

**FACULTAD DE INGENIERÍA**

**DEPARTAMENTO DE INGENIERÍA ELÉCTRICA**

**Avance 1**

**Diseño y construcción de un sistema electrónico para el control de acceso biométrico de huella dactilar gestionado por plataforma WEB.**

**Alumno : Juan Sotomayor Chacón**

**Carrera : Ingeniería civil industrial en electrónica**

**Profesor Guía : Jorge Gianotti Hidalgo**

**Antofagasta, Mayo de 2016**

# ÍNDICE

[LISTA DE FIGURAS iii](#_Toc468182996)

[LISTA DE TABLAS iv](#_Toc468182997)

[LISTA DE ACRÓNIMOS v](#_Toc468182998)

[SIMBOLOGÍA vi](#_Toc468182999)

[1 INTRODUCCIÓN 1](#_Toc468183000)

[1.1 Objetivos 2](#_Toc468183001)

[1.1.1 Objetivo general 2](#_Toc468183002)

[1.1.2 Objetivos específicos 2](#_Toc468183003)

[1.2 Planteamiento de la investigación 3](#_Toc468183004)

[1.1.3 Modelos planteados para el hardware 6](#_Toc468183005)

[1.1.4 Justificación del modelo seleccionado 10](#_Toc468183006)

[1.3 METODOLOGÍA 12](#_Toc468183007)

[2 TÉCNICAS DE IDENTIFICACIÓN Y AUTENTIFICACIÓN DE USUARIOS. 14](#_Toc468183008)

[2.1 Contraseñas 16](#_Toc468183009)

[2.2 Identificación por Radio Frecuencia (RFID) 17](#_Toc468183010)

[2.2.1 Funcionamiento de la Identificación por Radio Frecuencia (RFID) 17](#_Toc468183011)

[2.2.3 Clasificación 19](#_Toc468183012)

[2.2.4 Regulación y estandarización 21](#_Toc468183013)

[2.3. Biometría 22](#_Toc468183014)

[2.3.1. Sistemas biométricos 24](#_Toc468183015)

[2.3.2. Lector huella digital 30](#_Toc468183016)

# LISTA DE FIGURAS

Figura 1.1. Ejemplo de un sistema de control de acceso en red. 4

Figura 1.2. Arquitectura módulo control de acceso, modelo 1. 7

Figura 1.3. Arquitectura módulo control de acceso, modelo 2. 8

Figura 1.4. Arquitectura módulo control de acceso, modelo 3. 9

Figura 1.5. Arquitectura módulo control de acceso, modelo 3. 12

Figura 2.1. Esquema de funcionamiento de autentificación mediante contraseña. 16

Figura 2.2. Esquema y componentes de un sistema RFID. 18

Figura 2.3. Etapas o procesos que componen los sistemas: a. matriculación; b. verificación; c. identificación. 27

Figura 2.4. Método de lectura de huella digital óptico. 32

Figura 2.5. Método de lectura de huella digital capacitivo. 32

# LISTA DE TABLAS

[Tabla 1.1. Características microcontrolador v/s Raspberry Pi. xv](#_Toc468119660)

# LISTA DE ACRÓNIMOS

HTTP: Hypertext Transfer Protocol.

PC: Personal Computer.

LAN: Local Area Network.

WAN: Wide Area Network.

CCD: Charged Coupled Device.

RTC: Real Time Clock

RFID: Radio Frequency Identification

GPIO: General Purpose Input/Output

IMEI: International Mobile Equipment Identity.

IP: Internet Protocol.

TCP: Transmission Control Protocol.

HTTP: Hypertext Transfer Protocol.

UART: Universal Asynchronous Receiver Transmitter.

USB: Universal Serial Bus.

PHP: Hipertext Preprocessor

HTML: Hiper Text Markup Language.

WWW: World Wide Web.

# SIMBOLOGÍA

Alfabeto latino:

|  |  |  |
| --- | --- | --- |
| A | Área transversal | m2 |
| I | Corriente de soldadura | A |
| Q | Caudal | l/min |

Alfabeto griego:

|  |  |  |
| --- | --- | --- |
| η | Eficiencia | % |
| δ | Disolución | % |

CAPÍTULO

# INTRODUCCIÓN

La evolución de la ciencia y de la tecnología ha permitido evolucionar también a los sistemas de seguridad y de control de acceso de los que la sociedad puede disponer. En un principio consistían en medios físicos, tales como cerraduras, rejas, trabadores, etc., fácilmente vulnerables con tiempo y herramientas; animales tales como perros guardianes; vigilantes tales como policías, serenos, veladores. Todos estos sistemas fueron evolucionando hasta crear sistemas más complejos como cerraduras electrónicas, alarmas o sistema de observación por video.

El control de acceso se viene realizando tradicionalmente en grandes edificios y recintos de gran ocupación. Hoy en día estos sistemas representan un plus importante de seguridad para cualquier tipo de empresa o actividad. El control de acceso básicamente permitirá diferenciar:

* Qué personas tienen acceso a las dependencias de trabajo.
* A qué dependencias concretas tienen acceso.
* En que horario tienen acceso.

Una gran ventaja que aportan estos sistemas es tener un registro con todos los accesos que se producen en las instalaciones. De esta manera se puede controlar y prevenir cualquier evento interno (robo, sabotaje, etc.), ya que se pueden recuperar el registro de fichajes de un día determinado a una hora en cualquier punto de la instalación donde exista dicho control.

En la actualidad son muchos los sistemas de control de acceso electrónicos que aparecen en el mercado para solventar la demanda existente. Se pueden encontrar una multitud de lectores, tarjetas, y programas informáticos que lo realizan, pero realmente la diferencia está en el cumplimiento de las expectativas de los clientes.

Una de las soluciones en la actualidad es la identificación de las personas mediante su huella digital. Gracias a su unicidad y constancia a través del tiempo, las huellas digitales han sido utilizadas para la identificación de las personas por más de un siglo, más recientemente volviéndose automatizada debido a los avances en las capacidades de la computación.

El presente proyecto tiene como finalidad diseñar y construir un sistema de control de acceso gestionado por una plataforma web. La forma de identificación de usuarios, es mediante el sistema biométrico de huella digital y a través de identificación por radiofrecuencia (RFID), se estudiará estas tecnologías en detalles para integrarlas a un módulo electrónico para el control de acceso, este debe ser capaz de registrar, identificar y autentificar a los usuarios del sistema, gestionar la información del sistema y manejar base de datos, controlar el actuador del punto de acceso (puerta de seguridad) y cumplir con los parámetros de seguridad, para dificultar la intervención física de terceros.

La plataforma web es la interfaz gráfica con la cual el administrador del sistema gestiona los recursos de los usuarios de forma remota como; ingresar, validar, editar y eliminar usuarios, configurar horarios de ingresos, estadísticas e historial de ingreso, exportar relatorios, etc. Esta herramienta brinda una mayor eficiencia y movilidad al administrador al permitir que desde cualquier lugar con conexión a internet tenga acceso a la plataforma.

## Objetivos

### Objetivo general

Diseñar y construir un sistema electrónico para el control de acceso biométrico de huella dactilar gestionado por una plataforma WEB.

### Objetivos específicos

* Investigación detallada del funcionamiento del sensor biométrico de huella dactilar y sistemas RFID (identificación por radiofrecuencia).
* Diseñar un módulo de control de acceso que sea capaz de identificar huellas dactilares y tarjetas RFID, lograr diferenciarlas entre sí, almacenarlas y modificarlas en la memoria de un microcontrolador, debe contar con un lector de memoria SD para almacenar el registro de los usuarios y el historial de ingreso de estos, de modo de respaldo.

El módulo debe tener conexión estable a una Red de Área Local (LAN), enviar y recibir información a un servidor de base de datos Mysql.

* Desarrollar una plataforma web en donde el administrador del módulo, tenga acceso a los usuarios registrados, con la opción de ingresar e editar datos personales, permitir y denegar acceso, ver historial y estadísticas de ingreso durante un periodo determinado.
* Realizar un estudio económico del sistema de control de acceso.
* Implementar el módulo control de acceso en un lugar determinado y verificar su correcto funcionamiento.

## Planteamiento de la investigación

Un sistema de control de acceso hace referencia al mecanismo que en función de la identificación ya autentificada permite acceder a datos o recursos. Básicamente encontramos sistemas de controles de acceso en múltiples formas y para diversas aplicaciones. Por ejemplo, encontramos sistemas de controles de acceso por software cuando digitamos nuestra contraseña para abrir el correo, otro ejemplo es cuando debemos colocar nuestra huella en un lector para desbloquear un teléfono inteligente. Estos casos, son ejemplos que permiten el acceso a datos. Sin embargo, este trabajo está enfocado en la seguridad electrónica, relacionada al acceso de recursos para la apertura de una puerta.

Un sistema de control de acceso es un sistema electrónico que restringe o permite el acceso de un usuario a un área específica, validando la identificación por medio de diferentes tipos de lectura (clave por teclado, tarjetas de proximidad o biometría) y a su vez controlando el recurso (puerta) por medio de un dispositivo eléctrico como un electroimán, solenoide, pestillo o motor.

Básicamente los controles de acceso se clasifican en dos tipos:

* Sistemas de Control de Acceso Autónomos
* Sistemas de Control de Acceso en Red

Los Sistemas de Control de Acceso Autónomos son sistemas que permiten controlar una o más puertas, sin estar conectados a un PC o un sistema central, por lo tanto, no guardan registro de eventos. Aunque esta es la principal limitante, algunos controles de acceso autónomos tampoco pueden limitar el acceso por horarios o por grupos de puertas, esto depende de la robustez de la marca. Es decir, los más sencillos solo usan el método de identificación (ya sea clave, proximidad o biometría) como una "llave" electrónica.

Los Sistemas de Control de Acceso en Red son sistemas que se integran a través de un PC local o remoto, donde se hace uso de un software de control que permite llevar un registro de todas las operaciones realizadas sobre el sistema con fecha, horario, autorización, etc. Van desde aplicaciones sencillas hasta sistemas muy complejos y sofisticados según se requiera. En la figura se representa un ejemplo de un Sistema de Control de Acceso en Red.

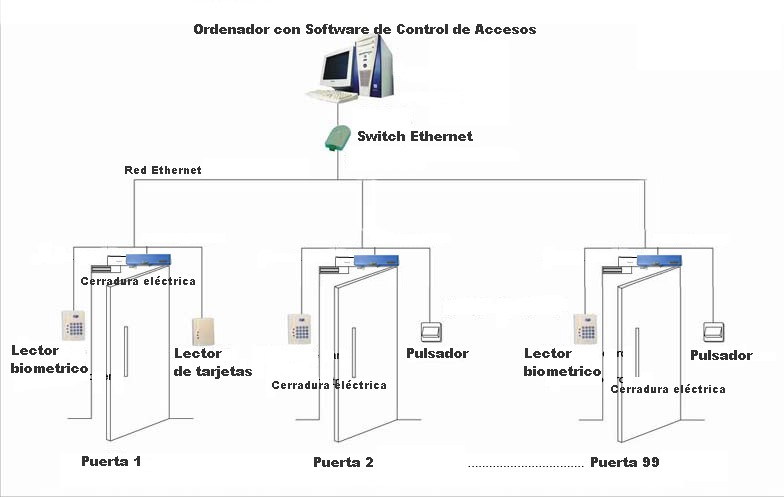


Figura 1.1 Ejemplo de un sistema de control de acceso en red.

En este trabajo se desarrollará un sistema de control de acceso en red, para el control físico de una puerta, se debe implementar un mecanismo electrónico que autentifique al usuario y en base a ello otorgar acceso a alguna dependencia, este sistema involucra el desarrollo de un software y hardware.

El software está asociado a una plataforma web para la gestión de la información, por medio de una interfaz gráfica, el administrador del sistema puede controlar los recursos que están disponibles para los usuarios; crear, editar y eliminar el perfil de los usuarios, configurar permisos, establecer horarios de acceso, exportar e imprimir informes y relatorios, entre otras funciones.

El hardware corresponde a un módulo electrónico de control de acceso, su función principal es realizar la autentificación de usuarios a través de diferentes métodos como; contraseñas, huella dactilar (biometría) y tarjetas RFID.

El módulo electrónico cuenta principalmente con los siguientes componentes:

* **Controlador**, este puede ser un microcontrolador o computador, es el encargado de gerenciar los diferentes sensores y principal comunicador con la plataforma web.
* **Pantalla**, el usuario puede visualizar gráficamente opciones de configuración e instrucciones.
* **Teclado**, necesario para realizar las configuraciones del módulo e ingreso de contraseñas de acceso.
* **Lector RFID**, este puede leer etiquetas RFID a una distancia de varios centímetros, utilizado para el registros de etiquetas al sistema y identificación de las mismas.
* **Sensor biométrico**, Lector de acceso biométrico de huella dactilar. Identifica al usuario a través de su huella dactilar (característica única e irrepetible para cada persona), lo que da un nivel de seguridad superior a cualquier otro sistema que utilice otro tipo de identificadores.
* **Reloj de tiempo real (RTC)**, utilizado para almacenar los horarios de las actividades en los registro.
* **Conector Ethernet o Wifi**, es necesario tener conectividad a una red de área local (LAN[[1]](#footnote-1)) o una red de área extensa (WAN[[2]](#footnote-2)), para realizar la transferencia de datos entre la plataforma y el módulo electrónico.
* **Relé**, dispositivo electromagnético, funciona como un interruptor controlado por un pulso electrónico, es el encargado de activar el circuito eléctrico del control de la puerta.

Conociendo los componentes necesarios para la implementación del módulo de control de acceso, a continuación se plantean diferentes modelos para el hardware.

### Modelos planteados para el hardware

Se proponen 3 modelos para la arquitectura del hardware del módulo de control de acceso:

1. El controlador del hardware es un microcontrolador[[3]](#footnote-3) este es el encargado de gerenciar cada uno de los periféricos, como se muestra en la figura 1.2, este ejecuta instrucciones almacenadas como números binarios organizados secuencialmente en la memoria principal, puede ser programado en diferentes lenguajes de programación como; visual basic, C, C++, assembler, Python, etc.

Este módulo electrónico interactúa con los usuarios, realiza la matriculación, verificación e identificación, controla la activación del relé para el actuador instalado en la puerta, funciona como servidor, este gestiona y administra la plataforma web, incluye un reloj de tiempo real y una memoria externa para el almacenamiento y registro de la información.



Figura 1.2 Arquitectura módulo control de acceso, modelo 1.

1. El controlador del hardware es un computador de placa reducida, se propone utilizar una “Raspberry Pi”, su sistema operativo oficial es RaspBian, una versión adaptada de Debian, aunque es compatible con diversos sistemas operativos, la Raspberry Pi cuenta con pines GPIO (General Purpose Input/Output), un sistema de Entrada/Salida de propósito general, las cuales son utilizadas para el gerenciamiento de los periféricos (ver figura 1.3). Cuenta con 4 puertos USB, adaptador para una memoria µSD, conector Ethernet y Wifi. Es compatibles con diferentes lenguajes de programación como; C++, Visual Basic, Phyton, Java, Javascript, HTML, PHP, Ruby, Node.js, etc.



Figura 1.3 Arquitectura módulo control de acceso, modelo 2.

Este módulo tiene las mismas funciones que el anterior, con la diferencia que este puede ejecutar diferentes procesos y tareas de forma simultáneas, e instalar servidores dedicados para el manejo de la plataforma web, es compatible con diferentes bases de datos (Mysql, MongoDB, Firebase) para el registro de la información.

1. Este modelo está compuesto por 2 hardware, el primero es el módulo de control de acceso, cuyo controlador principal es un microcontrolador, este comanda los sensores que interactúan con los usuarios, encargado de realizar los procesos de matriculación, verificación e identificación de los usuarios. Este hardware es gerenciado por un controlador maestro (Raspberry Pi) a través de un puerto serial (ver figura 1.4).



Figura 1.4 Arquitectura módulo control de acceso, modelo 3.

El segundo hardware corresponde a la computadora (Raspberry Pi), cumple la función de servidor y administra toda la información de la plataforma web, almacena los registros de los usuarios, permite el acceso a estos, contiene los historiales de acceso, etc. Este hardware integra un circuito con un reloj de tiempo real, para llevar el control del tiempo del servidor y un relé para el control del actuador de la puerta.

Este último funciona como un controlador maestro, está siempre recibiendo información del módulo de control de acceso, y cuando recibe una petición de un usuario este gestiona la información y envía una respuesta de vuelta.

### Justificación del modelo seleccionado

Los modelos planteados del hardware para el módulo de control de acceso utilizan como controlador principal un microcontrolador o un computador de placa reducida (Raspberry Pi), en la tabla 1.1 se pueden observar las principales características de cada controlador.

Tabla 1.1 Características microcontrolador v/s Raspberry Pi.

|  |  |  |
| --- | --- | --- |
|  | Microcontrolador (ATmega2560) | Raspberry Pi |
| Memoria RAM | 0.008 [MB] | 1 [GB] |
| Pines de Entrada/Salida | 54 | 40 |
| Velocidad de reloj | 16 [MHz] | 1.2 [GHz] |
| Multitarea | No | Si |
| Network | Ninguno | Ethernet y Wifi |
| Voltaje de entrada | 7 a 12 [V] | 5 [V] |
| Memoria Flash | 256 [KB] | Tarjeta SD, 2 a 16 [GB] |
| Puertos USB | 1 | 4 |
| Sistema operativo | Ninguno | Distribuciones de Linux |

La Raspberry Pi es 75 veces más rápido que el microcontrolador y tiene 125.000 veces más de memoria RAM. La Raspberry Pi es una computadora independiente que puede ejecutar un sistema operativo real en Linux. Puede realizar varias tareas, soportar cuatro puertos USB y puede conectarse de forma inalámbrica a Internet. En pocas palabras, es lo suficientemente potente como para funcionar como una computadora personal.

Puede sonar que Raspberry Pi es superior al microcontrolador, pero eso es sólo cuando se trata de aplicaciones de software. Por otra parte el microcontrolador tiene la capacidad de trabajar con pines analógicos y en tiempo real, esta flexibilidad le permite trabajar con casi cualquier tipo de sensor o chip.

Raspberry Pi puede procesar varias tareas, éste puede ejecutar múltiples programas en segundo plano mientras está activado. Por ejemplo, puede estar funcionando como un servidor y transmitiendo información por un puerto USB.

El modelo seleccionado es el número 3, en este modelo se aprovecha las ventajas de usar el microcontrolador y la Raspberry Pi, el módulo de control de acceso es controlado por el microcontrolador, es el encargado de gestionar la parte sensorial, el usuario interactúa con este módulo por medio de una pantalla LCD y un teclado matricial, en este dispositivo se realizan los procesos de matriculación, verificación e identificación de los usuarios. Cada vez que el usuario interactúa con este módulo se envía una petición a la Raspberry Pi, este procesa la información, y envía una respuesta.

La Raspberry Pi es el controlador principal del *sistema de control de acceso*, este aloja la plataforma web y almacena la información del sistema, tiene la capacidad de ejecutar procesos diferentes para la gestión del módulo de control de acceso, por lo que este sistema funcionara en tiempo real, además este integra los adaptadores de red ethernet y wifi de fácil configuración.

El módulo de control de acceso es instalado al exterior del lugar a controlar, y la Raspberry Pi se encuentra en el interior (ver figura 1.5), dando más seguridad e independencia al sistema, los usuarios que interfieran con el módulo exterior no podrán tener acceso a la información del sistema, ni manipular el actuador para la apertura de la puerta.

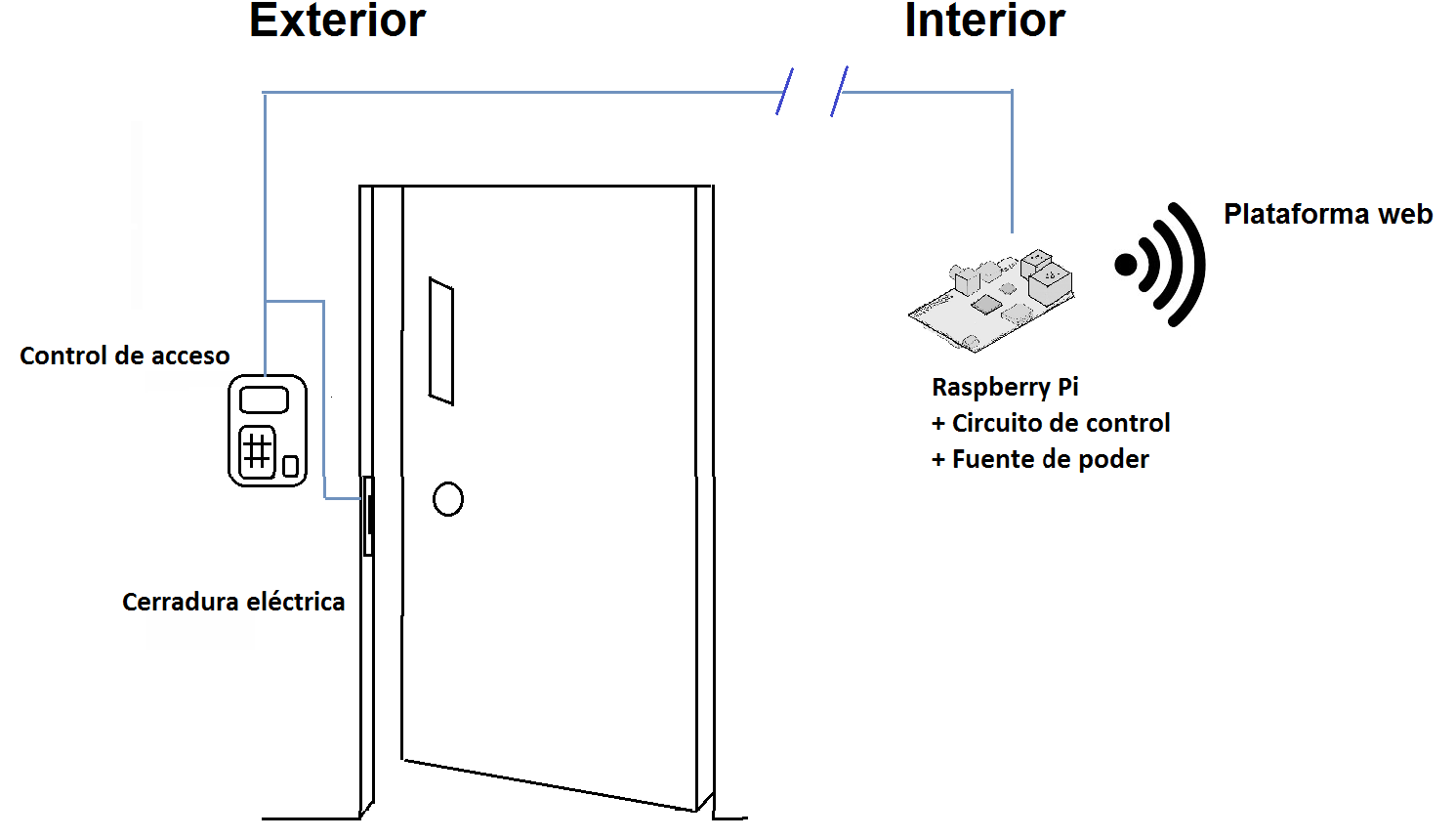


Figura 1.5 Arquitectura módulo control de acceso, modelo 3.

## METODOLOGÍA

Para realizar el diseño y construcción de este proyecto, es necesario dividir el trabajo por etapas, el capítulo 1 corresponde a la introducción, en donde se definen los objetivos del proyecto, descripción del planteamiento de la investigación y el análisis de diferentes soluciones para el diseño del hardware del proyecto.

En el capítulo 2, se desarrolla las principales técnicas de identifación y autenticación de usuarios del módulo de control de acceso, es primordial conocer la teoría del funcionamiento de los sensores que realizan estas funciones.

El capítulo 3 aborda el diseño del sistema de control de acceso, en esta etapa se describe el esquema del sistema de control de acceso, selección y justificación de los componentes que se utilizarán y diseño de los circuitos que forman parte del sistema de control de acceso.

Luego en el capítulo 4, abarca la metodología de construcción del módulo electrónico del control de acceso, principalmente la fabricación de los circuitos del prototipo, el montaje de esta y pruebas de funcionamiento de todos los componentes.

Posterior a la fabricación del hardware, en el capítulo 5 se desarrolla la plataforma web, principalmente la programación de la interfaz gráfica del sistema de control de acceso, se implementa la gestión de perfiles y permisos de usuarios, la exportación de informes e historial de usuarios, configuración del servidor. Además se comprueba el correcto funcionamiento del software con el hardware.

Una vez creada la plataforma web y con el hardware funcionando, en el capítulo 6 se muestran los resultados obtenidos luego del diseño y construcción del sistema de control de acceso, se menciona el funcionamiento del sistema, sincronización total entre la plataforma web y el módulo electrónico.

El capítulo 7 aborda el análisis económico del proyecto, los costó de implementación, viabilidad, análisis de mercado y un posible plan de negocio. Finalmente en el capítulo 8, se muestran las conclusiones y los resultados esperados en el corto y mediano plazo luego del término del proyecto.

**CAPITÚLO**

# TÉCNICAS DE IDENTIFICACIÓN Y AUTENTIFICACIÓN DE USUARIOS

La identificación digital forma parte indisoluble de la mayoría de servicios en Internet y en las tecnologías de la información. Por ejemplo, para subir un vídeo en un servidor web, se pide que el usuario esté registrado y se identifique para poder llevar a cabo la publicación del contenido. Por otra parte, para utilizar una tarjeta magnética de acceso, es preciso que el usuario esté registrado en la plataforma de control. Para realizar acciones tan variadas como hacer un pago mediante tarjeta de crédito, utilizamos esta misma tarjeta para identificarnos. O bien para hacer gestiones bancarias a través de Internet, lo primero que haremos es especificar quién somos.

Esta identificación digital puede ser relativamente sencilla. Basta con disponer de un nombre de usuario, usar como identificador la dirección de correo electrónico o, en el caso de un pago, usar el número de tarjeta de crédito. Ahora bien, para la mayoría de servicios, además de la identificación digital, es necesaria una autenticación de esta identidad.

Mediante la autenticación de la identidad, el servicio se asegura de que el usuario es quien dice ser.

El concepto de "quien dice ser" lo resuelve el identificador de usuario: mediante una cadena de caracteres se denota cuál es la identidad del usuario. Y para demostrar la autenticidad de la identidad del usuario se pueden usar cuatro aproximaciones distintas:

**1)** El usuario es quien dice ser si demuestra conocer algo que solamente este conoce. Por ejemplo, conoce una palabra secreta de acceso.

**2)** El usuario es quien dice ser si posee algún objeto, como por ejemplo una tarjeta magnética para el acceso a un edificio.

**3)** El usuario es quien dice ser si posee alguna característica física que sólo él tiene: por ejemplo, la huella dactilar.

**4)** El usuario es quien dice ser si es capaz de hacer algo de forma única: por ejemplo, el patrón de escritura o la forma de andar.

Pese a tratarse de cuatro formas de abordar la autenticación de la identidad, no existe una frontera clara entre algunas de ellas. Además, es perfectamente posible el uso de varias de estas técnicas de forma combinada, para conseguir mayores grados de seguridad.

Por ejemplo, disponer de una tarjeta con códigos de seguridad para permitir operaciones bancarias a través de Internet (tarjeta de coordenadas) podría verse como una mezcla entre los dos primeros casos: el usuario posee la tarjeta, pero podría decirse que es conocedor de una información, aunque en este caso la tenga escrita.

Por otra parte, todas estas formas de abordar la autenticación no están exentas de problemas de seguridad. Por ejemplo, la tarjeta con códigos podría ser robada y usada por otro usuario. Otro caso podría ser la obtención de una clave de acceso mediante un correo electrónico fraudulento.

La usurpación de identidad consiste en que una entidad use con éxito el mecanismo de identificación que identifica a otra identidad.

En este apartado se exponen las principales técnicas y tecnologías para implantar la identificación y autenticación de usuarios en un sistema de control de acceso de personas.

## 2.1 Contraseñas

La autenticación por medio de contraseñas es relativamente sencilla: el usuario “*A”* envía su identificador “*IDA”* y acto seguido su contraseña “*CSA”*. La implementación del protocolo de identificación puede precisar que ambas informaciones se manden en un mismo mensaje, o bien que primero se pida el nombre de usuario y después la contraseña.

Esta contraseña es usada por el servicio para validar la identidad del usuario. Si *A* es el único conocedor de *CSA*, es altamente probable que el usuario sea realmente *A*. En la figura 2.1, el usuario utiliza su contraseña para validarse al servicio. Este dispone de una lista de pares con usuarios y contraseñas para comprobar las identidades. Ante una contraseña correcta, el servicio manda un mensaje de autenticación correcta al equipo del usuario. Algunos servicios incluye una hora de caducidad de esta autenticación, tras la cual el usuario deberá volver a autenticarse.

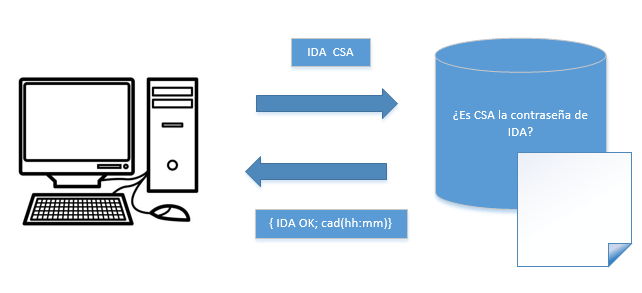


Figura 2.1 Esquema de funcionamiento de autentificación mediante contraseña.

La contraseña es una cadena de caracteres de longitud arbitraria. En algunos escenarios, se usa una versión reducida de la contraseña, formada tan sólo por unos pocos números. En este caso la contraseña se conoce con el nombre de PIN, en algunos entornos se utiliza el término PIN cuando en realidad la contraseña está formada tanto por letras como por números.

Así como un mismo servicio o sistema no permite que haya dos usuarios con el mismo identificador, es perfectamente posible que dos o más usuarios tengan la misma contraseña.

## 2.2 Identificación por Radio Frecuencia (RFID)

La identificación por radio frecuencia (RFID) se está convirtiendo en algo común en la vida cotidiana en estos días la podemos encontrar en tarjetas de pago, también es utilizado en el sistema de cobro de las autopistas o carreteras, por otra parte es utilizado por empresa para llevar el control del inventario de productos y equipos, la mayoría de nosotros encontramos etiquetas RFID al menos un par de veces a la semana y nunca pensamos en lo que se puede hacer con esta tecnología.

### 2.2.1 Funcionamiento de la Identificación por Radio Frecuencia (RFID)

El intercambio de un sistema RFID implica dos actores: un iniciador y un objetivo. El iniciador, es un lector o lector/escritor de dispositivo, este inicia el intercambio mediante la generación de un campo magnético y escucha las respuestas de cualquier objetivo que se encuentre dentro del radio, ver figura 2.2. El objetivo, es una etiqueta, que responde cuando se recoge una transmisión desde un iniciador y responderá con un número identificador único (UID).

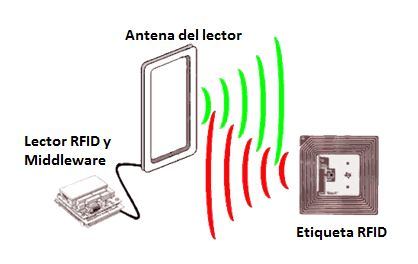


Figura 2.2 Campos magnético generado por un sistema RFID.

Existen 3 componentes básicos en un sistema RFID, ver figura 2.3.

1. La etiqueta o transponder de RFID consiste en un pequeño circuito, integrado con una pequeña antena, capaz de transmitir un número de serie único hacia un dispositivo de lectura, como respuesta a una petición. Algunas veces puede incluir una batería.

2. El lector, (el cual puede ser de lectura o lectura/escritura) está compuesto por una antena, un módulo electrónico de radiofrecuencia y un módulo electrónico de control, sirve para energizar la tarjeta de identificación y capturar su número, para posteriormente enviarlo a un sistema de control o un computador que se encargue de procesar los datos.

3. Un controlador o un equipo anfitrión, comúnmente una PC o Workstation, Este se encarga de recibir y procesar los datos pertenecientes al número de identificación de la etiqueta presentada en la lectora, la cual corre una base de datos y algún software de control

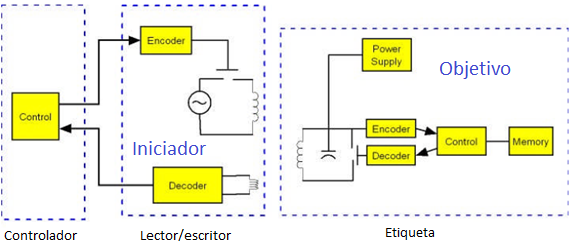


Figura 2.3 Esquema y componentes de un sistema RFID.

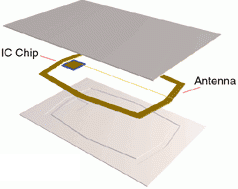
Las etiquetas RFID tienen una pequeña cantidad de memoria a bordo, como se muestra en la figura 2.4, por lo general menos de 1 kilobyte. Un dispositivo iniciador puede leer estos datos, y si se trata de un dispositivo de lectura/escritura, se puede escribir en el etiquetar también. Esto le permite almacenar pequeñas cantidades de información asociados con la tarjeta. Por ejemplo, a veces se utiliza en sistemas de transporte que utilizan RFID, para realizar un seguimiento del valor que queda en la tarjeta. Sin embargo, desde los sistemas de RFID en general, están conectados en red a una base de datos, es más común para almacenar un registro de datos indexada por el UID de la etiqueta en una base de datos remota, y almacenar toda la información acerca de la etiqueta en esa base de datos remota.

Figura 2.4 Estructura etiqueta RFID.

### 2.2.3 Clasificación

La tecnología de identificación por radiofrecuencia puede ser dividida principalmente en 3 categorías según el tipo de etiqueta:

1. Sistemas pasivos, en los cuales las etiquetas de RFID no cuentan con una fuente de poder. Su antena recibe la señal de radiofrecuencia enviada por el lector y almacena esta energía en un capacitor. La etiqueta utiliza esta energía para habilitar su circuito lógico y para regresar una señal al lector. Estas etiquetas pueden llegar a ser muy económicas y pequeñas, pero su rango de lectura es muy limitado.

2. Sistemas activos. Utilizan etiquetas con fuentes de poder integradas, como baterías. Este tipo de etiquetas integra una electrónica más sofisticada, lo que incrementa su capacidad de almacenamiento de datos, interfaces con sensores, funciones especializadas, además de que permiten que exista una mayor distancia entre lector y etiqueta (20m a 100m). Este tipo de etiquetas son más costosas y tienen un mayor tamaño. Pueden permanecer dormidas hasta que se encuentran dentro del rango de algún lector, o pueden estar haciendo broadcast constantemente.

3. Sistemas Semi-Activos. Emplean etiquetas que tienen una fuente de poder integrada, la cual energiza la etiqueta para su operación, sin embargo, para transmitir datos, una etiqueta semi-activa utiliza la potencia emitida por el lector. En este tipo de sistemas, el lector siempre inicia la comunicación. La ventaja de estas etiquetas es que al no necesitar la señal del lector para energizarse (a diferencia de las etiquetas pasivas), pueden ser leídas a mayores distancias, y como no necesita tiempo para energizarse, estas etiquetas pueden estar en el rango de lectura del lector por un tiempo substancialmente menor para una apropiada lectura. Esto permite obtener lecturas positivas de objetos moviéndose a altas velocidades.

Tanto las etiquetas activas como los pasivos pueden adicionalmente ser clasificados de la siguiente forma:

* Solo Lectura (RO)

En estos dispositivos, los datos son grabados en la etiqueta durante su fabricación, para esto, los fusibles en el microchip de la etiqueta son quemados permanentemente utilizando un haz láser muy fino. Después de esto, los datos no podrán ser reescritos. Este tipo de tecnología se utiliza en pequeñas aplicaciones, pero resulta poco práctico para la mayoría de aplicaciones más grandes, que intentan explotar todas las bondades de RFID.

* Una Escritura, Muchas Lecturas (WORM)

Una etiqueta WORM, puede ser programado sólo una vez, pero esta escritura generalmente no es realizada por el fabricante sino por el usuario justo en el momento que la etiqueta es creada. Este tipo de etiquetas puede utilizarse en conjunto con las impresoras de RFID, las cuales escriben la información requerida en él.

* Lectura y Escritura (RW)

Estas etiquetas, pueden ser reprogramadas muchas veces, típicamente este número varía entre 10,000 y 100,000 veces, incluso mayores. Esta opción de reescritura ofrece muchas ventajas, ya que la etiqueta puede ser escrito por el lector, e inclusive por sí mismo en el caso de los tags activos. Estas etiquetas regularmente contienen una memoria Flash o FRAM para almacenar los datos.

### 2.2.4 Regulación y estandarización

Las etiquetas RFID de baja frecuencia (LF: 125 - 134 kHz y 140 - 148.5 kHz) y de alta frecuencia (HF: 13.56 MHz) se pueden utilizar de forma global sin necesidad de licencia. La frecuencia ultra alta (UHF: 868 - 928 MHz) no puede ser utilizada de forma global, ya que no hay un único estándar global. En Norteamérica, la frecuencia ultra elevada se puede utilizar sin licencia para frecuencias entre 908 - 928 MHz, pero hay restricciones en la energía de transmisión. En Europa la frecuencia ultra elevada está bajo consideración para 865.6 - 867.6 MHz. Su uso es sin licencia sólo para el rango de 869.40 - 869.65 MHz, pero existen restricciones en la energía de transmisión. El estándar UHF norteamericano (908-928 MHz) no es aceptado en Francia ya que interfiere con sus bandas militares. En China y Japón no hay regulación para el uso de la frecuencia ultra elevada. Cada aplicación de frecuencia ultra elevada en estos países necesita de una licencia, que debe ser solicitada a las autoridades locales, y puede ser revocada. En Australia y Nueva Zelanda, el rango es de 918 - 926 MHz para uso sin licencia, pero hay restricciones en la energía de transmisión.

Contrariamente a la creencia popular, no existe un protocolo RFID universal para esta tecnología. Hay docenas. Los estándares de RFID desarrollado por la Organización Internacional de Estándares (ISO), en conjunción con los principales participantes en el mercado. ISO funciona como un órgano de mediación para ayudar a los competidores en muchas industrias diferentes a desarrollar estándares interoperables de modo que incluso cuando compiten, sus tecnologías pueden a veces trabajar juntas. Los diferentes estándares de RFID definen las frecuencias de radio utilizado, las velocidades de transferencia de datos, los formatos de datos, entre otros parámetros. Por ejemplo, la norma ISO-11784 fue originalmente desarrollada para el rastreo de animales. Se opera en las frecuencias comprendidas entre 129 y 139.4 kHz, y su formato de datos incluye campos adecuados para la descripción de los animales para ser rastreado. También se puede encontrar lectores con el protocolo EM4100 y etiquetas que operan en el 125kHz distancia. Estos se utilizan a menudo como tarjetas de proximidad, y cuentan con una información muy limitada en su protocolo de datos, por lo general sólo un UID. Las normas ISO-14443 se desarrollaron para utilizar con los sistemas de pago y tarjetas inteligentes. Estas operan a 13,56 MHz. Incluyen características en su formato de datos para aumentar o disminuir los valores y para la codificación de datos.

## 2.3. Biometría

La biometría es la aplicación de las matemáticas y la ciencia de la computación para identificar individuos de acuerdo con sus características o rasgos físicos. La palabra biometría deriva del griego bios (que quiere decir vida) y metria (que quiere decir medida). Los rasgos biométricos son medidas extraídas del cuerpo humano vivo. Y, además, todos los rasgos biométricos son una combinación de anatomía y de comportamiento.

La biometría se está convirtiendo en un factor esencial para la identificación eficaz de las personas. Esto se debe a que los rasgos biométricos no se pueden compartir o extraviar y representan intrínsecamente las formas corporales del individuo que identifica. Reconocer a una persona por su cuerpo y después enlazar este cuerpo con una identidad establecida externamente forma una herramienta muy poderosa para la gestión de la identidad con unas consecuencias potenciales enormes, tanto positivas como negativas. En consecuencia, la biometría no es solo un problema fascinante en el campo de la investigación dedicado al reconocimiento de patrones, sino una tecnología que, usada correctamente, puede permitir una sociedad más segura, reducir el fraude y proveer interfaces persona-máquina fáciles de usar.

El reconocimiento biométrico se refiere al uso de diferentes características anatómicas (como huellas dactilares, cara o iris) y de comportamiento (como habla, firma o teclear). Estas características se denominan identificadores biométricos o rasgos biométricos y sirven para reconocer automáticamente a los individuos.

A continuación enumeramos los rasgos biométricos más utilizados, comentando aspectos sobre su calidad y uso:

• **Huellas dactilares**. El uso de las huellas dactilares como medio de identificación es de alta fiabilidad. Tiene buena aceptación y popularidad.

• **Ojo**. La identificación de un individuo a través del análisis del iris tiene una fiabilidad muy alta. El problema es la facilidad de uso. El análisis de la retina para identificar al individuo es más complejo todavía.

• **Forma de la mano**. Este sistema está bastante extendido, pero quizás presenta un poco menos de fiabilidad que los anteriores. Este sistema es susceptible de padecer ataques, puesto que no resultaría difícil recrear la forma de una mano usando un molde.

• **Cara**. El análisis de la cara, ya sea en 2D o 3D, es un buen medio para identificar a un individuo. Aun así, siempre es preferible un estudio 3D, ya que se mejoran los resultados con respecto el mero estudio de una imagen 2D, y se dificulta el éxito de ataques. La desventaja de los equipos 2D es que el sistema no distingue si lo que está capturando es realmente un rostro o una fotografía de un rostro.

• **Venas del dedo o la mano**. El estudio vascular de los dedos o de la mano proporciona alta fiabilidad, además no es muy complejo su análisis.

• **Voz**. Este sistema presenta bastante fiabilidad, pero también es susceptible a los ataques. Además este sistema padece de poca estabilidad, con lo cual deberían ser varias la toma de voces analizadas para reducir la tasa de errores.

Claramente, son varias las características biométricas que pueden usarse para identificar o autenticar. Estas pueden usarse individualmente o bien en combinación entre ellas, o bien procediendo a la autenticación mediante información adicional, como podría ser una contraseña.

### 2.3.1. Sistemas biométricos

En función del contexto de la aplicación biométrica, podemos diferenciar dos tipos de sistemas, los sistemas de verificación y los sistemas de identificación.

Los sistemas de verificación (también llamados de autentificación) autentifican la identificación de la persona mediante la comparación del rasgo biométrico acabado de capturar con el rasgo biométrico que el sistema ha capturado antes en el proceso de inscripción al sistema.

El usuario tiene que presentar su identificación mediante un carné o clave secreta. El sistema realiza una única comparación entre el rasgo biométrico que el usuario acaba de presentar con el rasgo biométrico que hay en la base de datos con la misma identificación presentada. La salida de un sistema de verificación es normalmente binaria: es la misma persona si los rasgos biométricos coinciden (son muy similares) o son dos personas diferentes en otro caso. En algunos casos, los rasgos biométricos y la identificación de la base de datos están en la propia tarjeta del usuario en forma encriptada. En este caso, se dice que disponemos de una base de datos distribuida entre todas las tarjetas de los usuarios.

Los sistemas de identificación reconocen a la persona a través de la busca del rasgo biométrico que más se asemeja al usado para identificarlo en toda una base de datos.

El usuario no aporta ninguna información de su identificación, como era el caso del sistema de verificación. El sistema lleva a cabo una comparación uno a muchos. Esto quiere decir que el rasgo biométrico del usuario desconocido se compara con muchos rasgos biométricos de una base de datos. Hay varias salidas a este sistema. La más sencilla es devolver el nombre de la persona (identificador) cuyo rasgo biométrico se asemeja al introducido. Otra posibilidad es deducir que este rasgo biométrico no pertenece a ninguna persona de la base de datos (este caso se da cuando las distancias del rasgo biométrico con todos los rasgos biométricos de la base de datos es superior a un umbral). Finalmente, y es el caso más usual en las aplicaciones forenses, el sistema no devuelve una sola persona sino una lista de candidatos. Es decir, devuelve las personas cuya distancia de sus rasgos biométricos con el rasgo biométrico introducido es inferior a un umbral.

Tanto los sistemas de verificación como de identificación necesitan un proceso previo llamado sistema de matriculación[[4]](#footnote-4). Este proceso se encarga de recoger el rasgo biométrico (o los rasgos biométricos) junto con la identificación de la persona. Este proceso es muy importante puesto que se encarga de relacionar la identificación de la persona con el rasgo biométrico. Normalmente, este proceso tiene lugar ante una persona autorizada que vela por la veracidad de los datos que aporta el usuario (carné de identidad, pasaporte) y controla que realmente sea este usuario el que presenta el rasgo biométrico al sistema. Además, durante el proceso de matriculado, esta persona verifica la calidad de los datos biométricos obtenidos. Si considera que los datos no tienen suficiente calidad, pide al usuario que vuelva a presentar el rasgo biométrico (huella dactilar, cara, iris) al sistema.

Es fundamental que los datos que se almacenan en la base de datos tengan la máxima calidad puesto que en los procesos de identificación o verificación no siempre se puede garantizar esta calidad. Algunos sistemas piden al usuario capturar varias veces el mismo rasgo biométrico (normalmente tres veces). El sistema puede elegir la mejor imagen o fusionarlas y así reducir los errores de captura.

Los tres sistemas antes mencionados usan los procesos siguientes (ver la figura 2.5):

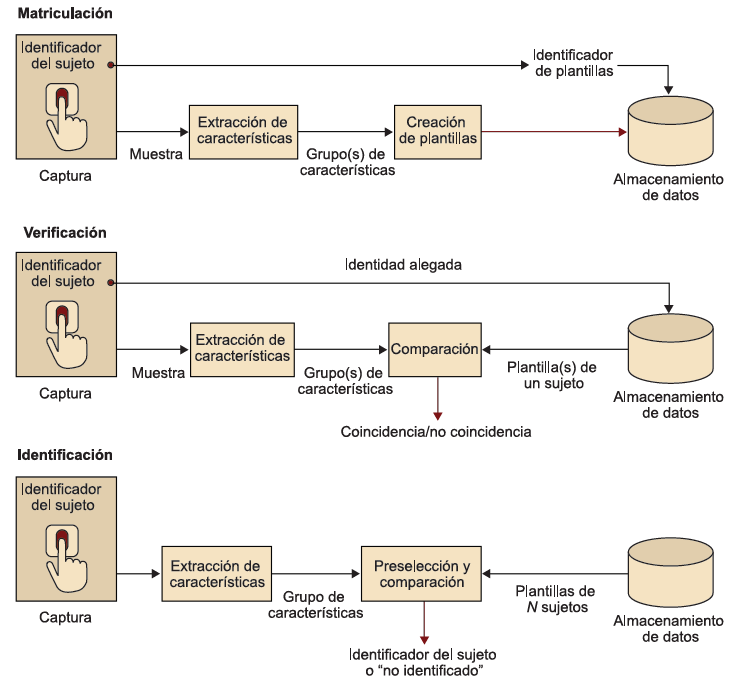


Figura 2.5. Etapas o procesos que componen los sistemas: a. matriculación; b. verificación; c. identificación.

• Captura: La representación digital del rasgo biométrico tiene que ser capturada. El sensor biométrico es usualmente un sistema para capturar una imagen (excepto la identificación del hablador, que es una máquina de grabar voz). Normalmente, la información capturada se denomina muestra[[5]](#footnote-5). A veces, el sistema de captura también incorpora otros periféricos para introducir información no biométrica o mostrar información.

• Extracción de las características: Con el objetivo de facilitar la comparación, aumentar la información y reducir el ruido, la representación original digital (imagen digital) se procesa normalmente con un extractor de características para generar una representación compacta y más identificadora llamada registro de identificación[[6]](#footnote-6) o conjunto de características[[7]](#footnote-7).

• Creación de la plantilla: La plantilla[[8]](#footnote-8) es una forma compacta de representar un conjunto de muestras de una sola característica biométrica (por ejemplo, se puede crear una plantilla de dieciséis muestras diferentes de la imagen de la cara de una misma persona). El proceso de creación de la plantilla recibe como entrada los registros de identificación y crea una información más compacta donde se intenta extraer la información que persiste en todas las muestras puesto que se consideran los rasgos característicos.

En algunos casos, esta plantilla está formada por una única muestra y por lo tanto se puede representar como un registro de identificación.

• Comparación: El proceso de comparación recibe como entrada un registro de identificación y una plantilla y calcula una distancia entre los dos. A veces, en lugar de una distancia obtiene una probabilidad de que representen un mismo individuo. En el proceso de verificación, hay un umbral interno al sistema que solo lo puede modificar el administrador del sistema. Si la distancia es inferior al umbral (o la probabilidad es superior al umbral), el sistema considera que los dos datos provienen de la misma persona, de lo contrario, se considera que provienen de dos personas diferentes.

• Selección o filtrado: En los sistemas de identificación con muchos datos (podemos hablar de 50 millones de huellas dactilares), el filtrado es un método para aumentar el tiempo de respuesta del sistema. Con técnicas típicas de las bases de datos, logran no tener que explorar la base de datos entera y así ganar tiempo.

• Almacenamiento de los datos: Es el proceso para almacenar la información del usuario. Esta información está compuesta por un identificador único (por ejemplo, el número del DNI o del pasaporte), la plantilla biométrica y otros datos (por ejemplo, la dirección o la profesión). En función de la aplicación, los datos se almacenan en sistemas de almacenamiento centralizados (para poder llevar a cabo la identificación) o en tarjetas inteligentes[[9]](#footnote-9) (para poder llevar a cabo la verificación). Además, se aplican técnicas de encriptación con todos los datos para que así el registro formado por el número del DNI más los rasgos biométricos sea indivisible.

Dependiendo del dominio de la aplicación, un sistema biométrico puede operar como un sistema en línea o como un sistema fuera de línea.

a) Los sistemas en línea requieren que la comparación se lleve a cabo rápidamente y se requiere una respuesta inmediata, por ejemplo es el caso del permiso para iniciar una aplicación o la entrada física de una persona a unas instalaciones. Normalmente, son sistemas de verificación.

b) Los sistemas fuera de línea no requieren que la respuesta sea inmediata y se tolera que haya un admisible retraso en la respuesta. Normalmente, son sistemas de identificación. Los sistemas en línea suelen ser completamente automáticos, requieren que el rasgo biométrico sea capturado con un sensor electrónico y no hay control humano de la calidad de los datos. Por otro lado, los sistemas fuera de línea son usualmente semiautomáticos. La captura del rasgo biométrico puede haber sido con un sistema no electrónico (por ejemplo, la captura de una huella dactilar dejada en la escena de un crimen) y hay un control de la calidad de los datos por parte de un especialista. Además, este especialista dispone de herramientas informáticas para arreglar los datos o ayudar al programa a que lleva a cabo la comparación biométrica.

Dependiendo de la aplicación, se llevan a cabo dos tipos de buscas en los sistemas de identificación, que son las buscas positivas y las buscas negativas:

a) Las buscas positivas son aquellas por las que queremos comprobar si aquel rasgo biométrico se encuentra en la base de datos, es decir, si el usuario ha sido matriculado. Deseamos saber la identificación de aquel rasgo biométrico. El caso más típico es introducir en el sistema una huella dactilar que hemos encontrado en una escena de un crimen o una cara que hemos podido fotografiar y queremos saber a quién pertenece.

b) Por otro lado, las buscas negativas son aquellas por las que queremos comprobar que aquel individuo no se ha matriculado. Deseamos saber que no hay ninguna persona matriculada con aquellos rasgos biométricos. La aplicación más usual es asegurarse de que una persona no quiere usar más de una vez un servicio que solo tiene derecho a usar una sola vez, como, por ejemplo, no cobrar varias veces una ayuda estatal o no votar varias veces en unas elecciones.

### 2.3.2. Lector huella digital

Los seres humanos tienen tarjetas de identificaron integradas, muy fácilmente accesibles, las cuales son diseños virtualmente únicos. Estas son diminutos “Valles y crestas” de piel en la punta de los dedos, en la figura 2.6 se muestra la imagen generada por un lector biométrico. Estas se forman por una combinación de factores genéticos y ambientales aleatorios, por lo que es única para cada persona.



Figura 2.6 Imagen capturada por un sensor biométrico.

Un lector de huellas dactilares es un dispositivo de [hardware](http://www.alegsa.com.ar/Dic/hardware.php) que permite escanear o leer una huella digital de un ser humano con el fin de identificarlo.

El funcionamiento de un lector de huella digital cumple dos tareas principales:

* Obtener una imagen de la huella digital.
* Comprar el patrón de valle y cresta de dicha imagen con los patrones de las huellas que tiene almacenadas.

El uso más típico de un lector de huellas dactilares es la [autentificación](http://www.alegsa.com.ar/Dic/autentificacion.php) de un [usuario](http://www.alegsa.com.ar/Dic/usuario.php) para permitirle o no el acceso a un dispositivo o servicio. También se incluyen en cerraduras para abrir puertas o para control de entrada-salida de personas de una empresa.

Hay 2 tipos de tecnología empleadas para estos dispositivos:

Lector óptico: esta tecnología utiliza diminutos [diodos](http://www.informaticamoderna.com/Electricidad_y_computadoras.htm#elem) que emiten luz, integrados en un sensor denominado CCD (Charged Coupled Device), el cuál detecta los relieves por medio de sombras e iluminación de la superficie del dedo, posteriormente forma un mapa digital con la información y determina que tenga la iluminación correcta y una vez realizada esta verificación, esta puede ser enviada a la computadora para su almacenamiento, de lo contrario seguirá creando la imagen digital. En la figura 2.7 se observa el método de lectura de un sensor óptico.

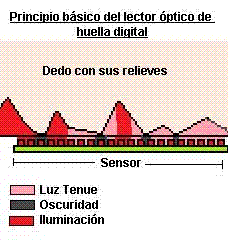


Figura 2.7. Método de lectura de huella digital óptico.

Lector capacitivo: esta tecnología utiliza diminutos [capacitores](http://www.informaticamoderna.com/Electricidad_y_computadoras.htm), los cuáles se cargan con diferentes cantidades de corriente de acuerdo a la posición de los relieves del dedo, de este modo crea un mapa digital con la información y no es necesario verificarla, sino que se envía de manera inmediata a la computadora, siendo una tecnología más fiable y veloz. En la figura 2.8 se observa el principio de funcionamiento del lector capacitivo de huella digital.

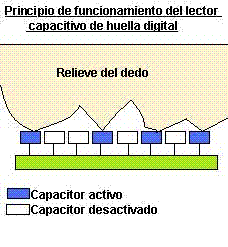


Figura 2.8. Método de lectura de huella digital capacitivo.

En general existen distintos problemas a los que hacer frente. El primero es el de la recogida de características: los sistemas deben obviar ruidos, imperfecciones o distintos matices que los sistemas captadores y sensores recogen a cada acceso de un individuo. En segundo lugar, se deben minimizar las tasas de errores del sistema de identificación: no se debe permitir la autenticación de un individuo no registrado o no válido y, al contrario, no se debe denegar la correcta autenticación de un individuo registrado o válido.

**CAPITÚLO**

# DISEÑO SISTEMA DE CONTROL DE ACCESO

El sistema de control de acceso consiste en controlar el acceso a un lugar físico determinado, el principal desafío es desarrollar un módulo electrónico con la tecnología para autentificar a los usuarios, a través de tres medios diferentes; contraseña, huella dactilar y etiquetas RFID. En el capítulo 1 se seleccionó un modelo para el hardware del sistema de control de acceso y este está compuesto por dos dispositivos diferentes.

El primer dispositivo corresponde al módulo de control de acceso, este comanda los sensores que interactúan con los usuarios, encargado de realizar los procesos de matriculación, verificación e identificación de los usuarios.

El segundo hardware corresponde a la computadora (Raspberry Pi), cumple la función de servidor y administra toda la información de la plataforma web, almacena los registros de los usuarios, permite el acceso a estos, contiene los historiales de acceso, etc. Este hardware integra un circuito con un reloj de tiempo real, para llevar el control del tiempo del servidor y un relé para el control del actuador de la puerta.

Este último funciona como un controlador maestro, está siempre recibiendo información del módulo de control de acceso, y cu7

ando recibe una petición de un usuario este gestiona la información y envía una respuesta de vuelta

.

Este hardware es gerenciado por un controlador maestro (Raspberry Pi) a través de un puerto serial (ver figura 1.4).



Figura 1.4 Arquitectura módulo control de acceso, modelo 3.

### Justificación del modelo seleccionado

Los modelos planteados del hardware para el módulo de control de acceso utilizan como controlador principal un microcontrolador o un computador de placa reducida (Raspberry Pi), en la tabla 1.1 se pueden observar las principales características de cada controlador.

La Raspberry Pi es 75 veces más rápido que el microcontrolador y tiene 125.000 veces más de memoria RAM. La Raspberry Pi es una computadora independiente que puede ejecutar un sistema operativo real en Linux. Puede realizar varias tareas, soportar cuatro puertos USB y puede conectarse de forma inalámbrica a Internet. En pocas palabras, es lo suficientemente potente como para funcionar como una computadora personal.

Puede sonar que Raspberry Pi es superior al microcontrolador, pero eso es sólo cuando se trata de aplicaciones de software. Por otra parte el microcontrolador tiene la capacidad de trabajar con pines analógicos y en tiempo real, esta flexibilidad le permite trabajar con casi cualquier tipo de sensor o chip.

Raspberry Pi puede procesar varias tareas, éste puede ejecutar múltiples programas en segundo plano mientras está activado. Por ejemplo, puede estar funcionando como un servidor y transmitiendo información por un puerto USB.

El modelo seleccionado es el número 3, en este modelo se aprovecha las ventajas de usar el microcontrolador y la Raspberry Pi, el módulo de control de acceso es controlado por el microcontrolador, es el encargado de gestionar la parte sensorial, el usuario interactúa con este módulo por medio de una pantalla LCD y un teclado matricial, en este dispositivo se realizan los procesos de matriculación, verificación e identificación de los usuarios. Cada vez que el usuario interactúa con este módulo se envía una petición a la Raspberry Pi, este procesa la información, y envía una respuesta.

La Raspberry Pi es el controlador principal del *sistema de control de acceso*, este aloja la plataforma web y almacena la información del sistema, tiene la capacidad de ejecutar procesos diferentes para la gestión del módulo de control de acceso, por lo que este sistema funcionara en tiempo real, además este integra los adaptadores de red ethernet y wifi de fácil configuración.

El módulo de control de acceso es instalado al exterior del lugar a controlar, y la Raspberry Pi se encuentra en el interior (ver figura 1.5), dando más seguridad e independencia al sistema, los usuarios que interfieran con el módulo exterior no podrán tener acceso a la información del sistema, ni manipular el actuador para la apertura de la puerta.

1. Es una red que conecta los ordenadores en un área relativamente pequeña. [↑](#footnote-ref-1)
2. Es una red de gran cobertura en la cual pueden transmitirse datos a larga distancia. [↑](#footnote-ref-2)
3. Circuito integrado programable, capaz de ejecutar las órdenes grabadas en su memoria. [↑](#footnote-ref-3)
4. Enrollment, en la bibliografía inglesa. [↑](#footnote-ref-4)
5. En inglés, Sample. [↑](#footnote-ref-5)
6. En inglés, Identification register. [↑](#footnote-ref-6)
7. En inglés, Feature set. [↑](#footnote-ref-7)
8. En inglés, Template. [↑](#footnote-ref-8)
9. En inglés, smart cards. [↑](#footnote-ref-9)