniendo los conceptos básicos tanto en su clasificación como en su funcionamiento básico de algunos sistemas de cifrado, se utilizarán dos algoritmos estándares, el sistema asimétrico RSA, y MD5 para comprobar la integridad del archivo.

Algunos elementos a considerar dentro de la seguridad informática se mencionan a continuación:

* *Seguridad física*; son todos los asuntos relacionados a los soportes físicos de la información, más que de la información, las medidas contra incendios y sobrecargas eléctricas, la prevención de ataques terroristas, las políticas de respaldos, restricción de acceso físico a las computadoras únicamente a personas autorizadas.
* *Seguridad de la información;* esto se refiere a la preservación de la información frente a observadores no autorizados. En este rubro se emplea tanto la criptografía simétrica como la asimétrica.
* *Seguridad del canal de comunicación; l*os canales de comunicación rara vez se consideran seguros, esto es un riesgo ya que en el mayor de los casos no se tiene control al pertenecer a terceros, resulta imposible asegurarse totalmente de que no se tienen escuchas o intervenciones.
* *Problemas de autenticación;* debido a los problemas del canal de comunicación, se requiere asegurar que la información que se recibe de la computadora, viene de *quien realmente se cree; para esto la criptografía asimétrica da una solución.*
* *Problemas de suplantación; en las redes se tiene el problema de que cualquier usuario autorizado, puede acceder al sistema desde fuera, y se tiene que garantizar que los usuarios no están siendo suplantados por intrusos.* [31]

#### Confidencialidad

La confidencialidad consiste en proteger la información contra la lectura no autorizada; incluye no sólo la protección de los datos transmitidos por medio de ataques pasivos sino también en función del contenido de una transmisión de datos, existen diferentes niveles de protección.

* Confidencialidad de la conexión: la protección de los datos de todos los usuarios en una conexión TCP.
* Confidencialidad no orientada a la conexión: la protección de los datos de todos los usuarios tiene un único bloque de datos.
* Confidencialidad de campos seleccionados: la confidencialidad de campos seleccionados en los datos del usuario en una conexión o en un único bloque de datos.
* Confidencialidad del flujo del tráfico: la protección de la información que podría extraerse a partir de la observación del flujo del tráfico. [32]

#### Autenticación

La autenticación en cuanto a telecomunicaciones se refiere a garantizar la autenticidad de la comunicación; que el emisor es quien dice ser realmente; mediante mecanismos para verificar quién está enviando la información.

Este servicio se encarga de que un mensaje se asegure al receptor, es decir que el mensaje pertenece a la fuente que dice ser y en la conexión de una terminal a un servidor se autentica la entidad origen y la destino; además que la conexión no la interviene una tercera persona para suplantar una de las dos partes para una transmisión o recepción no autorizada (autentificación del origen de los datos) . [32]

Existen diferentes métodos de autenticación que tienen como objetivo comprobar de manera segura su origen, que no exista una manipulación, su identidad, etc. Los grandes tipos dentro de los métodos de autenticación son:

* Autentificación de mensaje: garantizar la procedencia de un mensaje conocido, asegurar de que no es una falsificación (firma digital).
* Autentificación de usuario: mediante contraseña; se garantiza la presencia de un usuario legal en el sistema, mediante una contraseña secreta que le permita identificarse.
* Autentificación de dispositivo: se trata de garantizar la presencia de un dispositivo válido como una llave electrónica que sustituye a la contraseña para identificar a un usuario, otras como la biométrica, las huellas digitales, la retina, la voz.
* Autentificación basada en técnicas criptográficas. .[31]

#### Integridad de datos

Se refiere a proteger la información contra ser modificada por las entidades autorizadas, no solo la que está almacenada directamente en los sistemas de cómputo sino que también se deben considerar los respaldos, documentación, registros de contabilidad del sistema, tránsito en una red, entre otros.

La modificación incluye escritura, cambio, borrado, creación y re actuación de los mensajes transmitidos. La integridad de datos asegura que los datos recibidos no han sido modificados de ninguna manera, causadas por errores de hardware y/o software; causadas de forma intencional, de forma accidental o cuando se trabaja con una red. [33]

#### No Repudiación

La no repudiación significa que ni el origen ni el destino en un mensaje deben poder negar la transmisión. Quien envía el mensaje puede probar que, en efecto, el mensaje fue enviado y viceversa. Proporciona protección contra la interrupción, por parte de una de las entidades implicadas en la comunicación, de haber participado en toda o parte de la comunicación. [32] El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje. Las firmas digitales constituyen el mecanismo más empleado para este fin. [33]

#### Proceso Criptográfico

Formalmente se dice que un criptograma C es el resultado de aplicar un algoritmo criptográfico E. [35] Matemáticamente se entiende como una función, sobre el texto claro m, empleando una clave dada Kb (el subíndice indica que la clave es usada para el cifrado, y no tiene por qué ser la misma para descifrar, esto es para efectos de notación), este proceso se conoce como el cifrado de un texto claro:

*C = E(m, Kb)*

El proceso criptográfico que recupera el mensaje original m, es conocido como descifrado D que es obtenido a partir de un criptograma C; con una clave Ka, que es la clave usada para descifrar el mensaje:

*m = D(C, Ka)*

#### Cifrado

Al hablar hoy día de sistemas de comunicación segura, se introduce una herramienta que maneje la seguridad de redes y comunicaciones y esta es el cifrado, cuyo principio es mantener la privacidad de la comunicación entre un emisor (persona que envía un mensaje) y un destinatario o receptor (persona que recibe el mensaje). [36]

El cifrado permite a la tecnología la seguridad en la infraestructura de cómputo y comunicaciones; jugando ésta un rol importante para la criptografía moderna, esto fue descrito por uno de los iniciadores Ronald L. Rivest, al describir su frase “La necesidad es la madre de la invención, y las redes de las computadoras son la madre de la criptografía moderna”. [37]

*Criptografía* proviene de las palabras griegas “krypto” (ocultar), y “graphos” (escribir), por lo tanto es la ciencia que usa las matemáticas para cifrar la información, y el término *Criptoanálisis* es el proceso que descubre un texto claro o una clave de cifrado; por lo que destruye la protección criptográfica de la información; de forma genérica estudia las propiedades de la seguridad y posibilidades de romper las técnicas de los sistemas criptográficos; la *Esteganografía* es un método para ocultar la existencia de un mensaje, estas definiciones son de acuerdo a RFC 28286. [38]

En el criptosistema participa un emisor, un receptor, un algoritmo de cifrado (alteración del mensaje original mediante un algoritmo y de manera incomprensible a toda persona ajena al destinatario), algoritmo de descifrado, una clave pública o secreta según el tipo de cifrado simétrico o asimétrico.

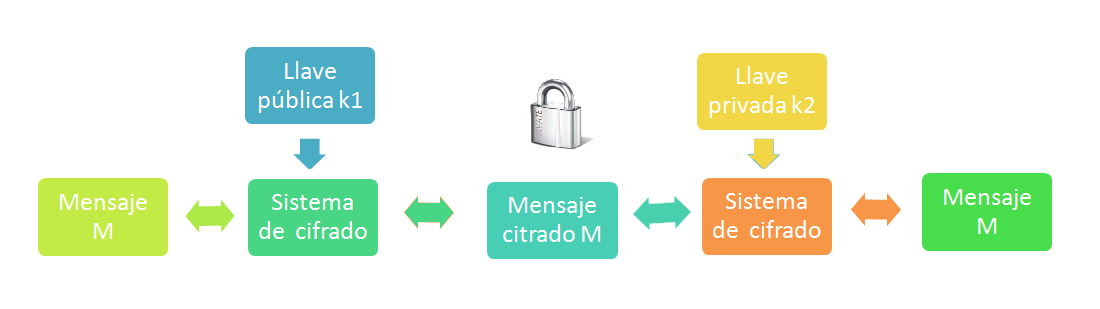
Cifrado Simétrico

La seguridad del cifrado simétrico *(brinda la confidencialidad de mensajes)* se basa en privacidad de su *clave secreta* ya que es la misma para el cifrado que para el descifrado. En este esquema de cifrado se tiene dos características muy importantes; la primera es una clave secreta (o clave única); que se usa en la entrada de un algoritmo cuyas operaciones elementales son la sustitución para causar una confusión y una transposición (reordenamiento) o permutación con el fin de manejar una difusión en cada elemento del texto claro. La clave que usa el emisor para cifrar el texto claro es la misma con la que el receptor descifrará el mensaje cifrado. Y la segunda es el algoritmo de cifrado en la que usa varias sustituciones y transformaciones para procesar el texto claro ya sea un cifrado de bloque (de tamaño fijo) en el proceso del texto uno de salida por uno de entrada; como por ejemplo el algoritmo DES, Triple DES7 y AES8; o un cifrado de flujo que procesa los elementos de entrada continuamente, produciendo la salida de un elemento cada vez, el esquema de este cifrado se muestra en la Fig. 1.1. [39]

##### *Fig. 1.1 Cifrado Simétrico*

Cifrado Asimétrico

En este esquema de cifrado se tienen dos aspectos de importancia; el primero es el uso de una clave pública (*k1)* y una privada *(k2)*; una es usada para el cifrado y otra para el descifrado, la seguridad está en la longitud de las claves y el costo computacional para romper el cifrado. El segundo aspecto es el uso de un algoritmo de cifrado; el algoritmo realiza diferentes transformaciones en el texto claro, si el emisor envía un mensaje privado al receptor, para cifrar el algoritmo usa la clave pública del receptor y el receptor lo descifra usando su clave privada; ejemplos de estos algoritmos son el RSA y el Gamal. [39] El esquema de este cifrado se muestra en la Fig. 1.2.

Fig. 1.2 Cifrado Asimétrico

#### Descripción RSA

Uno de los algoritmos de llave pública o algoritmos asimétricos más populares es el RSA, con una longitud de llave suficientemente grande, recomendable al menos de 768 bits; en la práctica se emplea para cifrar las claves de los cifrados simétricos de cada mensaje. Una de las aplicaciones de los algoritmos asimétricos es el cifrado de la información sin tener que transmitir la clave de descifrado, lo cual permite su uso en canales inseguros.

RSA es un cifrado de bloque en el que el texto claro *m* y el texto cifrado *C* son enteros entre 0 y *n* -1para algún *n*; la expresión del cifrado es la siguiente: *C = mb mod n*

Y el de descifrado es: *m = C a mod n*

donde *b* es la clave pública y *a* es la clave privada.

El proceso es el siguiente para el caso de que el emisor A envía un mensaje al receptor B, solicita a B su clave pública *KP*; A genera el mensaje cifrado *C* y como únicamente B posee la clave privada *Kp* podrá recuperar el mensaje original *m*; por lo tanto cabe resaltar que la llave pública es la que cifra los mensajes, mientras que la llave privada es la que permite el descifrado.

Si un atacante quiere recuperar la clave privada a partir de la llave pública, debe conocer los factores *p’* y *q* de *n*, y esto representa un problema computacionalmente intratable, siempre que p’ y q sean lo suficientemente grandes; ya que la seguridad es basada en la dificultad de factorizar números enteros largos, la probabilidad de que el número escogido pase el test y siga siendo primo son de una contra 260. Los fundamentos del criptosistema RSA son la aritmética modular y la teoría de números. [40]

#### Implementación del RSA en la infraestructura de Identificación y Autentificación Digital

Para el desarrollo de este trabajo se utilizará RSA como método de cifrado asimétrico ya que al ser una infraestructura de autentificación necesita la generación de llaves públicas y privadas, pública para el usuario del sistema que crea su identificación y privada para el sistema externo que solicite la identificación, es un algoritmo estándar cuya principal desventaja es la velocidad, esto debido al uso de números grandes para el cifrado, a su vez esta característica es lo que lo hace más seguro ya que es más complejo su descifrado.

La información que se cifrará será el conjunto de tres verificaciones (pública, privada y biométrica) almacenadas como un conjunto de caracteres en texto plano. Para implementarlo utilizaremos librerías RSA en Java cuyas características mostramos a continuación.

#### Descripción MD5

El algoritmo MD5 (Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) fue desarrollado por el profesor Ronald L. Rivest del MIT. MD5 toma como entrada un mensaje de longitud arbitraria y produce como salida de 128 bits "huella digital" o "resumen del mensaje" de la entrada. Se es computacionalmente imposible producir

dos mensajes que tengan el mismo mensaje de digerir.

El algoritmo MD5 está pensado para aplicaciones de firma digital, que debe ser un archivo de gran tamaño "comprimido" de una manera segura antes de ser encriptados con un privado (secreto) clave de un sistema de cifrado de clave pública tales como RSA. En esencia, MD5 es una manera de verificar la integridad de los datos, y es mucho más fiable que la suma de comprobación y muchos otros métodos de uso común. [52]

Codificación

La codificación del MD5 de 128 bits es representada típicamente como un número de 32 dígitos hexadecimal.

Características, Terminologías y notaciones

Funciones matemáticas que a partir de un conjunto (texto) crean un “resumen” (Hash) de forma que:

* + Si alguien varía algo del conjunto (aunque sea un solo bit) el resumen generado varía indefectiblemente.
  + Es prácticamente imposible obtener el mensaje a partir del hash.
  + A partir de una entrada cualquiera, calculan una cadena de bits de largo fijo.
  + Orden de dificultad de generar un mensaje que tenga un compendio dado, MD5: 2128
  + Orden de dificultad de generar dos mensajes distintos con el mismo compendio MD5: 264

#### Implementación del MD5 en la infraestructura de Identificación y Autentificación Digital

A pesar de haber sido considerado criptográficamente seguro en un principio, ciertas investigaciones han revelado vulnerabilidades que hacen cuestionable el uso de MD5 sin embargo, es un algoritmo que sigue siendo mayormente utilizado y cuyos ataques siguen siendo por fuerza bruta, esto conlleva la necesidad de una alta capacidad de cómputo, para su descifrado, permitiendo a nuestro sistema ganar tiempo para dar de baja la identificación en caso de robo y evitar la violación de acceso. Además al ser relativamente sencillo su revisión es menos compleja que otros similares como SHA-1, esto hace menos pesado el sistema que ya cuenta con un algoritmo más complejo como lo es RSA.

Lo utilizaremos como método para comprobar la integridad del archivo almacenado en el token, previamente cifrado, para comparar la suma MD5 de dicho archivo con un archivo MD5SUM con el resumen MD5 del primer archivo.

# Capítulo 2 Estado del arte

## 2.1 Planteamiento del problema

La identidad en la sociedad humana juega un roll muy importante y por ende, se entiende también la necesidad de contar con medios de control que brinden el acceso a recursos, instituciones, derechos, obligaciones, etc. de forma segura, tanto para el portador de la identificación, como del prestador de servicios o instancia que requiere de tal identificación.

Cuando se busca suplir esta necesidad, se suele recurrir a la creación de identificaciones con la impresión de micas con ciertos elementos de seguridad como marca de agua, holograma bidimensional, firma digitalizada, foto fantasma, entre otros. Lo malo que existe en ellas, es que no te permiten identificarte en múltiples organizaciones y se tiene que portar todas las identificaciones con las que se cuenta y en caso de robo o extravió de cartera, tener que ir a cada organización para solicitar identificaciones nuevas.

La problemática entonces, no es el simple hecho de la identificación, si no la posibilidad de extender sus capacidades en cantidad de información, portabilidad, seguridad y generalización y hacer uso de los avances tecnológicos actuales, esto bajo una buena propuesta de infraestructura que permita identificarte en múltiples organizaciones.

En cuanto a seguridad se refiere, es necesario verificar que el portador de la identificación es quien dice ser y para eso, existen diferentes tecnologías que apoyan el mecanismo de autentificación de usuarios tales como certificados digitales, claves de acceso/password, tarjetas inteligentes, tokens de seguridad, biométricos entre otros. En la Fig. 2.1 se muestran estas tecnologías así como su relación con la complejidad de implantación.



Fig. 2.1 Tecnologías que apoyan el mecanismo de autentificación

Y lo malo en ellas, es que individualmente generan problemas de seguridad como:

* La contraseña o PIN pueden ser vulnerables al espionaje mientras son transmitidas a la máquina de autenticación o al usuario.
* Son comúnmente falsificables.
* Robo y clonación de tarjetas inteligentes.
* No autorizan a los individuos, sino a los token.
* No prueba quien es la persona que tiene el token.
* Los biométricos todavía son caros y requieren hardware especializado.

## 2.2 Soluciones existentes

En la Tabla 2.1 mostramos las características generales de algunos sistemas que se utilizan en la actualidad donde se implementa la autentificación e identificación:

|  |  |  |  |
| --- | --- | --- | --- |
| ***Sistema*** | ***Descripción*** | ***Tecnología aplicada*** | ***Aplicaciones*** |
| ***ePass 2000 Token USB***  [54] | Es un dispositivo USB de autenticación de usuarios y portabilidad de certificados digitales, también almacena y genera claves de autenticación dentro del mismo de manera segura. | Basado en la tecnología SmartCard, generando 2 o hasta 3 cofactores para la autenticación de los usuarios apoyado de múltiples algoritmos de seguridad. | * Autenticación de usuarios dentro de una red VPN, SSL VPN y Portales WEB. * Firma de correos electrónicos, Documentos (Word, Excel, imágenes ), PDF. * Uso en áreas gubernamentales. * Transporte de manera segura de documentos críticos. |
| ***Documento Nacional de Identificación Electrónico (DNIe)***  [55] | Es un pequeño Circuito Integrado en una tarjeta, que contiene los datos de filiación de un ciudadano, lo datos biométricos (modelo dactilar, foto y firma) y sus respectivas claves, para así acreditar física y electrónicamente la identidad del titular. | La información contenida en la tarjeta es encriptada mediante el uso de algoritmos RSA, algoritmos de identificación de patrones en impresiones de huellas dactilares y claves Diffie-Hellman. | * Compras firmadas a través de internet * Trámites gubernamentales * Transacciones Interbancarias. * Acceso a edificios de trabajo. |
| ***TokensSecurID***  [56] | Dispositivo de autenticación en forma de tarjeta inteligente, que proveen un proceso fácil y de un solo paso para identificar positivamente a los usuarios de una red, previniendo el acceso de usuarios no autorizados. | La SecurID despliega un número único de 6 dígitos que cambia cada 60 segundos, combinado con un PIN personal del usuario dan como resultado un Passcode de 2 factores, lo que identificará al usuario. | * Protección de líneas telefónicas de acceso conmutadas. * Protección de Host y/o aplicaciones. * Control de acceso a redes LAN, TCP/IP y TACACS * Transacciones bancarias de forma segura. |
| ***DeepnetUnifiedAuthenticationPlatform*** [57] | Es una plataforma de autenticación única que permite gestionar hasta 10 métodos diferentes de autenticación, incluyendo contraseñas de un solo uso (OTP), tokens de seguridad, smartcards y biométrica. | Múltiples tecnologías no patentadas aplicadas a las diferentes aplicaciones que el sistema cuenta. | * Transacciones bancarias. * Identificación de usuarios mediante. telecomunicaciones. * Seguridad interna de redes y controlo de acceso de usuarios. * Control de acceso a zonas restringidas. |
| ***Firma Digital, IMSS*** [58] | Es un archivo con terminación PFX que, asociado con el Número Patronal de Identificación Electrónica permite a las empresas el acceso a los sistemas en Internet del IMSS. | Con el proceso de Certificación Digital cada registro patronal podrá obtener su Número Patronal de Identificación Electrónica y un certificado digital. | * Firmar electrónicamente la información que se quiere enviar al IMSS y sólo puede ser utilizado con una contraseña asociada no difundidle. |

##### 

##### 

##### Tabla 2.1 Descripción de sistemas semejantes

## 2.3 Propuesta de solución

La solución propuesta en este Trabajo Terminal a tal problemática y como mejora de las soluciones existentes, es la creación de una Infraestructura que al integrar diversas tecnologías para la identificación y la autentificación antes mencionadas, permita verificar la identidad y la autenticidad de una persona de manera segura garantizando el no repudio.

Esta Infraestructura de Identificación y Autentificación digital, está compuesta por tres módulos:

* Registro y generación de ID: Como se muestra en la Figura 2.2, en este módulo con la agrupación de información privada, pública y biométrica del usuario, la aplicación de RSA y MD5, la generación de firma digital y certificado digital, se genera una identificación digital única la cual posteriormente es guardada en un dispositivo TOKEN y así, se está lista para ser utilizada.

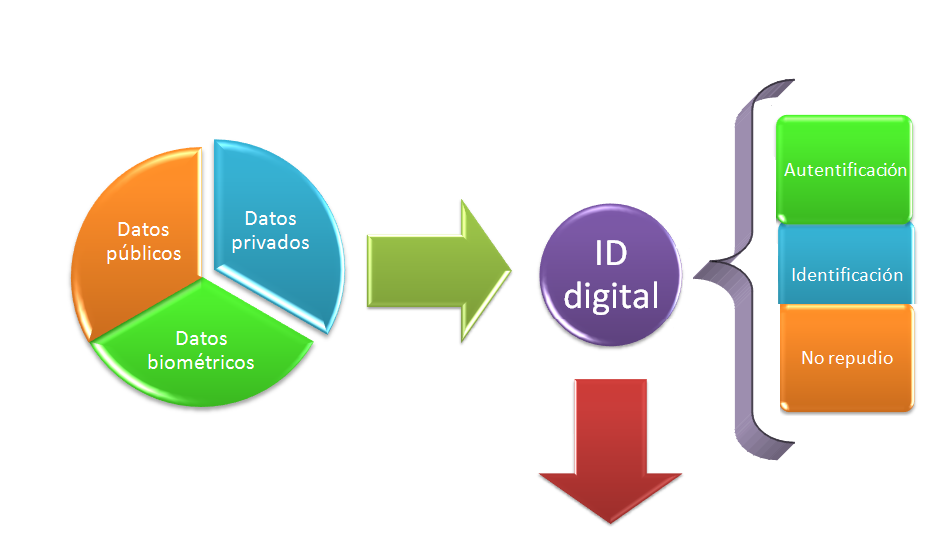


Figura 2.2 Representación de la Infraestructura de Identificación y Autentificación digital.

* Validación: En este módulo se verifica que la persona es quien dice ser al checar que, la información que se contiene en el token no esté modificada, que el certificado aun no caduque, la persona continúe en la base de datos del sistema.
* Administración: Modulo encargado de visualizar los reportes que se generan así como de dar de baja a usuarios que, por robo o extravió perdieron su token. Y de esta manera, pueden volver a realizar su identificación digital, guardarla en otro token y seguir haciendo uso de ella.

Las principales características que se tienen de este Trabajo Terminal son:

* Sencillez: Al eliminar la complejidad de uso de sus interfaces y sea apto para cualquier tipo de usuario.
* Robustibilidad: Considerando el número de variables, contener suficiente información con la seguridad adecuada para evitar la violación de datos, garantizando seguridad recíproca entre el servidor y el usuario.
* Movilidad: Al ser almacenado en cualquier TOKEN, obtiene mayor portabilidad y sencillez.

# Capítulo 3 Análisis

## 3.1 Estudio de Factibilidad

### 3.1.1 Factibilidad Operacional

El sistema ofrece una interfaz amigable y sencilla la cual permite que sea atractivo y fácil de usar para el usuario. Para poder hacer uso, solo basta con seguir el manual de usuario.

De esta forma no es necesario que el usuario tenga amplios conocimientos en el manejo de computadoras.

### 3.1.2 Factibilidad Técnica

* Se utilizan algunas herramientas libres y algunas con licencia comercial de software.
* En cuanto al IDE de desarrollo NetBeans se utilizará la versión 6.8 para Windows.

### 3.1.3 Estudio de Factibilidad Económica

#### Costo de desarrollo

Para la estimación del proyecto, se utilizara la herramienta COCOMO con la métrica Puntos de Función. Los puntos de Función se derivan con una relación empírica según las medidas contables (directas) del dominio de información del software y las evaluaciones de la complejidad del software.[59] Para esta métrica, se determinan cinco características del dominio que son:

* Entradas: Se cuenta cada entrada de usuario que proporciona diferentes datos orientados a la aplicación
* Salidas: Cada salida que proporciona información al usuario orientada a la aplicación, por ejemplo los mensajes de confirmación, de error, informes, etc.
* Peticiones: Entradas interactivas que producen la generación de alguna respuesta del software inmediata en forma de salida interactiva.
* Archivos: Archivos maestros lógicos, como por ejemplo una base de datos.
* Interfaces externas: Interfaces legibles por la máquina, como por ejemplo memorias USB o CD, que se utilizan para transmitir información a otro sistema.

Para nuestro sistema, tenemos los siguientes datos:

1.- Entradas.

* Pantalla Datos Privados
* Pantalla de Datos Públicos
* Pantalla módulo biométrico
* Pantalla Bienvenida de Verificación
* Pantalla Módulo biométrico Pantalla Administrador
* Pantalla Menú del Administrador
* Pantalla Visualizar Reportes
* Pantalla Eliminar usuario

2.- Salidas

* Cuadro de diálogo Error al llenar campos
* Cuadro de diálogo Error al obtener el CURP
* Cuadro de diálogo Verificar información
* Cuadro de diálogo Error en selección de imagen
* Cuadro de diálogo Error de conexión
* Cuadro de diálogo Error al comparar CURP
* Cuadro de diálogo Comparación exitosa
* Cuadro de diálogo Error al crear documentos
* Cuadro de dialogo Error al dar de alta en la BD
* Cuadro de diálogo Error al guardar en Token
* Pantalla Identificación lista
* Cuadro de diálogo Campos vacíos
* Cuadro de diálogo CURP mal escrito
* Cuadro de diálogo Usuario inexistente en la BD
* Seleccionar Token
* Cuadro de diálogo No existe certificado en Token
* Cuadro de diálogo Certificado expirado
* Pantalla Identificación y Autentificación exitosas
* Cuadro de Diálogo Verificación Fallida
* Cuadro de diálogo Solicitud de huella
* Pantalla Error en identificación y autentificación
* Cuadro de diálogo Contraseña inválida
* Cuadro de diálogo Excedió intentos
* Cuadro de diálogo Curp mal escrito
* Cuadro de Diálogo Campo del Curp vacío
* Cuadro de diálogo Usuario no encontrado en BD
* Reporte
* Cuadro de diálogo El usuario no existe en la BD
* Cuadro de diálogo Eliminación exitosa

3.- Peticiones.

* Recepción, procesamiento y manejo de datos.

4.-Archivos.

* Base de datos.
* Registros/Reportes.

5.- Interfaces externas.

* Token USB.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Parámetros de la medición. | Cuenta. | Simple. | Medio. | Complejo. | Total. |
| Número de entradas del usuario. | 8 | \*3 | \*4 | \*6 | 32 |
| Número de salidas del usuario. | 29 | \*4 | \*5 | \*7 | 145 |
| Número de peticiones del usuario. | 1 | \*3 | \*4 | \*6 | 4 |
| Numero de archivos. | 2 | \*7 | \*10 | \*15 | 20 |
| Numero de Interfaces externas. | 1 | \*5 | \*7 | \*10 | 7 |
| Cuenta Total. |  | | | | **208** |

##### *Tabla 3.1Cálculo de la cuenta total.[59]*

Antes de obtener los puntos de función, necesitamos obtener el valor de ajuste de la complejidad, el cual se obtiene sumando las respuestas de 14 preguntas, con un rango de 0 a 5, donde 0 es no importante o aplicable y 5 es absolutamente esencial.

Las 14 preguntas se muestran a continuación con sus respectivas respuestas:

|  |  |
| --- | --- |
| Pregunta | Respuesta |
| 1.- ¿Requiere el sistema copias de seguridad y de recuperación fiables? | 3 |
| 2.- ¿Se requiere comunicación de datos? | 5 |
| 3.- ¿Existen funciones de procesamiento distribuido? | 1 |
| 4.- ¿Es crítico el rendimiento? | 3 |
| 5.- ¿Se ejecuta el sistema en un entorno operativo existente y fuertemente utilizado? | 4 |
| 6.- ¿Requiere el sistema entrada de datos interactiva? | 5 |
| 7.- ¿Requiere la entrada de datos interactiva que las transacciones de entrada se lleven a cabo sobre múltiples pantallas u operaciones? | 3 |
| 8.- ¿Se actualizan los archivos maestros de forma interactiva? | 3 |
| 9.- ¿Son complejas las entradas, las salidas, los archivos o las peticiones? | 4 |
| 10.- ¿Es complejo el procesamiento interno? | 4 |
| 11.- ¿Se ha diseñado el código para ser reutilizable? | 4 |
| 12.- ¿Están incluidas en el diseño la conversión y la instalación? | 3 |
| 13.- ¿Se ha diseñado el sistema para soportar múltiples instalaciones en diferentes organizaciones? | 2 |
| 14.- ¿Se ha diseñado la aplicación para facilitar los cambios y para ser fácilmente utilizada por el usuario? | 5 |
| TOTAL | **49 puntos** |

##### *Tabla 3.2Cálculo del valor de ajuste de la complejidad.*

Para obtener los puntos de función, se ocupa la siguiente fórmula:

*PF = cuenta-total x [0.65 + (0.01 x Fi)] (1)*

Dónde:

*PF* = Puntos de Función

*cuenta-total*= resultado obtenido de la tabla 2.1

*Fi* = resultado obtenido de la tabla 2.2

Por lo tanto al sustituir nuestros datos en la fórmula (1) obtenemos:

*PF =208 \* [0.65+ (0.01\*49)]= 208 \* [0.65 + .49] = 208 \* 1.14 = 237.12*

Ahora, sacamos el equivalente en líneas de código en base a los Puntos de Función, de acuerdo a la siguiente tabla:

|  |  |
| --- | --- |
| Lenguaje o entorno de programación | Líneas de Código/Puntos de Función |
| 4GL | 40 |
| Ada 83 | 71 |
| Ada 95 | 49 |
| APL | 32 |
| BASIC – compilado | 91 |
| BASIC – interpretado | 128 |
| BASIC ANSI/Quick/Turbo | 64 |
| C | 128 |
| C++ | 29 |
| Clipper | 19 |
| Cobol ANSI 85 | 91 |
| Delphi 1 | 29 |
| Ensamblador | 320 |
| Ensamblador ( Macro) | 213 |
| Forth | 64 |
| Fortran 77 | 105 |
| Fox Pro 2.5 | 34 |
| Generador de Informes | 80 |
| Hoja de Cálculo | 6 |
| Java | **53** |
| Modula 2 | 80 |
| Oracle | 40 |
| Oracle 2000 | 23 |
| Paradox | 36 |
| Pascal | 91 |
| Pascal Turbo 5 | 49 |
| Power Builder | 16 |
| Prolog | 64 |
| Visual Basic 3 | 32 |
| Visual C++ | 34 |
| Visual Cobol | 20 |

##### *Tabla 3.3 Equivalencia de los Puntos de Función en Líneas de Código. [60]*

Por lo tanto, tenemos un total de 12567.36 líneas de código, ya que nuestro principal lenguaje de programación será Java.

Ya que tenemos estos datos, emplearemos ahora si el método de COCOMO.

Por un lado COCOMO define tres modos de desarrollo o tipos de proyectos:

* Orgánico: proyectos relativamente sencillos, menores de 50 KDLC líneas de código, en los cuales se tiene experiencia de proyectos similares y se encuentran en entornos estables.
* Semi-acoplado: proyectos intermedios en complejidad y tamaño (menores de 300 KDLC), donde la experiencia en este tipo de proyectos es variable, y las restricciones intermedias.
* Empotrado: proyectos bastantes complejos, en los que apenas se tiene experiencia y se engloban en un entorno de gran innovación técnica. Además se trabaja con unos requisitos muy restrictivos y de gran volatilidad. [61]

Y por otro lado existen diferentes modelos que define COCOMO:

* Modelo básico: Se basa exclusivamente en el tamaño expresado en LDC.
* Modelo intermedio: Además del tamaño del programa incluye un conjunto de medidas subjetivas llamadas conductores de costes.
* Modelo avanzado: Incluye todo lo del modelo intermedio además del impacto de cada conductor de coste en las distintas fases de desarrollo. [61]

Nosotros emplearemos el modelo intermedio, dado que realiza estimaciones con bastante precisión. Las fórmulas a utilizar son las siguientes:

|  |  |
| --- | --- |
| * Cálculo del Esfuerzo de Desarrollo | *E = a KLDC e \* FAE (persona x mes)* |
| * Cálculo de la duración del desarrollo | *T = c Esfuerzo d (meses)* |
| * Cálculo del personal | *P= E/T (personas)* |

Para calcular el esfuerzo, se necesita la variable de *KLDC*, lo cual equivale a kilo-líneas de código, y de acuerdo a nuestros datos, tenemos un total de *12. 56736 Kilo-líneas de código*, por lo cual nuestro tipo de proyecto es orgánico.

Ahora, es momento de obtener la variable FAE, la cual se obtiene de multiplicar los valores evaluados en 15 conductores de coste observados a continuación:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proyecto Software. | a | e | c | d |
| Orgánico. | 3.2 | 1.05 | 2.5 | 0.38 |
| Semi-acoplado. | 3.0 | 1.12 | 2.5 | 0.35 |
| Empotrado. | 2.8 | 1.20 | 2.5 | 0.32 |

##### Tabla 3.4 Coeficientes para los diferentes tipos de proyecto. [61]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Conductores de coste. | VALORACIÓN. | | | | | |
| ***Muy bajo*** | ***Bajo*** | ***Nominal*** | ***Alto*** | ***Muy***  ***alto*** | ***Extra Alto*** |
| Fiabilidad requerida del software | 0.75 | 0.88 | 1.00 | 1.15 | 1.40 | - |
| Tamaño de la base de datos | - | 0.94 | 1.00 | 1.08 | 1.16 | - |
| Complejidad del producto | 0.70 | 0.85 | 1.00 | 1.15 | 1.30 | 1.65 |
| Restricciones del tiempo de ejecución | - | - | 1.00 | 1.11 | 1.30 | 1.66 |
| Restricciones del almacenamiento principal | - | - | 1.00 | 1.06 | 1.21 | 1.56 |
| Volatilidad de la máquina virtual | - | 0.87 | 1.00 | 1.15 | 1.30 | - |
| Tiempo de respuesta del ordenador | - | 0.87 | 1.00 | 1.07 | 1.15 | - |
| Capacidad del analista | 1.46 | 1.19 | 1.00 | 0.86 | 0.71 | - |
| Experiencia en la aplicación | 1.29 | 1.13 | 1.00 | 0.91 | 0.82 | - |
| Capacidad de los programadores | 1.42 | 1.17 | 1.00 | 0.86 | 0.70 | - |
| Experiencia en S.O. utilizado | 1.21 | 1.10 | 1.00 | 0.90 | - | - |
| Experiencia en el lenguaje de programación | 1.14 | 1.07 | 1.00 | 0.95 | - | - |
| Prácticas de programación modernas | 1.24 | 1.10 | 1.00 | 0.91 | 0.82 | - |
| Utilización de herramientas software | 1.24 | 1.10 | 1.00 | 0.91 | 0.83 | - |
| Limitaciones de planificación del proyecto | 1.23 | 1.08 | 1.00 | 1.04 | 1.10 | - |

##### *Tabla 3.5 Elementos necesarios para sacar la FAE. [61]*

Por lo tanto, la FAE es igual a: 1.130.

Finalmente, se hacen los cálculos correspondientes:

Cálculo del esfuerzo del desarrollo:

*E = a KLDC e \* FAE = 3.2 \* (12. 56736) ^1.05 \* 1.130 = 65.0077 personas /mes.*

Cálculo tiempo de desarrollo:

*T = c Esfuerzo d = 2.5 \* (47.71 )^0.38 = 10.85 meses.*

Productividad:

*PR = LDC/Esfuerzo = 12567.36 /65.0077 = 193.32 LDC/personas mes.*

Personal promedio:

*P = E/T = 65.0077 /10.85 = 5.9914 personas.*

Si se toma en cuenta que cada persona-mes cuenta alrededor de $8000, el proyecto tendría un costo de $

|  |  |
| --- | --- |
| Parámetro | Valor |
| Esfuerzo. | 65.0077 persona/mes. |
| Tiempo de desarrollo. | 10.85 meses. |
| Cantidad de hombres. | 5.9914 personas. |
| Costo estimado con COCOMO. | $520053.52 |

##### Tabla 3.6 Estimación con COCOMO.

#### Costo de hardware y licencias

No se utilizó Hardware y se desea que la tecnología a utilizar sea software libre, que además de disminuir los costos nos brinde herramientas que nos permitan cumplir con los requerimientos del Sistema:

Finalmente, el informe detallado de los costos del proyecto se muestra a continuación:

|  |  |
| --- | --- |
| Detalle. | Costo Total. |
| Hardware | $ 500 |
| Desarrollo | $ 520,053.52 |
| Componentes Adicionales | $ 1000 |
| Licencias | $0 |
| Total | **$ 521,553.52** |

##### Tabla 3.7 Costo Total del Proyecto.

### 3.1.4 Estudio de Factibilidad Legal

Licencias de software

El proyecto a desarrollar está basado en software libre por lo que se pretende ahorrar los costos de licenciamiento.

Normatividad legal

Durante el desarrollo del proyecto será indispensable apegarse a las leyes vigentes:

* *LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES Y LOS ARTÍCULOS 3, FRACCIONES II Y VII, Y 33, ASÍ COMO LA DENOMINACIÓN DEL CAPÍTULO II, DEL TÍTULO SEGUNDO, DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL.*
* El artículo 6º en sus fracciones II y III sobre los datos personales y la información relativa a la vida privada.
* Artículo 16 Constitucional.

## 3.2 Análisis de requerimientos

### 3.2.1 Requerimientos No Funcionales

Los requerimientos no funcionales hacen relación a las características del sistema que aplican de manera general como un todo, más que a rasgos particulares del mismo. Estos requerimientos son adicionales a los requerimientos funcionales que debe cumplir el sistema, y corresponden a aspectos tales como:

#### Atributos de Calidad del Sistema.

Desempeño:

El sistema deberá ofrecer un tiempo de respuesta considerable en verificación y validación de información.

Escalabilidad:

El sistema debe ser construido sobre el modelo en RUP, permitiendo con cada revisión, que se puedan agregar nuevas funcionalidades de modo que afecten lo menos posible al código.

Al mismo tiempo debe tener la capacidad de que el sistema se expanda en un futuro, para que puedan agregársele o actualizarse funcionalidades.

Facilidad de uso:

El uso del sistema debe ser simple y sencillo, sin embargo también estará especificado en el manual de usuario para que no existan problemas mayores.

El sistema, en caso de error debe mostrar un mensaje, para poder saber que fue lo que ocasionó la falla.

Facilidad para las Pruebas:

El sistema debe contar con la facilidad para identificar y localizar los errores durante la etapa de pruebas.

Mantenibilidad:

El sistema deberá ser fácil de mantener, para esto tendrá que estar adecuadamente documentado, para que sea entendible para quienes se encarguen de esta etapa.

Validación de Información:

El sistema debe validar automáticamente el tipo de datos introducidos en los formularios para evitar introducir datos de tipo incorrecto a la base de datos.

### 3.2.2 Requerimientos Funcionales

Propósito del análisis de requerimientos

Los requisitos funcionales permiten mantener declaraciones explícitas de lo que el sistema no debe hacer. Además describir la funcionalidad o los servicios que se espera que éste provea, dependiendo totalmente del tipo de software y del sistema que se desarrolle.

Para el desarrollador de sistemas esta información le permite dar interpretaciones de un requerimiento ambiguo con el fin de simplificar su implementación. Sin embargo, a menudo no es lo que el cliente desea y por lo tanto se tienen que estipular nuevos requerimientos y se deben hacer cambios al sistema, retrasando la entrega de éste e incrementando el costo.

En principio, la especificación de requerimientos funcionales de un sistema debe estar completa y ser consistente. La consistencia significa que los requerimientos no tienen definiciones contradictorias.

Seguridad en el manejo de información

Los administradores solo podrán acceder a consultar reportes o eliminar la cuenta de los usuarios, solo si se encuentra un registro previo en la base de datos y si el usuario permite el acceso.

Restricciones de los usuarios

El administrador podrá acceder a la información contenida en la base de datos de usuarios para realizar: consulta de reportes, y bajas de usuarios.

El usuario no podrá modificar sus datos una vez verificados y almacenados.

#### Requerimientos funcionales del Proyecto

Administración de usuario.

* El sistema permitirá dar de alta a un nuevo usuario.
* El sistema permitirá dar de baja a un usuario.

Modificación de información de usuario.

* El sistema no permitirá modificar información del usuario.

Selección de usuario.

* El sistema debe permitir al administrador seleccionar de un registro al usuario que desea dar de baja del sistema
* El sistema debe permitir al administrador acceder a los reportes generados por determinado usuario, cuando se le solicite.

Creación de Identificación.

* El usuario puede introducir datos privados.
* El usuario puede subir la imagen de su CURP.
* El usuario puede identificarse mediante su información biométrica.

# Capítulo 4 Diseño

## 4.1 Diagrama de Casos de Uso

La figura 4.1 muestra los procesos principales del sistema a través de los casos de uso y los actores a quienes sirven.

### 4.1.1 Definición de actores del sistema.

Usuario

Este actor representa a la persona que desea generar su identificación digital.

Instancia externa de verificación

Este actor representa al sitio web al que se le solicitará información para validar el documento público (CURP). <http://consultas.curp.gob.mx/>.

*Instancia externa OCR*

Actor que representa al sitio web de donde se obtienen los caracteres del documento público por el reconocimiento óptico de caracteres. <http://www.newocr.com/>

Módulo biométrico

Este actor representa al sistema de reconocimiento de huella dactilar que proporciona datos biométricos al sistema.

Sistema verificador

Este actor representa al proveedor de servicios, al que el usuario le hace una petición que requiera del uso de la identificación previamente almacenada en el Token.

BD Sistema

Representa a la base de datos en donde se guarda información relacionada con los usuarios, administradores y reportes de acciones.

Administrador

Este actor representa a la persona que puede consultar los reportes de acciones y eliminar cuentas de usuario.

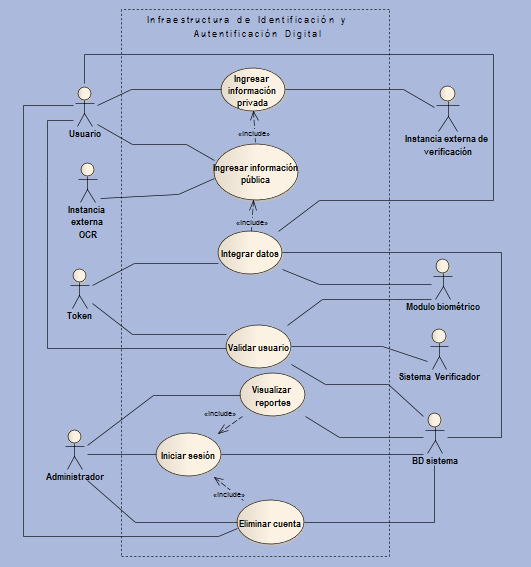


Fig. 4.1 Diagrama de casos de uso de la Infraestructura de identificación y autentificación digital.

### 4.1.2 Descripciones detalladas de cada Casos de Uso

|  |  |  |
| --- | --- | --- |
| **INGRESAR INFORMACIÓN PRIVADA** | | |
| **Versión** | 1.0 | |
| **Actores** | Usuario, Instancias externa de verificación | |
| **Descripción** | En este caso de uso, el usuario captura en el formulario del sistema sus datos privados como nombre, fecha de nacimiento, domicilio, entre otros, y se verifica el formulario.  En seguida, se verifica si la información privada capturada por el usuario corresponde a algún documento oficial de la instancia externa de verificación <http://consultas.curp.gob.mx/> y se extrae el CURP del documento que regresa. | |
| **Flujo** | **Paso** | **Acción** |
| 1 | Usuario llena formulario de información privada. |
| 2 | El sistema verifica formulario. |
| 3 | Se manda la información del usuario a la instancia externa y se verifica su existencia. |
| 4 | Se extrae el CURP de la instancia externa. |
| **Excepciones** | **Paso** | **Acción** |
| 2.1 | Si existen datos inválidos en el formulario, se le avisa al usuario para que modifique o inserte de nuevo los datos. |
| 2.2 | Si existen campos que no contengan información, se le avisa al usuario para que llene tales campos. |
| 3.1 | El internet del usuario sea lento o se encuentre sin conexión. Esto se avisa al usuario pidiéndolo que verifique su conexión. |
| 4.1 | Si no existe la información proporcionada por el usuario en la instancia externa, se le avisa al usuario para que lo intente de nuevo. |

##### *Tabla 4.1.2.1 Descripción de Caso de uso ingresar información privada*

|  |  |  |
| --- | --- | --- |
| **INGRESAR INFORMACIÓN PÚBLICA** | | |
| **Versión** | 1.0 | |
| **Actores** | Usuario, Instancia externa OCR. | |
| **Descripción** | En este caso de uso, el usuario escanea la imagen de su CURP y sube al sistema tal imagen, la cual manda a la instancia externa <http://www.newocr.com/> quien por medio de OCR (Reconocimiento Óptico de caracteres), obtienen los 18 caracteres que integran el CURP.  Después se compara tal CURP con el obtenido de la instancia externa de verificación en el caso de uso ingresar información privada. | |
| **Flujo** | **Paso** | **Acción** |
| 1 | El usuario sube al sistema su imagen previamente escaneada. |
| 2 | Se obtienen los caracteres que conforman la imagen con la Instancia externa OCR. |
| 3 | Se extraen únicamente los 18 dígitos que conforman el CURP. |
| 4 | Se verifica si los dígitos corresponden con el formato del CURP. |
| 5 | Se compara tal CURP con el obtenido de la Instancias externa de verificación. |
| **Excepciones** | **Paso** | **Acción** |
| 2.1 | No se encuentran caracteres del CURP. En este caso, se le avisa al usuario para que cambie la imagen. |
| 3.1 | El internet del usuario sea lento o se encuentre sin conexión. Esto se avisa al usuario pidiéndolo que verifique su conexión. |
| 4.1 | No corresponden al formato, se realizan cambios como el “0” por la “O” el 1 con la “L” y viceversa. |
| 5.1 | No coincida la comparación de CURPs, en este caso se pide al usuario que introduzca una imagen nueva de su CURP y se regresa al paso uno de este caso de uso. |

##### *Tabla 4.1.2.2 Descripción de Caso de uso ingresar información pública*

|  |  |  |
| --- | --- | --- |
| **INTEGRAR DATOS** | | |
| **Versión** | 1.0 | |
| **Actores** | Módulo Biométrico, BD Sistema, Token, Usuario. | |
| **Descripción** | En este caso de uso se generará la identificación, se cifrara, se crearan los certificados y las firmas digitales y se dará de alta al usuario en la base de datos del sistema. | |
| **Flujo** | **Paso** | **Acción** |
| 1 | Obtener texto plano del módulo biométrico. |
| 2 | Crear certificado digital y firma digital. |
| 3 | Aplicar hash al texto plano. |
| 4 | Cifrar texto plano. |
| 5 | El usuario introduce su Token y lo selecciona en el sistema. |
| 6 | Guardar en Token, llave privada, texto plano cifrado, firma digital y certificado digital. |
| 7 | Dar de alta al usuario en BD del sistema integrando información personal, firma digital y hash. |
| 8 | Genera reporte y almacenarlo en la BD Sistema. |
| **Excepciones** | **Paso** | **Acción** |
| 7.1 | Que exista un registro con esta información en la BD del sistema. |

##### *Tabla 4.1.2.3 Descripción de Caso de uso integrar datos*

|  |  |  |
| --- | --- | --- |
| **VALIDAR USUARIO** | | |
| **Versión** | 1.0 | |
| **Actores** | Sistema verificador, BD Sistema, Usuario, Token. | |
| **Descripción** | Este caso de uso es el que nos permite dar un ejemplo de cómo se usaría la identificación que genera nuestro sistema. El sistema verificador solicita que el usuario se identifique con su Token, CURP y contraseña, se verifica la existencia del registro de la BD de Sistema, se verifica la firma digital así como el certificado digital, se descifra, se verifica el checksum del hash (MD5) , confirmando la autentificación del usuario.  Finalmente se generará un reporte de acceso. | |
| **Flujo** | **Paso** | **Acción** |
| 1 | Usuario solicita a Sistema Verificador ser identificado |
| 2 | Sistema Verificador solicita a usuario identificación. |
| 3 | Usuario introduce su CURP, contraseña y ruta de Token. |
| 3 | Se verifica en la BD Sistema si aún existe el registro. |
| 4 | Se verifica el certificado digital y la firma digital. |
| 5 | Se regresa el resultado de la identificación y autentificación. |
| 6 | Se genera reporte de acceso y se almacena en la BD sistema. |
| **Excepciones** | **Paso** | **Acción** |
| 3.1 | Si no se encuentra el usuario en la base de datos de sistema, se manda un mensaje de error de que el usuario no existe por lo que no podrá autenticarse. |
| 4.1 | En el caso de no encontrar los archivos dentro del Token, se manda un mensaje de error y no podrá autenticarse. |
| 5.1 | En caso de ser falsa la identificación, se abre el modulo biométrico y se pide al usuario introducir tal información. Se descifra la información biométrica del Token, y se compara con la actual. Si no coincide, se manda un mensaje de error y no podrá autenticarse el usuario. |

##### *Tabla 4.1.2.4 Descripción de Caso de uso validar usuario*

|  |  |  |
| --- | --- | --- |
| **INICIAR SESIÓN** | | |
| **Versión** | 1.0 | |
| **Actores** | Administrador , BD Sistema | |
| **Descripción** | En este caso de uso se realizará la verificación del administrador. | |
| **Flujo** | **Paso** | **Acción** |
| 1 | El administrador introduce su contraseña y se verifica en la BD Sistema. |
| **Excepciones** | **Paso** | **Acción** |
| 1.1 | Si no coincide la contraseña 3 veces seguidas, se cierra automáticamente la infraestructura. |

##### *Tabla 4.1.2.5 Descripción de Caso de uso iniciar sesión.*

|  |  |  |
| --- | --- | --- |
| **VISUALIZAR REPORTES** | | |
| **Versión** | 1.0 | |
| **Actores** | Administrador , BD Sistema | |
| **Descripción** | En este caso de uso se realizará la visualización de reportes de los usuarios. | |
| **Flujo** | **Paso** | **Acción** |
| 1 | El administrador introduce el CURP del usuario. |
| 2 | Sistema verifica la existencia del usuario en la base de datos de sistema. |
| 3 | El sistema hace la solicitud de los reportes que necesita el administrador. |
| 4 | Se le muestran los reportes al administrador. |
| **Excepciones** | **Paso** | **Acción** |
| 1.1 | Si el CURP que introduce el administrador tiene longitud diferente a 18, se le manda un mensaje de error para que lo intente de nuevo. |
| 2.1 | Si no se encuentra el registro se manda mensaje de error al administrador. |

##### *Tabla 4.1.2.6 Descripción de Caso de uso visualizar reportes*

|  |  |  |
| --- | --- | --- |
| **ELIMINAR CUENTA** | | |
| **Versión** | 1.0 | |
| **Actores** | Administrador , BD Sistema | |
| **Descripción** | En este caso de uso el administrador, podrá dar de baja a usuarios del sistema, esto con el fin de que si al usuario se le llegara a extraviar su Token, solo llama al administrador para que este lo elimine del Sistema. | |
| **Flujo de datos** | **Paso** | **Acción** |
| 1 | El administrador introduce el CURP del usuario. |
| 2 | Sistema verifica la existencia del usuario en la base de datos de sistema. |
| 3 | El sistema hace la solicitud eliminar usuario y se elimina. |
| 4 | Se avisa al administrador que fue eliminada la cuenta. |
| **Excepciones** | **Paso** | **Acción** |
| 1.1 | Si el CURP que introduce el administrador tiene longitud diferente a 18, se le manda un mensaje de error para que lo intente de nuevo. |
| 2.1 | Si no existe el registro, se termina con el proceso pues ya fue eliminada anteriormente y se avisa al administrador. |

##### *Tabla 4.1.2.7 Descripción de Caso de uso eliminar cuenta*

## 4.2 Diagramas de secuencia

En un diagrama de secuencia se describen las interacciones entre un grupo de objetos mostrando de forma secuencial los envíos de mensajes entre objetos. [62] Realizamos un diagrama de secuencia por caso de uso.

4.2.1Diagrama de secuencia Ingresar información privada

El usuario captura su información privada (datos personales) en el módulo privado donde se hace una validación del formulario para verificar que los datos estén escritos correctamente, de caso contrario se notifica al usuario. Después el módulo privado manda la información del usuario a la instancia externa y se verifica su existencia regresando el documento CURP del usuario del que se extraen los 18 caracteres que conforman el CURP, y se muestra al usuario su información para que valide si corresponde a su información.

##### 

Fig. 4.2.1 Diagrama de secuencia Ingresar información privada.

4.2.2 Diagrama de secuencia Ingresar información pública

El usuario sube su información pública al módulo público después se manda tal imagen a la instancia externa OCR de donde se obtienen los caracteres de la imagen y se regresan al módulo público en donde se extraen únicamente los 18 dígitos que conforman el CURP, y se verifica si los dígitos corresponden con el formato del CURP.

Finalmente, se compara tal CURP con el obtenido de la Instancias externa de verificación.

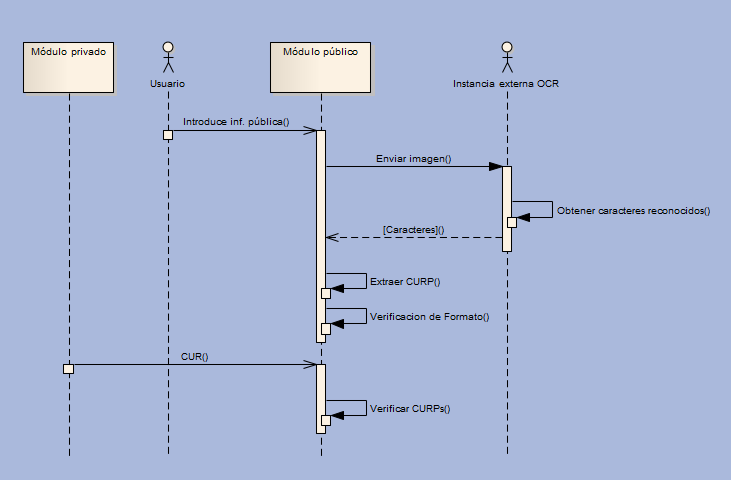


Fig. 4.2.2Diagrama de secuencia Ingresar información pública.

4.2.3 Diagrama de secuencia Integrar datos

El usuario introduce su información biométrica al módulo biométrico y este manda al módulo integrar datos, un texto plano, después, se generan después el certificado digital y firma digital. Se aplica el método hash al texto plano del biométrico y después se cifra con RSA el mismo texto plano.

El usuario introduce su Token y lo selecciona para guardar en el la llave privada, texto plano cifrado, firma digital y certificado digital.

Posteriormente se da de alta al usuario en la base de datos del sistema guardando firma digital, hash e información personal.

Por último se genera un reporte y es guardado en la BD.

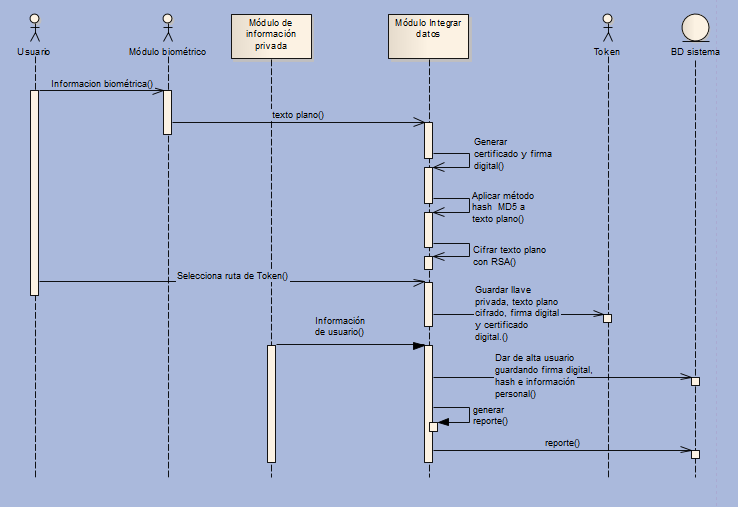


Fig. 4.2.3 Diagrama de secuencia Integrar datos.

4.2.4 Diagrama de secuencia Validar usuario

El usuario solicita un servicio, la instancia proveedora de servicios (sistema verificador) le solicita verificar su identidad, por lo que el usuario introduce su CURP y contraseña al igual que su Token, usuario y contraseña. Se consulta en la base de datos si existe el registro. Se verifican el certificado y la firma digital con cosas como fecha de caducidad hablando del certificado así como de que existan en el Token. Se envía al sistema verificador el resultado de la identificación y autentificación del usuario. Finalmente se genera un reporte de acceso y lo almacena en la base de datos del sistema. En caso contrario, realiza el descifrado del texto plano del Token y solicita al usuario su información biométrica para realizar una validación entre ellas y regresar al sistema verificador una respuesta de autentificación.

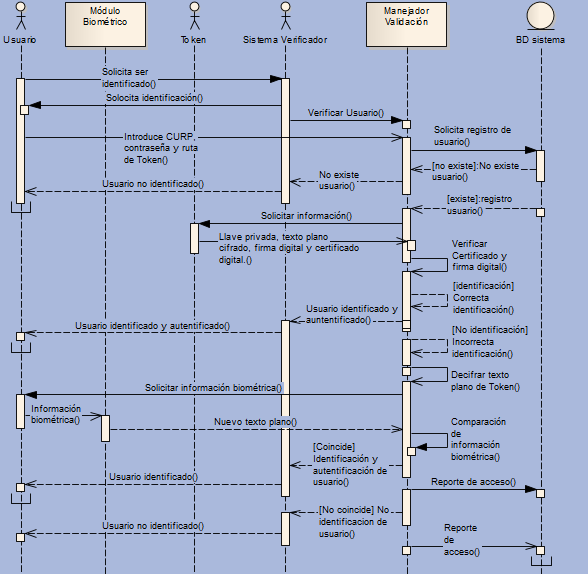


Fig. 4.2.4 Diagrama de secuencia Validar usuario

4.2.5 Diagrama de secuencia Iniciar sesión

El administrador para poder acceder a la infraestructura, introduce su contraseña y esta se verifica en la BD Sistema.

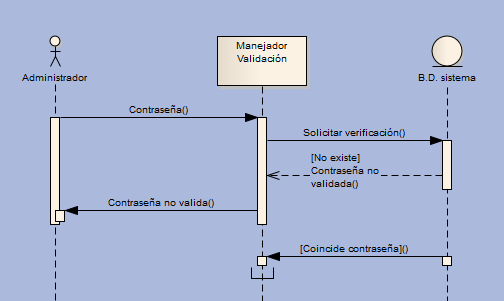


Fig. 4.2.5 Diagrama de secuencia Iniciar sesión

4.2.6 Diagrama de secuencia Visualizar reportes

El administrador introduce el CURP del usuario y se verifica que se contengan 18 caracteres. Se verifica la existencia del usuario en la base de datos de sistema y se hace la solicitud de visualizar los reportes del usuario y se le muestran los reportes al administrador.

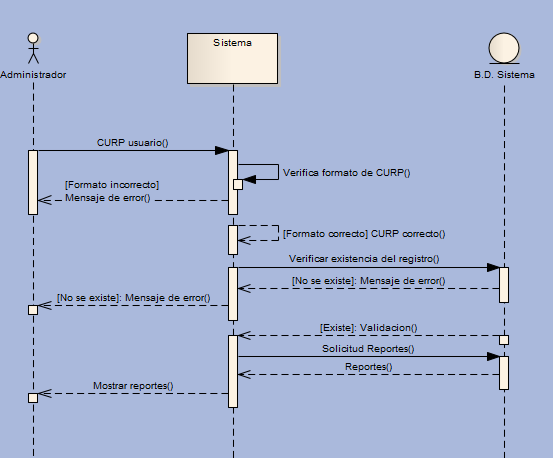


Fig. 4.2.6 Diagrama de secuencia Visualizar reportes

4.2.7 Diagrama de secuencia Eliminar cuenta

El administrador introduce el CURP del usuario y se verifica que se contengan 18 caracteres. Se verifica la existencia del usuario en la base de datos de sistema y se hace la solicitud de eliminar cuenta de usuario, se elimina y se notifica que fue eliminada.

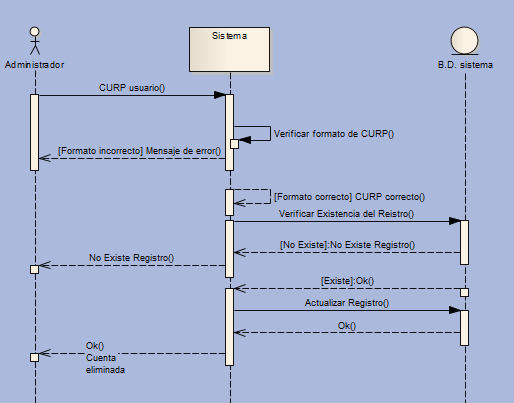


Fig. 4.2.7 Diagrama de secuencia Eliminar cuenta

## 4.3 Diagrama de actividades

Los diagramas de actividades muestran el flujo de trabajo desde el punto de inicio hasta el punto final detallando muchas de las rutas de decisiones que existen en el progreso de eventos contenidos en la actividad. Estos también pueden usarse para detallar situaciones donde el proceso paralelo puede ocurrir en la ejecución de algunas actividades. [63].

### 4.3.1 Diagrama de actividades Primer Módulo

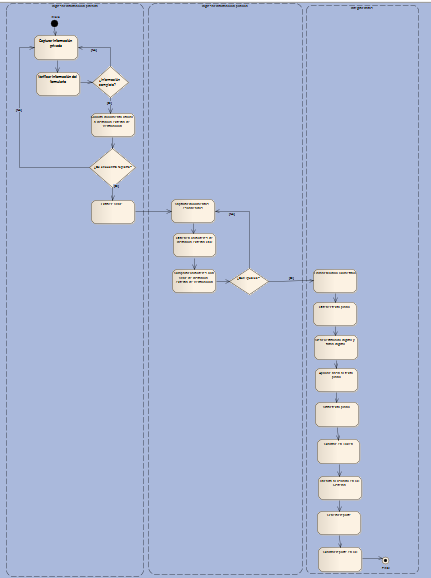


Fig. 4.3.1 Diagrama de actividades general Primer Módulo

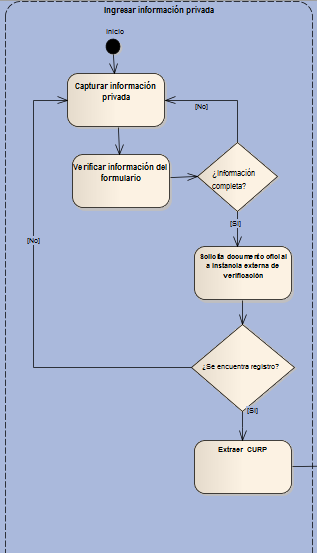
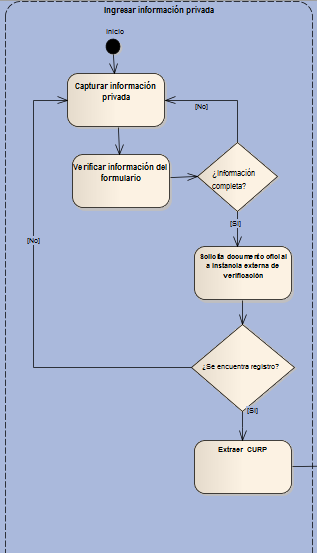
4.3.1.1 Zoom del diagrama de actividades Primer Módulo-Ingresar información privada. 

Fig. 4.3.1.1 Zoom del diagrama de actividades Primer Módulo-Ingresar información privada.

4.3.1.2 Zoom del diagrama de actividades Primer Módulo-Ingresar información pública.

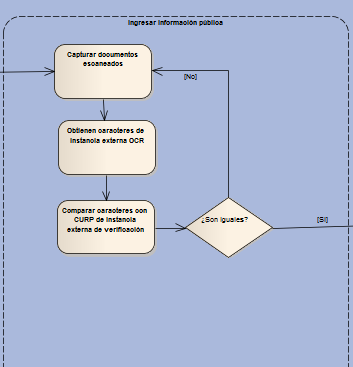


Fig. 4.3.1.2 Zoom del diagrama de actividades Primer Módulo-Ingresar información pública.

4.3.1.3 Zoom del diagrama de actividades Primer Módulo-Integrar datos

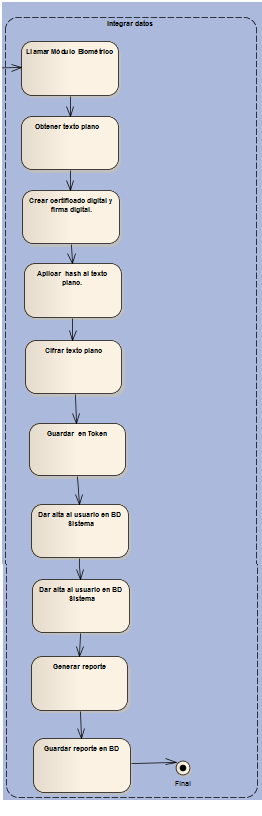


Fig. 4.3.1.3 Zoom del diagrama de actividades Primer Módulo-Integrar datos

### 4.3.2 Diagrama de actividades Segundo Módulo

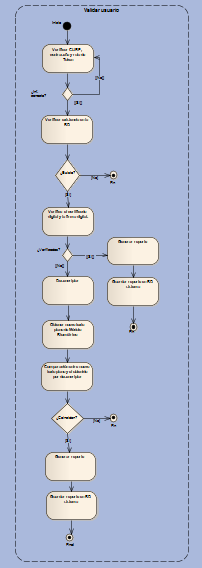


Fig. 4.3.1 Diagrama de actividades Segundo Módulo

4.3.2.1 Zoom del diagrama de actividades Segundo Módulo Parte de arriba

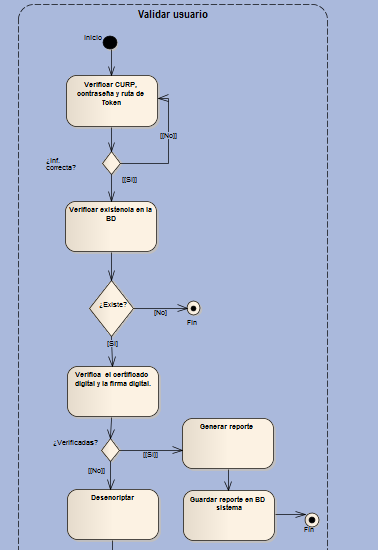


Fig. 4.3.2.1 Zoom del diagrama de actividades Segundo Módulo arriba

4.3.2.2 Zoom del diagrama de actividades Segundo Módulo parte de abajo

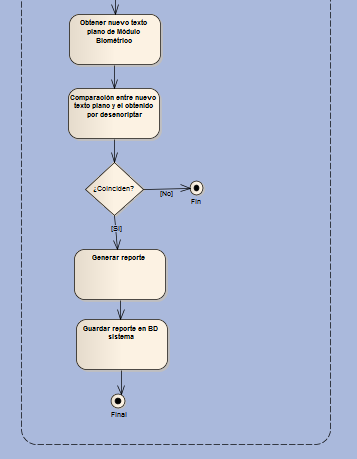


Fig. 4.3.2.2 Zoom del diagrama de actividades Segundo Módulo abajo

### 4.3.3 Diagrama de actividades Tercer Módulo

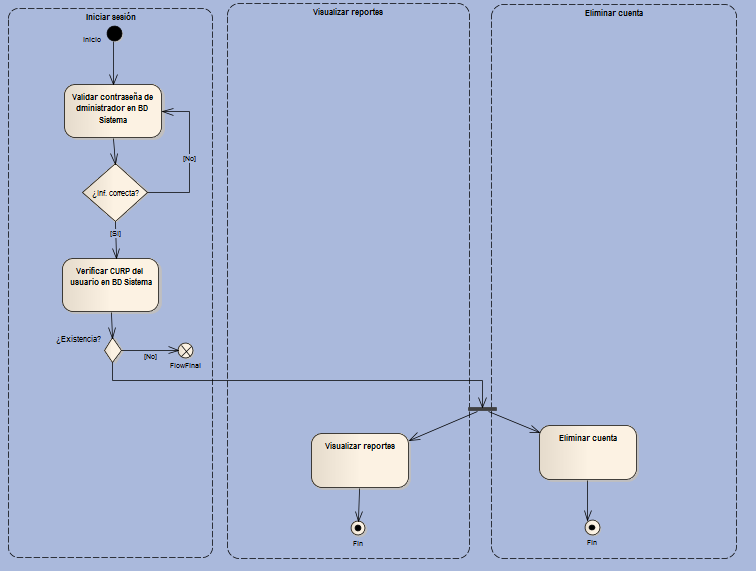


Fig. 4.3.1 Diagrama de actividades Tercer Módulo

## 4.4 Diagrama de clases

## 

Fig. 4.4.1 Diagrama de clases del Módulo de registro y generación de ID

## 

Fig. 4.4.2 Diagrama de clases del Módulo de Validación

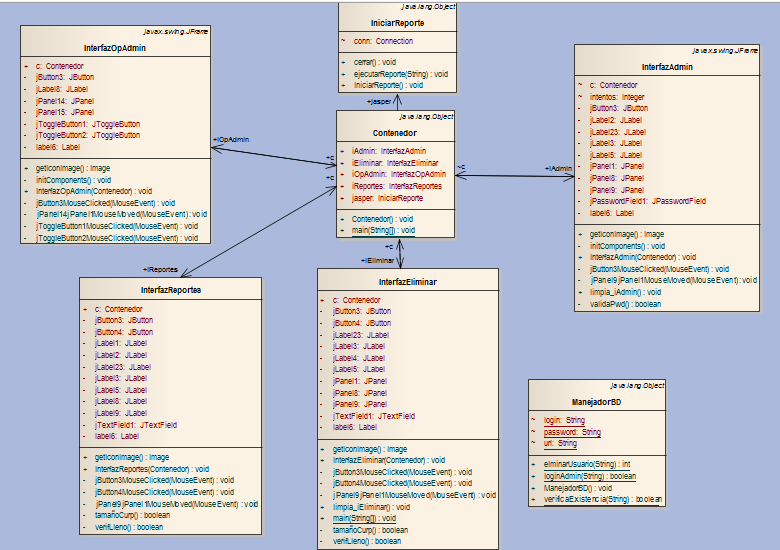


Fig. 4.4.3 Diagrama de clases del Módulo de Administrador

## 4.5 Modelado de Base de Datos

El modelo entidad-relación es el modelo conceptual más utilizado para el diseño conceptual de bases de datos. El objetivo del diseño conceptual es describir el contenido de información de la base de datos y no las estructuras de almacenamiento que se necesitarán para manejar esta información. En la figura siguiente se muestra el diagrama entidad-relación de la base de datos requerida para el proyecto.

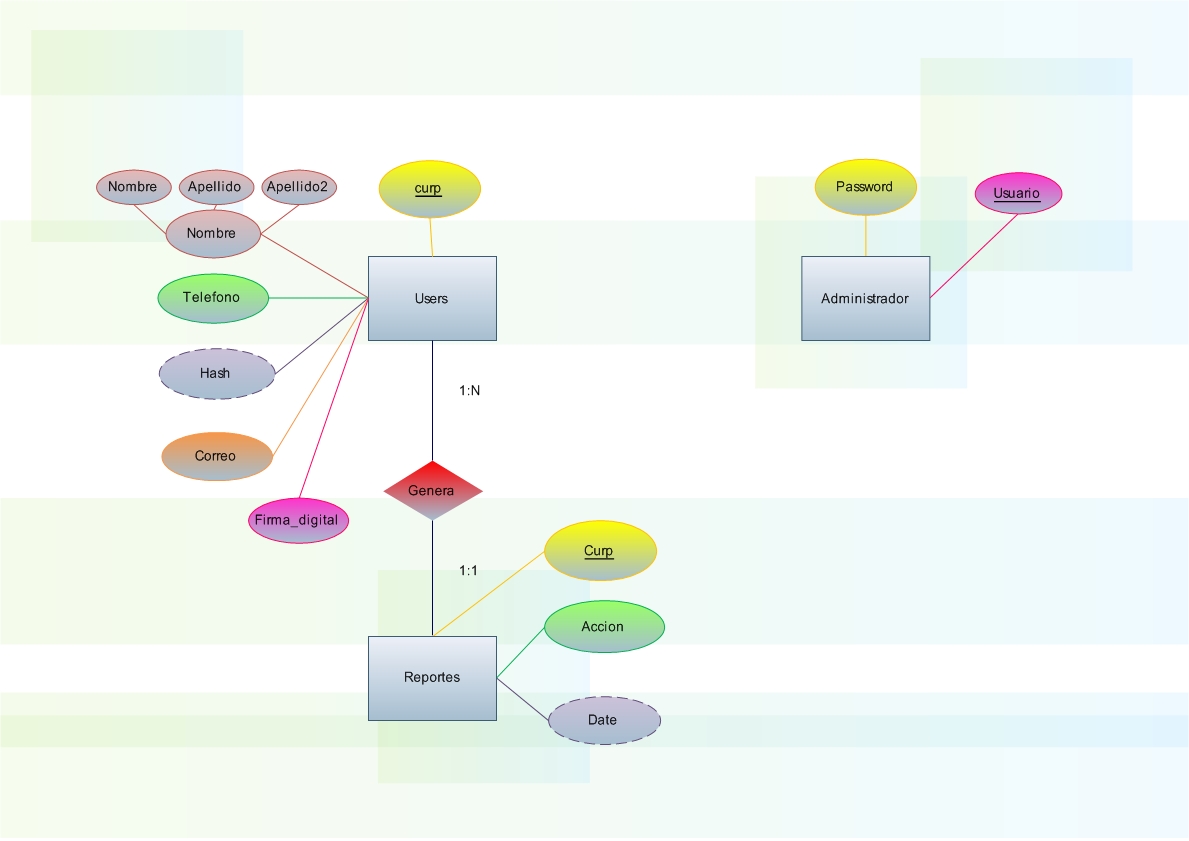


Fig. 4.5.1 Diagrama Entidad-Relación de la BD

El diseño lógico parte del esquema conceptual y da como resultado un esquema lógico. Un esquema lógico es una descripción de la estructura de la base de datos en términos de las estructuras de datos que puede procesar un tipo de SGBD.

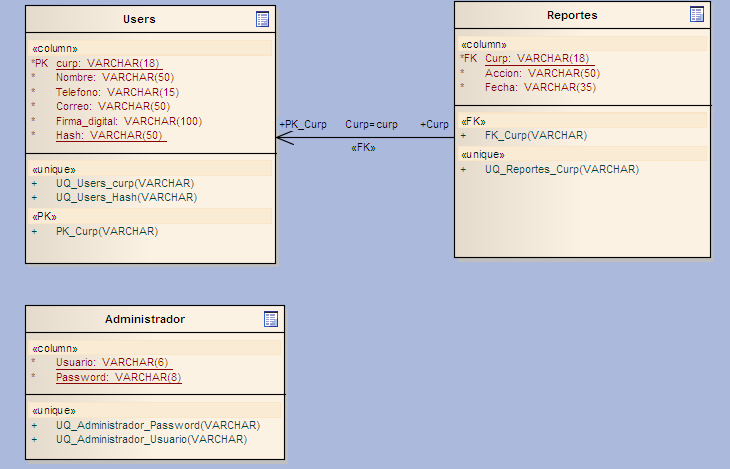


Fig. 4.5.2Diagrama lógico de la BD

# Capítulo 5 Desarrollo

La infraestructura de Identificación y Autentificación Digital pretende reunir varios datos de una persona con el fin de crear un ID digital que permita al usuario identificarse, autentificarse y garantice el no repudio al momento de realizar cierta operación.

Para el desarrollo de la infraestructura el IDE NetBeans nos permitió crear una interfaz gráfica de usuario (GUI) de forma sencilla al contar con sus dos modos de vista diseño y código fuente. En el modo de vista de diseño permite arrastrar y soltar los diversos componentes con los que cuenta, y en el modo vista de código fuente podemos ver el código creado y agregar funcionalidad con código propio. La interfaz tiene como principal característica la sencillez de uso de manera que el usuario logre crear su ID digital de forma amigable, rápida y sin dificultades.

Está dividida en 3 módulos, de acuerdo al tipo de usuario que desee utilizarla:

* *Módulo de registro y generación de ID*. Enfocado a cualquier persona que desee crear su identificación digital.
* *Módulo de Validación. E*ste módulo se podrá colocar en cualquier lugar donde se requiera de la identificación de un usuario.
* *Módulo de Administrador.* Para uso exclusivo del administrador de la infraestructura, podrá visualizar reportes y eliminar cuentas de usuarios.

## 5.1 Módulo de registro y generación de ID

Este primer módulo permite al usuario crear por única vez su ID digital el cual se irá creando con la información del usuario obtenida paso a paso. Para un mejor entendimiento se describirá a continuación todo el proceso de creación mostrando las pantallas del Módulo en orden de aparición.

Para iniciar se muestra una pantalla de Bienvenida con un botón para pasar a la siguiente pantalla.



Fig. 5.1 Pantalla de Bienvenida del Módulo de registro y creación de ID digital

La siguiente pantalla es un formulario que el usuario debe llenar con sus datos privados.



Fig. 5.2 Pantalla Datos Privados

Al dar clic en el botón de Verificar se validará que los datos estén escritos correctamente en caso contrario aparecerá un cuadro de diálogo que le indique al usuario que campo no es correcto.

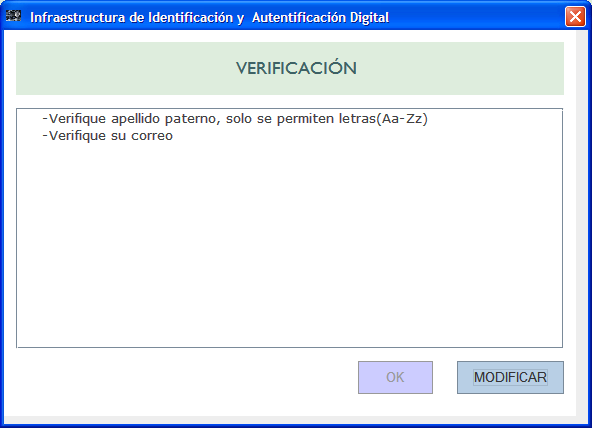


Fig. 5.3 Cuadro de diálogo Error al llenar campos

Una vez que todos los datos estén correctos utilizamos el Web Service de la página http://consultas.curp.gob.mx que hace una consulta de curp para poder utilizarlo necesitamos hacer una petición al servidor con los datos nombre, apellido paterno, apellido materno, sexo, fecha de nacimiento y entidad federativa de nacimiento pedidos en el formulario para realizar dicha petición utilizamos la clase URLConnection la cual crea un vínculo (petición/respuesta) entre la computadora que cuenta con la aplicación y el servidor.

Para poder realizar la (petición/respuesta) se siguen los siguientes pasos [64]:

1. Crear una URL.

La forma más sencilla para crear un objeto URL es con una cadena que representa la dirección URL como la vemos en las páginas. En este caso es la dirección URL a la que deseamos hacer la petición.

*String request = "http://consultas.curp.gob.mx/CurpSP/curp1.do;jsessionid=850fe715a70bc1df0b3eb02f210f0411a5f59cdcb9c06f111a277f76f49279de.e3qMaNqRax0Me3uTa3qKaxmQb41ynknvrkLOlQzNp65In0";*

*URL url = new URL(request);*

La dirección del objeto URL creado anterior representa una dirección URL absoluta.

1. Crear el objeto URLConnection y establecer la conexión para que se pueda escribir en él.

La clase abstracta URLConnection es una superclase y una URL. Las instancias de esta clase se pueden utilizar tanto para leer y escribir en el recurso referenciado por la dirección [65].

El objeto de conexión se crea mediante la invocación del método de la URL openConnection( ).

*URLConnection conn = url.openConnection();*

Una conexión URL se puede utilizar para entrada y / o salida. Al cambiar el valor del parámetro doOutput a true indicamos que la aplicación tiene la intención de escribir datos en la conexión a la URL. Como el valor predeterminado de este campo es false se debe modificar el parámetro de configuración mediante el método setDoOutput.

*conn.setDoOutput(true);*

1. Obtener un flujo de salida de la conexión.

El programa crea un flujo de salida en la conexión y se abre un OutputStreamWriter en ella.

*OutputStreamWriter wr = new OutputStreamWriter(conn.getOutputStream());*

1. Escribir la secuencia de salida.

Debemos escribir los datos necesarios para la secuencia de salida.

*wr.write(datos);*

*wr.flush();*

Los datos escritos en el stream de salida en el lado del cliente son la entrada para el servlet en el servidor. Con el método flush() vaciamos el flujo de salida.

1. Obtener flujo de entrada de la conexión.

El servlet lee la información escrita en este caso los datos del usuario, realiza la consulta del curp y nos devuelve cierta información. Ahora lo que debemos hacer es leer esa cadena que ha enviado el servidor con la respuesta, para esto debemos crear un flujo de entrada y obtenerlo de la conexión con el método getInputStream().

*BufferedReader rd = new BufferedReader(new InputStreamReader(conn.getInputStream()));*

1. Leer la secuencia de entrada.

*String line = rd.readLine()*

1. Cerrar el flujo de salida.

Una vez finalizado el proceso de escritura se debe cerrar el flujo se salida con el método close(), liberando así el recurso.

*wr.close();*

1. Cerrar el flujo de entrada

De la misma manera debe ser cerrado el flujo de entrada.

*rd.close();*



Fig. 5.4Fragmento de código para obtener curp parte 1



Fig. 5.5 Fragmento de código para obtener curp parte 2

En caso de que la conexión a internet falle o no se encuentre el curp del usuario se le informa al usuario y se le da la oportunidad de corregir sus datos.

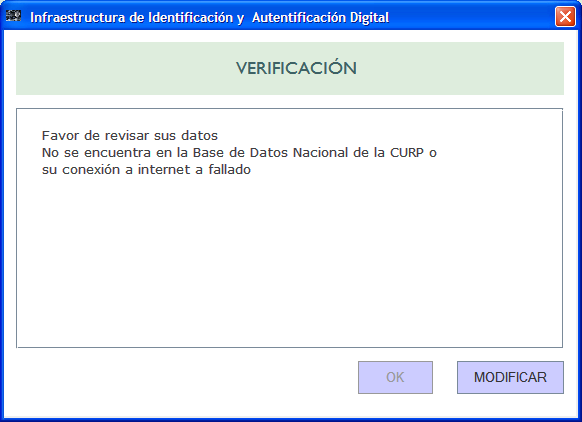


Fig. 5.6 Cuadro de diálogo Error al obtener el Curp

Si la petición se realizó correctamente y el curp fue obtenido del Web Service se le muestra un cuadro de diálogo para que verifique sus datos, el usuario podrá modificar algún dato o continuar con el proceso.



Fig. 5.7 Cuadro de diálogo Verificar información

Si el usuario dio clic en Ok continuará con el proceso y visualizará la siguiente pantalla.

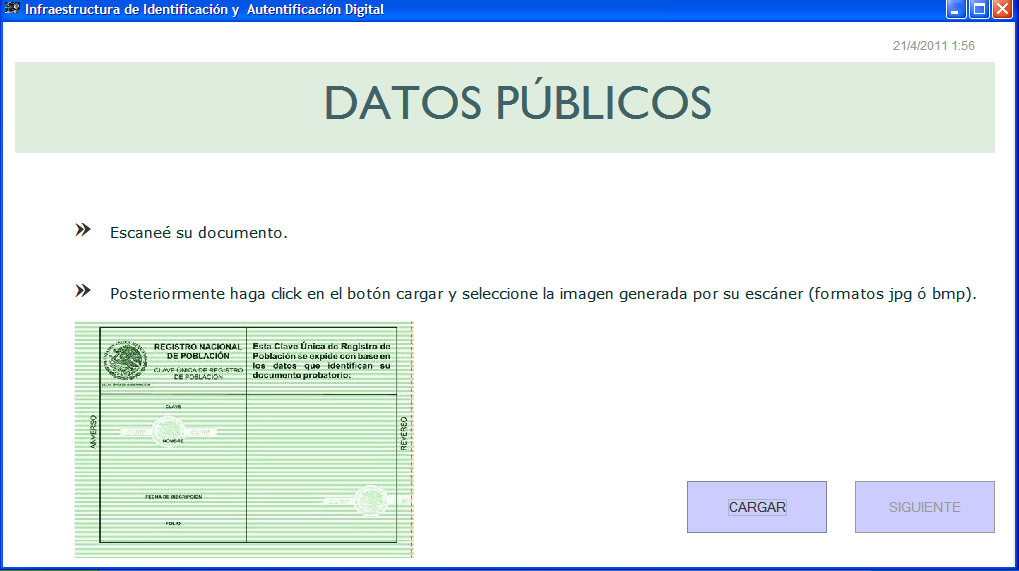


Fig. 5.8 Pantalla de Datos Públicos

En esta parte se le pedirá al usuario que escanee su curp y lo guarde de preferencia en un formato .jpg. Al dar clic en el botón Cargar podrá elegir la imagen de su curp para posteriormente utilizar el Web Service de Reconocimiento Óptico de Caracteres OCR http://www.newocr.com

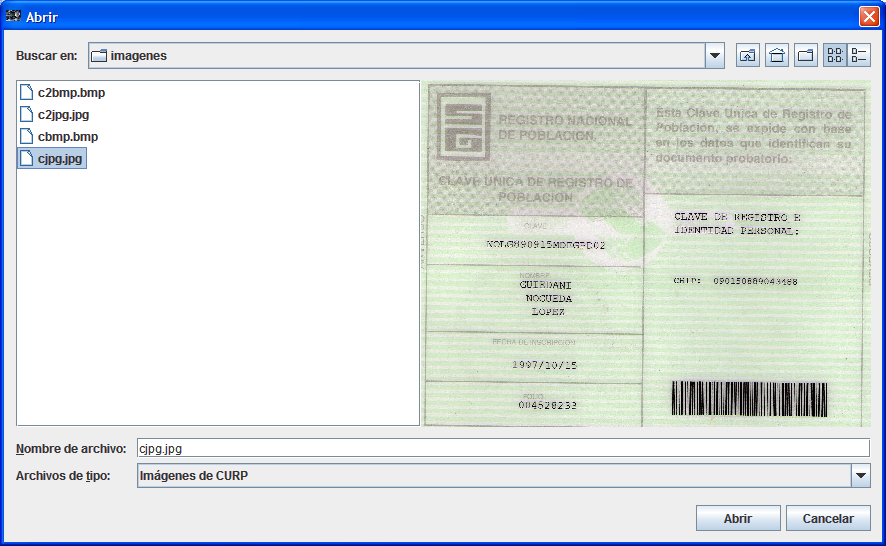


Fig. 5.9 Selector de archivos para elegir imagen del curp

En caso de que el usuario no haya seleccionado alguna imagen le aparecerá el siguiente cuadro de diálogo.



Fig. 5.10 Cuadro de diálogo Error en selección de imagen

En este caso debido a que se debe mandar un archivo (imagen del curp) para utilizar el proceso del servidor utilizamos la API org.apache.http para establecer comunicación HTTP.

* Protocolo HTTP

La tecnología Hyper-Text Transfer Protocol (HTTP) es el protocolo más importantes utilizado en internet hoy en día, los servicios Web principalmente para las aplicaciones orientadas a usuario como este trabajo. El funcionamiento básico es que el cliente estable una conexión TCP con el servidor, hace una petición, el servidor le responde y se cierra la conexión. Para que se haga una idea el lector de la sencillez, en la primera versión ampliamente utilizada del protocolo, el cliente solo podía invocar tres operaciones en el servidor: GET para pedir una página, HEAD para pedir la cabecera de una página y POST para enviar datos a una URL.

***Librería org.http.apache***

Aunque el paquete java.net proporciona funcionalidad básica para acceder a recursos a través de HTTP, no proporciona toda la flexibilidad o la funcionalidad necesaria para muchas aplicaciones. HttpClient busca llenar este vacío ofreciendo un eficiente y actualizado paquete rico en características de ejecución del lado del cliente de las normas HTTP más recientes y las recomendaciones.

A continuación se enlistan las características que permitieron su adecuación al proyecto:

* Basado en estándares, Java puro, la aplicación de las versiones de HTTP 1.0 y 1.1
* La plena aplicación de todos los métodos HTTP (GET, POST, PUT, DELETE, HEAD, OPCIONES, y TRACE) en un marco orientado a objetos extensible.
* Soporta encriptación con HTTPS (HTTP sobre SSL).
* Conexiones transparentes a través de servidores proxy HTTP.
* Túnel HTTPS conexiones a través de servidores proxy HTTP, a través del método CONNECT.
* Solicitud de los flujos de salida para evitar el almacenamiento en búfer cualquier órgano contenido en streaming directamente del servidor.
* Respuesta flujos de entrada para leer de manera eficiente el cuerpo de la respuesta por streaming directamente del servidor.
* Conexiones persistentes con KeepAlive en HTTP/1.0 y la persistencia en HTTP/1.1
* Acceso directo al código de respuesta y cabeceras enviadas por el servidor.
* La capacidad de establecer tiempos de espera de conexión.
* El código fuente está disponible libremente bajo la licencia Apache.
* Obtención de Curp mediante el uso de este protocolo

Se utilizó la clase base para implementar HttpClient. Esta clase sirve como controlador de propósito especial para el manejo de un aspecto particular del protocolo HTTP. Además proporciona métodos para crear instancias de los objetos:

Librería

*java.lang.Object*

*org.apache.http*

Implementaciones

Crear un nuevo cliente HTTP de parámetros y un administrador de conexión.

*public DefaultHttpClient(ClientConnectionManager conman, HttpParams params)*

Contexto: Se utilizó HttpContext que representa una asignación entre el URL ruta raíz de una solicitud a un HttpHandler, se invoca para controlar las solicitudes destinadas a la ruta raíz de HTTPServer o HttpsServer.

HttpContext representa el estado de ejecución de un proceso de HTTP. Es una estructura que se puede utilizar para asignar un nombre de atributo a un valor de atributo. El propósito principal del contexto HTTP es facilitar el intercambio de información entre los diversos componentes relacionados lógicamente.

Las instancias HttpContext son creadas con el uso de métodos de HTTPServer y HttpsServer

Librería

*java.lang.Object*

*org.apache.http.protocol.BasicHttpContext*

Implementaciones

*HttpContext localContext = new BasicHttpContext();*

Petición HttpPost: El método POST se utiliza para solicitar que el servidor de origen acepte la entidad incluida en la solicitud como un nuevo subordinado del recurso identificado por el URL en la solicitud de línea. En este trabajo fue utilizado para proporcionar un bloque de datos, como el resultado de la presentación de un formulario, a un proceso de manipulación de datos

Librerías

*java.lang.Object*

*org.apache.http.message.AbstractHttpMessage*

*org.apache.http.client.methods.HttpRequestBase*

*org.apache.http.client.methods.HttpEntityEnclosingRequestBase*

*org.apache.http.client.methods.HttpPost*

Implementaciones

*HttpPost httppost = new HttpPost("http://www.newocr.com/”);*

Mediante el método AddHeader(<Name>, <Value>), permite agregar un header con el valor dado.

*httppost.addHeader("referer", "http://www.newocr.com/");*

**Paquete org.apache.http.entity.mime**

Para el envío de datos (imagen del curp) se utilizó este paquete de apoyo a la codificación MIME de varias entidades (Extensiones Multipropósito de Correo Internet) para permitir la inserción de documentos (como imágenes, sonido y texto) en un mensaje. MIME describe el tipo de contenido del mensaje y el tipo de código usado con encabezados.

MIME incorpora las siguientes características:

1) Capacidad de enviar múltiples adjuntos en un solo mensaje

2) Longitud ilimitada del mensaje

3) Uso de conjuntos de caracteres no pertenecientes al código ASCII

4) Uso de texto enriquecido (diseños, fuentes, colores, etc.)

5) Adjuntos binarios (ejecutables, imágenes, archivos de audio o video, etc.), que se pueden dividir de ser necesario

* Envío de Archivo y texto.

Para fines de nuestra aplicación mandamos un archivo binario (application/octet-stream), y creamos un StringBody para el texto que se enviara, en caso del web service newocr, este nos pide el envío del idioma del archivo (Imagen CURP) y su posición, la cual se mandará sin ningún cambio en particular; en cuanto al formato utilizamos UTF-8 por ser un formato Unicode aceptado por el web service utilizado.

Librerías

*java.lang.Object*

*org.apache.http.entity.mime.content.AbstractContentBody*

*org.apache.http.entity.mime.content.FileBody*

*org.apache.http.entity.mime.content.StringBody*

*java.lang.Object*

*java.nio.charset.Charset*

Implementaciones

*pública StringBody ( String texto,Charset charset)*

*FileBody bin = new FileBody(new File(imagen1.getAbsolutePath().toString().replace('\\','/')), "application/octet-stream");*

*StringBody \_1 = new StringBody("spa", Charset.forName("UTF-8"));*

*StringBody \_r = new StringBody("0", Charset.forName("UTF-8"));*

Subir archivos por multipartes. Para mandar varios datos en una petición, se utilizaron librerías que permitieran el envío multiparte.

Por un lado la clase MultipartEntity para codificar una entidad HTTP que contiene varias partes de cuerpo, nos permite subir documentos multiparte, que para nuestro caso utilizamos en modo BROWSER\_COMPATIBLE, indicando que los datos enviados no contienen ningún encabezado Content-Transfer-Encoding.

Por otro lado HttpMultipart representa una colección de órganos contenidos de codificación MIME (multipartes). Esta clase es capaz de operar en los modos (RFC 822, RFC 2045, RFC 2046 compatible) o los modos de compatibilidad con el navegador. Finalmente se mandan las partes del cuerpo del mensaje por separado con el método *addPart* y se manda la petición.

Librerías

*java.lang.Object*

*org.apache.http.entity.mime.HttpMultipart*

*org.apache.http.entity.mime.MultipartEntity*

Implementaciones

*MultipartEntity reqEntity = new MultipartEntity(HttpMultipartMode.BROWSER\_COMPATIBLE);*

*reqEntity.addPart("l", \_1);*

*reqEntity.addPart("r", \_r);*

*reqEntity.addPart("userfile", bin);*

*httppost.setEntity(reqEntity);*

Para obtener la respuesta de la petición previa, primero se reciben los headers (getAllHeaders()), se libera la entidad y se hace la petición de respuesta con el header correspondiente a través de HTTP GET para recuperar toda la información (en forma de una entidad), es identificada por el Request-URL, para simplificar el proceso de obtención de respuesta utilizamos *ResponseHandler,* porque es un controlador que encapsula el proceso de generar una respuesta de un objeto con solo procesar un HttpResponse y devolver un valor (String) correspondiente a esa respuesta del cual obtenemos los datos de interés (CURP).

Librerías

*java.lang.Object*

*org.apache.http.HttpResponse*

*java.lang.Object*

*org.apache.http.message.AbstractHttpMessage*

*org.apache.http.client.methods.HttpRequestBase*

*org.apache.http.client.methods.HttpGet*

*java.lang.Object*

*org.apache.http.impl.client.BasicResponseHandler*

Implementaciones

*HttpResponse response = httpclient.execute(httppost, localContext1);*

*HttpGet httpget = new HttpGet(location);*

*ResponseHandler<String> responseHandler = new BasicResponseHandler();*

*String responseBody = httpclient.execute(httpget, responseHandler);*

Cerrar Http-Client

*httpclient.getConnectionManager().shutdown();*

Si se desea saber más sobre el uso y aplicaciones de esta librería puede recurrir al tutorial en línea [66].

En caso de que la conexión a internet falle se le mostrará al usuario un cuadro de diálogo.

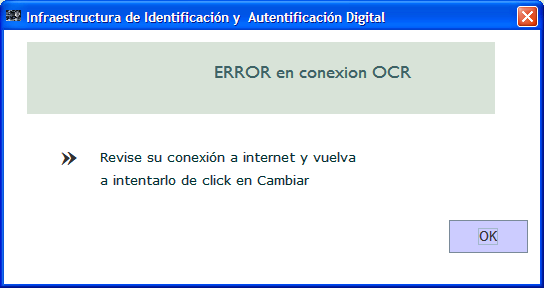


Fig. 5.11 Cuadro de diálogo Error de conexión

Una vez obtenida la cadena de caracteres del Curp de la imagen escaneada se hace una comparación con el Curp obtenido de la página de consultas Curp para ver que coincidan en caso y mostrará al usuario un cuadro de diálogo con el resultado de la comparación.

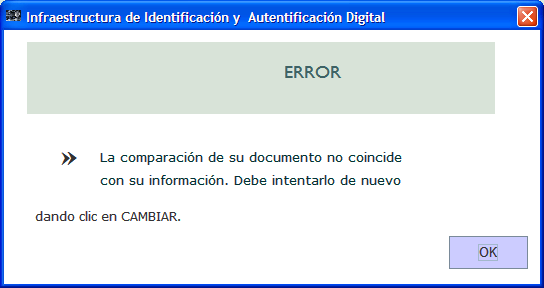


Fig. 5.12 Cuadro de diálogo Error al comparar curp

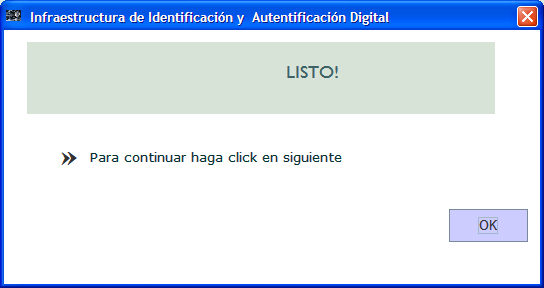


Fig. 5.13 Cuadro de diálogo Comparación exitosa

Una vez que la comparación fue exitosa se continúa con el proceso y se le solicita al usuario siga los pasos para generar su dato biométrico.



Fig. 5.14 Pantalla módulo biométrico

Biometric Password Manager “BioPod” de APC

Dispositivo biométrico utilizado en este proyecto para el módulo biométrico, es un dispositivo de seguridad biométrica, que asocia una contraseña a un usuario, proporciona identificación mediante huella digital en todos los sistemas operativos.

Su funcionamiento es sencillo APC BioPod se conecta a la computadora mediante puerto USB.



Fig. 5.15 Biometric Password Manager Biopod

Obtenida la cadena de caracteres asociada a la huella del usuario esta es guardada en un documento de texto plano.

Una vez que se ha pasado por los módulos privado, público y biométrico se procede a sacar el certificado, la firma digital y cifrar el texto plano.

Lo primero que se necesita es generar un par de llaves que estarán asociadas al usuario las cuales se utilizarán para realizar las demás operaciones.

**Paquete java.security**

El paquete java.security consiste básicamente en clases abstractas e interfaces que encapsulan conceptos de seguridad como certificados, claves, resúmenes de mensajes y firmas digitales.

La clase KeyPairGenerator es la que utilizamos para generar nuestro par de llaves la pública y privada. El par de llaves se comienza su construcción utilizando el método getInstance para el proyecto el algoritmo de cifrado que utilizaremos el RSA y el Bouncy Castle Provider (BC).

*KeyPairGenerator keyGen = KeyPairGenerator.getInstance("RSA", "BC");*

Con el método initialize se inicializa el generador de par de llaves con un tamaño de clave determinado y con una fuente de aleatoriedad.

*keyGen.initialize(1024, new SecureRandom());*

Finalmente para generar el par de llaves usamos el método generateKeyPair.

*KeyPair pair = keyGen.generateKeyPair();*

Con el par de llaves creado debemos generar el certificado digital.

Un *certificado de clave pública* es un punto de unión entre la clave pública de una entidad y uno o más atributos referidos a su identidad. El certificado garantiza que la clave pública pertenece a la entidad identificada y que la entidad posee la correspondiente clave privada [67].

El formato de certificados X.509 es un estándar del ITU-T (*International Telecommunication Union-Telecommunication Standarization Sector*) y el ISO/IEC (*International Standards Organization / International Electrotechnical Commission*) que se publicó por primera vez en 1988 [67].

**Bouncy Castle**

Para la creación del certificado optamos por trabajar con Bouncy Castle ya que es un proyecto de software libre que desarrolla librerías criptográficas que son libres y nos ofrece un provider e infraestructura adicional para poder trabajar para con el JCE de java.

Para generar en certificado utilizamos la clase X509V3CertificateGenerator para generar un certificado X509 V3.

Librería

*org.bouncycastle.jce.X509V3CertificateGenerator*

Para ponerle los elementos al certificado creado utilizaremos los métodos de esta clase: setSerialNumber para establecer el número de serie del certificado, setIssuerDN para nombre completo del emisor que es la entidad cuya clave privada se utiliza para firmar el certificado, setNotBefore para establecer la fecha en que es emitido el certificado, setNotAfter para establecer la fecha de vencimiento del certificado, setSubjectDN para establecer el tema que describe la a la entidad asociada con la clave privada, setPublicKey para asignarle la llave pública y setSignatureAlgoritm para elegir el algoritmo con el que se va a firmar el certificado en este caso es MD5withRSAEncription.

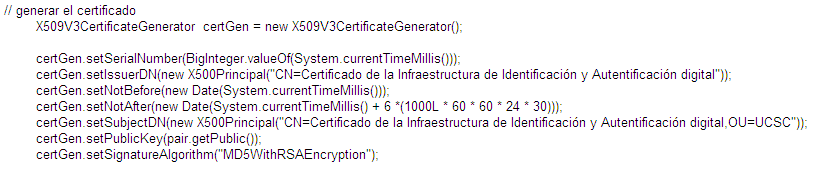


Fig. 5.16 Fragmento de código que genera el certificado

Una vez creado el certificado se genera la firma digital que se puede explicar de manera sencilla como un conjunto de datos que aseguran la identidad del emisor de un mensaje, las ventajas son que es auténtica y difícil de falsificar.

Para crear la firma digital en este proyecto se utilizó la clase Signature de java que se utiliza para proporcionar aplicaciones de la funcionalidad de un algoritmo de firma digital. Las firmas digitales se utilizan para garantizar la autenticidad e integridad de los datos digitales [68].

Librería

*java.security.Signature*

Para crear la firma digital se crea un objeto que implemente un algoritmo de firma en este caso MD5withRSA del Bouncy Castle provider BC.

*Signature signer = Signature.getInstance("MD5withRSA","BC");*

Se inicializa el objeto de la firma con el método initSign que recibe la llave privada asociada al usuario.

*signer.initSign(priv);*

Se actualizan los datos que se van firmar con el método update en este caso el dato es el password que el usuario introdujo en el formulario de información privada.

*signer.update(data.getBytes());*

Finalmente con el método sign obtenemos los bytes de firma del dato actualizado

*signer.sign();*

El siguiente paso es realizar dos procesos con el texto plano que contiene el dato biométrico el primero es aplicarle un algoritmo hash el resultado se guardará en la base de datos y el segundo es cifrarlo para guardarlo en el Token.

Para el proceso del algoritmo hash se utiliza la clase MessageDigest de java.security proporciona a las aplicaciones la funcionalidad de un algoritmo de resumen del mensaje, como MD5 o SHA. Para generar un resumen del mensaje la función hash toma los datos de un tamaño arbitrario y devuelve como salida un valor hash de longitud fija [69].

Librería

*java.security.MessageDigest*

Para inicializar el objeto MessageDigest con el algoritmo que se desea implementar en el caso de este proyecto MD5 se utiliza el método getInstance.

*MessageDigest md = MessageDigest.getInstance("MD5");*

Los datos se procesan con el método update.

*md.update(dataBytes, 0, nread);*

Con la función digest se completa el cálculo del valor hash mediante la realización de las operaciones finales como por ejemplo el relleno con caracteres y devuelve el arreglo de bytes que corresponde al valor hash resultante.

*byte[] mdbytes = md.digest();*

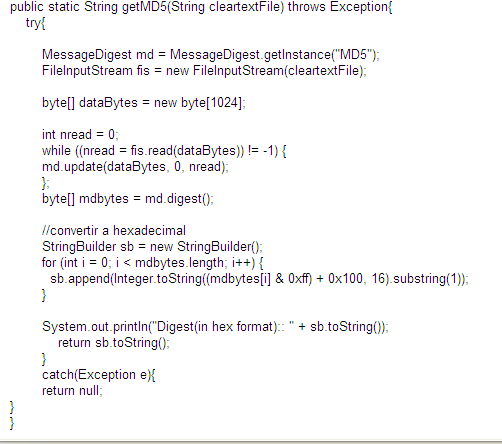


Fig. 5.17 Fragmento de código método algoritmo hash

Para el proceso de cifrado utilizamos el paquete javax.crypto que proporciona clases e interfaces para realizar operaciones criptográficas [70].

Librería

*javax.crypto.\**

La clase Cipher provee funcionalidades para el cifrado y descifrado de datos. Creamos un objeto de cifrado con el método getInstance pero el parámetro en este caso es una “transformación”. Una transformación es una cadena que describe el funcionamiento (o conjunto de operaciones) que se realizará en la entrada dada para producir una salida, consta de un algoritmo de cifrado y un esquema de relleno.

*Cipher cipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");*

El siguiente paso es inicializar el objeto debe ser inicializado por uno de los 4 modos, están definidos como constantes enteras de la clase Cipher, en este caso como se desea cifrar utilizamos la constante ENCRYPT\_MODE y como segundo parámetro utilizamos la llave pública asociada al usuario.

*cipher.init(Cipher.ENCRYPT\_MODE, key);*

Para ejecutar el cifrado se utiliza el método doFinal que recibe como parámetro un arreglo de bytes del texto plano (sin cifrar) que devuelve un arreglo de bytes del texto cifrado.

*cipherText = cipher.doFinal(text);*

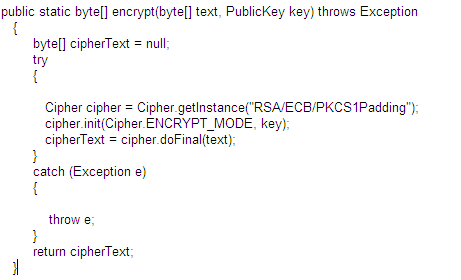


Fig. 5.18 Fragmento de código Cifrar

En caso de que en el sistema ocurra algún error al generar alguno de los procesos mencionados anteriormente se le mostrará al usuario el siguiente cuadro de diálogo.



Fig. 5.19 Cuadro de diálogo Error al crear documentos

La siguiente pantalla es en donde se seleccionará el token en el que se desea guardar el ID digital.



Fig. 5.20 Pantalla Guardar información en Token

Al dar clic a la imagen aparecerá el siguiente selector se archivos.

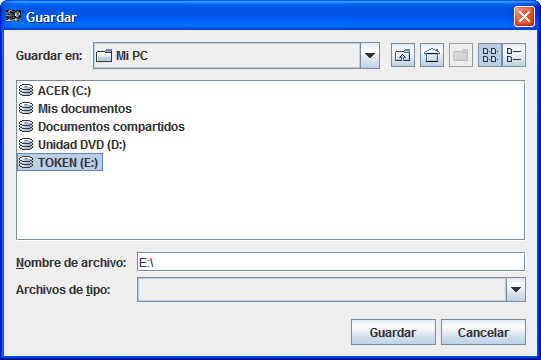


Fig. 5.21 Selector de Token

Es en esta parte donde se da de alta al usuario en la base de datos del sistema y se guardan en el token.

Para el manejo de la base de datos utilizamos el paquete java.sql que proporciona la API para el acceso y procesamiento de los datos almacenados usando el lenguaje de programación java.

Librería

*java.sql.\**

Para establecer la conexión con la base de datos necesitamos incluir el jar del Conector de la base de datos de MySQL *mysql-connector-java-5.1.6-bin.jar*.

Lo primero que debemos hacer es inicializar el driver.

*Class.forName("com.mysql.jdbc.Driver").newInstance();*

El servidor de MySQL debe estar arrancado, para establecer la conexión la clase DriverManager tiene el método getConnection que se encargará de intentar encontrar el controlador adecuado los parámetros que recibe son una url de base de datos de la forma jdbc: *subprotocol* : *subname* para la base de datos del sistema la url es la siguiente:

*static String url = "jdbc:mysql://localhost/sistemaid";*

Queda de esta manera jdbc:mysql porque se utiliza el driver jdbc para MySQL, localhost porque el servidor de la base de datos está en la misma computadora que el programa y sistemaid porque es el nombre de la base de datos.

Los otros dos parámetros son el usuario y el password para acceder a la base de datos.

*Connection conn = DriverManager.getConnection(url,login,password);*

Para insertar en la base de datos la información del usuario creamos un objeto de la Inteface PreparedStatement que representa una sentencia SQL precompilada.

*PreparedStatement stmt1 = conn.prepareStatement("INSERT INTO users (curp, nombre, telefono, correo, password, firma\_digital, hash) " + "VALUES (?,?,?,?,?,?,?)");*

Con el método setString es posible convertir de tipo de dato String a un SQL varchar.

*stmt1.setString(1,evaluar); // ID*

*stmt1.setString(2,nombre\_completo); // Nombre*

*stmt1.setString(3,tel); // telefono*

*stmt1.setString(4,correo); // correo*

*stmt1.setString(5,contraseña); //hash*

*stmt1.setString(6,firma\_digital);*

*stmt1.setString(7,hash);*

La instrucción executeUpdate ejecuta la instrucción SQL del objeto PreparedStatement.

*stmt1.executeUpdate();*

En caso de que el usuario ya se encuentre dado de alta en la base de datos se le aviso por medio de un cuadro de diálogo.



Fig. 5.22 Cuadro de diálogo Error al dar de alta en la BD

Si al momento de guardar los archivos en token ocurre algún error el usuario será avisado para que verifique la ruta de su token.



Fig. 5.23 Cuadro de diálogo Error al guardar en Token

Si e l usuario fue dado de alta con éxito se guarda en la base de datos un reporte.

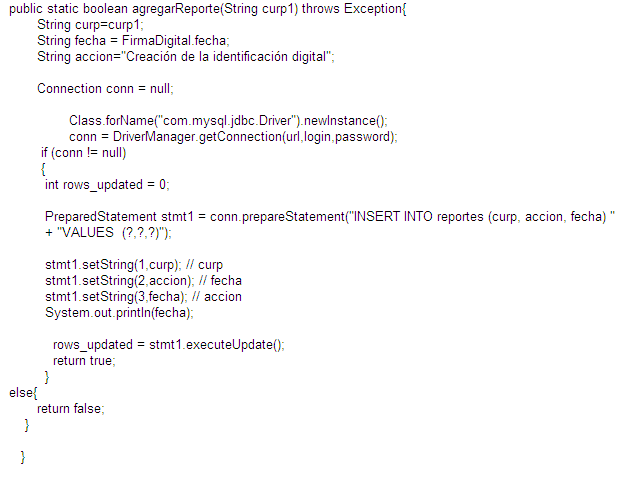


Fig. 5.24 Fragmento de código Guardar reporte en BD

Si la ID digital fue creada y guardada exitosamente el proceso habrá terminado mostrando la siguiente pantalla al usuario.



Fig. 5.25 Pantalla Identificación lista

Una vez terminado el proceso el usuario podrá visualizar en su token los siguientes archivos: la firma digital llamada “sig”, el certificado digital llamado “certificado”, el texto biométrico cifrado nombrado “ciphertext”, y la llave privada “privatekey”.

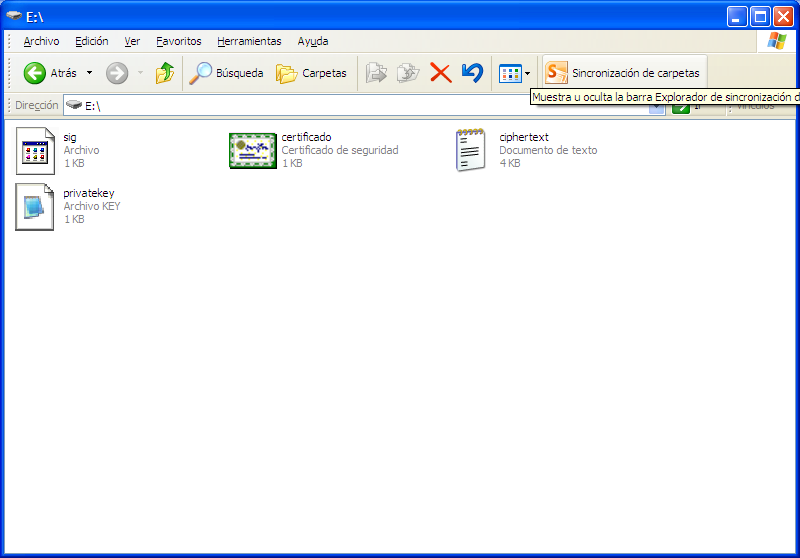


Fig. 5.26 Archivos guardados en el token

## 5.2 Módulo de Validación

Este módulo está diseñado para realizar el proceso de identificación y autentificación de un usuario.

En la primera pantalla se le solicita al usuario que introduzca su curp contraseña y que seleccione la ruta de su Token.



Fig. 5.27 Pantalla Bienvenida de Verificación

En caso de que algún campo esté vacío se le informará al usuario.

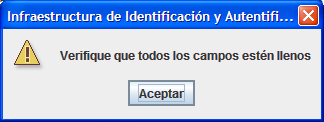


Fig. 5.28 Cuadro de diálogo Campos vacíos

En caso de que el Curp no cumpla con los 18 caracteres se le mandará al usuario una alerta.

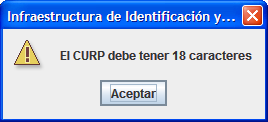


Fig. 5.29 Cuadro de diálogo Curp mal escrito

Una vez validados los campos se verifica si el usuario existe en la base de datos, si el usuario no existe se le pide al usuario que verifique sus datos.

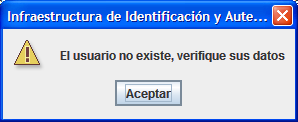


Fig. 5.30 Cuadro de diálogo Usuario inexistente en la BD

Para seleccionar la ruta del Token el usuario verá al dar clic en Seleccionar un selector de archivo.

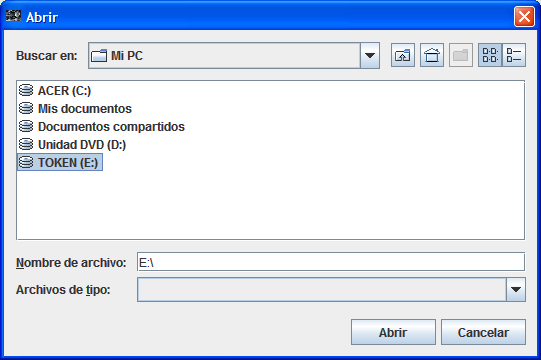


Fig. 5.31 Seleccionar Token

Otro elemento que se verifica es que el certificado digital exista en la ruta especificada, en caso contrario se le informa al usuario del sistema.

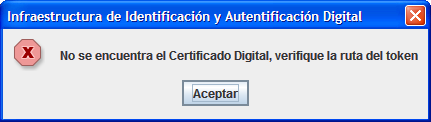


Fig. 5.32 Cuadro de diálogo No existe certificado en Token

Si el certificado existe se debe de verificar si aún se encuentra vigente ya que por seguridad tienen una caducidad de 6 meses.

Para volver a generar el certificado y poder verificar su fecha de vencimiento utilizamos la clase CertificateFactory.

Librería

*java.security.cert.CertificateFactory;*

El método getInstance devuelve un objeto de fábrica de certificado que implementa el tipo de certificado especificado.

*CertificateFactory cf = CertificateFactory.getInstance("X509");*

Después se utiliza el método generateCertificate que genera un objeto certificado y lo inicializa con los datos leídos de la secuencia de entrada inStream  el certificado devuelto es guardado en un objeto perteneciente a la clase X509Certificate que nos proporciona una forma estándar para acceder a todos los atributos de un certificado X.509.

*X509Certificate c = (X509Certificate) cf.generateCertificate(fr);*

Por último para comprobar que la fecha dada está dentro del período de validez del certificado utilizamos el método checkValidity que recibe como parámetro la fecha actual.

*c.checkValidity(today);*

En caso de que la fecha no sea válida se le informa al usuario para que se comunique con el administrador y se guarda reporte en la base de datos.

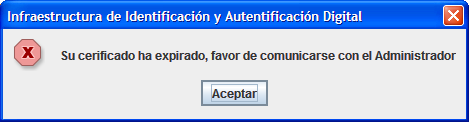


Fig. 5.33 Cuadro de diálogo Certificado expirado

Una vez corroborado que el certificado se encuentra vigente se extrae la llave pública para realizar este proceso se debe de realizar nuevamente el proceso de creación del certificado explicado anteriormente solo que ahora utilizamos el método getPublicKey de la clase X509Certificate y se guarda en un objeto de la clase PublicKey que sirve para proporcionar seguridad de tipo de llave pública.

*publicKey=c.getPublicKey();*

Posteriormente se necesita verificar la firma para realizar dicho proceso se utiliza la clase Signature.

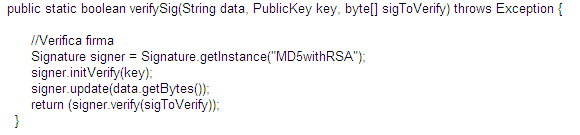


Fig. 5.34 Fragmento de código Verificar Firma

Se genera la firma con los métodos de la clase Signature

*Signature signer = Signature.getInstance("MD5withRSA","BC");*

Se inicializa el objeto para la verificación con el método initVerify que recibe la llave pública obtenida del certificado.

*signer.initVerify(key);*

Se actualizan los datos que se van verificar con el método update en este caso el dato es el password que el usuario acaba de introducir.

*signer.update(data.getBytes());*

Para realizar la verificación se utiliza el método verify que recibe los bytes de la firma que se quiere verificar en este caso la que se encontraba en el Token.

*signer.verify(sigToVerify);*

En caso de que la verificación de la firma sea correcta el usuario se ha podido identificar y autenticar correctamente y se le mostrará la siguiente pantalla.

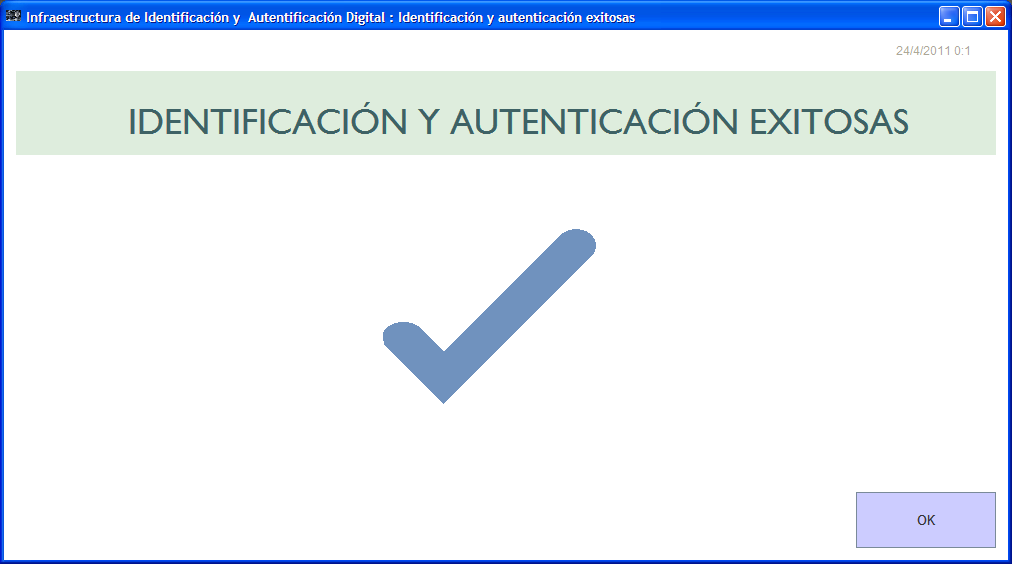


Fig. 5.35 Pantalla Identificación y Autentificación exitosas

En caso de que la verificación de la firma arroje que el usuario no coincide se le solicitará que pase su huella para realizar la verificación biométrica e intentar verificar la identidad del usuario.

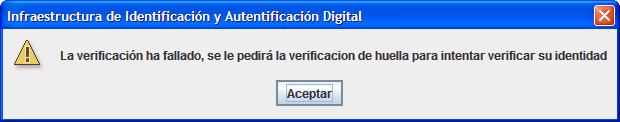


Fig. 5.36 Cuadro de Diálogo Verificación Fallida

El usuario verá la pantalla del módulo biométrico.



Fig. 5.37 Pantalla Módulo biométrico

Al dar clic en la imagen se le solicita al usuario coloque su dedo para realizar la verificación biométrica.

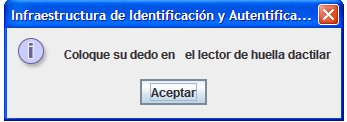
**

Fig. 5.38 Cuadro de diálogo Solicitud de huella

Si la verificación de huella dactilar falla el usuario no pudo identificarse y visualizará la siguiente pantalla y podrá intentarlo nuevamente.



Fig. 5.39 Pantalla Error en identificación y autentificación

## 5.3 Módulo de Administrador

En este módulo el administrador podrá visualizar reportes de acciones y eliminar cuentas de la base de datos. Por seguridad de la información solo existe un administrador que fue creado desde el sistema.

En la primer pantalla se solicita se introduzca la contraseña del administrador.

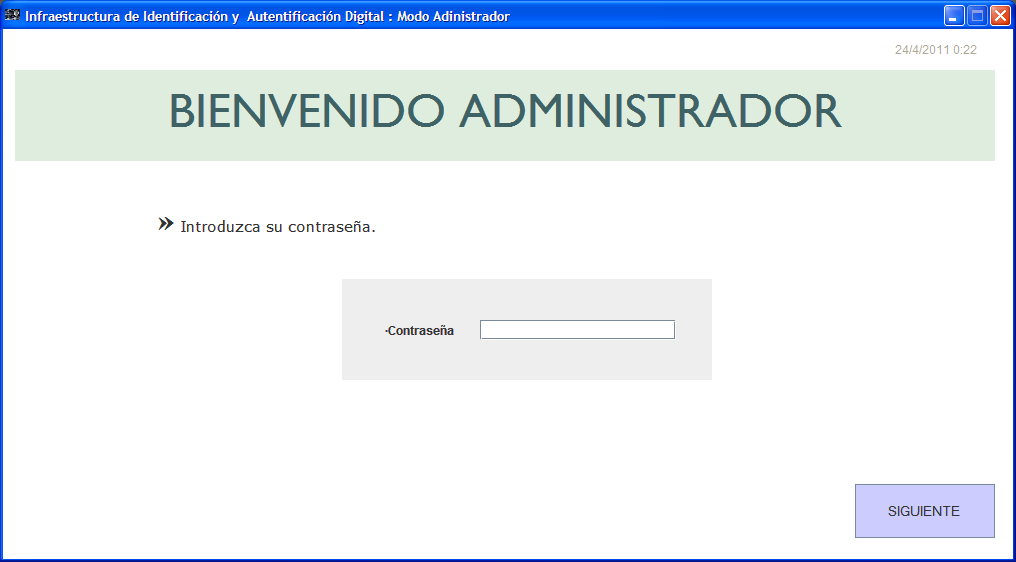


Fig. 5.40 Pantalla Administrador

En caso de que la contraseña sea inválida se le informará al usuario.

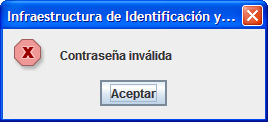


Fig. 5.41 Cuadro de diálogo Contraseña inválida

El administrador solo tiene 3 oportunidades para introducir su contraseña en caso de excederlas se le avisará y el programa se cerrará.

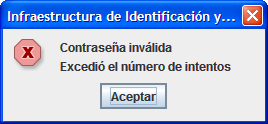


Fig. 5.42 Cuadro de diálogo Excedió intentos

Al introducir la contraseña correctamente el administrador visualizará las opciones Visualizar y Eliminar para elegir alguna debe dar clic en la imagen que desee.



Fig. 5.43 Pantalla Menú del Administrador

Si elige Visualizar Reportes se mostrará la siguiente pantalla en la que debe introducir el Curp del usuario del que desea ver el reporte.



Fig. 5.44 Pantalla Visualizar Reportes

En caso de que el curp no sea del tamaño establecido se le informará al usuario.

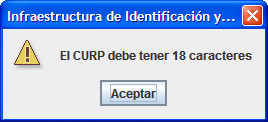


Fig. 5.45 Cuadro de diálogo Curp mal escrito

En caso que el campo esté vacío se mostrará el siguiente cuadro.

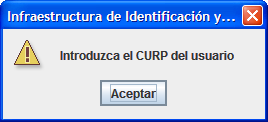


Fig. 5.46 Cuadro de Diálogo Campo del Curp vacío

Se verifica que el usuario exista en la base de datos.

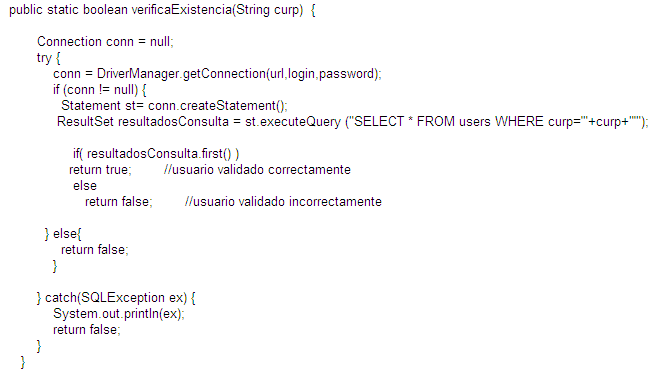


Fig. 5.47 Fragmento de código Verificar existencia en BD

Para realizar la consulta de usuario a la base de datos utilizamos un objeto de la Interface Statement utilizado para la ejecución de una sentencia SQL estática y devolver los resultados que produce.

*Statement st= conn.createStatement();*

Para guardar el resultado de la consulta realizada utilizamos un objeto de la Interface ResultSet una tabla de datos que representan un conjunto de resultados generados por la ejecución de una consulta a la base de datos.

*ResultSet resultadosConsulta = st.executeQuery ("SELECT \* FROM users WHERE curp='"+curp+"'");*

Utilizamos resultadosConsulta.first() para posicionarnos en la primer fila si esta función devuelve un false es que no encontró ningún resultado.

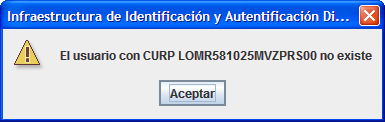


Fig. 5.48 Cuadro de diálogo Usuario no encontrado en BD

En caso de haberlo encontrado se muestra el reporte.

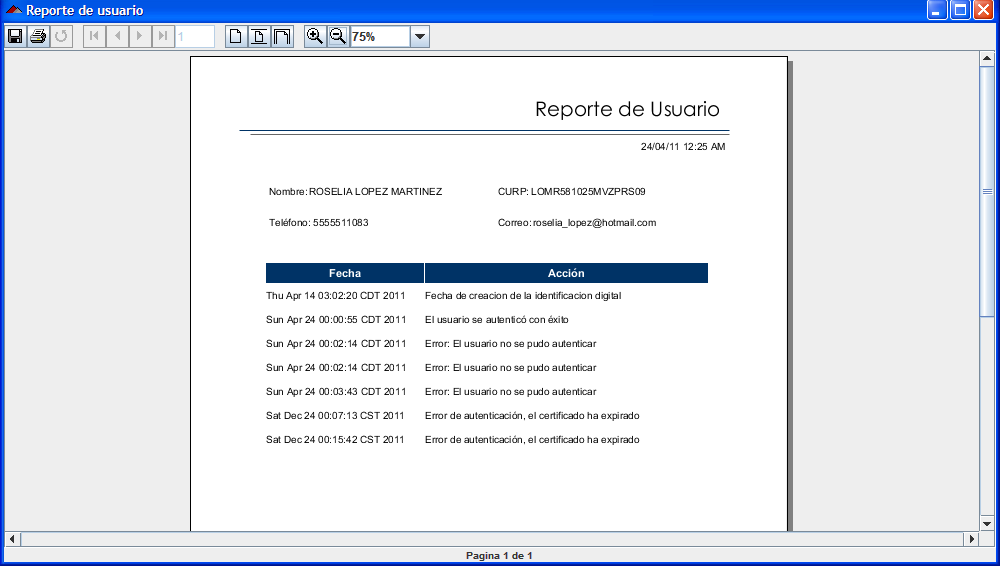


Fig. 5.49 Reporte de usuario

Para la generación de reportes utilizamos las librerías de Jasper Reports que es una herramienta de código abierto escrita en java se puede descargar de

Para la generación del reporte primero se debe generar un .jrxml en el que se debe configurar como se quiere el informe y posteriormente con las librerías que ayudan a compilar y mostrar en pantalla.

El .jrxml fue creado con la herramienta iReport que es un constructor y diseñador de informes con facilidad de uso para jasper reports escrito en Java. Para el proyecto se utilizó el plugin para el IDE NetBeans y el .jrxml quedó de la siguiente manera:

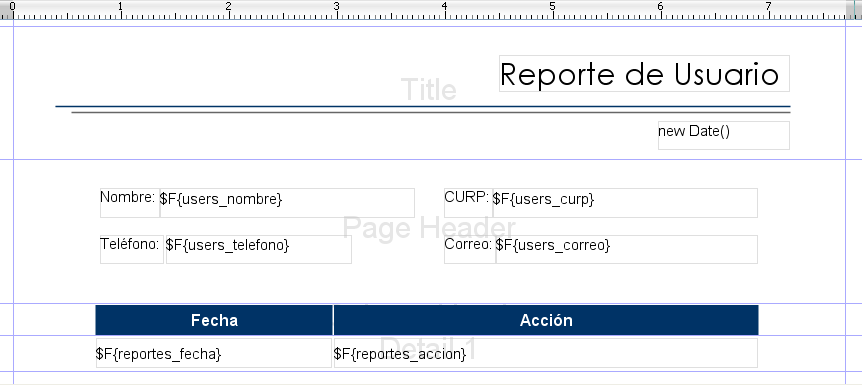


Fig. 5.50 Reporte.jrxml

iReports cuenta con una función para compilar que genera el archivo Reporte.jasper, la cual se utilizó para este proyecto.

Posteriormente se utiliza los métodos de las librerías de Jasper Reports para visulizar el reporte.

Librerías

*net.sf.jasperreports.engine.\*;*

*net.sf.jasperreports.engine.util.JRLoader;*

*net.sf.jasperreports.view.\*;*

*net.sf.jasperreports.view.save.JRPdfSaveContributor.\*;*

*net.sf.jasperreports.view.JRViewer.\*;*

*net.sf.jasperreports.view.save.JRMultipleSheetsXlsSaveContributor.\*;*

Se genera un objeto de tipo Jasper Reports

*JasperReport masterReport=null;*

Con la función loadObject de la clase JRLoader se carga el archivo Reporte.jasper

*masterReport=(JasperReport) JRLoader.loadObject(archivo);*

Finalmente se lanza el Viewer que tiene Jasper Reports.

*JasperPrint jasperPrint=JasperFillManager.fillReport(masterReport,parametro,conn);*

En caso de que el usuario elija la opción eliminar en el menú del administrador visualizará la siguiente pantalla.

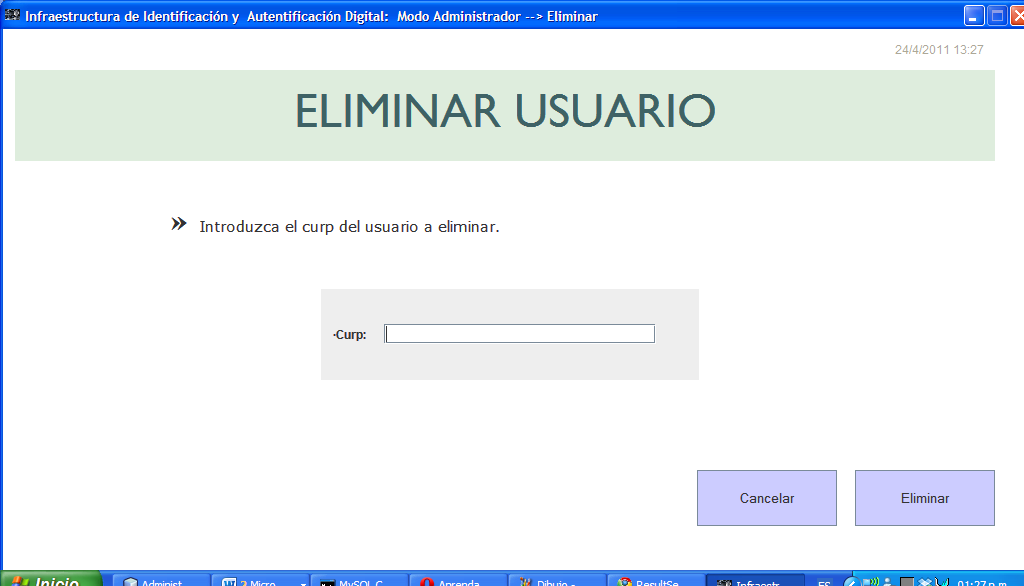


Fig. 5.51 Pantalla Eliminar usuario

Se hacen las verificaciones si el campo está vacío y si el tamaño del Curp es correcto en caso contrario se le informa al usuario.

En caso de que el usuario no exista se le muestra al usuario el siguiente cuadro de diálogo.

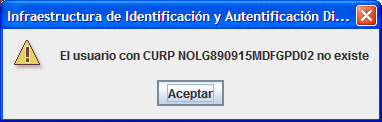


Fig. 5.52Cuadro de diálogo El usuario no existe en la BD

En caso de que el usuario exista se elimina de la base de datos. Crea un objeto de la Interface Statement con el método executeUpdate que ejecuta una sentencia de una instrucción INSERT, UPDATE o DELETE , o instrucciones SQL DDL.

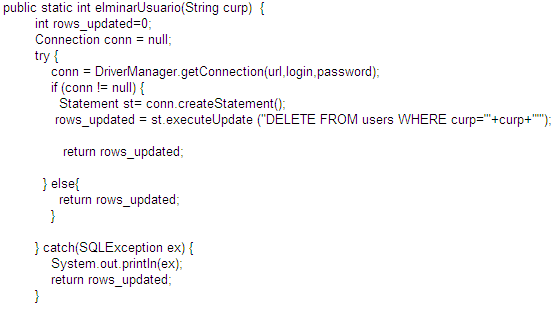
**

Fig. 5.52 Fragmento de código Eliminar usuario

Se le informa al administrador que el usuario se eliminó de forma exitosa.

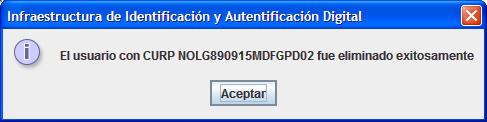


Fig. 5.53 Cuadro de diálogo Eliminación exitosa

# Capítulo 6 Trabajo a futuro

Al ser necesarios mundialmente hoy en día, nuevos e innovadores métodos que tengan como objetivo garantizar al 100% la identidad y autenticidad de las personas, el Trabajo Terminal presentado, pretende ser una base de conocimientos para nuevos Trabajos Terminales y personas o grupos que se interesen en darle continuidad al tema.

Pues sabiendo que las tecnologías con las que se logra dicho objetivo avanzan continuamente, sería una buena opción añadir nuevas tecnologías y en conjunto lograr un gran impacto dentro del hábito de seguridad de información e identificación y autentificación de personas.

# Capítulo 7 Conclusiones

Con la culminación del presente trabajo, se ha desarrollado una infraestructura de identificación y autentificación agrupando tecnologías que apoyan el mecanismo de autenticación tales como password, certificados digitales, información biométrica por huella dactilar, cifrado con RSA y utilización del método hash MD5, con información pública y privada del usuario validadas por instancias externas, cumpliendo así con los objetivos principales que se busca en cualquier método de identificación y autentificación: seguridad, portabilidad y sencillez.

Se crearon 3 módulos para brindar un mejor funcionamiento:

* Módulo de registro y generación de ID
* Módulo de administración
* Módulo de Validación.

# Referencias

**[1]Sitio web La Cota Observatorio Tecnológico.**

Publicado el Mayo 23 de 2008 por Juan José Andrés Gutiérrez

<http://www.lacofa.es/index.php/general/identidad_federada>

**[2]Sitio web Caisel - Controles de Acceso y Seguridad**

<http://www.microelectronic.com.ar/historia.htm>

**[3] Sitio web Innovaciones Tecnológicas**

Artículo: Respaldos de información

<http://www.innovacionate.com/index.php/categorias/servicios/77-respaldos-de-informacion.html>

**[4] Sitio web Mastermagazine**

Publicado en 2004 por Analia Lanzillotta

Artículo: Definición de Hacker

<http://www.mastermagazine.info/termino/5204.php>

**[5]Libro: Hackers-Los piratas del Chip y de Internet**

Publicado en 2001por Claudio Hernández

Versión Electrónica

**[6] Sitio web Wikipedia**

Publicado el 5 abril 2011

Artículo: seguridad de la información

<http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n>

**[7]Libro: Lenguaje, Identidad y Cultura**

Quinta Edición

Publicado en 2000 por Álvaro Mina Paz

Versión Electrónica

**[8]Sitio web Instituto Tecnológico de Veracruz.**

Publicado el 1 de Agosto de 2007 por Herbet Saal Gutierrez

Artículo: Relaciones entre lenguaje y pensamiento

<http://capacitacionencostos.blogia.com/2007/010814-biometria-y-la-identificacion-automatica-de-personas.php>

**[9]Sitio web Blog El Clarín.**

Artículo: Símbolos y Reflexiones

<http://blogs.clarin.com/el-rincon-de-fredy-clarin/2010/04/23/>

**[10]Instituto Forense de Investigaciones Latinoamericanas A.C..**

Publicado el 23 de Marzo de 2010 por Dr. Rafael Hernández de la Torre

Artículo: Tatuaje como medio de investigación criminalística

<http://www.ifil.org.mx/index.php?option=com_content&view=article&id=75:tatuaje-como-medio-de-investigacion-criminalistica&catid=43:ponencias&Itemid=59>

**[11]Sitio web Wikipedia.**

Artículo: Historia de las instituciones en Mesopotamia

<http://es.wikipedia.org/wiki/Historia_de_las_instituciones_en_Mesopotamia>

**[12]Sitio web Wikipedia.**

Artículo: Firma

<http://es.wikipedia.org/wiki/Firma>

**[13]Artículo PDF**

Publicado el 28 de febrero de 2001 por Rodolfo Herrera Bravo

Artículo: El documento electrónico y la firma digital en el sector público chileno

<http://www.ieid.org/congreso/ponencias/Rodriguez,%20Gladys.pdf>

**[14]Artículo PDF**

Publicado por Dra. Gladys Rodríguez

Artículo: de la firma autógrafa a la firma digital: perspectiva venezolana

<http://rodolfoherrera.galeon.com/firmadigital.pdf>

**[15]**S**eguridad y Certificación en el Comercio Electrónico.**

Editorial Biblioteca Fundación

p. 165.

**[16]Artículo de Seguridad de la Información**

Publicado en 1999 por Lucena López y Manuel José.

Artículo: Criptografía y Seguridad en Computadores. Dpto. de Informática Universidad de Jaén.

Edición virtual. Capítulo 2-Página 23.

[http://www.kriptopolis.org](http://www.kriptopolis.org/).

**[17]Comercio Electrónico y derecho.**

Editorial Astrea.

p. 443.

**[18]“ Las Firmas Electrónicas y la Seguridad de la Comunicaciones en Línea”**

Artículo: Compilador Lorenzo La Carrero.

Editorial Cámara Venezolana de Comercio Electrónico

p 143-152.

**[19]Sitio web Gobierno de México**

Artículo: Documentos de Identificación Oficial

[http://www.gob.mx/](http://www.gob.mx/wb/egobierno/egob_documentos_de_identificacion_oficial)

**[20]Sitio web Definicion.de**

Artículo: Definición de tarjeta

<http://definicion.de/tarjeta/>

**[21]Sitio web**

Artículo: Tarjetas Magnéticas

<http://www.a3m.eu/es/tarjetas-plasticas/tarjetas-blancas/tarjetas-magneticas.html>

**[22]Sitio web El Rincón de la Ciencia**

Publicado en Enero del 2007 por Norberto Ligonio

Artículo: Tecnología RFID

<http://centros5.pntic.mec.es/ies.victoria.kent/Rincon-C/Curiosid2/rc-98/rc-98.htm>

**[23]Sitio web La Comunidad de RFID en Latinoaméricana**

Publicado el 27 de mayo de2010

Artículo: RFID en las bibliotecas de Guía

<http://www.rfidpoint.com/noticias/rfid-en-las-bibliotecas-de-guia/>

**[24]Trabajo de TIM 2004**

Publicado en 2004 por Jose Chust Vandrell y Ramon Cruz Soria

Artículo: Smart Cards

**[25]Sitio web Soluciones en tarjetas plásticas**

Publicado el 01 de Junio de 2010

Artículo: Sobre Smart Cards (Tarjetas Inteligentes)

<http://www.tangoid.com.ar/tangoid/sobre-smart-cards-tarjetas-inteligentes>

**[26]Sitio web Soluciones en tarjetas plásticas**

Publicado el 13 de diciembre de 2008

Artículo: Biometria-huellas digitales

<http://cinthyadeleo.wordpress.com/2008/12/13/biometria-huellas-digitales/>

**[27]Sitio web Biometría**

Artículo: Reconocimiento de voz

<http://www.biometria.gov.ar/metodos-biometricos/voz.aspx>

**[28]Sitio web YVKE Mundial**

Publicado el 7 de Dic de 2009 por Francisco Fagundez

Artículo: Biometría facial permite reconocer un rostro de miles parecidos

<http://www.radiomundial.com.ve/yvke/noticia.php?38552>

**[29]Sitio Web Certificados Copitec**

Artículo: Certificado de la ACC

<http://www.certificadoscopitec.org.ar/info_conocer.htm>

**[30] Sitio Web CERES**

Artículo: Cifrado digital-Certificados digitales

<http://www.cert.fnmt.es/popup.php?o=faq>

**[31]Criptografía y Seguridad en Computadoras**

4ta Edición

Publicado por Manuel Lucena López

<http://ccia.ei.uvigo.es/docencia/SSI/cripto.pdf>

**[32]FUNDAMENTOS DE SEGURIDAD EN REDES**

1ª Edición

Publicado en 2003 por Stallings, William

Plaza edición: MADRID

**[33] Sitio web CSIC**

Publicado en el 2000 por [Gonzalo Álvarez Marañón](http://www.iec.csic.es/%7Egonzalo/)

Artículo: Servicios de seguridad

<http://ccia.ei.uvigo.es/docencia/SSI/cripto.pdf>

**[34]Blog: Proyecto de Redes: Seguridad de la Información**

Publicado en 2008 por Oswaldo Puican Alarcón

<http://proyecto-de-redes.blogspot.com/2008_01_01_archive.html>

**[35]Artículo PDF “LAS MATEMÁTICAS EN LA CRIPTOLOGÍA “**

Por Paz Morillo

Artículo: Matemática Aplicada IV. Universidad Politécnica de Catalunya

**[36] A. Ribagorda y J. Sancho, “Seguridad y Protección de la Información”**

1ª Edición

Publicado en 1994

Ed. Centro de Estudios Ramón,

pp. 22-31.

**[37] R. Rivest, “Criptography as Duct Tape”**

Artículo: Senate Commerce

Publicado en 12 de Enero de 1997 por MIT University

**[38]C. Benett, F. Bessete, G. Brasard, L. Salvai, “Experimental Quantum Cryptography” University Montreal, Canadá**

Publicado en 2004 por Springer Journal.

**[39]W. Stallings, *“Fundamentos de Seguridad en Redes: Aplicaciones y Estándares”***

2ª Edición

Prentice Hall

Publicado en 2004

pp. 27-85.

**[40] Módulos de Instrucción Seguridad en Redes de Computadores**

1º versión

Publicado en Noviembre 2004 por Carlos Manzo Campos

**[41]U.S. Department of Commerce, National Institute of Standards and Technology, Specification for the Advanced Encryption Standard (AES),**

FIPS PUB 197

Publicado el Noviembre de 2001.

**[42]Burr, W.E., “Selecting the Advanced Encryption Standard,”**

IEEE Security & Privacy, Vol. 1

Publicado el 2 marzo de 2003

pp. 43–52.

**[43]M. Fergus, “A simple algebraic representation of Rijndael”**

Publicado en 2003

**[44]D. Berstein, “Cache-timing attacks on AES”**

Publicado en 2005 por Illinois University.

**[45]D. Osvik, A. SHAmir, E. Tromer, “Cache Attacks and Countermeasures: the Case of AES”**

IEEE Security & Privacy

Publicado en 2005 por Weizmann Institute of Scienc

**[46]R. Rivest, A. SHAmir and L. Adleman, “*A method for obtaining digital signatures and public-key* cryptosystems**

Vol. 21

Publicado el Febrero de 1978 por ACM Communications

pp.1-16.

**[47]F. Blake, “Advances in Elliptic Curve Cryptography”**

Publicado en 1989 por Oxford University, UK.

**[48]Diffie, W., and M. E. Hellman, "New Directions in Cryptography,"**

Vol. IT-22

Publicado el Noviembre de 1976

Artículo: IEEE Transactions on Information Theory

pp. 644-654.

**[49]C. Benett, F. Bessete, G. Brasard, L. Salvai, “Experimental Quantum Cryptography University Montreal**

Publicado en 2004 por Springer Journal.

**[50]A. Menezes, P. Van, “Applied Cryptography”**

CRC, Ed.

Publicado en1996.

pp. 9-48

**[51] W. Mao, “Modern Cryptography, Theory and Practice”**

Ed. Prentice

Publicado en 2003.

Chapter 8.

**[52] Sitio Web MD5 Homepage**

1991 por [Mordechai T. Abzug](http://www.gl.umbc.edu/%7Emabzug1).

<http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html>

**[53] Sitio msdn**

Artículo : MD5

<http://msdn.microsoft.com/es-es/library/system.security.cryptography.md5%28v=vs.80%29.aspx>

**[54] Documento PDF MacroSeguridad**

Artículo: ePass 2000 Token USB

<http://www.coacom.net/broadchuremacroseguridad/White%20Paper%20ePass%20Token%20USB%20%282%29.pdf>

**[55] Portal de DNI**

Artículo: información del DNI

<http://www.dnielectronico.es/informacion_general.html>

**[56] Sitio Web ChannelPlanet**

Publicado el 14 de abril de 2000por Eliana Salgado.

Artículo: Tokens: seguridad avanzada para acceso a información.

<http://www.channelplanet.com/?idcategoria=8249>

**[57] Sitio Web DEEPNET SECURITY**

Artículo: Deepnet Unified Authentication Platform

<http://www.ireo.com/fabricantes-y-productos/deepnet-security/unified-authentication-platform/resumen/>

**[58]Sitio Web El Instituto Mexicano del Seguro Social**

Artículo: Información al patrón -Certificado digital

<http://idse.imss.gob.mx/certificacion/>

**[59] Ingeniería de Software: Un Enfoque Práctico.**

5ª edición.

Roger S. Pressman.

McGraw-Hill

**[60] Equivalencia de los Puntos de Función en Líneas de Código.**

<http://alarcos.inf-cr.uclm.es/doc/pgsi/doc/teo/8/pgsi-t8.pdf>

**[61] Sitio Web COCOMO.**

www.enciclopedia.galeon.com/cocomo.doc

**[62] UML 2 Iniciación, ejemplos y ejercicios corregidos**

ENI ediciones

Laurent Debrauwer y Fien Van der Heyde

**[63] Sitio Web SPARX System**

Artículo: Diagrama de Actividades UML 2

http://www.sparxsystems.com.ar/resources/tutorial/uml2\_activitydiagram.html

**[64] The java Tutorials**

Working with URL´s

Reading from and Writing to a URLConnection

<http://download.oracle.com/javase/tutorial/networking/urls/readingWriting.html>

**[65] Java™ Platform, Standard Edition 6 API Specification**

Traducción Class URLConnection

<http://download.oracle.com/javase/1.4.2/docs/api/java/net/URLConnection.html>

**[66] HTTPClient Tutorial**

Oleg Kalnichevski

<http://hc.apache.org/httpcomponents-client-ga/tutorial/html/index.html>

**[67]Curso de Seguridad en java**

**Certificados Digitales**

Sergio Talens-Oliag

Diciembre 1999

<http://www.uv.es/sto/cursos/seguridad.java/html/>

**[68] Java™ Platform, Standard Edition 6 API Specification**

Traducción Signature

http://download.oracle.com/javase/6/docs/api/java/security/Signature.html

**[69] Java™ Platform, Standard Edition 6 API Specification**

Traducción Clase MessageDigest

http://download.oracle.com/javase/6/docs/api/java/security/MessageDigest.html

**[70] Java™ Platform, Standard Edition 6 API Specification**

Traducción Package javax.crypto

http://download.oracle.com/javase/6/docs/api/javax/crypto/package-summary.html

# 

# Definición de términos

A

1. **AES (Advanced Encryption Standard):** es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.
2. **AIDC("Automatic Identification and Data Capture")**: Métodos de identificación automática de objetos, recolectando datos sobre ellos, y adicionando esos datos directamente a sistemas de computación.
3. **ANSI( American National Standards Institute):** es una organización sin ánimo de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos.
4. **Autenticación o autentificación**: es el acto de establecimiento o confirmación de algo (o alguien) como auténtico, es decir que reclama hecho por, o sobre la cosa son verdadero.

B

1. **Biometría:** es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos. El término se deriva de las palabras griegas "bios" de vida y "metron" de medida.

C

1. **Cocomo (Modelo Constructivo de Costes):** Es un modelo matemático de base empírica utilizado para estimación de costes de software. Incluye tres submodelos, cada uno ofrece un nivel de detalle y aproximación, cada vez mayor, a medida que avanza el proceso de desarrollo del software: básico, intermedio y detallado.
2. **Criptoanálisis:** (del griego kryptós, "escondido" y analýein, "desatar") es el estudio de los métodos para obtener el sentido de una información cifrada, sin acceso a la información secreta requerida para obtener este sentido normalmente.
3. **Criptograma:** es un mensaje cifrado cuyo significado resulta ininteligible hasta que es descifrado.
4. **Criptosistema:** conjunto de transformaciones que convierten un texto en claro en un texto cifrado y viceversa, seleccionándose un, o unos, algoritmo particular mediante una clave.
5. **CURP (Clave Única de Registro de Población):** es un código único de Identidad tanto para residentes como para ciudadanos mexicanos. Tiene 18 caracteres, lo que impide que se generen duplicados.

E

1. **ElGamal:** se refiere a un esquema de cifrado basado en problemas matemáticos de algoritmos discretos. Es un algoritmo de criptografía asimétrica basado en la idea de Diffie-Hellman y que funciona de una forma parecida a este algoritmo discreto.
2. **EMV ("Europay MasterCard VISA"):** es un estándar de interoperabilidad de tarjetas IC ("Tarjetas con chip") y TPV, para la autentificación de pagos mediante tarjetas de crédito y débito.
3. **ePurse ( Monedero electrónico Vehicular)** permite almacenar una cantidad variable de dinero en una etiqueta de radio frecuencia que es adherida al parabrisas. El proceso de pago es rápido, sencillo y seguro.

F

1. **FIPS 140-1: e**specifica las prácticas recomendadas para implementar criptoalgoritmos, tratamiento de material de clave y búferes de datos y trabajar con el sistema operativo. Proveedores de software envían sus productos a un proceso de evaluación para demostrar su implementación de este estándar.
2. **FIPS 140-2 (Federal Information Processing Standard - Estándares federales de procesamiento de la información)**es un estándar de seguridad de ordenadores del gobierno de los Estados Unidos para la acreditación de módulos criptográficos.

G

1. **GSM("Groupe Special Mobile"):** es un sistema estándar, completamente definido, para la comunicación mediante teléfonos móviles que incorporan tecnología digital.

H

1. **Hash:** Función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. Un hash es el resultado de dicha función o algoritmo.

I

1. **IBM (International Business Machines):** Es una empresa multinacional que fabrica y comercializa herramientas, programas y servicios relacionados con la informática.
2. **IEEE (Institute of Electrical and Electronics Engineers) :** asociación técnico-profesional mundial dedicada a la estandarización. Es la mayor asociación internacional sin ánimo de lucro formada por profesionales de las nuevas tecnologías.
3. I**EEE P1363 8Standard for Public-Key Cryptography)**: Grupo de trabajo del IEEE dedicado a la criptografía de clave pública.
4. **IFE(Instituto Federal Electoral):**es el responsable de cumplir con la función estatal de organizar las elecciones federales de México, es decir, las relacionadas con la elección del Presidente de los Estados Unidos Mexicanos y de los Diputados y Senadores que integran el Congreso de la Unión.
5. **IIMSS (Instituto Mexicano del Seguro Social)**: es una institución gubernamental, autónoma y tripartita (Gobierno Federal, Patrones y Trabajadores), dedicada a brindar servicios de salud y seguridad social a la población que cuente con afiliación al instituto, llamada entonces asegurado o derechohabiente.
6. **Integridad de datos:**  se refiere a la corrección y completitud de los datos en una base de datos.
7. **ISO (Organización Internacional para la Estandarización):** organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.

M

1. **MD5SUM:** es una herramienta de seguridad que sirve para verificar la integridad de los datos.
2. **MIT (Instituto Tecnológico de Massachusetts):** es una de las principales instituciones universitarias dedicadas a la docencia y a la investigación en Estados Unidos, especialmente en ciencia, ingeniería y economía.

N

1. **NIST(National Institute of Standards and Technology):** es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología.
2. **NBS (National Bureau. Standards)**: Agencia federal estadounidense que desarrolla normas para las tarjetas de identificación del gobierno para empleados federales y contratistas con el fin de prevenir el acceso a personal no autorizado a los edificios y sistemas de cómputo del gobierno.

O

1. **OTP(one-time password):** contraseña de un solo uso que tiene el propósito de dificultar el acceso no autorizado a recursos protegidos, como por ejemplo la cuenta de usuario de un sistema de computación.

P

1. **PIN(Personal Identification Key - Número de Identificación Personal):** es una contraseña o clave numérica que se utiliza para acceder a móviles, cajeros automáticos, servicios de telefonía, etc.

R

1. **Repudio:** denegación, por una de las entidades implicadas en una comunicación, de haber participado en la totalidad o en parte de una comunicación.
2. **RFC (Request For comments - Solicitud de Comentarios)**. Es el nombre que se da a una serie de normas que definen el protocolo TCP/IP, así como sus documentos relacionados.
3. **RSA (Rivest, Shamir y Adleman):** es un sistema criptográfico de clave pública desarrollado en 1977. En la actualidad, RSA es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.
4. **RSA SecurID:** es un mecanismo desarrollado cerca Seguridad de RSA para realizarse autentificación del dos-factor para un usuario a un recurso de la red.

**b. Diseño de sistemas computacionales**

S

1. **SSL (Secure Sockets Layer -Protocolo de Capa de Conexión Segura):** Protocolo criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

T

1. **TOKEN (también token de autenticación o token criptográfico)** es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.
2. **TACACS ( Terminal Access Controller Access Control System - sistema de control de acceso mediante control del acceso desde terminales**): es un protocolo de autenticación remota que se usa para comunicarse con un servidor de autenticación comúnmente usado en redes Unix.

U

1. **USB (Universal Serial Bus - bus universal en serie):** es un puerto que sirve para conectar periféricos a una computadora o dispositivo.