Universidad Nacional Autónoma de México

Facultad de Ingeniería

SISTEMA DE SEGURIDAD PARA ESTACIONAMIENTOS

TESIS

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACIÓN

PRESENTAN:

ARMANDO GÓMEZ BOLAÑOS

MARTIN GÓMEZ JAIME

DIRECTORA DE TESIS:

MA. JAQUELINA LÓPEZ BARRIENTOS

Mexico, D.F. **2015**

Dedicatorias

Dedico esta Tesis principalmente a mi madre quien me apoyo en todo momento, por todos los medios a su alcance y de manera incondicional para que lograra realizarme profesionalmente, mis logros son tuyos también.

A mi padre y hermanos, por demostrarme con su ejemplo a persistir a pesar de las dificultades a las que me enfrenté durante el largo camino recorrido y enseñarme que nunca es tarde para alcanzar los objetivos propuestos.

A mis amigos quienes fueron un soporte emocional fundamental durante la carrera, Mariel, Martin, Edgar, Omar, Marco, Jorge, Miguel, Alexis y Axel.

A mis profesores, por tener la paciencia y el empeño para transmitir sus conocimientos y enseñarnos a aprender.

A la UNAM por dejarme ser parte de su gran familia que la hace ser hoy en día una de las mejores universidades a nivel mundial.

Y finalmente, pero no por ello menos importante, a la profesora Jaquelina por asesorarnos y alentarnos a cerrar un ciclo, por su ecuanimidad e inagotable buen humor, por su asesoría siempre puntual, y su grandísima paciencia.

A todos ellos, Muchas Gracias.

Armando Gómez Bolaños

Dedico esta Tesis a mis padres, que siempre me han dado lo mejor de ellos y me impulsan con su esfuerzo todos los días a ser una mejor persona.

A mis hermanos que son mis mejores amigos, el mejor regalo que me han dado mis padres y mi apoyo incondicional cuando tengo dificultades.

A cada uno de mis maestros que me han compartido su conocimiento, su tiempo y sus experiencias. Gracias por su paciencia.

Un agradecimiento especial a la profesora Jaquelina porque creyó en este proyecto, nos animó siempre para por fin concluirlo y estuvo ahí para escucharnos, resolver nuestras dudas, guiarnos.

A Dios que ha puesto a las personas correctas en mi camino y son pieza importante cada vez que cumplo uno de mis sueños.

Muchas Gracias

Martin Gómez Jaime

Índice de Figuras

Índice de tablas

Índice General

Introducción

En México la delincuencia es un problema que aumenta todos los días y se ha salido del control a las autoridades. Los delitos que más se cometen son robo, secuestro y homicidio relacionado muchas veces al narcotráfico que se extiende por varias zonas de la república.

Entre los delitos más comunes en nuestro país y sobre todo en nuestra ciudad se encuentra el robo de vehículos, el cual mantiene cifras altas desde el año 2003. Según cifras de la **Asociación Mexicana de Instituciones de Seguros (AMIS)** en 2011 se alcanzó la máxima cantidad de vehículos hurtados por los delincuentes, con 84,444 unidades. En el período de julio de 2010 a julio de 2011 de los 84,444 vehículos robados, el 47% se encontraban estacionados.

De julio del 2012 a junio del 2013 se robaron en el país 71 mil 565 vehículos asegurados; la AMIS reveló que en los últimos 12 meses, el robo de vehículos asegurados en el país presentó una tendencia a la baja, sin embargo, en algunos estados de la república, como el Estado de México presentó un incremento del 16% con 22 mil 130 vehículos robados. En el Estado de Nuevo León son tres mil 859 unidades robadas, Jalisco con 7 mil 811 autos, Chihuahua con 2 mil 372 y Sinaloa 3 mil 410 unidades. Además en lo referente a los niveles de recuperación el Estado de México llegó a 26%, Jalisco con 35%, Sinaloa con 36%, en el DF la recuperación disminuyó en el último año de 52% al 49%, esto representa un semáforo rojo y se deberán tomar cartas en el asunto declaro Ricardo Arias Titular de la AMIS.

En un país con un alto índice de robos, es difícil mantener un automóvil 100% seguro, presenta un riesgo estacionarlo en la calle, a unos cuantos pasos de la casa u oficina o incluso dentro de un estacionamiento.

Muchos de los estacionamientos de las oficinas o unidades habitacionales no cuentan con un control de acceso y un registro completo de los carros que entran y salen del mismo. La vigilancia particular debe ocuparse del control de acceso del personal y

de los automóviles, que no siempre cuenta con sistemas y mecanismos automatizados que permitan brindar una plena atención y un servicio expedito, ocasionando con ello pérdida de tiempo en el reconocimiento de personas y automóviles.

Como se observa es necesario contar con sistemas de seguridad y control de acceso en estacionamientos controlados mediante el uso de tecnología a fin de reducir el número de autos robados en el país mientras se encuentran estacionados

Objetivo del Proyecto

Crear un Sistema de Seguridad Automatizado para un estacionamiento, con el fin de reducir el índice de robo de autos en nuestro país, así como contar con la ventaja de la agilización de entrada y salida de los autos al estacionamiento.

En el primer capítulo se hace un análisis de los sistemas de seguridad más utilizados actualmente en nuestro país, se plantea a su vez el uso de nuevas tecnologías para robustecer la seguridad en los estacionamientos y evitar así el robo de vehículos.

En el segundo capítulo se hace una investigación de la tecnología RFID, y se menciona el RFID que se utilizará para el desarrollo de una maqueta que muestre el funcionamiento real del sistema de seguridad.

En el tercer capítulo se realiza una investigación de los sistemas de biometría existentes en el mercado y se selecciona uno de ellos para la implementación de la maqueta.

En el cuarto capítulo se definen algunos conceptos de las herramientas de software utilizadas y de la metodología de trabajo para el desarrollo del sistema de seguridad.

En el quinto capítulo se explica cómo realizar la integración de los elementos que conforman el sistema de seguridad para su funcionamiento esencial.

Capítulo 1

Antecedentes Históricos

1.1.-Robos de automóviles en México

Para la mayoría de los mexicanos la adquisición de un automóvil representa años de trabajo, esfuerzo y ahorro, sobre todo hoy en día que la situación económica del país se encuentra tan deteriorada. Para muchas de las familias el adquirir un automóvil es un sueño hecho realidad, lamentablemente la ola de violencia y la delincuencia en el país ha disparado gravemente el número de autos robados con o sin violencia en algunas ciudades de México. La AMIS (Asociación Mexicana de Instituciones de Seguros) periódicamente da a conocer cifras impresionantes en sus comunicados del robo de autos que están asegurados, las cifras son alarmantes y desgraciadamente estas cifras únicamente toman en cuenta a los automóviles que cuentan con un seguro, hoy en día en el país solamente el 27% de autos cuenta con seguro, de un total de 27.8 millones. Como podemos ver en la (*Figura 1.1*), según los datos de la AMIS, el número de autos asegurados robados a nivel nacional en el periodo julio 2010-junio 2011 alcanzó la cifra de 84,444 unidades, lo que representa un incremento del 11% con respecto a las cifras de 2009-2010.

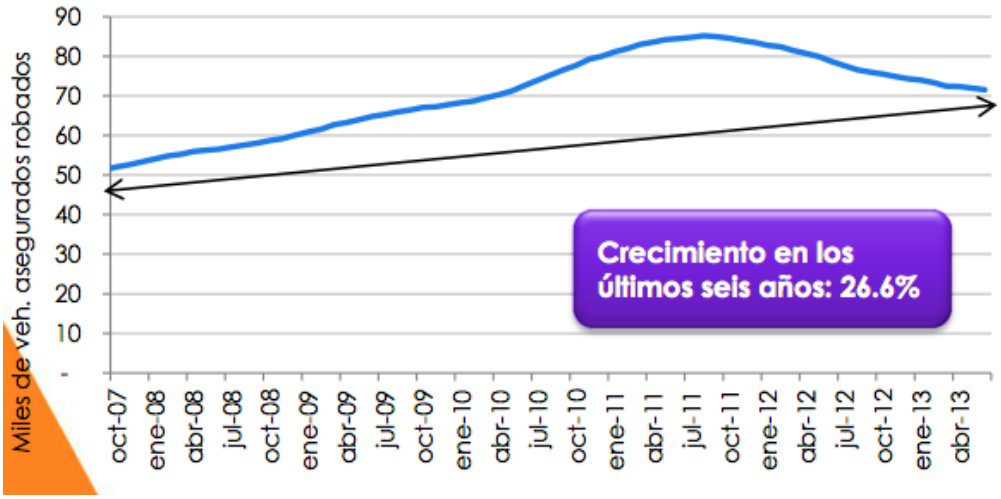


Figura 1.1. Robo de vehículos asegurados con cifras anualizadas en cada mes. Julio 2007 –Junio 2013

Afortunadamente la tendencia de robo vehicular de 2011 a la fecha va a la baja en la mayoría de las ciudades de México, Aun así hay mucho por hacer ya que el número

de vehículos robados sigue siendo alto. En un artículo recientemente publicado por el diario *La Jornada* del 1 de agosto del 2013 afirma que la recuperación de autos robados que están asegurados se ha "estancado" en el país e incluso durante el último año bajó uno por ciento al pasar de 45 a 44 por unidades por cada centenar cuando debería superar 50 por ciento, advirtió Recaredo Arias, director de la Asociación Mexicana de Instituciones de Seguros (AMIS), en conferencia de prensa. Calificó de "preocupante" tal tendencia a la baja y destacó que del primero de julio de 2012 al 30 de junio de 2013, este índice cayó 2.9 por ciento en el Distrito Federal al pasar de 52 a 49 unidades recuperadas. La capital presentó mejores cifras que en otras entidades y en el estado de México, dijo, "es bajísima" ya que sólo se recuperaron 26 vehículos de cada cien, en Jalisco 35 y en Sinaloa 36. Por arriba del DF, en Chihuahua y Nuevo León se recuperaron 58 y 93 por ciento de vehículos robados, respectivamente. (*Figura 1.2*).

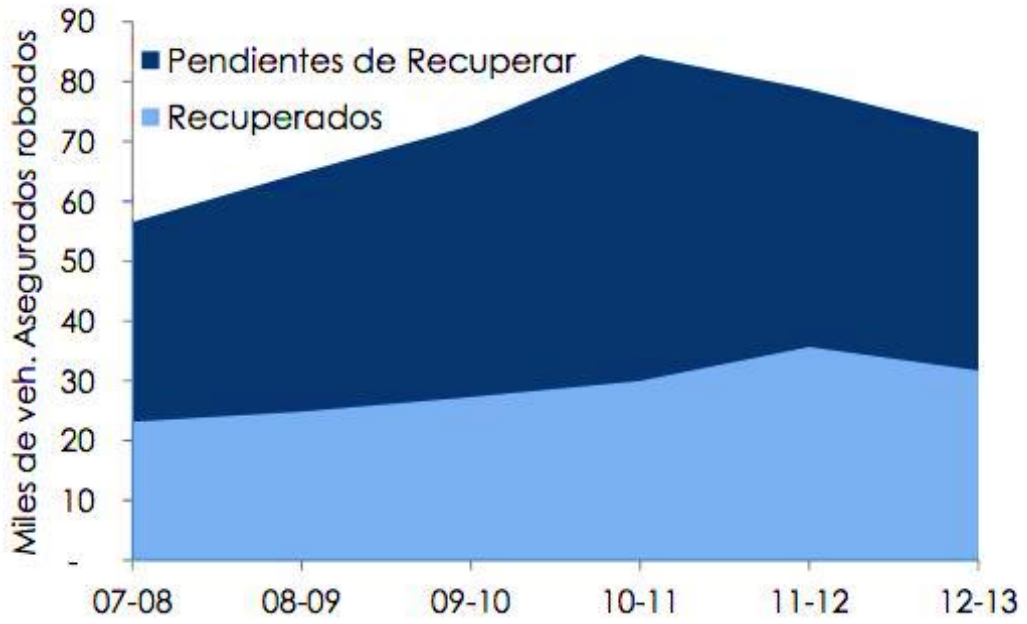


Figura 1.2. Vehículos asegurados robados recuperados y pendientes por recuperar

En un país con un alto índice de robos, es difícil mantener un automóvil 100% seguro, presenta un riesgo estacionarlo en la calle, a unos cuantos pasos de la casa u oficina o incluso dentro de un estacionamiento ya sea este público o incluso privado.

El robo con violencia ha presentado también un aumento del 4% en 2013 con respecto a 2012 según las estadísticas de la AMIS. El robo de autos estacionados representa el 43% del total de los robos en 2013, casi la mitad, como se observa en la (*Figura 1.3*). Esto quiere decir que de los 71,600 autos robados en 2013 aproximadamente 30,800 se encontraban estacionados, mientras que 40,800 fueron robados haciendo uso de la violencia.

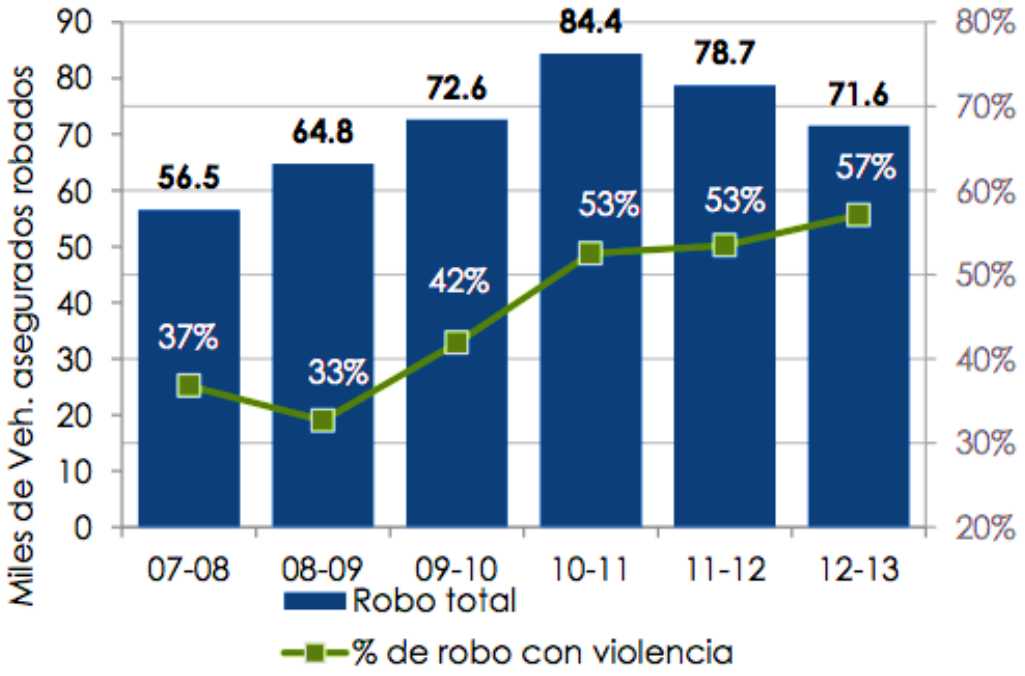


Figura 1.3. Porcentaje de robo con violencia de vehículos asegurados a nivel nacional a julio-junio en cada periodo

Como se aprecia en las gráficas anteriores a pesar de que el robo vehicular ha ido a la baja ligeramente, sigue siendo un problema muy grave, tan solo en el distrito federal ocupa el octavo lugar entre los 10 delitos más cometidos y en cerca de la mitad de las ocasiones el auto se encuentra estacionado.

1.2.-Fallas en los Sistemas de Seguridad en Estacionamientos

Actualmente es común encontrar estacionamientos de complejos empresariales, unidades habitacionales o centros comerciales donde no se tiene un control adecuado de los automóviles que salen y entran del mismo, se encuentran resguardados por personal que es contratado por una empresa, es decir, que el peso de la seguridad de los automóviles recae sobre un grupo de personas incluso ajenas a la empresa que presume resguardar el automóvil de sus empleados.

Dicho lo anterior se puede imaginar lo vulnerables que pueden llegar a ser los sistemas utilizados en la actualidad en los estacionamientos.

Fallas más comunes en los estacionamientos a cargo de personal:

- Si el personal del estacionamiento reconoce a la persona a la vista, no le pide una identificación para salir o entrar. Es muy común que el personal de vigilancia ceda el paso a quien de vista cree reconocer, pero como todas las personas, al final de una jornada de trabajo suelen tener errores debido al cansancio u otros factores que merman el desempeño del trabajador. En el caso del personal de vigilancia, el precio puede ser muy caro, tan caro como un automóvil.

- El personal puede ser sobornado para salir o entrar del estacionamiento. Cuántas veces no se ha sabido de casos en los que las propias autoridades tienen nexos con el crimen organizado y abusan de su poder como autoridad para cometer con mayor facilidad delitos en ocasiones muy bien remunerados, en la mayoría de los sistemas de seguridad el personal es el que tiene la mayor responsabilidad

sobre las acciones que realizan los sistemas electrónicos, esto representa una grave vulnerabilidad.

- Para evitar abrir y cerrar el portón o pluma el personal contratado deja abierto el acceso a altas horas de la noche. En ocasiones cuando el vigilante necesita dejar su puesto por unos instantes, pero no es posible dejar esperando a los usuarios, lo más común es dejar libre el acceso, para que puedan entrar y salir sin mayor complicación, esta es otra de las prácticas más comunes en los estacionamientos de unidades habitacionales de nuestro país.

De acuerdo a las fallas más comunes, uno de los principales defectos de los sistemas de seguridad en los estacionamientos es la falta de una tecnología capaz de encargarse del control de acceso a los estacionamientos, y sobre todo que se realice de manera desatendida.

Sin embargo el creciente desarrollo de la tecnología ha llevado a que en muchos lugares se implementen nuevas herramientas para desempeñar de manera correcta la difícil labor de registrar la entrada y salida de los vehículos principalmente con el fin de cobrar las fracciones de tiempo que los autos hicieron uso del estacionamiento. A continuación se mostrarán algunas de las tecnologías más utilizadas como control de acceso en estacionamientos de nuestro país.

1.3.-Uso de la Tecnología en los Estacionamientos

En la actualidad se hace uso de tecnologías básicas de control de acceso en los estacionamientos del país.

Una de las más comunes en los centros comerciales son las máquinas expendedoras de boletos.

1.3.1.-Máquinas expendedoras de boletos

Este tipo de tecnología la podemos encontrar en la mayoría de los centros comerciales, se trata de una máquina que expide boletos a los usuarios cuando estos ingresan al estacionamiento (*Figura 1.4*).

En el boleto imprimen un código de barras, así como la hora y fecha en la que el vehículo ingresó.

Figura 1.4. Máquina expendedora de boletos

Al salir, el usuario debe ingresar el boleto en una máquina que se encarga de comparar la hora de entrada con la hora actual en ese momento, solicita al usuario que ingrese el dinero correspondiente y así realiza el cobro por el uso del estacionamiento de acuerdo a la tarifa preestablecida por hora en el centro comercial, por ultimo reimprime en el boleto para identificarlo como pagado. Cabe señalar que en el caso en el que algún usuario extravíe el boleto de estacionamiento deberá pagar una multa que va desde los 50 pesos a los 150 aproximadamente, una vez pagada la multa y acreditado la propiedad del automóvil el usuario puede salir del establecimiento.

No obstante, el uso de esta tecnología no ha sido pensado como método de seguridad para evitar el robo del vehículo, sino como una manera de calcular el costo del uso del estacionamiento, el cual está en función del tiempo que fue utilizado por el usuario.

1.3.2.-Cámaras de vigilancia

Las cámaras de vigilancia (*Figura 1.5*), son utilizadas en muchos establecimientos, combinándolos con las máquinas expendedoras de boletos, o simplemente como auxiliar del personal de vigilancia del estacionamiento. Generalmente se colocan a la altura del parabrisas de los autos que entran y salen del establecimiento, con el fin de grabar en video tanto las placas del auto como el rostro del conductor y de su acompañante en caso de existir. Dichas grabaciones pueden ser de gran utilidad ya que recopilan datos importantes y sin errores como por ejemplo: la fecha y hora en que el auto entró y salió del establecimiento, las placas del auto, la apariencia del conductor y del acompañante, así como sus movimientos al momento de entrar y salir del estacionamiento. Sin embargo, esto de ninguna manera impide que en un determinado momento el automóvil sea sustraído ilícitamente del estacionamiento, es decir, los datos que la grabación

colecciona simplemente nos sirven como apoyo en una investigación pericial que ayude a identificar a los actores del robo, así como la hora y demás datos relevantes, pero de ninguna forma ayuda a impedir que el robo se cometa.

Figura 1.5. Cámara de vigilancia

1.3.3.-Barreras

En la gran mayoría de los casos se hace uso de plumas (*Figura 1.6*), las cuales son un tipo de barrera que se interpone al paso del vehículo, este tipo de barreras es de las más comunes debido a su precio y su facilidad de uso, no obstante existen varios tipos, su principal diferencia radica en la resistencia al impacto que podrían recibir.

Figura 1.6. Pluma

Existe otro tipo de barreras más sofisticadas que brindan un mayor nivel de seguridad, de las cuales algunas son imposibles de violar sin que el automóvil sufra algún tipo de daño, como por ejemplo los topes poncha llantas (*Figura 1.7*), los cuales son topes con pequeñas puntas de acero retráctiles, capaces de ponchar las llantas de los autos si estos llegasen a pasar por encima de las puntas.

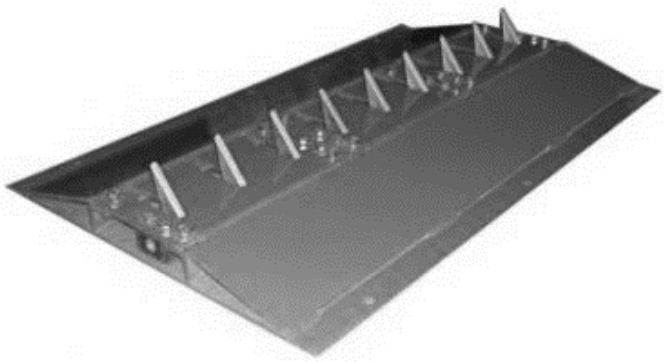


Figura 1.7. Tope poncha llantas

1.3.4.-RFID

Actualmente en algunos lugares del país se ha comenzado a utilizar la tecnología RFID. Esta tecnología se ha popularizado en las industrias para agilizar la recolección de datos de sus productos para su almacenamiento y distribución es decir, es de gran utilidad en la realización de los inventarios, sin embargo se limitará la información al uso que se les da en los estacionamientos, así como su principal objetivo que tienen en cada sistema implementado.

La empresa llamada ***ComercityUs*** ofrece sistemas para estacionamientos de paga, dichos sistemas ofrecen monitorear la entrada y salida de los vehículos, cobrar y registrar cargos de aparcado, si es el caso. Ofrecen llevar un registro de los autos que desean utilizar el estacionamiento por períodos de tiempo que van desde un día a semanas o meses. Ofrece de manera general la automatización en las siguientes tareas:

- Analizar los patrones de tráfico para maximizar el uso de las instalaciones.
- Aumentar la seguridad dentro de las instalaciones.
- Mejorar el manejo del personal durante los periodos de mayor actividad.
- Aliviar congestiones.
- Mejorar los servicios al cliente.

Otra empresa que brinda servicios para estacionamientos haciendo uso de la tecnología RFID es ***Sic Transcore***, una empresa Argentina presente en varios países de América Latina, especialista en estacionamientos de zonas residenciales.

Sus sistemas hacen uso de dispositivos RFID de largo alcance, las etiquetas RFID son colocadas en los parabrisas de los automóviles con acceso permitido al estacionamiento de la zona residencial, las antenas se encargan de reconocer el automóvil registrado y dejarlo entrar al estacionamiento, registrando hora y fecha de la acción, generalmente esta empresa hace uso de cámaras de vigilancia a la entrada y salida del estacionamiento, como un complemento para coleccionar mayor información de datos.

En México el robo de autos es un problema muy recurrente y nadie está exento de sufrir este tipo de delito, muchos de los estacionamientos de las oficinas o unidades habitacionales no cuentan con un control de acceso y un registro completo de los autos que entran y salen del mismo.

La vigilancia particular debe ocuparse del control de acceso del personal y de los automóviles, que no siempre cuenta con sistemas y mecanismos automatizados que permitan brindar una plena atención y un servicio expedito, ocasionando con ello pérdida de tiempo en el reconocimiento de personas y automóviles.

De manera que como se observa es necesario contar con sistemas de seguridad y control de acceso en estacionamientos controlados mediante el uso de tecnología a fin de reducir el número de autos robados en el país mientras se encuentran estacionados.

Unas de las tecnologías capaces de coadyuvar en la prevención de robos de autos de los estacionamientos y que se proponen combinar en el presente trabajo con el fin de aumentar en gran medida el nivel de seguridad en los estacionamientos del país son: la tecnología RFID, los lectores de huella digital y las barreras llamadas plumas.

Aunque en la actualidad en México la tecnología RFID sólo se utilice como método de cobranza en estacionamientos o como control de acceso de

mediana seguridad, en el presente trabajo se propone implementarlo con otro control de acceso muy conocido ya en muchas partes de nuestro país y con un nivel de seguridad muy alto, hablamos de los controles de acceso biométricos, en específico el lector de huella digital, el cual nos brindará un mayor nivel de seguridad, evitando así que el auto sea extraído del estacionamiento por una persona no autorizada. En los capítulos posteriores se dará una explicación detallada del funcionamiento de las tecnologías que se propone implementar en los estacionamientos del país.

Capítulo 2

Identificador por Radiofrecuencia (RFID)

2.1-Concepto de RFID

RFID es una valiosa herramienta tecnológica que ha apoyado mayormente a empresas debido a su virtud de obtener datos de manera rápida y a distancia. Esta tecnología mantiene la promesa de remplazar las técnicas existentes de identificación, como por ejemplo los códigos de barras. La RFID ofrece ventajas estratégicas para las empresas, ya que puede dar seguimiento a los productos de un inventario en la cadena de suministros de dicha empresa, así mismo tiene la capacidad de proveer visibilidad del tránsito en tiempo real (por sus siglas en inglés ITV In-Transit Visibility) y un monitoreo general de los activos de la empresa. Básicamente es un sistema de identificación de productos u objetos que puede servir tanto en sistemas de seguridad como en sistemas de inventarios en bodegas o cuestiones similares. Actualmente está comenzando a ser usado en nuestro país como método de cobro en casetas o como método de identificación personal en empresas.

A continuación se muestran los orígenes de esta tecnología.

2.2.-Surgimiento de RFID.

La RFID no es una tecnología nueva, se empezó a utilizar en la segunda guerra mundial, sin embargo se consideró una tecnología demasiado cara para fines comerciales. Esta primera versión de la tecnología RFID se denominó IFF (Identify Friend or Foe), con un dispositivo electrónico en un avión se podía distinguir desde tierra en una base militar si la aeronave era amiga o enemiga.

Los avances en las comunicaciones RF continuaron después de la segunda guerra mundial, durante las décadas de los años 50's y 60's como se describe en la Tabla 2.1. En la década de los 60's las pruebas de las aplicaciones fueron iniciadas, seguidas por el primer producto comercial, así, las compañías comenzaron a

investigar soluciones para sistemas antirrobo, las cuales revolucionaron la industria de los RFID.

El primer sistema RFID pasivo multibit funcional, con un rango de algunos metros, apareció a principios de los 70's y continuó su desarrollo en la década de los 80's.

Tabla 2.1. Evolución de la RFID

Década	Evento
1940's	Se Inventó un radar para identificación de aviones enemigos, se desarrolló en la segunda guerra mundial (1948) conocido como IFF.
1950's	Exploración temprana de la Tecnología RFID, experimentos en laboratorios.
1960's	Desarrollo de la teoría de RFID. Comienzo de pruebas de aplicaciones.
1970's	Explosión en el desarrollo de RFID. Primeras Implementaciones de RFID.
1980's	Las aplicaciones comerciales de RFID entran en auge.
1990's	Surgen estándares RFID forma parte de la vida cotidiana

Recientemente, RFID ha experimentado un crecimiento exponencial debido al desarrollo de los circuitos integrados, uso de radiofrecuencias, y un aumento en el interés de la industria comercial y gubernamental. Así pues, la primera década del siglo XXI vio el movimiento internacional hacia esta tecnología extendiendo en gran medida su adopción.

La industria de la distribución vio en esta tecnología un enorme potencial para mejorar la cadena de suministros, desde la fabricación hasta la venta. En 1999 se constituyó el Auto-ID center, formado por el MIT, Coca-Cola, Wal-Mart, Gillette y

Sun Microsystems entre otros. El centro cumplió uno de los principales objetivos por el que fue creado, la coordinación de definición de los estándares técnicos que rigen la tecnología RFID y posteriormente fue desmantelado en octubre de 2004.

Actualmente al hablar de RFID se hace referencia a un pequeño circuito, con una antena, que al recibir energía vía radio desde un emisor exterior responde con una señal, indicando su estado y posición, así como con un identificador del objeto.

Aunque RFID es ya una tecnología madura, su despegue en el mundo de la distribución está vinculado a la introducción del estándar de codificación EPC (Código Electrónico de Producto), que permite rastrear y trazar el recorrido de los productos a medida que éstos viajan entre todos los socios de una cadena de suministro.

2.3.-Funcionamiento

En un sistema RFID son requeridos cuatro componentes fundamentales para que la información viaje entre los dispositivos:

- Un trasponedor (comúnmente llamado tag o etiqueta) el cual es programado con información única que lo identifica.

- Un transceptor (comúnmente llamado lector) éste se encarga de llevar la información que recibe la antena desde la etiqueta y entregarla a un dispositivo el cual puede ser un equipo de cómputo.

- Una antena integrada al lector para comunicarse con el transponedor, la cual se conecta al lector comúnmente por medio de cable coaxial.

- Una interface lectora, o middleware, la cual se encarga de conducir la información de los elementos de hardware que conforma el RFID hacia las aplicaciones de software del cliente.

El funcionamiento de un sistema RFID es simple, consiste en la comunicación aérea entre una antena lectora y una receptora (etiqueta), a cierta frecuencia, de manera que al establecerse la comunicación es posible adquirir y dar cierto tratamiento a la información o datos transmitidos.

Por ahora nos concentraremos en una etiqueta RFID pasiva con el objetivo de explicar paso a paso cómo trabaja un sistema RFID (Figura 2.1).

1.-La etiqueta es activada cuando pasa a través de un campo de radiofrecuencia, el cual es generado por una antena conectada a un lector.

2.-La etiqueta envía una respuesta previamente programada.

3.-La antena que generó el campo de radio frecuencia y que está conectada al lector, detecta la respuesta.

4.-El lector envía los datos provenientes de la etiqueta hacia la interfaz lectora.

5.-La interfaz lectora envía la información a la aplicación correspondiente para que se le dé el trato adecuado.

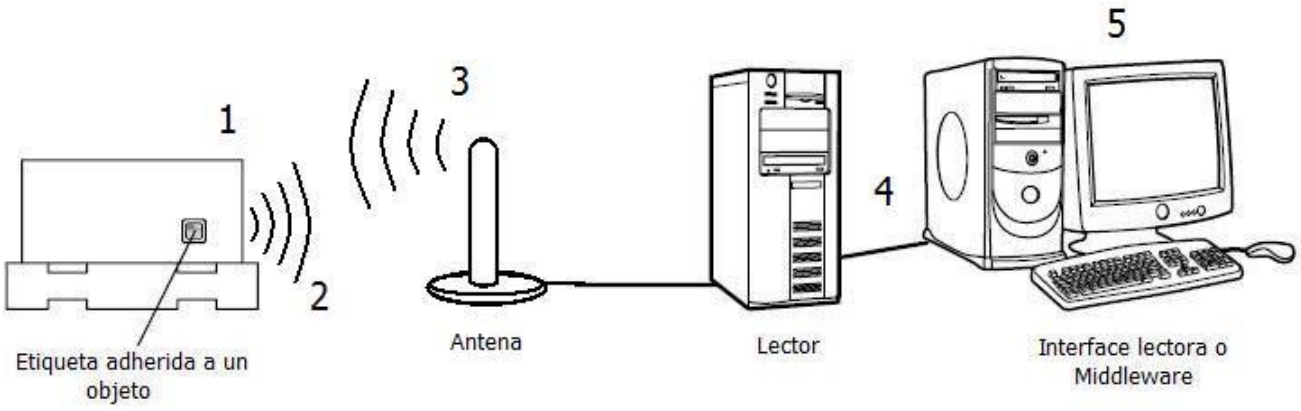


Figura 2.1. Esquema de funcionamiento

Ahora se detallará el funcionamiento de cada uno de los elementos que componen un sistema RFID, así como las diversas clasificaciones que existen para cada elemento.

2.4.-Elementos de RFID

Los dispositivos de hardware con los que cuenta todo sistema RFID está compuesto por etiquetas, lectores y antenas sin embargo es necesario precisar y conocer los diferentes tipos de etiquetas, lectores y antenas que existen así como sus principales características a fin de determinar el uso de aquellos que correspondan a las necesidades de la aplicación a implementar.

2.4.1.-Etiquetas RFID

Está formada por dos elementos básicos, un chip, o circuito integrado y una antena. Este circuito integrado tiene la capacidad de almacenar una serie de números los cuales conforman el identificador de la etiqueta, la capacidad de memoria del chip está en función del modelo y varía de decenas a millares de bytes. También cuenta con una pequeña antena cuyo propósito es permitirle al chip, el cual contiene los datos de identificación, transmitir dicha información de la etiqueta al lector.

Existen dos tipos principales de memorias:

- **Sólo lectura**: El código de identificación que contiene es único y es personalizado durante la fabricación de la etiqueta.
- **De lectura y escritura**: La información de identificación puede ser modificada por el lector.

La etiqueta RFID la cual como ya se dijo contiene los datos de identificación del objeto al que se encuentra adherido, genera una señal de radiofrecuencia para transmitir dichos datos. La señal es captada por un lector RFID, el cual se encarga de leer la información y pasarla en formato digital a la aplicación específica que utiliza RFID en el equipo de cómputo.

Sin embargo, el funcionamiento varía dependiendo del tipo de tecnología que se utilice en las etiquetas, así como en los lectores RFID y en las antenas. Existen tres tipos diferentes de etiquetas, las cuales se caracterizan por la manera en que transmiten los datos.

A continuación se muestran las clasificaciones de etiquetas RFID con base en las diferentes implementaciones que se les han hecho:

a) Etiquetas Activas

Se les llaman etiquetas activas a aquellas que cuentan con su propia batería, la cual les brinda energía para emitir la señal que el lector requiere para realizar la lectura de los datos contenidos en dichas etiquetas (Figura 2.2). Estas etiquetas son mucho más fiables (tienen menos errores) que las pasivas debido a su capacidad de establecer sesiones con el lector. Algunas de ellas integran sensores de registro de temperatura y otras variables que pueden usarse para monitorizar entornos de alimentación o productos farmacéuticos. Otros sensores asociados con RFID incluyen humedad, vibración, luz, radiación, temperatura. Algunas etiquetas activas pueden emitir su señal a una distancia mayor a 1km. Además las etiquetas activas cuentan con mayor capacidad de almacenamiento, algunas de ellas pueden tener hasta 8Mb de memoria, esto les permite almacenar no sólo un número identificador, sino la información completa del producto u objeto al que están adheridas, incluso existen modelos que envían al lector el estado de su batería para poder cambiarla a tiempo sin interrumpir su funcionamiento de manera inoportuna. A pesar de su elevado costo son muy utilizadas debido al ahorro que representan en muchas empresas, ya que con estas etiquetas se puede llevar un inventario de los productos en bodegas, en aparadores o incluso de los productos que están siendo transportados, lo que facilita llevar a cabo

estudios de ventas y de producción, reduciendo una cantidad impresionante de errores, costos, tiempo y trabajo del personal de la empresa.

Figura 2.2. Etiqueta RFID activa

b) Etiquetas Pasivas

Se les llaman etiquetas pasivas a aquellas que no cuentan con una batería que les suministre energía para transmitir su información (Figura 2.3). La señal que les llega de los lectores induce una corriente eléctrica suficiente para que el chip envíe su información al lector. Este tipo de etiquetas trabaja a distancias mínimas de 10cm y máximas de 3 metros aproximadamente, dependiendo de la frecuencia a la que estén trabajando, así como del diseño y tamaño de la antena. Debido a que no cuentan con una batería su tamaño suele ser muy pequeño, pueden incluirse en una etiqueta de papel, o incluso más recientemente se les inserta debajo de la piel a personas o animales para rastrearlos en caso de extravío.

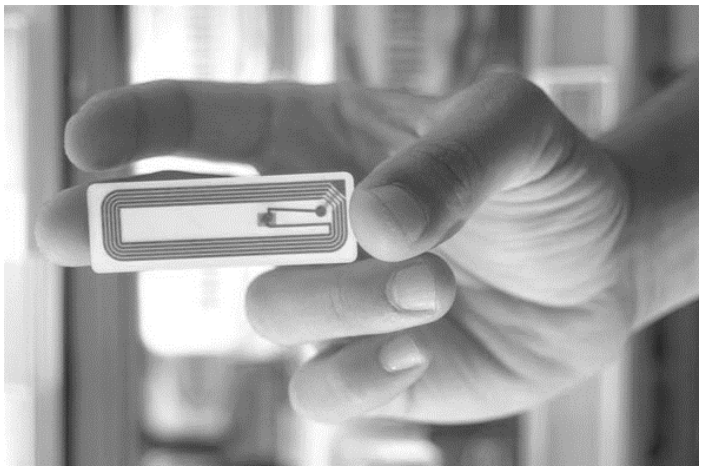


Figura 2.3 Etiqueta RFID pasiva

c) Etiquetas Semi-pasivas

Por último tenemos las etiquetas semi-pasivas, este tipo de etiquetas combinan las características de las dos anteriores, por un lado utilizan batería independiente a la del lector, sin embargo no utilizan la energía de esa batería para transmitir su información, sino que la utilizan para que el chip esté siendo alimentado y así eliminar la necesidad de diseñar una antena que recoja la energía de la señal portadora del lector para alimentar todo el circuito, sin embargo para transmitir su información utiliza la señal del lector y la refleja hacia él de igual forma que las etiquetas pasivas. Una de las ventajas de estas etiquetas es que trabajan a un mayor rango de distancia que las etiquetas pasivas pero menor que las etiquetas activas, sin embargo su tiempo de vida es mayor que el de las etiquetas activas.

2.4.2.-Lector RFID

Está compuesto por una o más antenas, un transceptor y un decodificador. El lector envía periódicamente señales para ver si hay alguna etiqueta en sus inmediaciones, actividad que puede variar según el tipo de lector, ya que actualmente existen etiquetas que envían una señal al lector para que éste

permanezca totalmente inactivo por largos períodos de tiempo, de manera que cuando el lector capta una señal de una etiqueta por medio de la antena, extrae la información y se la manda a la interface lectora para que los datos sean utilizados por alguna aplicación. Hoy en día existe una amplia variedad de lectores, a continuación se mencionan algunos tipos de lectores, los más utilizados en la actualidad.

a) Lectores Portátiles

Este tipo de lectores son utilizados en situaciones donde se requiere que el lector tenga movilidad, en caso por ejemplo en los que se requiera hacer excepciones en la obtención de datos de un grupo de objetos o cuando es más eficiente acercar el lector a los objetos que los objetos al lector. Estos lectores se presentan con forma de pistola para una mayor comodidad del trabajador, como se muestra en la figura 2.4. Muchos de estos lectores cuentan con opción de lectura y escritura sobre las etiquetas, las cuales deben de ser compatibles con esta opción.

Figura 2.4. Lector RFID portátil

b) Lectores fijos

Los lectores fijos pueden ser configurados para tener hasta 8 antenas conectadas, lo que les da una capacidad de escanear una gran cantidad de etiquetas a la vez. Además cuentan con aplicaciones que les permite hacer filtrados en los escaneos, muchos de estos lectores son colocados en bandas transportadoras con el fin de que se obtenga la información de los productos mientras se acomodan en las bodegas o se preparan para ser transportados, también cuentan con conexión a internet para enviar rápidamente la información a la interfaz de aplicación. Figura 2.5.

Figura 2.5. Lector RFID fijo

2.4.3.-Antenas

Un lector RFID utiliza una o varios tipos de antenas. Las antenas son muy importantes en cualquier sistema de envío y recepción de ondas de radio ya que son los dispositivos que transmiten y reciben las señales. Para un lector RFID las antenas cuentan con las siguientes características:

Alto direccionamiento: Las propiedades de direccionamiento de una antena son el parámetro guía de la comunicación punto a punto, al contrario de la comunicación tipo broadcast, ya que en la comunicación tipo broadcast se busca extender la señal para que un mayor número de receptores la obtengan, como por ejemplo las señales radiofónicas, en cambio si queremos que la señal llegue a sólo ciertos destinatarios lo que se hace es direccionar la señal, como por ejemplo en una señal de internet de tipo inalámbrica. En el caso de un sistema RFID se busca que la señal transmitida y la señal recibida estén confinadas a un área específica, no que se difunda hacia otras zonas RFID o campos de transmisión de otros sistemas que puedan causar interferencia. Por eso es de suma importancia saber elegir el tipo de antena que se requiere, ya sea lineal o circular, para señales tipo broadcast en caso que así se requiera.

Ganancia: La ganancia es una especie de medida de lo bien o mal que una antena transmita su señal, por ejemplo como ya se mencionó en las señales radiofónicas se busca extender la señal con el objetivo de que un mayor número de radio escuchas sintonicen la señal, mientras que en una señal de RFID se busca concentrar la señal y dirigirla específicamente a una zona limitada que es en la que las etiquetas entraran para ser leídas. Mientras más ganancia tengan estas antenas, mayor será su alcance y tendrán mayor concentración en la zona específica, así mismo las lecturas se realizarán con mayor efectividad.

Polarización: La polarización de las antenas es simplemente la orientación que la onda electromagnética tendrá. Los dos tipos básicos de polarización son: La polarización lineal y la circular. Si se utiliza una antena de tipo dipolo, las cuales son antenas básicas, la señal será de forma lineal, estas antenas son fácilmente reconocibles ya que tienen forma cilíndrica (Figura 2.6). Pero si utilizan antenas con polarización circular la

señal transmitida será en forma circular, como en el ejemplo de la estación de radio.

En resumen, al elegir una antena se debe considerar que tenga un alto nivel de direccionamiento para poder referir su señal hacia un área específica y que no se propague por todas partes, que tenga una alta ganancia para que las lecturas sean rápidas y libres de errores y por último es necesario elegir la antena según el diseño del sistema, si las lecturas se hacen de manera lineal o circular, para elegir la polarización de la antena.

Figura 2.6. Antena tipo dipolo

2.5.-Ventajas sobre los códigos de barras

La tecnología RFID se utiliza en casos en donde antes se usaban los códigos de barras, poco a poco la tecnología RFID ha ido desplazando a los códigos de barras,

a continuación se presenta una comparativa entre estas dos técnicas de obtención de información con el fin de determinar las ventajas o desventajas que tiene una sobre la otra.

Códigos de Barras:

Modificación de los datos: En los códigos de barras no se puede modificar la información una vez que las líneas están impresas.

Seguridad de los datos: Los códigos de barras han sido ampliamente adoptados, y los estándares son bien conocidos, sin embargo sus datos no cuentan con un sistema de encriptación.

Cantidad de datos de transmisión: Los códigos de barras pueden tener poco más de 30 caracteres de datos.

Costos: Su valor va de fracciones de centavos a unos cuantos pesos.

Tiempo de vida útil: Su tiempo de vida es muy corto, debido a que son etiquetas impresas, sin embargo, también pueden estar impresas sobre el empaque del producto, esto puede alargar su período de vida un poco más.

Distancia de lectura: Requieren estar en la línea de visión y a unos cuantos centímetros de distancia.

Número de códigos que pueden ser leídos a la vez: Sólo un objeto puede ser escaneado a la vez.

Potencial de interferencia: Los códigos de barras se vuelven ilegibles cuando se dañan las líneas verticalmente. Tal daño ocurre cuando una línea es eliminada por completo o alterada, o cuando un espacio en blanco es marcado con una línea oscura. El lector también presenta interferencias cuando está

expuesto a mucho polvo, suciedad, u objetos o manchas que obstruyan el lente lector.

RFID:

Modificación de los datos: La habilidad para modificar los datos está en función del estándar que se haya elegido. Utilizando el estándar EPC (Electronic Product Code) existen dos clases, las cuales son:

Etiquetas Clase 0: Estas son de sólo lectura, lo que significa que el usuario debe utilizar el número que se imprimió de fábrica en la etiqueta.

Etiquetas Clase 1: Estas son etiquetas de Lectura/Escritura, lo que significa que se puede programar en el mismo negocio el número que se desee tenga cada etiqueta, también se les conoce como etiquetas WORM (Write Once Read Many).

Seguridad de los datos: Dependiendo de la clase y la versión o generación de las etiquetas se pueden cifrar los datos con el objetivo de que su información no sea leída por otros lectores RFID.

Cantidad de datos de transmisión: Dependiendo de la manufactura, las etiquetas contienen 64, 96, 128, 256 o 512 bits de información.

Costos: Sus precios están entre los 10 y los 500 pesos mexicanos por etiqueta, aproximadamente. Sin embargo está disminuyendo su valor con el paso del tiempo.

Tiempo de vida útil: Se ha estimado que en etiquetas activas es aproximadamente de 10 años, mientras que en las pasivas puede llegar a ser hasta de 20 años, dependiendo del tipo de material con el que estén fabricadas.

Distancia de lectura: En etiquetas activas llegan a ser lecturas de poco más de 1Km de distancia, mientras que las pasivas realizan lecturas que van desde pocos centímetros de distancia hasta 2 o 3 metros.

Número de códigos que pueden ser leídos a la vez: Un lector RFID es capaz de leer cientos de etiquetas cercanas a la vez.

Potencial interferencia: Algunos materiales como metales o líquidos pueden interferir en la lectura de etiquetas pasivas. Las etiquetas activas son menos susceptibles a las interferencias, sin embargo se han reportado casos de interferencias cuando se encuentran dentro de contenedores metálicos.

Como se aprecia, tanto los código de barras como la tecnología RFID realizan tareas similares, sin embargo los RFID son mucho más poderosos en todos los aspectos, el uso que se les da en la actualidad no es sólo para fines de control de inventarios sino que también auxilian en cuestiones comerciales (cobro de tarifas), como medio de control de accesos, e incluso para evitar robos o secuestros de bienes materiales, animales o personas. Además, transfiere mayor información, la distancia de comunicación es mucho mayor, puede leer varias etiquetas a la vez y en algunos casos la lectura de los datos se da sin que los dispositivos tengan una línea de visión directa, sin embargo su principal desventaja es el costo y en algunos casos su nivel de complejidad, pero eso depende del grado de sofisticación que se requiera en el sistema.

2.6.- Estandarización

Los sistemas RFID utilizan distintas frecuencias, es por ello que los órganos de gobierno internacionales, como la Comisión Federal de Comunicaciones (FCC) en Estados Unidos y el Instituto Europeo de Estándares de Telecomunicaciones (ETSI) en Europa, regulan tales frecuencias. Generalmente las más comunes son:

Baja Frecuencia: Low Frequency (LF), alrededor de 125 kHz.

Alta Frecuencia: High Frequency (HF), 13.56 MHz.

Ultra Alta Frecuencia: Ultrahigh Frequency (UHF), 850-930 MHz.

Los estándares de RFID abordan cuatro áreas fundamentales:

- Protocolo en la interfaz aérea: Especifica el modo en el que etiquetas RFID y lectores se comunican mediante radiofrecuencia.
- Contenido de los datos: Especifica el formato y semántica de los datos que se comunican entre etiquetas y lectores.
- Certificación: Pruebas que los productos deben cumplir para garantizar que cumplen los estándares y que pueden inter-operar con otros dispositivos de distintos fabricantes.
- Aplicaciones: Usos de los sistemas RFID.

Como en otras áreas tecnológicas, la estandarización en el campo de RFID se caracteriza por la existencia de varios grupos de especificaciones competidoras. Por una parte está ISO, y por otra Auto-ID Centre (conocida desde octubre de 2003 como EPC Global). Hay varios estándares de interfaz RFID, cada uno con capacidades distintas, ventajas y desventajas. Hasta diciembre de 2004, el sistema de clasificación de primera generación (GEN-1) de EPC Global era el más utilizado. Después de diciembre de 2004, la segunda generación de este sistema (GEN-2) fue favorecida y se convirtió en el estándar a seguir.

Los estándares EPC para etiquetas son de dos clases, como se mencionó anteriormente:

- **Clase 0**: Etiqueta simple, pasiva, de sólo lectura con una memoria no volátil programable una sola vez desde su fabricación.

- **Clase 1**: Etiqueta de sólo lectura que se programa por el administrador del sistema para el cual se requirió, y se puede leer una infinidad de veces, llamada también WORM (Write Once – Read Many).

Sin embargo en los últimos años ha aumentado el número de clases debido a la necesidad de clasificar las etiquetas en función de su utilidad o características particulares, sobre todo en tiendas de consumibles de EE.UU donde ha incrementado su uso notablemente. Consecuentemente se presentan las clases 2, 3, 4 y 5:

- **Clase 2**: Etiquetas pasivas de escritura y lectura, que pueden ser sobre escritas en cualquier punto de la cadena de suministros.
- **Clase 3**: Lectura-Escritura con sensores internos que le permiten almacenar parámetros como temperatura, presión y movimiento, pueden ser pasivas o activas.
- **Clase 4**: Etiquetas activas de Lectura y Escritura, con transmisores integrados, pueden comunicarse con otras etiquetas y lectores.
- **Clase 5**: Similar a la clase 4 pero con funcionalidades añadidas, pueden proveer energía a otras etiquetas y comunicarse con otros dispositivos además de los lectores.

Anteriormente las clases operaban bajo el estándar Generación 1 (GEN1), lo que hacía que las distintas clases de etiquetas no fueran interoperables, además no eran compatibles con los estándares de ISO. Sin embargo en diciembre del 2004 EPC Global desarrolló el estándar denominado Generación 2 (GEN2), el cual permite:

- Un estándar de interoperabilidad global
- Velocidades de lectura más rápidas y más flexibles
- Un desempeño más preciso y rápido mediante el uso de protocolos anti-colisión avanzados.
- Un modo más fácil de instalar muchos lectores en una sola operación para los usuarios finales.

- Seguridad y Privacidad Mejorada.

Adicionalmente, las etiquetas Clase 1 Gen 2 RFiD son compatibles con las etiquetas Gen-1 Clase 0 y Clase 1 y reemplazan las especificaciones de ambas clases. Las etiquetas Clase 1 Gen 2 tienen un estándar abierto que cualquier fabricante puede usar para fabricar sus propias etiquetas.

En cuanto a la Organización Internacional de Estándares (ISO) ésta ha reconocido al estándar promovido por EPC Global para el desarrollo de despliegues RFID en la cadena de suministro EPC Gen 2 Clase 1 UHF como un estándar ISO con validez mundial, incorporándole como una enmienda a su estándar referido a la utilización de dispositivos para operar en entornos RFID UHF (860-960 MHz) 18000-6, quedando reflejado finalmente como ISO 18000-6C, lo que permite interoperabilidad entre los estándares de ISO y EPC Global.

Para la demostración práctica de la propuesta que aquí se presenta como proyecto de tesis se construyó una maqueta en la que se hace uso de los sistemas básicos de cada tecnología que integran el sistema de seguridad, en el caso del sistema RFID se utiliza un dispositivo que cuenta con una interfaz de salida tipo Firewire, por lo que se puede conectar al computador por medio de un cable Firewire-USB. Las dimensiones del circuito son de 8.1cm de largo por 6.9cm de ancho, cuenta con una antena integrada lo que permite su comunicación con una etiqueta de tipo pasiva. Debido a que este circuito es sencillo no cuenta con la capacidad de lectura/escritura, ni con un sistema anticolisión, sin embargo tiene la capacidad de dar un voltaje de salida de 5V lo que le permite la manipulación de algún otro dispositivo que utilice 5V de entrada para lo cual hay que programar el dispositivo previamente, el circuito se muestra en la Figura 2.7.

Figura 2.7. Circuito RFID

Las etiquetas con que funciona este sistema RFID son pasivas, es de clase 0 lo que significa que su número de identificación viene grabado de fábrica, el alcance de lectura es de aproximadamente 10cm, aunque ésta varía dependiendo de la forma y tamaño de la etiqueta, en nuestro caso utilizamos una etiqueta tipo tarjeta como la que se muestra en la figura 2.8, sin embargo se pueden utilizar de otro tipo de etiquetas, específicamente para este sistema se pueden adquirir etiquetas de tipo llavero (Figura 2.9), o tipo disco (Figura 2.10).

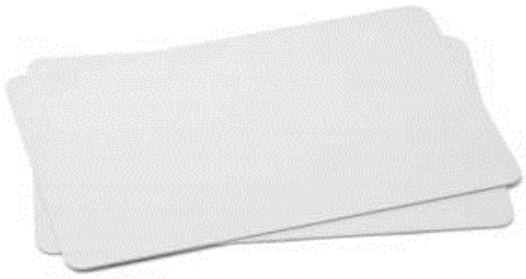


Figura 2.8. Etiqueta RFID tipo tarjeta

Figura 2.9. Etiqueta RFID tipo llavero

Figura 2.10. Etiqueta tipo disco

Capítulo 3

Biometría

3.1-Concepto de Biometría

La biometría se refiere a todas aquellas técnicas que permiten identificar y autenticar personas basándose en uno o más rasgos conductuales o físicos particulares de cada persona. El término se deriva de las palabras griegas "*bios*" de vida y "*metron*" de medida. La biometría permite la autenticación de usuarios con base en sus características físicas como su huella dactilar, patrón de iris, estructura de su voz, forma y aspecto de su escritura, entre otros. Por medio de los métodos mencionados la biometría provee mayor seguridad a los sistemas de control de acceso tradicionales utilizados para proteger activos personales o empresariales.

3.2.-Surgimiento de la biometría

Se han encontrado evidencias de que alrededor del año 500 A.C. las transacciones comerciales entre los babilonios eran registradas en unas pastillas de arcilla que incluían la impresión de la huella digital.

Alrededor del siglo XIV, el explorador y escritor español Joao de Barros, escribió que los primeros mercaderes chinos incluían la impresión de las huellas digitales en sus transacciones de negocios.

En los comienzos de la historia egipcia, los comerciantes eran identificados por sus características físicas para diferenciar entre los comerciantes de confianza y conocida reputación y transacciones exitosas previas, de aquellos que recién se iniciaban en los negocios.

A mediados de 1800, con el gran crecimiento de las ciudades surgen nuevas técnicas de identificación demandadas por la justicia, la cual, en ese momento, pretendía imponer castigos más severos a los infractores reincidentes y flexibles a aquellos que infringían la ley por primera vez. Esto requería de un sistema que pudiera medir y registrar distintos rasgos que identificaran a los infractores. El primero de los dos

métodos utilizados fue el sistema inventado por el Parisiense Alphonse Bertillon el cual se basaba en la medición de varios parámetros físicos (Antropometría). Dichos parámetros eran registrados en unas tarjetas que luego se ordenaban según la altura, el largo de los brazos y algunos otros parámetros. A finales del siglo XIX el inglés Sir. Francis Galton, quien era experto en el sistema Bertillon, realizó estudios más detallados sobre las huellas dactilares, estudiando su estabilidad, unicidad y morfología. Sus trabajos, complementados por los de Vucetich, Henry, Hershel y Faulds (cada uno de forma independiente), consiguieron que la identificación por huella dactilar fuera aceptada y se convirtiera en el método de identificación biométrica más utilizado a nivel mundial.

Los sistemas biométricos modernos comienzan a surgir en la segunda mitad del siglo XX junto con el desarrollo de los sistemas computarizados. En los años 90 se produce una gran explosión en este campo, creando tecnologías masivas, más económicas y al alcance de la mano de mayor cantidad de usuarios, lo que introduce a los sistemas biométricos en un sinfín de aplicaciones que utilizamos día a día.

3.3.-Tipos de Sistemas biométricos

Existen dos clases de métodos de identificación que usan la biometría, por reconocimiento fisiológico y por reconocimiento de comportamiento.

3.3.1.-Reconocimiento Fisiológico

La biometría fisiológica mide una parte específica de la estructura o forma de una porción del cuerpo de una persona. Los tipos de biometría fisiológica incluyen:

a) Huella digital: Esta tecnología es la más difundida y posee varios años de existencia. Las huellas digitales poseen una serie de surcos que forman un

modelo único para cada individuo y que se definen durante el desarrollo fetal.

b) Geometría de mano: El escaneo de mano involucra la medición y análisis de la morfología de esta parte del cuerpo humano. Estos sistemas están basados en la medida de la mano extendida, en la forma, la dimensión de la palma y la longitud de los dedos.

c) Reconocimiento facial: El reconocimiento facial es un método poco "invasivo", y el más familiar para la persona, es un método muy cercano al modo más natural que la persona utiliza para reconocerse. Los sistemas que se encargan del reconocimiento facial se basan en las mediciones que hacen de ciertas partes del rostro humano. Las aplicaciones son ya numerosas y van desde el reconocimiento estático al dinámico, es decir, en movimiento.

d) Reconocimiento de iris: El iris es la región del ojo tras la pupila, su estructura es enormemente distintiva para el reconocimiento de la persona. Los iris son todos distintos, incluso también entre gemelos, su diseño es muy difícil de modificar (ni siquiera con una intervención quirúrgica). La velocidad de lectura de los sistemas actuales y su nivel de precisión es muy alta, además de que proporciona una alta fiabilidad por lo que su uso ha sido principalmente para sistemas militares, sin embargo, su costo es actualmente de los más altos entre los diferentes tipos de sistemas biométricos. Si bien los primeros sistemas de lectura de iris requerían una notable participación por parte de las personas, los modelos actuales son mucho más amigables para el usuario.

e) Reconocimiento de retina: También la retina tiene un esquema vascular típico de cada individuo, imposible de modificar o replicar. La adquisición

de la imagen requiere que el individuo se mantenga en posición fija frente al lector, por lo que requiere la plena colaboración del usuario, un aspecto que supone un freno para su utilización masiva.

f) Reconocimiento de voz: Estos sistemas se basan en el reconocimiento de voz, es decir, cuando un usuario desea acceder al sistema pronunciará unas frases con el objetivo de que el sistema evalúe la frecuencia de su voz; en algunos modelos, los denominados de texto dependiente, el sistema tiene almacenadas un conjunto muy limitado de frases que es capaz de reconocer, así el usuario se limita a pronunciar su nombre o alguna otra frase corta, de forma que el reconocedor lo entienda y lo autentique. Estos modelos proporcionan poca seguridad en comparación con los de texto independiente, donde el sistema va proponiendo a la persona la pronunciación de ciertas palabras extraídas de un conjunto bastante grande, lo habitual es que las frases tengan una cierta entonación, pronunciación de los diptongos y palabras con muchas vocales para maximizar la cantidad de datos que se pueden analizar. Conforme va hablando el usuario, el sistema registra toda la información que le es útil; cuando termina la frase, ya ha de estar en disposición de facilitar o denegar el acceso, en función de la información analizada y contrastada con la de la base de datos. El habla es considerado uno de los sistemas biométricos más exactos, debido a su naturalidad. Se ha podido establecer que los patrones y las frecuencias con los que cada persona dice una misma palabra son completamente únicos. El reconocimiento de voz funciona mediante la digitalización del discurso de un individuo. Cada palabra se descompone en segmentos, los cuales tienen 3 o 4 tonos dominantes que son capturados en forma digital y que se plasman en una tabla o espectro, para conformar el "*voice print*" (una especie de plantilla de la voz). Éste se guarda como una tabla de números, en la que cada frecuencia dominante se expresa como un dato binario. Cuando la persona pronuncia su frase de

acceso, los fragmentos son comparados con los de la tabla, y el acceso es concedido o denegado. Sin embargo para autenticar a un usuario utilizando un reconocedor de voz se debe disponer de ciertas condiciones para el correcto registro de los datos, como ausencia de ruidos, reverberaciones o ecos; idealmente, estas condiciones han de ser las mismas siempre que se necesite la autenticación.

El principal problema del reconocimiento de voz es la inmunidad frente a *replay attacks*, un modelo de ataques de simulación en los que un atacante reproduce (por ejemplo, por medio de una grabadora de sonidos) las frases o palabras que el usuario legítimo pronuncia para acceder al sistema. Este problema es especialmente grave en los sistemas que se basan en textos preestablecidos: volviendo al ejemplo anterior, el del nombre de cada usuario, un atacante no tendría más que grabar a una persona que pronuncia su nombre ante el autenticador y luego reproducir ese sonido para conseguir el acceso; casi la única solución consiste en utilizar otro sistema de autenticación junto al reconocimiento de voz.

Existe también un método de reconocimiento basado en al ácido desoxirribonucleico, presente en la sangre, el cual arroja patrones diferentes para cada individuo. Como dato biométrico es extremadamente fiable, pero su utilización está restringida a las aplicaciones de naturaleza jurídica por diversas razones, entre las cuales se encuentra, el tiempo necesario para realizar los exámenes en el laboratorio; por lo que no es posible utilizar este elemento biométrico como sistema de reconocimiento en tiempo real o en algún sistema de control de acceso.

3.3.2.-Reconocimiento por Comportamiento

La biometría de comportamiento está enfocada a la forma en que el individuo *hace* algo, en lugar de concentrarse en una medida estática de una parte

específica de su cuerpo. Algunas técnicas de biometría de comportamiento son:

a) Reconocimiento de firmas: Es quizás la tecnología biométrica más natural, ya que estamos muy habituados al uso de nuestra firma como método de reconocimiento. Es una tecnología barata, porque sólo se necesita una tableta de escritura conectada a la PC. El proceso de análisis se realiza en dos áreas distintas: la firma en sí y el modo en que se efectúa. Los datos almacenados incluyen la velocidad, la presión, la dirección, el largo del trazado y las áreas donde la lapicera se levanta. Sin embargo presenta ciertas desventajas ya que se ha comprobado que un individuo nunca firma de manera idéntica dos veces, y a lo largo de su vida, el cambio puede ser sustancial.

b) Dinámica de teclado: Se basa en reconocer a una persona por la forma en que escribe por medio de un teclado, se mantiene la hipótesis de que el ritmo de teclado es característico de una persona, y prototipos existentes parecen reafirmar esa hipótesis. Sin embargo, además de ser una técnica basada en el comportamiento y por lo tanto potencialmente imitable, tiene la limitación de no poder ser utilizada con usuarios que no saben escribir por medio de un teclado o incluso sin él.

Todos los sistemas biométricos cuentan con ventajas y desventajas, es por ello que existen ciertos conceptos para conocer el rendimiento del sistema biométrico antes de implementarlo.

3.4.-Rendimiento

En un sistema de Biometría típico, la persona se registra con el sistema cuando una o más de sus características físicas o de conducta son obtenidas, procesadas por un

algoritmo numérico, e introducidas en una base de datos. Idealmente, cuando entra, casi todas sus características concuerdan; entonces cuando alguna otra persona intenta identificarse, no empareja completamente, por lo que el sistema no le permite el acceso. Las tecnologías actuales tienen tasas de error que varían ampliamente, desde el 60%, hasta el 99,9%.

El rendimiento de una medida biométrica se define generalmente en los siguientes términos:

- Tasa de falso positivo (*False Acceptance Rate* o FAR).
    - Cuando se ***acepta*** a alguien que ***no es***; por ejemplo, alguien podría clonar una credencial de identificación, o adueñarse de los números confidenciales de una persona para hacer una transacción en perjuicio de su legítimo dueño y hasta falsificar su firma.

- Tasa de falso negativo (*False NonMatch Rate* o FNMR, también *False Rejection Rate* o FRR).
    - Consiste en ***no aceptar*** a alguien que ***sí es***, pero su identificación no se pudo realizar debido a múltiples motivos, como puede ser: que la huella del usuario esté dañada, o a que tenga una capa de pintura o alguna sustancia que impida tomar apropiadamente la imagen, o a que el lector no tenga la calidad suficiente para tomar correctamente la lectura.

- Tasa de error igual (*Equal Error Rate* o EER).

    - Es cuando se da un ajuste entre la tasa de FAR y la tasa de FRR de manera que estos sean iguales, como se muestra en la figura 3.1.

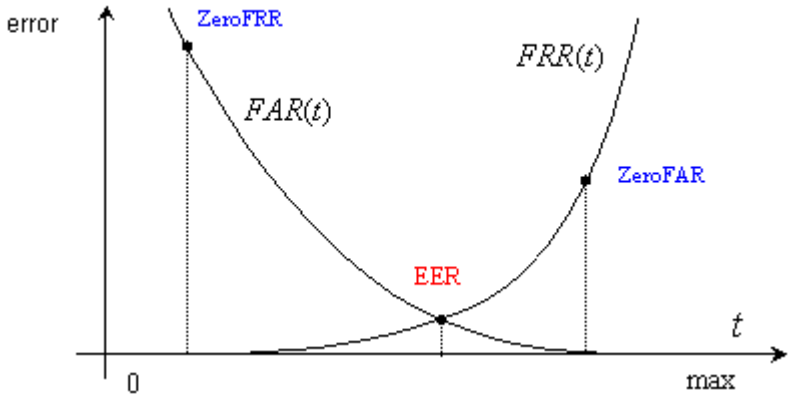


Figura 3.1. Gráfica de *Equal Error Rate*

En los sistemas biométricos reales el FAR y el FRR pueden transformarse cambiando ciertos parámetros. Una de las medidas más comunes de los sistemas biométricos reales es la tasa (*Equal Error Rate* o EER), también conocida como la tasa de error de cruce (*Cross-over Error Rate* o CER). Cuanto más bajo es el EER o el CER, se considera que el sistema es más exacto.

Ahora se presenta la tabla 3.1 dónde se muestra una comparativa entre las características más importantes de los sistemas biométricos utilizados actualmente.

Tabla 3.1. Comparativa de sistemas biométricos

	Ojo (iris)	Ojo (retina)	Huellas dactilares	Geometría de mano	Escritura y firma	Voz	Cara
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Media	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy alta	Alta	Alta	Media	Media	Media
Aceptación	Media	Baja	Alta	Alta	Muy alta	Alta	Muy alta
Estabilidad	Alta	Alta	Alta	Media	Baja	Media	Media

Pese a que el uso de sistemas biométricos de huella dactilar no es de máxima seguridad, su nivel es muy alto, además es fácil de utilizar para los usuarios, barato y estable, por lo que este sistema ha sido elegido para su implementación en nuestro sistema de seguridad. Así pues, se detalla a continuación su funcionamiento y los diferentes tipos de sistemas de huella dactilar que existen, ya que son muy diversos y es importante conocer los más utilizados.

3.5.-Sistemas Biométricos de Huella Dactilar

Las huellas digitales son características exclusivas de los primates. En la especie humana se forman a partir de la sexta semana de vida intrauterina y no varían en sus características a lo largo de toda la vida del individuo.

Son las formas caprichosas que adopta la piel que cubre las yemas de los dedos. Están constituidas por rugosidades que forman salientes y depresiones. Las salientes se denominan "*crestas papilares*" y las depresiones "*surcos interpapilares*" los cuales son tomados como patrones para la identificación de la huella, también existe otro patrón denominado "*minucia"* (término utilizado en la medicina forense que significa "*punto característico*"), las cuales son características locales de las crestas que se localizan en una bifurcación o al final de la misma. Más adelante se detallara el uso de los patrones mencionados.

En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene aceite, que se retiene en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie, queda un residuo de ésta, lo cual produce un facsímil o negativo de la huella.

Las huellas digitales se pueden tomar de cualquiera de los 10 dedos, sin embargo comúnmente se toman de los dedos índices, tanto por comodidad al capturarlas, como porque estos dedos están menos propensos que los pulgares a sufrir accidentes que dejen cicatriz.

Son únicas e irrepetibles aún en gemelos idénticos, debido a que su diseño no está determinado estrictamente por el código genético, sino por pequeñas variables en las concentraciones del factor del crecimiento y en las hormonas localizadas dentro de los tejidos. Cabe señalar que en un mismo individuo la huella de cada uno de sus dedos es diferente.

3.5.1.-Métodos de reconocimiento dactilar

Como ya se mencionó, la huella dactilar consta de crestas papilares (las líneas que cruzan en sentido ascendente la yema de los dedos) y surcos (los espacios entre las crestas). La combinación de crestas y surcos es única en cada individuo.

La identificación por huella dactilar se puede dividir en dos grandes grupos:

- Específica.- Basada en los puntos de discontinuidad de terminaciones y bifurcaciones, denominados puntos de minucia.

- General o de aproximación macroscópica.- Se tienen en consideración el sentido de las crestas papilares, por ejemplo arcos, curvas y espirales.

La identificación automática de huellas dactilares en sistemas digitales, se hace basándose en los puntos de minucia. A continuación en la figura 3.2 se muestran 8 variedades de minucias, según su clasificación.

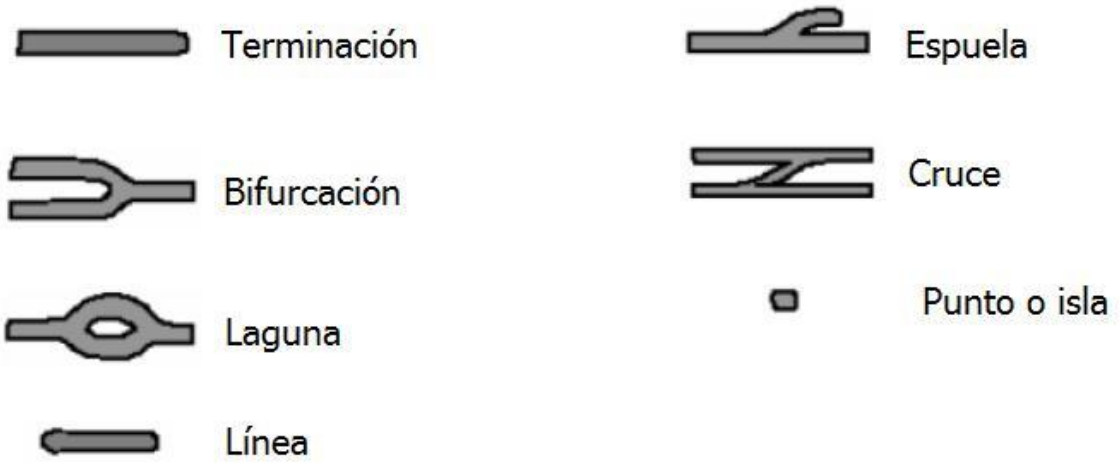


Figura 3.2. Principales minucias

Existe una amplia variedad de minucias (18 hasta el momento) sin embargo, la mayoría de los sistemas se enfoca solamente a dos de las 18 minucias (véase figura 3.3), la terminación y la bifurcación, esto debido a que el resto de las minucias puede verse como la combinación de estas dos.

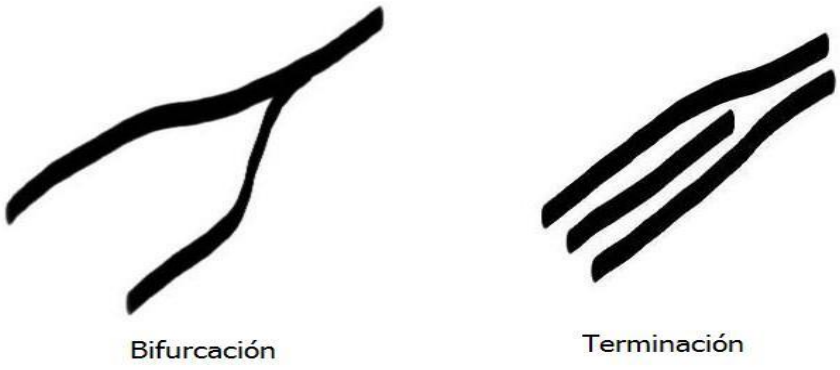


Figura 3.3. Bifurcación y terminación

A continuación se muestran los pasos que sigue un software para evaluar una huella digital:

1.- El hardware del sistema extrae una representación de la huella digital.

2.- Se identifican las minucias. Una huella dactilar completa consta con un promedio de 100 puntos de minucia. El área que se evalúa consta con un promedio de 30 a 60 puntos de minucia dependiendo del dedo y del sensor.

3.- Los puntos de minucia se representan por una línea de puntos en un sistema de coordenadas. Éstos se añaden con el ángulo de la tangente del punto de minucia local a un código dactilar, del cual se determina una plantilla de referencia.

4.- Una vez obtenida la plantilla se compara con las demás que tengan el mismo número de minucias. Cabe señalar que las plantillas no se generan como una imagen, sino como puntos en un sistema de coordenadas, los cuales son convertidos a una cadena de números binarios, a los que se les da el tratamiento requerido para la identificación del usuario.

Dichos puntos se ejemplifican en la figura 3.4:

Figura 3.4. Pasos para evaluar una huella dactilar de manera digital

Cabe señalar que no todos los dispositivos de reconocimiento de huella dactilar funcionan de la misma manera, existen distintos métodos para obtener la lectura de la huella digital, es por ello que a continuación se muestran los distintos métodos que utilizan ciertos dispositivos para extraer lo mejor posible una representación de una huella dactilar.

3.5.2.-Métodos de lectura de huella dactilar

Existen diversos tipos de dispositivos que se utilizan para hacer lectura de una huella dactilar, la diversidad de estos dispositivos se basa principalmente en el tipo de tecnología o método que éstos utilizan para realizar su labor. Los dispositivos y sus características son los siguientes:

a) Ópticos.- Éstos funcionan al colocar el dedo sobre una base transparente, que es iluminada por pequeños diodos. Las huellas digitales están conformadas por crestas y surcos, cuando las crestas hacen contacto con la base del lector absorben la luz, mientras que los valles la reflejan. De esta forma, se crea una imagen con zonas más claras que otras, lo que

genera un perfil de la huella. Es importante tomar en cuenta que este tipo de sensores son susceptibles a producir errores si la huella está húmeda, sucia o si se trata de una persona mayor, ya que en algunas ocasiones la piel pierde su firmeza lo que afecta la lectura hecha con estos sensores.

b) Termoeléctricos.- El método termoeléctrico utiliza un sistema único para reproducir el dedo completo "arrastrándolo" a través del sensor. Durante este movimiento se realizan tomas sucesivas y se pone en marcha un software especial que reconstruye la imagen del dedo.

El sensor mide la temperatura diferencial entre las crestas papilares y el aire retenido en los surcos. Este método proporciona una imagen de gran cualidad incluso cuando las huellas dactilares presentan alguna anomalía como resequedad, desgaste o cuando presentan pequeñas cavidades entre las cimas y los surcos de la huella. La tecnología termal permite también su uso bajo condiciones medioambientales extremas, como temperaturas muy altas, humedad, suciedad o contaminación de aceite y agua sobre la huella del dedo. Además, algunos de estos dispositivos cuentan con la ventaja de auto limpiado del sensor, con lo que se evitan las huellas latentes, se denomina así a las huellas que permanecen en el sensor una vez utilizado, lo cual puede ocasionar problemas no sólo en las lecturas posteriores sino que en ocasiones son copiadas las huellas para falsificarlas y acceder así al sistema. Una desventaja es el calentamiento del sensor mismo que aumenta el consumo de energía considerablemente, pero es necesario ya que evita la posibilidad de un equilibrio térmico entre el sensor y la superficie de la yema dactilar.

c) Capacitivos.- El método capacitivo es uno de los más populares. Al igual que otros escáneres, genera una imagen de la cresta y los valles.

En la superficie de un circuito integrado de silicona se dispone un arreglo de sensores capacitivos conductores cubiertos por una capa aislante. La capacitancia en cada sensor es medida individualmente depositando una carga fija sobre ese sensor.

La mayor ventaja es que se requiere una huella real pero se pueden presentar problemas si la yema del dedo está húmeda o muy seca. En este caso se obtendrán imágenes negras o pálidas.

d) Campo eléctrico.- El sensor de campo eléctrico funciona con una antena que mide el campo eléctrico formado entre dos capas conductoras (la más profunda situada por debajo de la piel del dedo). La tecnología basada en los campos eléctricos afirma ser útil para cualquiera y poder trabajar bajo cualquier condición, por dura que ésta sea, como por ejemplo piel húmeda, seca o dañada.

Esta tecnología origina un campo entre el dedo y el semiconductor adyacente que simula la forma de los surcos y crestas de la superficie epidérmica. Los sensores reproducen una imagen clara que corresponde con mucha exactitud a la huella dactilar y que es mucho más nítida que la producida por sensores ópticos o capacitivos. Esto permite a la tecnología de campo eléctrico la lectura de huellas que otras tecnologías no podrían.

En la tecnología de campo eléctrico, la antena mide las características de la capa subcutánea de la piel generando y detectando campos lineales geométricos que se originan en la capa de células de la piel situada bajo la superficie de la misma.

Esto contrasta con los campos geométricos esféricos o tubulares generados por el sensor capacitivo que sólo lee la superficie de la piel. Como resultado, huellas que con sensores capacitivos son casi imposibles de leer, se pueden reproducir con éxito por sensores de tecnología de

campo eléctrico. Una desventaja es la baja resolución de la imagen y el área pequeña de imagen lo que produce un índice de error alto (EER).

e) Presión.- Se trata de decenas de miles de diminutos transductores de presión que se montan sobre la superficie del sensor. Un diseño alternativo utiliza conmutadores que están cerrados cuando son presionados por una cresta, pero permanecen abiertos cuando están bajo un surco. Esto sólo proporciona un bit de información por píxel, en lugar de trabajar con una escala de grises. Los sensores de presión son capaces de censar huellas húmedas o secas por igual. Además cuentan con un área mucho mayor para censar lo que les permite capturar la huella completa disminuyendo así los errores.

Existen diversos sistemas con diferentes características, por lo que es importante identificar el medio en el que se implementará para un mejor aprovechamiento de los activos económicos de la empresa donde se implementará y un funcionamiento óptimo del sistema.

Para nuestro proyecto se utilizará un lector de huella dactilar marca *DigitalPersona* que cuenta con las siguientes características:

- Resolución en píxeles: 512 dpi
- Área para captura de imagen: 14.6 mm (ancho) 18.1 mm (largo)
- Escala de grises de 8-bits (256 niveles de gris).
- Tamaño del lector: 65mm x 36mm x 15.56mm.
- Compatible con especificaciones USB 1.0, 1.1 y 2.0 (Full Speed)
- Voltaje de suministro 5,0V ±5% suministrados por USB
- Corriente de suministro: exploración 190 mA (típica)
- Corriente de suministro: modo inactivo 140 mA (típica)
- Corriente de suministro: modo en suspensión 1,5 mA (máxima)
- Temperatura, operación 0 ‡- 40 ‡ C
- Humedad, operación 20% – 80% sin condensación
- Temperatura, almacenamiento -10 ‡ – 60 ‡ C

- Humedad, almacenamiento 20% – 90% sin condensación.
- FAR 0.001%
- FRR 0.1%

Estas características son las más comunes en sensores de bajo costo y son utilizados generalmente para identificar personas en gimnasios, empresas, clubes o incluso en algunos bancos. Son utilizados en interiores bajo condiciones de temperatura regular y baja humedad.

Para su uso en un estacionamiento dependería de las condiciones medio ambientales del mismo, así como de la robustez en seguridad que se deseé. En nuestro caso utilizaremos este sensor para ejemplificar a pequeña escala el funcionamiento de nuestro sistema de seguridad, sin embargo bajo ciertas circunstancias y dadas las características con las que cuenta, podría utilizarse este sensor en un caso real.

Capítulo 4

Conceptos de las Herramientas de Software y Metodología de Trabajo

4.1.-Base de datos

Una base de datos es una colección de información almacenada y organizada en un mismo contexto con un fin determinado. Las bases de datos pueden clasificarse de acuerdo a su modelo de administración de datos

4.2.-Conceptos de Bases de Datos

Para un mejor entendimiento de la información, se definen los siguientes conceptos:

Modelo de base de datos: Un modelo de datos es un conjunto de conceptos que sirven para describir la estructura de una base de datos, contiene los métodos para almacenar, recuperar y administrar la información.

Entidad: Objeto que puede distinguirse de otros, está formada por varios atributos, cada ejemplar que se despliegue de ella debe tener las mismas características pero debe ser diferente de otro ejemplar. Existen entidades fuertes y débiles:

-Fuertes: existen por sí mismas y tienen clave primaria.
-Débiles: no tienen suficientes atributos para distinguirse de las demás.

Relación: En una base de datos es una asociación, vinculación o correspondencia entre entidades.

Grado: El grado de una relación se define como el número de entidades que participan en una relación.

Tupla: cada una de las filas de una relación. Contiene la información relativa a una única entidad.

Atributo: cada una de las características que posee una entidad.

Cardinalidad: número de tuplas que contiene una relación.

Dominio: Rango o conjunto de posibles valores de un atributo.

Clave primaria: Es un campo o a una combinación de campos que identifica de forma única a cada fila de una tabla.

Clave foránea: Es uno o más campos de una tabla que hacen referencia al campo o campos de clave primaria de otra tabla.

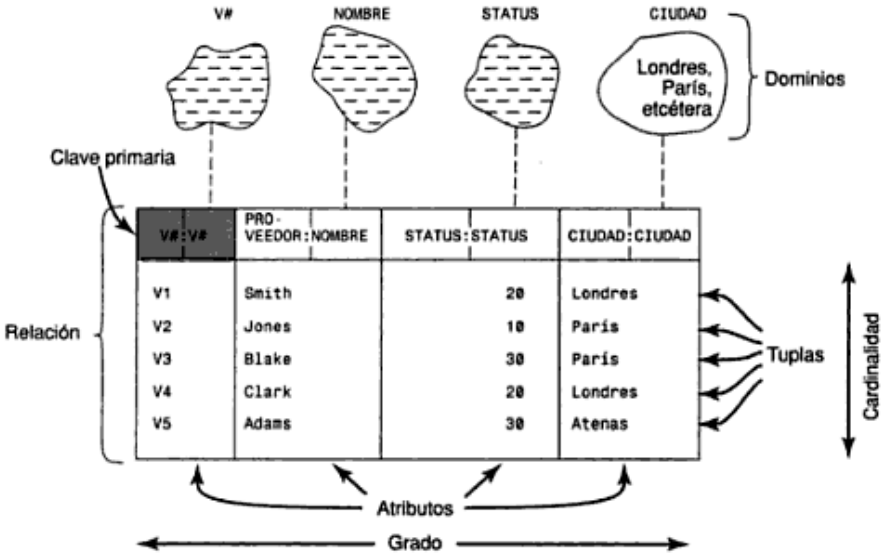


Figura 4.1. Elementos de una base de datos Relacional

Modelo Relacional

El modelo de datos relacional es el más utilizado en la actualidad para modelar y administrar datos dinámicamente. Las bases de datos relacionales son independientes de la aplicación, este modelo se basa en tablas de datos relacionados. Las tablas están compuestas por registros (filas) que representarían las tuplas, y campos (las columnas de una tabla).

El lugar y la forma en que se almacenan los datos no tiene relevancia, la información puede ser recuperada y almacenada por consultas de una forma flexible mediante

SQL (Lenguaje Estructurado de Consultas), un estándar de los sistemas de gestión de base de datos.

Durante el diseño de la base de datos relacional pasa por un proceso al que se le conoce como normalización de una base de datos

Modelo Entidad-Relación

Es una herramienta para el modelado de datos, se basa en la percepción del mundo real que consiste en un conjunto de objetos llamados entidades, y de sus características denominadas atributos, así como de las relaciones entre sus objetos.

Cardinalidad Relacional.

Se define la carnidalidad relacional, como el grado de participación de las entidades en una relación.

(1:1) Una a Una:

Una entidad A esta asociada únicamente con una entidad B asociada con una entidad A.

(1:*) Una a Muchos:

Una entidad A está relacionada con cualquier número de entidades B, pero una entidad B puede asociarse con una entidad en A.

(*:*) Muchos a Muchos:

Una entidad en A esta asociada con cualquier número de entidades en B, y una entidad en B está vinculada con cualquier número de entidades en A.

4.3.-Sistemas de gestión de Bases de datos (SGDB)

Es un conjunto de programas que gestionan y controlan el acceso a la base de datos. Se compone de un lenguaje de definición de datos (DDL), un lenguaje manipulación de datos (DML) y un leguaje de consulta (SQL).

A continuación se lista sus funciones:

- Almacenamiento, extracción y actualización de datos.
- Cuenta con un catálogo accesible para el usuario.
- Soporta transacciones (Actualizaciones).
- Servicio de control de concurrencia.
- Servicio de recuperación.
- Servicio de Autorización de acceso.
- Soporte de comunicación con otros sistemas.
- Servicio de utilerías.
- Servicios de integridad.
- Servicio de independencia de datos.

SQL Server

Es un sistema para la gestión de base de datos producido y lanzado por Microsoft en 1989, basado en el modelo relacional. Sus lenguajes de consulta son T-SQL y ANSI SQL.

Principales características:

- Soporte de Transacciones.
- Soporta procedimientos almacenados.
- Permite trabajar en modo cliente-servidor.
- Gran variedad de herramientas Administrativas y de desarrollo.
- Incluye herramientas para extraer y analizar datos.

MySQL

Sistema de gestión de bases de datos relacional multihilo y multiusuario, creado por MySQL AB alrededor de los 90´s.

Principales características:

- Soporte de comunicación con múltiples lenguajes de programación.
- Es un sistema multiplataforma.
- Ofrece un sistema de contraseñas y privilegios seguro.
- Soporta gran cantidad de datos.
- Cuenta con varios mecanismos de almacenamiento.
- Conectividad segura.
- Replicación.

- Software libre con esquema de licenciamiento dual.

Oracle

Sistema de Gestión de base de datos objeto-relacional desarrollado por Oracle Corporation a finales de los 70´s, se considera en el mercado como uno de los sistemas de base de datos más complejos.

Principales características:

- Soporte de transacciones.
- Estabilidad.
- Soporta gran cantidad de datos
- Escalabilidad.
- Soporte multiplataforma.
- Cuenta con un lenguaje de diseño de base de datos muy complejo (PL/SQL).
- Replicación.
- Conectividad Segura.

El sistema de gestión de base de datos propuesto para el desarrollo del proyecto es MySQL, por su fácil interacción con múltiples lenguajes de programación, también se puede administrar en distintos sistemas operativos, nos brinda seguridad y es un software libre.

4.4.-Lenguaje de programación

Un lenguaje de programación se define como un sistema estructurado y diseñado principalmente para expresar procesos que pueden ser efectuados por una computadora. Existen principalmente tres tipos de lenguajes de programación:

Lenguaje máquina.- Lenguaje que comprende la máquina de forma directa, está escrito en código binario.

Lenguaje simbólico.- También conocido como lenguaje de bajo nivel, utiliza mnemotécnicos para la representación de las instrucciones.

Lenguaje de alto nivel.- Utilizan lenguaje "natural", es decir que utilizamos en la cotidianeidad.

Para el desarrollo de software orientado a aplicaciones que interactúen con el ser humano se utiliza el lenguaje de alto nivel.

Actualmente existe una gran variedad de lenguajes de programación de alto nivel que podemos elegir para satisfacer diversas necesidades. Si bien es cierto que muchos de ellos se pueden utilizar en diferentes ámbitos, siempre suele haber algún lenguaje que destaque entre los demás para determinada área. Por ejemplo para el desarrollo web suele utilizarse un lenguaje llamado HTML y JavaScript, ya que son lenguajes precisamente orientados al desarrollo de páginas web, permite hacer referencias a imágenes, videos o artículos contenidos en otros sitios web.

En nuestro caso buscamos un lenguaje de programación que nos facilite el desarrollo de una interfaz de usuario así como la implementación de los dispositivos RFID, sensor biométrico de huella digital y cámara web. Existen varios lenguajes que satisfacen dichos requerimientos, para fines prácticos tomaremos los tres lenguajes que cumplen con la mayoría de los requerimientos particulares para el desarrollo del programa. A continuación se muestra una tabla comparativa de C++, Visual Basic y Java.

Tabla 4.1. Comparativa de Lenguajes de programación

Lenguaje	Orientado a Objetos	Libre	Multiplataforma	Incluida en API's de dispositivos	Fácil conectividad con Base de Datos	Fácil conectividad con cámara web
C++	☆	☆	☆	☆	☆	
Java	☆	☆	☆	☆	☆	☆
Visual Basic	☆			☆		

Como se observa en la tabla C++ y Java cumplen con la gran mayoría de los requerimientos de nuestro sistema, sin embargo Java es un lenguaje con el que nos familiarizamos más, lo que nos ahorra considerablemente el tiempo de desarrollo y permite que el sistema se instale en múltiples plataformas, por otro lado el hardware propuesto para la implementación cuenta con librerías java que facilita su integración.

4.5.-Metodología de desarrollo del programa

Para el desarrollo de un software se utiliza una metodología, ya que todo software cuenta con un ciclo de vida, es decir, atraviesa un conjunto de fases, desde que nace la idea inicial hasta que el software es retirado o reemplazado. Con el fin de seguir un orden se han creado varios modelos de ciclos de vida dependiendo del tipo de software a desarrollar.

Para demostrar el funcionamiento del sistema de seguridad, se desarrolla una aplicación Java que integra los dispositivos ya antes mencionados, de los diversos modelos de ciclo de vida para el desarrollo de software se ha utilizado el modelo iterativo, este es un modelo derivado del ciclo de vida en cascada (Figura 4.2).

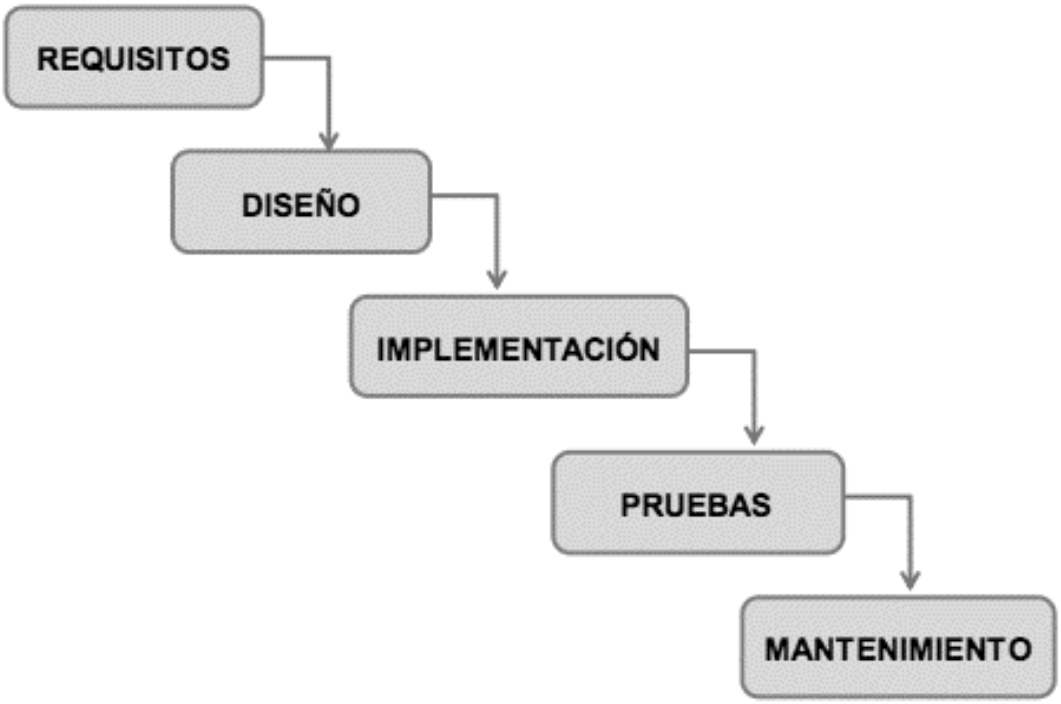


Figura 4.2. Modelo de ciclo de vida en cascada

El modelo de ciclo de vida iterativo (Figura 4.3) busca reducir el riesgo que surge entre las necesidades del usuario y el producto final por malos entendidos durante la etapa de recogida de requisitos. Consiste en la iteración de varios ciclos de vida en cascada. Al final de cada iteración se le entrega al cliente una versión mejorada o con mayores funcionalidades del producto. El cliente es quien después de cada iteración evalúa el producto y lo corrige o propone mejoras. Estas iteraciones se repetirán hasta obtener un producto que satisfaga las necesidades del cliente. Este modelo se suele utilizar en proyectos donde los requisitos no están claros por parte del usuario, sin embargo en nuestro caso, aunque los requisitos estaban claros, el programa se prestó para hacerle algunas mejoras, por lo que se hizo necesaria la creación de distintos prototipos o mejoras para presentarlos y conseguir nuestra conformidad.

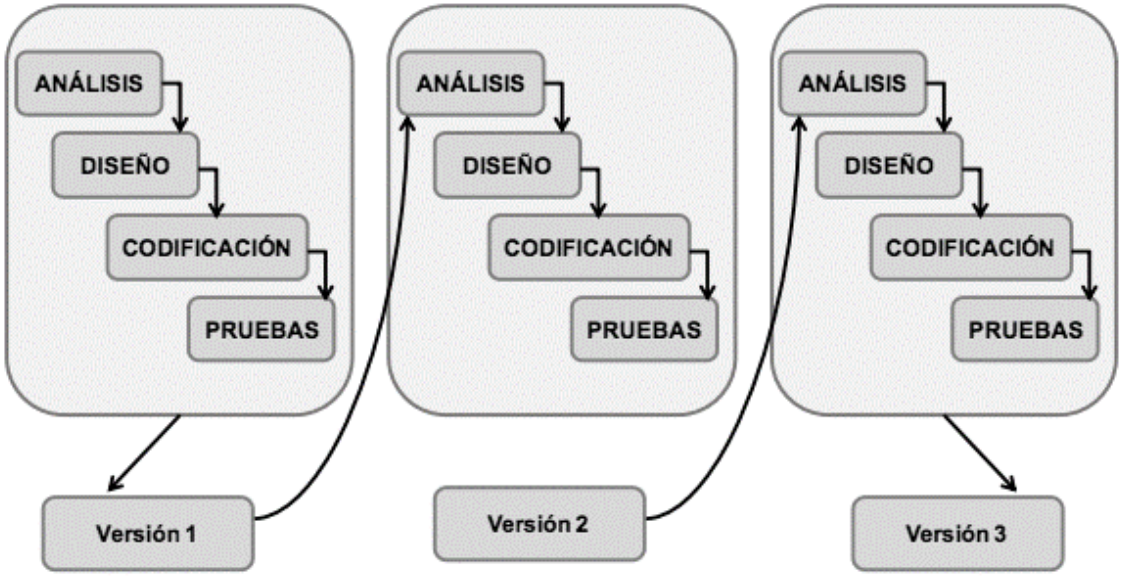


Figura 4.3. Modelo de ciclo de vida iterativo

La principal ventaja de este modelo es que no hace falta que los requisitos estén totalmente definidos al inicio del desarrollo, sino que se pueden ir refinando en cada una de las iteraciones, tiene la ventaja de realizar el desarrollo en pequeños ciclos, lo que permite gestionar mejor los riesgos y gestionar mejor las entregas.

Capítulo 5

Diseño e Implementación de un Sistema de Seguridad para un Estacionamiento

5.1-Diseño e implementación del Sistema

Una vez definido el objetivo, se describe a continuación el diseño de un sistema de seguridad que integre los elementos antes mencionados con el fin de disminuir el riesgo de robo de auto en un estacionamiento.

El estacionamiento debe contar con una entrada independiente de la salida, es decir, los automóviles tendrán una sola entrada y una sola salida, independiente una de la otra. La entrada y la salida deberán contar con una barrera tipo pluma que restrinja el paso vehicular. Adicionalmente se recomienda instalar una cámara de circuito cerrado a la entrada y a la salida, teniendo así un registro en video de los eventos que se realicen en el estacionamiento (véase la figura 5.1).

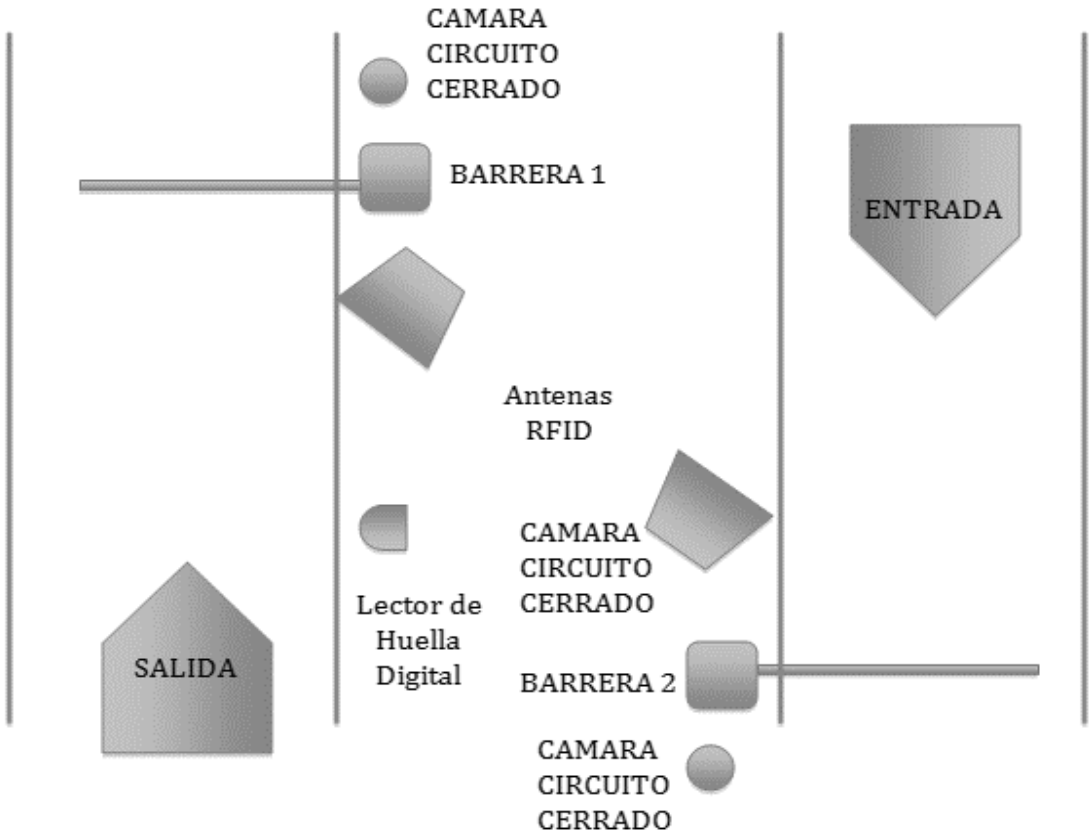


Figura 5.1. Diseño de la entrada y la salida

Ambos dispositivos, RFID y Lector de huella digital, se relacionan por medio de una interfaz alojada en un servidor, éste debe contener una base de datos con tres tablas: la primera contiene los datos del auto, la segunda los de los usuarios y la tercera un historial de eventos. Dicha interfaz tiene tres funciones elementales:

- Registro: Permite al administrador del estacionamiento ingresar los datos del automóvil y de los usuarios nuevos a las tablas de la base de datos y así registrar a los usuarios y su o sus automóviles al estacionamiento. Al momento del registro se asigna e instala un tag a cada vehículo, cada tag contiene un número único (ID) que lo diferencia de los demás y lo relaciona con el automóvil y con la huella digital del usuario que cuente con los permisos para conducir dicho auto. Esta información es especialmente importante ya que se utiliza en el proceso de validación.

- Validación: Esta función se comporta de manera diferente dependiendo de si se desea salir o entrar al estacionamiento.

    - Entrada: Cuando se desee ingresar al estacionamiento el software de validación por medio del Lector RFID lee el ID del tag, en ese momento el proceso de validación se encarga de verificar que el auto esté registrado en el estacionamiento, de ser así la Pluma permitirá el ingreso al automóvil y, de no contar con un registro en el estacionamiento la Pluma negará el ingreso del vehículo.

    - Salida: Si el usuario desea salir del estacionamiento entonces el software, por medio del lector RFID lee el ID del tag y valida si la huella

obtenida por medio del Lector de Huella digital cuenta con los permisos para conducir dicho automóvil, de ser así la pluma permite el egreso del automóvil y almacena la fecha, hora y usuario que conduce el auto en ese momento. En caso que la validación no sea exitosa, es decir que no se encuentre ninguna relación entre el usuario y el automóvil, la Pluma no permitirá el egreso del automóvil.

- Monitoreo: Se muestran los últimos eventos ocurridos en el estacionamiento, además los almacena en una tabla contenida en la base de datos. Cuenta también con una opción de búsqueda que permite al administrador obtener la información de algún evento en particular.

En resumen el sistema de seguridad en cuestión debe contar con cuatro elementos fundamentales:

1. Lector RFID
2. Lector de Huella digital
3. Interfaz de validación
4. Barrera vehicular tipo pluma

Ahora bien, cada elemento del sistema requiere ciertas características para el óptimo funcionamiento del sistema, las cuales se comentan a continuación.

1. El lector RFID debe contar con las siguientes características básicas:

- Lectura de mediano o largo alcance (2m a 3m) Lineal.
- Etiquetas RFID pasivas adheribles al parabrisas
- Capacidad para conectar dos antenas a un mismo lector RFID
- Capacidad para operar en exteriores

2. El lector de huella digital como se mencionó anteriormente, será instalado únicamente a la salida del estacionamiento, se encargará de autenticar al usuario que intente extraer el automóvil del estacionamiento. Las características mínimas para este dispositivo son las siguientes :

- Capacidad para operar en exteriores
- Un mínimo de 500 dpi
- Velocidad de lectura menor a 2 segundos
- Opción de autenticación por contraseña

3. Interfaz de validación que para este propósito se refiere a la integración de los dispositivos de autenticación que se comunican a través de un software de propósito específico el cual se ha diseñado y programado para este proyecto de tesis, al igual que los dispositivos anteriores, también debe cumplir con características básicas:

- Capacidad de integrar el Lector RFID, Lector de Huella Digital y la Barrera tipo pluma, es decir, deberá enviar y/o recibir información de los distintos dispositivos y darle el tratamiento requerido.
- Comparar los datos obtenidos del RFID, del Lector de Huella Digital con los datos almacenados en la base de datos y emitir un resultado correcto.
- Almacenar datos de los usuarios y de sus automóviles.

4. La barrera es un elemento importante ya que las características que lo definan a éste serán las que le proporcionen mayor o menor seguridad al sistema al momento de evitar la salida no autorizada de un vehículo.

Para un sistema de seguridad básico moderado se utiliza una barrera tipo pluma con las siguientes características:

- Brazo metálico para exteriores de 3 a 4 metros de longitud, dependiendo del escenario.
- Sensor anti-impacto, para evitar que la pluma baje antes de tiempo y dañe el automóvil o a algún transeúnte.
- Velocidad de apertura de 3 a 5 segundos.
- Control manual y automático.

Cabe señalar que la barrera tipo pluma es un dispositivo cuyo fin es restringir el paso del vehículo, sin embargo no cuenta con la capacidad física de detener el automóvil, más se complementa muy bien con la cámara de seguridad. Para ello existen otro tipo de barreras como la barrera poncha llantas, que sí impide el paso de vehículos pero el tiempo de acción es mucho mayor a la barrera tipo pluma.

A continuación se describe el diseño de la aplicación que integra las partes mencionadas.

5.2.-Diseño de la Aplicación

La aplicación que será utilizada para gestionar los dispositivos del sistema de seguridad, debe realizar funciones elementales mencionadas con anterioridad, además debe contar con una interfaz amigable y sencilla para el usuario administrador, debe estar alojada en un servidor dedicado a brindar servicio todo el tiempo que el estacionamiento lo requiera y debe ser compatible con la mayoría de los sistemas operativos que existen hoy en día. Para cumplir con dichos objetivos hemos elegido Java como lenguaje de programación ya que tiene la capacidad de

lograr tales objetivos. Java es un lenguaje multi-plataformas, lo cual le permite trabajar en entornos Windows, Linux, Unix en todas sus diferentes versiones.

El diseño y programación de ventanas es muy amigable para el programador y el resultado es amigable y cómodo para el usuario final, además es un lenguaje orientado a objetos, lo cual permite ahorrar líneas de código mejorando así el desempeño del programa, cuenta con API's (Interfaz de Programación de Aplicaciones) que ayudan a agilizar el desarrollo de nuevas funciones en el sistema, y tiene la ventaja de ejecutar varios procesos a la vez (Multithreaded).

Es un sistema seguro, robusto y además tiene la gran ventaja de ser libre, es decir que no es necesario adquirir ningún tipo de licencia para desarrollar software por medio de este lenguaje de programación. Para el desarrollo del sistema hicimos uso de un entorno de desarrollo llamado NetBeans versión 7.2.

Con el objetivo de hacer la interfaz fácil de usar, intuitiva, fácil de entender y segura, decidimos diseñar la interfaz por medio de ventanas. La interfaz contará con tres ventanas fundamentales para el uso del sistema:

Ventana principal o de monitoreo
Ventana de usuario y de vehículo nuevo.
Ventana de búsqueda

Ahora bien, a continuación se detalla el contenido de cada ventana:

a) Ventana principal.

Como se puede apreciar en la figura 5.2, esta ventana cuenta con un campo de información, para mostrar al administrador del sistema, los últimos eventos en el estacionamiento, los datos del usuario y del automóvil que salió o entró al estacionamiento. También contendrá una barra de opciones, dicha barra permitirá al administrador abrir una ventana nueva para agregar registros nuevos y/u otra para realizar una búsqueda.

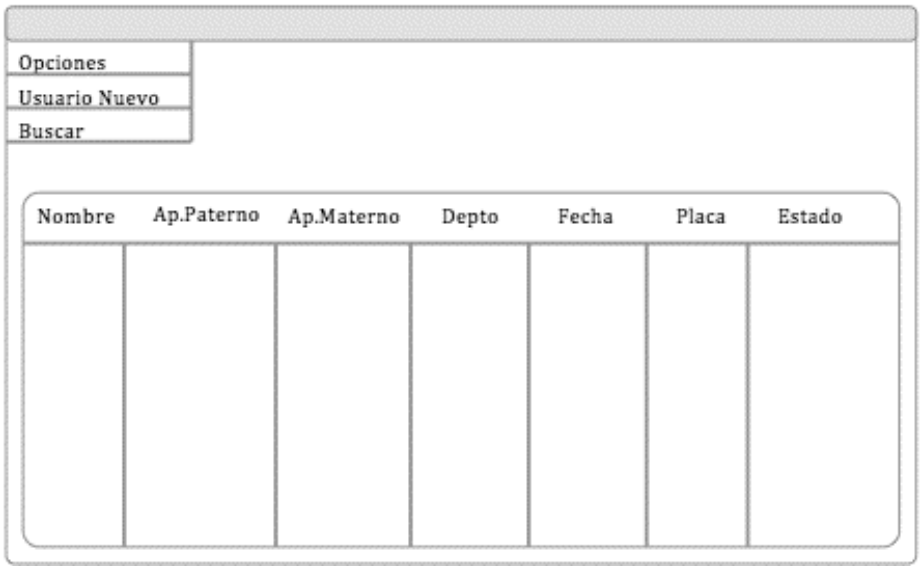


Figura 5.2. Ventana principal

b) Ventana de usuario y vehículo nuevo.

Como se aprecia en la figura 5.3 la ventana de usuario y de vehículo nuevo contara con dos campos para ingresar datos, un campo para ingresar los datos del usuario, y otro para ingresar los datos del automóvil. Contará con botones para deshacer los cambios, guardar los cambios, o salir de la pantalla y regresar a la pantalla principal.

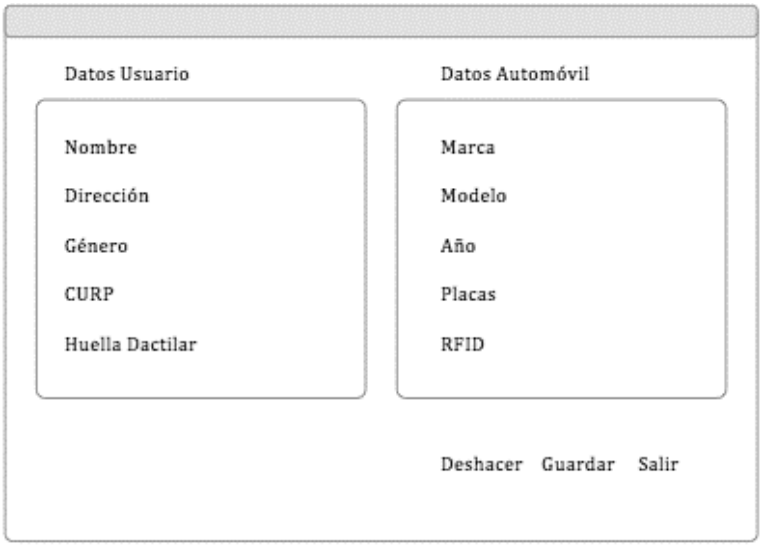


Figura 5.3. Ventana de usuario y vehículo nuevo

c) Ventana de búsqueda.

La ventana de búsqueda contará con un campo para que el administrador del sistema realice búsquedas de eventos realizados por un auto o persona en particular. Contendrá un menú en el que el administrador podrá elegir una opción de búsqueda e ingresara los datos para que el sistema le arroje la información deseada, como se observa en la figura 5.4.

Figura 5.4. Ventana de búsqueda

5.3.-Diseño de la base de datos.

Para un mejor entendimiento el nombre de la base de datos será "estacionamiento", la cual estará compuesta de únicamente tres tablas, dos de las cuales relacionadas por un campo, que permitirá la integridad de la misma y la interacción con la aplicación al momento de almacenar datos.

Tabla Usuarios

Debe contener el registro de los usuarios del sistema, a fin de almacenar información personal para la ubicación del mismo, tabla 5.1.

Tabla 5.1. Datos de Usuario

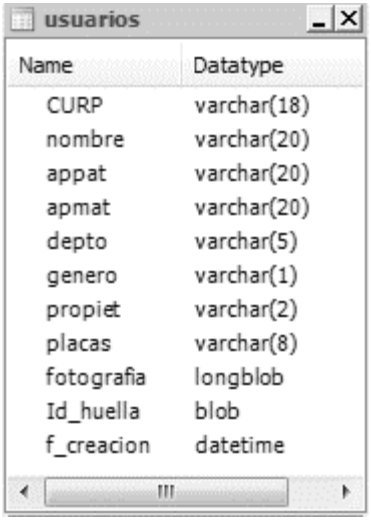


Tabla Auto

Contiene las características del auto, almacenara el estado del auto y la fecha de la última entrada o salida al estacionamiento, tabla 5.2.

Tabla 5.2. Datos del Auto

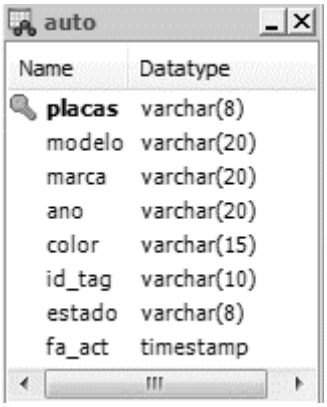
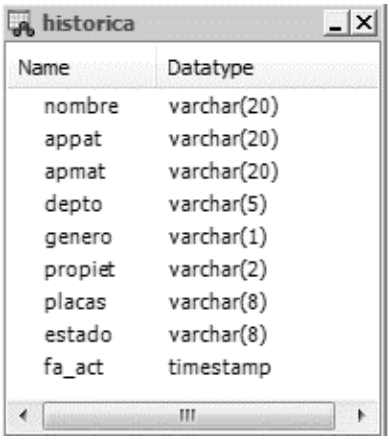


Tabla Historia

Guardará el historial de los autos y usuarios que salieron y entraron del estacionamiento, esta tabla será creada con fines de auditoría en caso de alguna aclaración con el estado del auto, Tabla 5.3.

Tabla 5.3. Histórica



A continuación se muestra el modelo entidad relación de la base de datos (Figura 5.5).

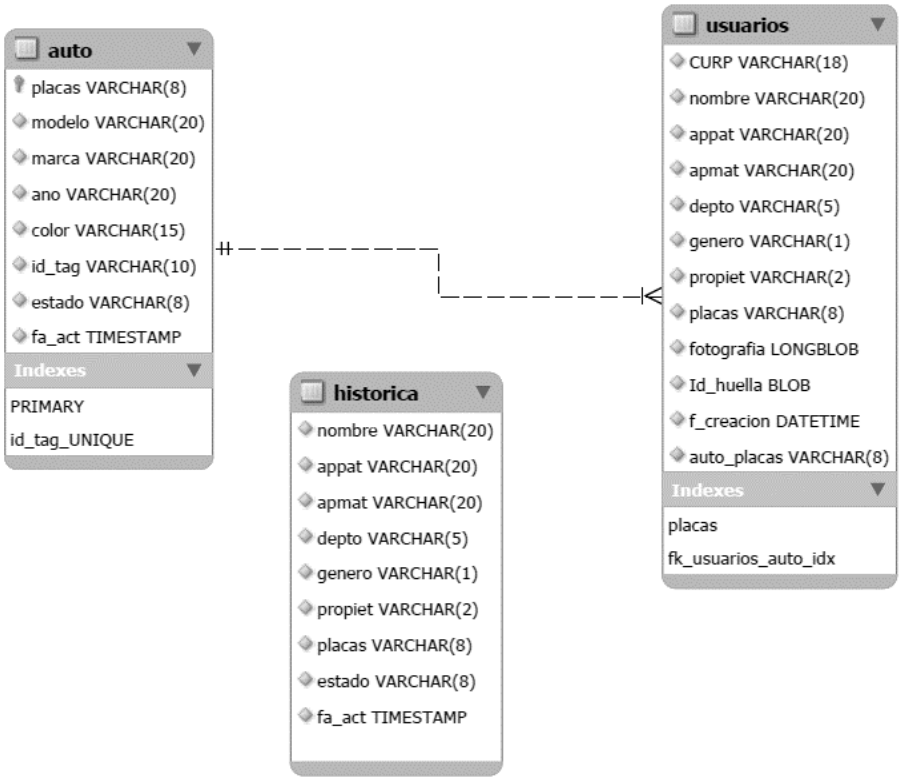


Figura 5.5. Modelo Entidad-Relación

5.4.-Casos de Uso.

A continuación se listan una serie de casos de uso en los cuales nos hemos basado para que el sistema funcione de manera eficiente en cualquier situación, sin embargo existen diversos casos no ideales que se pueden presentar una vez que el sistema entre en funcionamiento, para tales casos siempre queda la posibilidad de actualizar el sistema según la frecuencia y nivel de riesgo de dichos eventos.

I.-Entrada al estacionamiento.

1.-El usuario llega al estacionamiento

2.-La antena detecta el tag y lo compara con la bandera de ingreso, la cual verifica que el auto no haya sido marcado como ingresado.

3.-De ser positiva la comparación, es decir, el auto está registrado en el sistema, y está marcado como fuera o egresado, la pluma se levanta.

4.-El sistema marca el auto como ingresado y enciende una bandera.

5.-El auto ingresa y se dirige a su lugar asignado por la administración de la unidad.

I.I.-Entrada de un auto emergente o no registrado por motivos de emergencia.

1.-El usuario avisa a la administración en el horario establecido, por los medios acordados, que desea un tag emergente por causas de fuerza mayor.

2.-La administración informa al vigilante del estacionamiento para que éste le facilite al usuario un tag emergente a su llegada, y registre electrónicamente los datos del auto, los datos del usuario y el ID del tag.

3.-La administración dará de baja temporalmente el auto que por motivos de emergencia no entrará al estacionamiento hasta nuevo aviso del usuario.

4.-El usuario se comprometerá a devolver el tag por un periodo no mayor a 20 días, de lo contrario el tag será dado de baja y se le negará el acceso al estacionamiento, debido al número limitado de tags emergentes.

4.1.-De no haber tags disponibles el usuario podrá adquirir uno para su uso personal, pero deberá avisar a administración para asignar cada tag a cada auto, y de esta forma limitar el número de tags que el usuario pueda tener activos.

4.2.-El número de tags activos estará limitado por el número de cajones que posee el usuario.

5.-El usuario debe pedir a la administración que cambie el tag emergente por el tag de su auto original antes de tratar ingresar el mismo al estacionamiento.

II.-Salida del estacionamiento.

1.-El auto llega a la salida del estacionamiento.

2.-La antena detecta el tag y verifica que sea un auto registrado.

3.-De ser un auto registrado pide al usuario que ingrese su huella digital, posteriormente compara el ID del auto con la huella digital y verifica que corresponda el auto con el usuario.

4.-De ser positiva la comparación, el sistema levanta la pluma para dejar salir el auto.

5.-El auto sale y el sistema lo marca como egresado con una bandera.

III.-Cortes de energía eléctrica.

1.-En caso de cortes de energía eléctrica, el vigilante deberá avisar de inmediato a la administración, y deberá llevar un registro de los autos que ingresan y de los autos que salen de manera manual, en una bitácora.

2.-Dicha bitácora deberá contener los datos del auto, como son: modelo, color, marca, placas y hora de ingreso o de egreso, así como los datos del usuario como son: Nombre completo y dirección de residencia o departamento en el que labora.

2.1.-El sistema puede contar con equipo electrónico extra en el que el vigilante pueda verificar por medio de las placas del auto si es que está registrado en el sistema, así mismo pueda verificar por medio del nombre del usuario si éste está registrado en el sistema.

2.2.-De ser usuarios registrados se les dejara entrar, y a la salida deben ser usuarios registrados y deben ser los conductores asignados al auto en cuestión.

*Es recomendable contar con una planta de energía independiente, que pueda proveer de energía al sistema para que no existan cortes y su eficiencia no se vea afectada de ninguna manera.

IV.-Entrada en falso.

1.-El auto llega a la entrada del estacionamiento.

2.-La antena lee el tag y le brinda el acceso, abre la pluma, y marca la bandera como ingresada.

3.-El auto por alguna razón no ingresa.

4.-En tal caso el usuario debe comunicar al vigilante y él a su vez a la administración para cambiar la bandera de ingresado a egresado, y así el auto pueda entrar al estacionamiento.

V.-Salida en falso.

1.-El auto llega a la salida del estacionamiento.

1.1.-La antena lee el tag y espera por la huella digital, de no brindar la huella digital en un determinado tiempo, se cancela la petición y espera al nuevo usuario.

1.2.-El usuario ingresa su huella digital y el sistema lo marca como egresado del estacionamiento.

2.-El auto por alguna razón no sale.

3.-En tal caso el usuario debe comunicar al vigilante y éste a su vez a la administración para cambiar la bandera de egresado a ingresado, y así el auto pueda entrar al estacionamiento.

VI.-Fallo del tag del auto a la entrada.

1.-El conductor desea salir con el auto del estacionamiento y no es detectado por el lector RFID.

2.-Se verifican los datos de cliente, modelo y números de placa para asegurar que pertenece al estacionamiento.

3.-Se le comunica de inmediato al administrador para que autorice el préstamo de un tag emergente.

4.-El administrador en un periodo de 15 días deberá contactar al cliente para colocar un nuevo tag al auto. Dicho tag debe estar actualizado en la base de datos.

VII.- Fallo del tag del auto a la salida.

1.-El auto llega al estacionamiento y no es detectado por el lector RFID.

2.-Se verifican los datos de del vehículo y usuario en la base de datos.

3.-Se le comunica de inmediato al administrador para que autoricé el préstamo de un tag emergente.

4.-El administrador en un periodo de 15 días deberá contactar al cliente para colocar un nuevo tag al auto. Dicho tag debe estar actualizado en la base de datos.

VIII.-Fallo de lector RFID a la entrada y/o a la salida.

1.-El auto llega al estacionamiento y no es detectado por el lector.
2.-Se verifica que no haya error en el tag.

3.-Se le notifica al administrador, el cual deberá instalar un nuevo lector en un periodo máximo de 3 días (leer NOTA 1).

4.-Se pondrá a funcionar un lector de repuesto que pertenece a la administración. Hasta que se instale un nuevo lector.

NOTA 1:

Si el lector RFID del estacionamiento falla, se le notificara al cliente quien podrá exigir la garantía. En caso de no existir garantía tendrá que comprar otro lector para poder ser instalado en el estacionamiento por la administración.

IX.-Fallo del sensor biométrico.

1.-El conductor desea salir con el auto del estacionamiento.

2.-El auto es detectado pero la huella del conductor es rechazada

3.-Se verifica que efectivamente el sensor biométrico no esté funcionando.

4.-Se le notifica al administrador, quien deberá instalar y configurar un nuevo sensor en el menor tiempo posible (leer NOTA 2).

5.-Se pondrá a funcionar un sensor de repuesto que pertenece a la administración. Hasta que se instale uno nuevo.

NOTA 2:

Si el sensor biométrico del estacionamiento falla, se le notificará al cliente, quien podrá exigir la garantía del mismo. En caso de no existir garantía tendrá que comprar otro sensor para ser instalado y configurado en el estacionamiento por la administración.

5.5.-Hardware y Software.

Hoy en día existe una gran variedad de dispositivos y programas que pueden utilizarse para la implementación de un sistema como el que se ha realizado, sin embargo no todos son los indicados para su implementación, elegir los dispositivos correctos depende en gran medida de los requerimientos del proyecto, del entorno físico en el que se vaya a implementar, de los niveles de seguridad deseados, y del presupuesto con el que se cuente. Sin embargo para un caso ideal como el que se presenta en este proyecto existen dispositivos que podrían funcionar muy bien para el desarrollo del sistema.

5.5.1.-Recomendación de dispositivos para caso real.

Para fines prácticos se ha supuesto un escenario de un estacionamiento en una unidad habitacional de aproximadamente 200 a 250 automóviles, y un promedio de 2 posibles conductores por vehículo, lo que da un total de 400 a 500 conductores aproximadamente. Con base en los datos anteriores se procedió a buscar el dispositivo que cumpliera con los requerimientos necesarios para desempeñar las funciones del sistema y que además tuviera el menor costo en relación a sus capacidades.

5.5.2 Sistema RFID.

Según el análisis realizado a diferentes dispositivos RFID se concluyó que el más adecuado según la relación funcionalidad/costo es el siguiente (véase figura 5.6).

Artículo: Lector/grabador UHF A1000/19

Marca: Ferakmon

Descripción: consta de antena con conexión serial y TCP/IP incorporada, que permite un alcance de hasta 6 metros de lectura en línea visible. Ideal para entornos de largo alcance o para espacios de lectura reducidos. Fácil instalación aguanta intemperie.

Aplicaciones:

- Logística y gestión de almacenes: Flujo de bienes, gestión de almacenes y gestión de correos, paquetería y equipaje.
- Gestión inteligente de aparcamiento: Gestión de parking y cargo automático.
- Gestión de líneas de productividad: Producción de procesos de identificación.
- Inspección de pruebas de falsificación de producto: usando funciones de protección de escritura en los tags e identificando los productos.
- Otras aplicaciones: Usado ampliamente en gestión de clubs, bibliotecas, escuelas, gestión de consumo, de tiempos, etc.

Especificaciones Técnicas:

Rango de Lectura: Hasta 6 metros

Potencia: 0~30dBm, software programable

Velocidad de Lectura: 64bits<6ms

Antena: Polarización circular de la antena integrada

Alimentación: 9V DC.

Medida: 280mm x 280mm x 70 mm

Peso: 1.5 kg

Temperatura de operación: -20 ^{0}C ~ +80 ^{0}C

Costo: USD $1,031.00

Figura 5.6. Lector/grabador UHF A1000/19

Cuenta con software programable así como con API programable en JAVA, C++ y .NET lo cual es de suma importancia ya que brinda la posibilidad de modificar o crear funciones nuevas para este dispositivo.

También existe un dispositivo de Motorola que cumple con los requerimientos para desempeñar las funciones requeridas por el sistema. Figura 5.7.

Artículo: Lector RFID Fijo FX7400

Marca: Motorola

Descripción: Fácil de implementar, utilizar y administrar, la Serie FX7400 de lectores RFID fijos de alto rendimiento de Motorola es ideal para implementaciones empresariales a nivel mundial en entornos de espacio reducido y orientados al cliente. Combina un diseño sumamente compacto con un completo set de funciones empresariales altamente integradas, incluidas las siguientes: autodescubrimiento y configuración específica de la aplicación para facilitar su instalación; Potencia sobre Ethernet (POE) para evitar costosas pérdidas de potencia; y avanzadas funciones especialmente diseñadas para proteger la transmisión de datos. Esta exclusiva combinación convierte a la Serie FX7400 de lectores RFID fijos en la opción ideal para aplicaciones de administración de activos empresariales e inventario de comercios minoristas en cualquier tipo de entorno donde la implementación RFID requiera de un espacio reducido.

Especificaciones Técnicas:

Rango de Lectura: Hasta 6m
Potencia: +15 -+ 30dBm
Antena: Polarización circular
Alimentación: +24Vcc o POE

Medida: 19.5cm x 14.9cm x 4.32cm

Peso: 0.82 kg

Temperatura de operación: -20 ^{0}C a +55 ^{0}C

Humedad: 5 – 95%, sin condensación

Costo: USD $1,230.00

Soporte API: .NET, C y JAVA

A diferencia del lector anterior éste cuenta con una memoria interna de 64 MB para almacenar los datos recabados de los tags. Además cuenta con capacidad para 4 antenas marca Motorola.

Figura 5.7. Lector RFID Fijo FX7400

5.5.3.-Recomendación de Lector de Huella Digital

Para el caso del lector de Huella Digital se encontraron distintos dispositivos que cumplen plenamente con las características requeridas por el sistema de seguridad, uno de ellos fue mencionado en el capítulo anterior, debido a sus características, diseño y costo el lector de huella digital llamado U.are U,

4000b es utilizado incluso en bancos nacionales para la identificación de usuarios. A continuación se recomiendan dos dispositivos más que cumplen con los requerimientos de funcionalidad:

Artículo: U. are U. 4500

Marca: Digital Persona

Descripción: El lector de huella digital U.are.U 4500 en un periférico USB ideal para múltiples usuarios en ambientes compartidos. Utiliza tecnología de escaneo óptico de huella digital para lograr una excelente calidad de imagen, una amplia área de lectura y una enorme fiabilidad. El dispositivo está diseñado para trabajar conjuntamente con el sistema DigitalPersona Pro Enterprise, el cual es un sistema desarrollado por Digital Persona para la autenticación de usuarios. El dispositivo U.are.U cuenta también con un Kit de desarrollo (SDK), lo que le permite a los desarrolladores integrar el dispositivo a cualquier sistema de seguridad. Figura 5.8.

Especificaciones Técnicas:

Resolución: 512 dpi

Área de captura: 14.6 mm X 18.1 mm

8-bit escala de grises (256 niveles de gris)

Compatible con USB 1.0, 1.1 y 2.0 (Full Speed)

Voltaje: 5.0V ±5% administrado por USB

Temperatura de operación: 0 - 40 C

Humedad de operación: 20% - 80% no condensada

Temperatura de almacenamiento: 10 - 60 C

Humedad de almacenamiento: 20% - 90% no condensada

Peso: 105 g.

Interface USB: 2.0 Full-speed High Power Device

FAR 0.001%

FRR 0.1%

Costo: $1,390.00 MN.

Figura 5.8. Lector de Huella digital U. are U. 4500

Artículo: Fingkey Hamster II DX

Marca: Nitgen

Descripción: Este lector de huella digital posee un sensor de identificación de presencia de dedo. Una vez el dedo es detectado sobre el sensor se puede proseguir a activar el escáner para capturar la huella dactilar, no es necesario pulsar ninguna tecla (Véase figura 5.9).

Conectado al puerto USB de un PC permite aprovechar las ventajas y seguridad de la autenticación biométrica. Cuenta también con un kit de desarrollo (SDK) en java para entornos Windows y Linux.

Especificaciones Técnicas:

Resolución escáner óptico: 500 dpi

Rango de temperatura: 0 ºC a 40 ºC

Alimentación: DC 5 [V]

Dimensiones: 61 x 80 x 47 (mm)

FAR 0.001%

FRR 0.1%

Costo: $2,900.00 MN

Figura 5.9. Lector de Huella Fingkey Hamster II DX

5.5.4.- Material utilizado para la simulación.

Debido a los altos costos de los materiales y a que no se contaba con un escenario propicio para llevar a cabo la implementación del sistema en un caso real, se optó por construir un modelo que ejemplificara de manera tangible el funcionamiento del sistema, para lo cual se utilizó el hardware descrito en el capítulo 2 y 3, correspondientes a RFID y al lector de huella digital, adicionalmente se utilizó una serie de materiales tanto de hardware como de software que se listan a continuación:

- RFID 1024_0 marca Phidget, con cable USB/firewire y tags GEN 2 tipo credencial.
- Lector de Huella Digital U. are U. 4000b marca Digital Persona, con cable USB.
- Cámara Web de 3 megapixeles marca Logitech, conectada por medio de USB al equipo. En las pruebas también se ocupó la cámara web integrada a la laptop de 0.3 megapixeles.
- Laptop Acer con sistema operativo Windows Professional 7 a 32bits en la que se integraron los dispositivos por medio de una aplicación desarrollada en Java (lenguaje de programación multiplataforma), por lo puede funcionar también en un sistema operativo UNIX.
- NetBeans 7.0, el cual se puede descargar de manera gratuita, como entorno de desarrollo java.

  Así mismo se utilizó una librería de Java para la integración de la cámara web llamada JMF (Java Media Framework), la cual no se incluye dentro del JDK ni en el JRE de java, sin embargo es gratuita, se puede encontrar y descargar fácilmente en Internet.
- También se utilizaron librerías de Java incluidos en el RFID y en el lector de huella digital, así como ejemplos de código y los drivers propios de los dispositivos incluidos en la compra de los sensores.

Como se puede apreciar, los materiales con los que se desarrolló la maqueta son relativamente fáciles de conseguir y en su mayoría baratos, lo cual abre aún más la gama de posibilidades para aplicaciones de seguridad de este tipo a otras áreas de oportunidad.

Con base en los objetivos del proyecto los dispositivos seleccionados por sus características cumplen plenamente con el trabajo a realizar, además le dan

al sistema un bajo costo para su implementación en un estacionamiento de proporciones moderadas.

Además se pueden implementar diversos modelos de dispositivos de acuerdo a los requerimientos del escenario, ampliando las posibilidades de escalabilidad y mejoras tanto de software como de hardware.

En versiones posteriores a este sistema se le pueden implementar mejoras como por ejemplo, avisos de lugares libres en el estacionamiento, enviar mensajes a dispositivos móviles de los eventos realizados, desarrollarse en estacionamientos públicos, entre otros.

5.6.-Configuración de Software y Hardware.

Para el funcionamiento del sistema se requiere del uso de software en su mayoría libre, el cual funge como plataforma a nuestro sistema. A continuación se muestra como se configuró cada programa utilizado para la simulación.

a) JAVA KIT 7 Update 3.

Este programa se descarga desde la página del proveedor:

https://www.java.com/es/download/

Una vez descargado se procede a ejecutar el archivo, aparecerá una imagen como la siguiente. Figura 5.10. El programa ejecuta un *Wizard*, el cual es una interface que facilita al usuario la instalación de la aplicación.

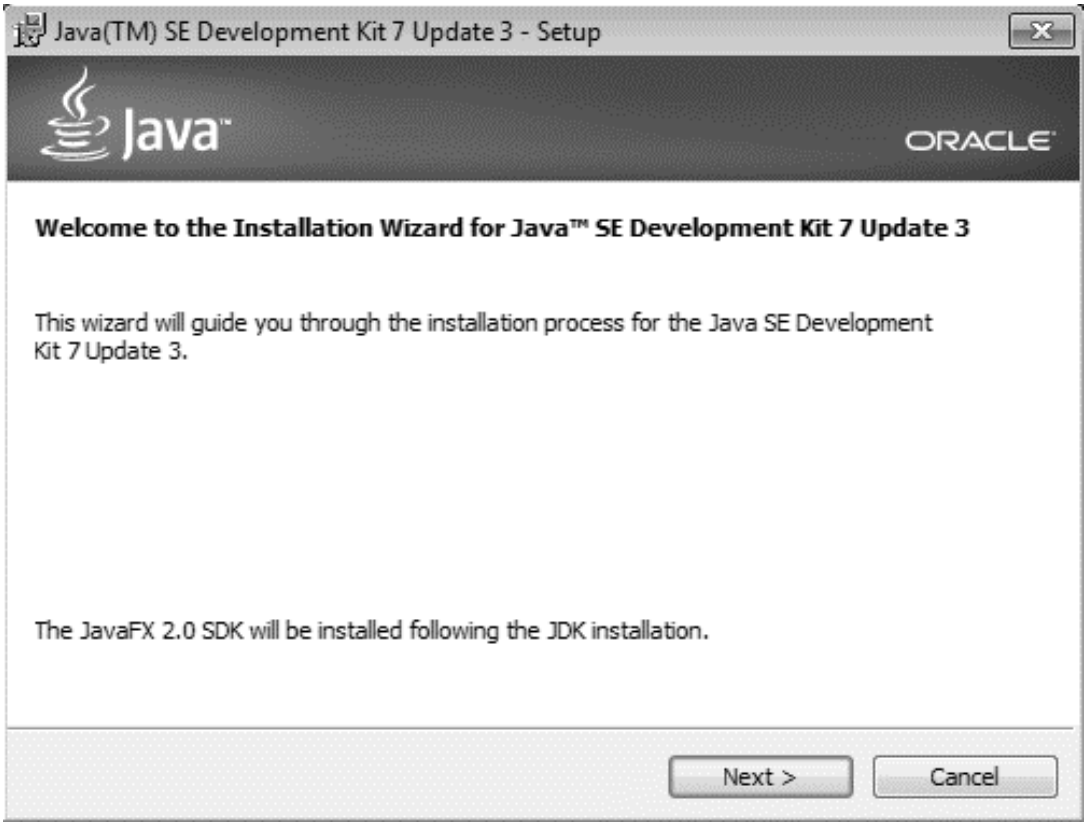


Figura 5.10. Wizard de Java

En la siguiente ventana aparecerán los módulos los cuales contienen las librerías, ejemplos y demás herramientas necesarias para desarrollar todo tipo de software.

No es necesario hacer ningún tipo de cambios en la selección de dichos módulos. Figura 5.11.

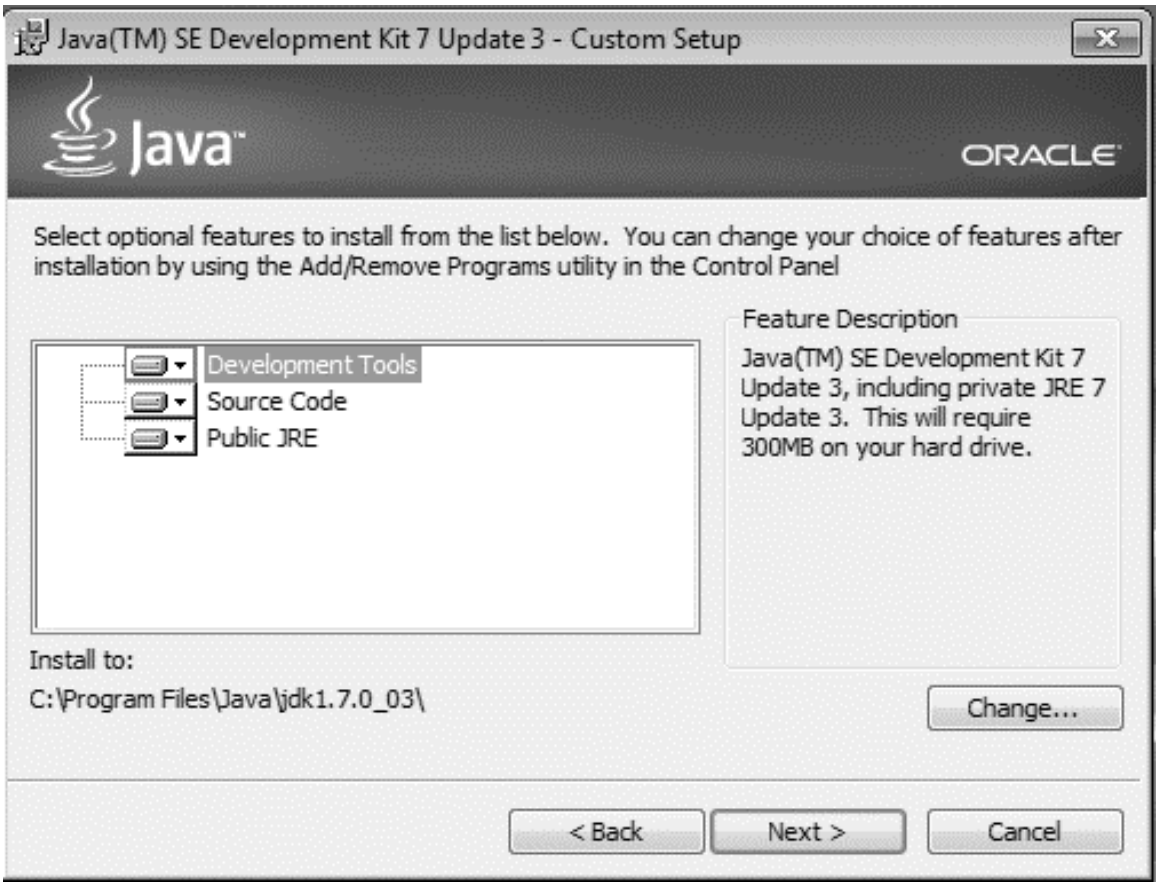


Figura 5.11. Selección de características

Posteriormente aparecerá una barra de estado indicando que está cargando la configuración deseada, al terminar aparecerá la ventana siguiente (Figura 5.12). En esta ventana se pide ubicar la ruta donde serán instalados los archivos del programa. No es necesario hacer ningún tipo de cambios en la ruta, hacemos click en Next.

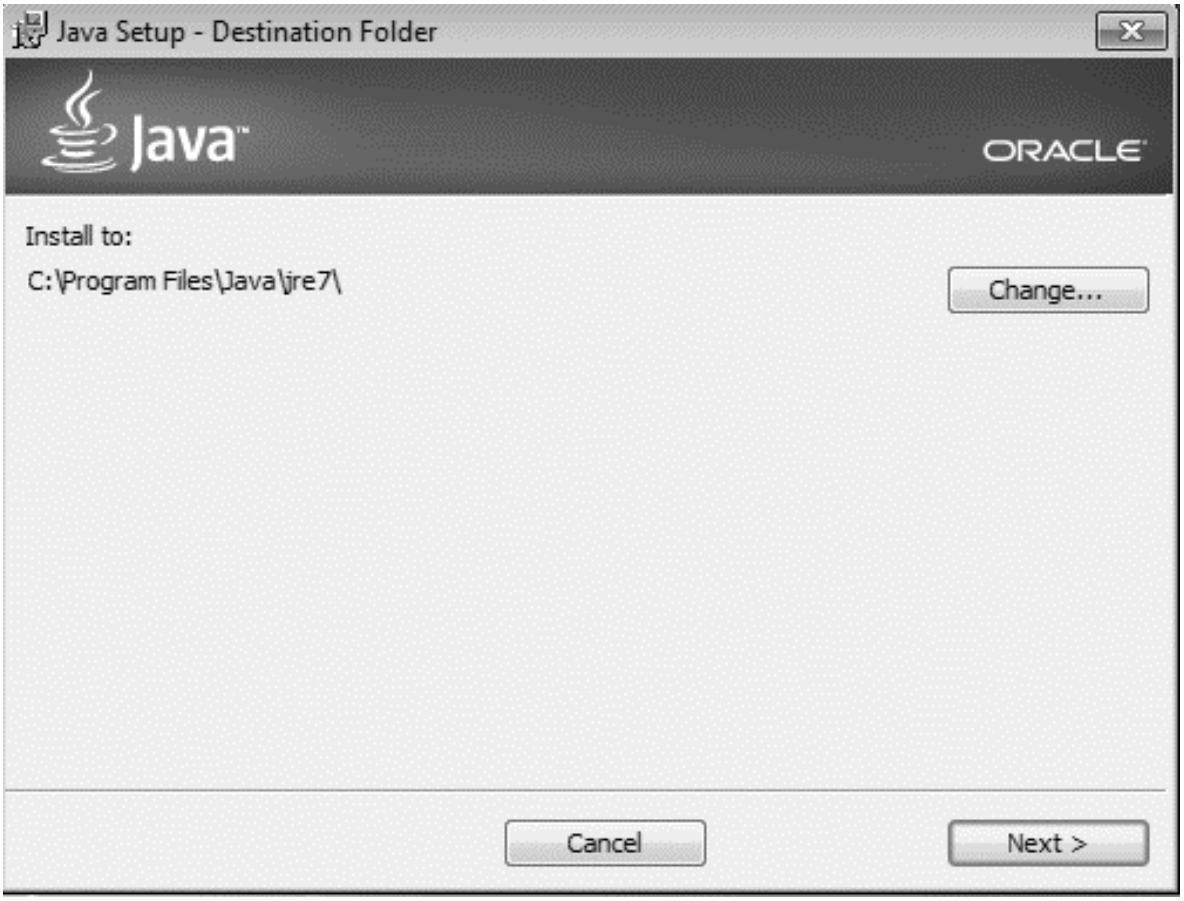


Figura 5.12. Selección de la ruta de instalación de JAVA

Aparecerá de nuevo una barra de estado, indicando que los archivos de instalación están siendo almacenados en el equipo. Al terminar se presentará la ventana de la Figura 5.13, en la cual se muestra la opción de registro a la página del proveedor para recibir ofertas y/o promociones de sus aplicaciones y servicios. No es necesario el registro por el momento, sin embargo en un determinado momento podría llegar a ser útil el registro para tener más información de las actualizaciones o servicios del proveedor, dado que en estos momentos se realiza un prototipo el registro no se realizó.

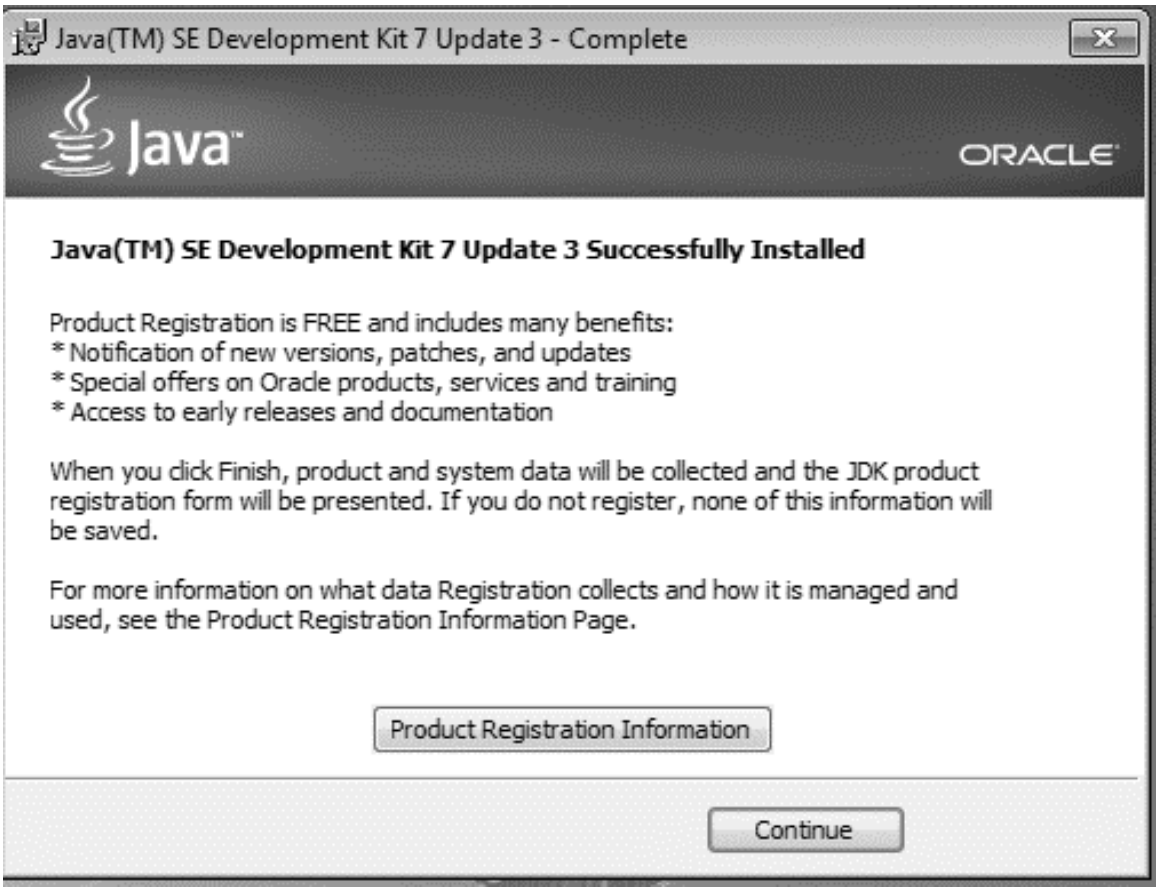


Figura 5.13. Registro del Producto JAVA

Con esto se concluye la instalación de la plataforma base, la cual proporciona las librerías necesarias para desarrollar la aplicación.

b) SDK Digital Persona

Ahora se requiere instalar el driver o controlador para el lector de huella digital, este driver es proporcionado por el proveedor al momento de adquirir el sensor, su costo está incluido en el paquete.

Se inserta el CD entregado por el proveedor, ahí dentro se debe buscar una carpeta llamada "sdk dpersona", dentro de esa carpeta se encuentran dos carpetas más, una con el driver compatible con Windows y otro para Linux (Figura 5.14), en este caso se abre la carpeta para Windows.

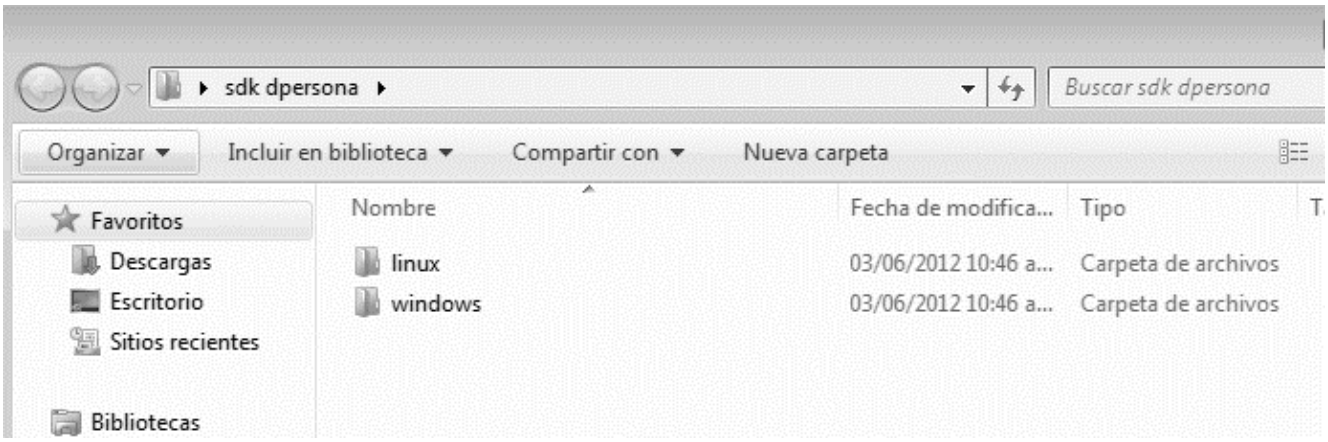


Figura 5.14. Sub carpetas Windows y Linux

Dentro de la carpeta Windows se haya la carpeta nombrada SDK y se da doble clic en el ejecutable llamado "Setup". Figura 5.15.

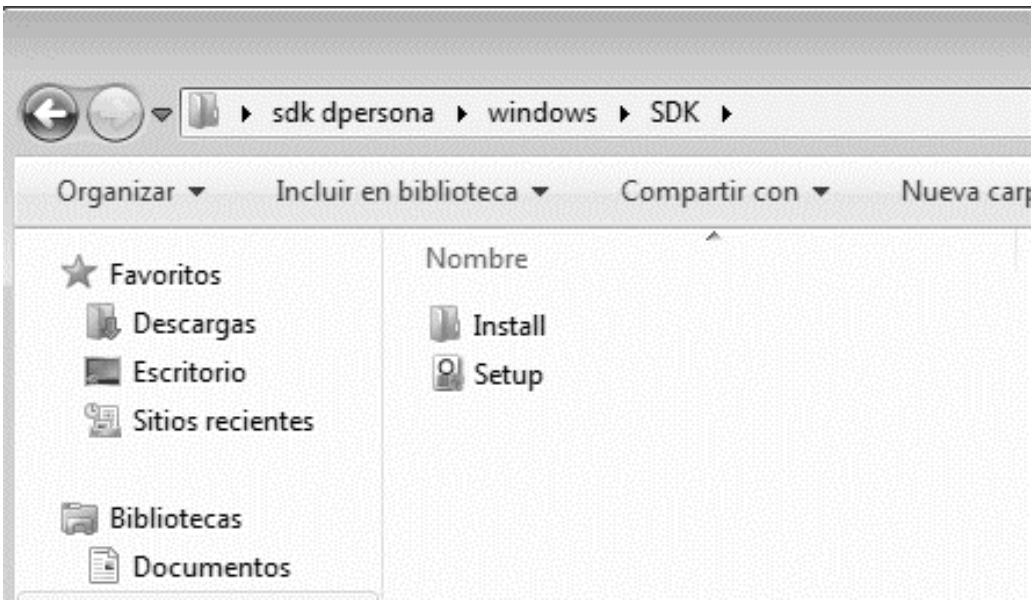


Figura 5.15. Archivo Ejecutable "Setup"

Se ejecutará el *Wizard* de instalación del programa y aparecerá la siguiente ventana (Figura 5.16). Se da click en "Next".

Figura 5.16. Wizard de Instalación del Driver Digital Persona

Se presentará una ventana con las cláusulas de la licencia del programa (Figura 5.17), en el que el usuario se hace responsable de cualquier uso indebido del mismo, como por ejemplo hacer uso del driver del dispositivo para realizar alguna operación que vaya en contra de las leyes del país donde se ejecuta la operación. Debido a que la aplicación no se desarrollará para fines ilegítimos y por el momento no se hará de manera comercial, entonces se selecciona "*I accept the terms in the license agreement*".

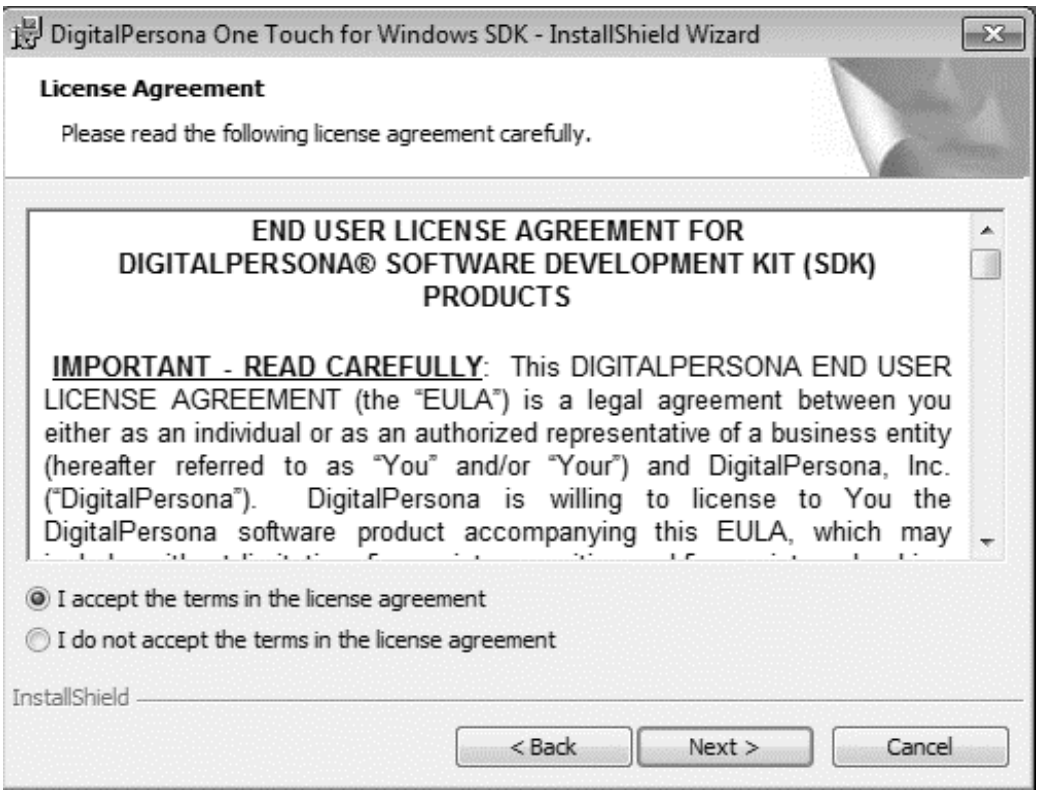


Figura 5.17. Términos de licencia del producto

Posteriormente se selecciona la ruta de instalación de los archivos. No es necesario hacer cambios en la ruta de instalación. Figura 5.18. Se da click en "Next".

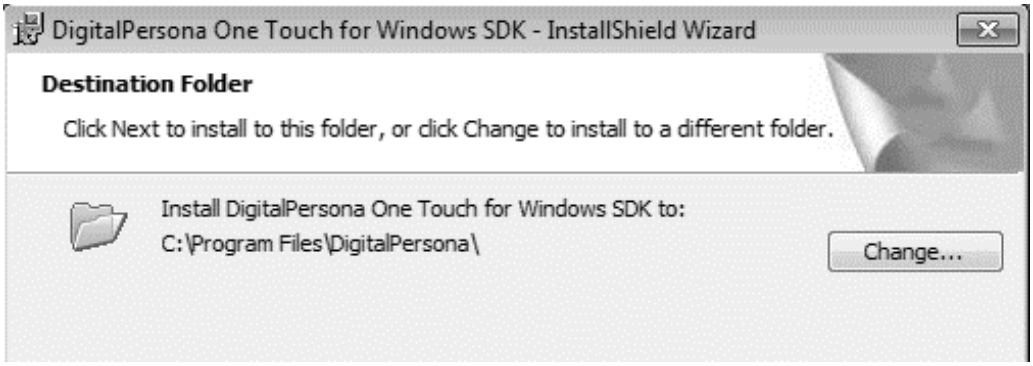


Figura 5.18. Selección de ruta de instalación

Hay que seleccionar la paquetería que se desea instalar, en este caso únicamente Java.

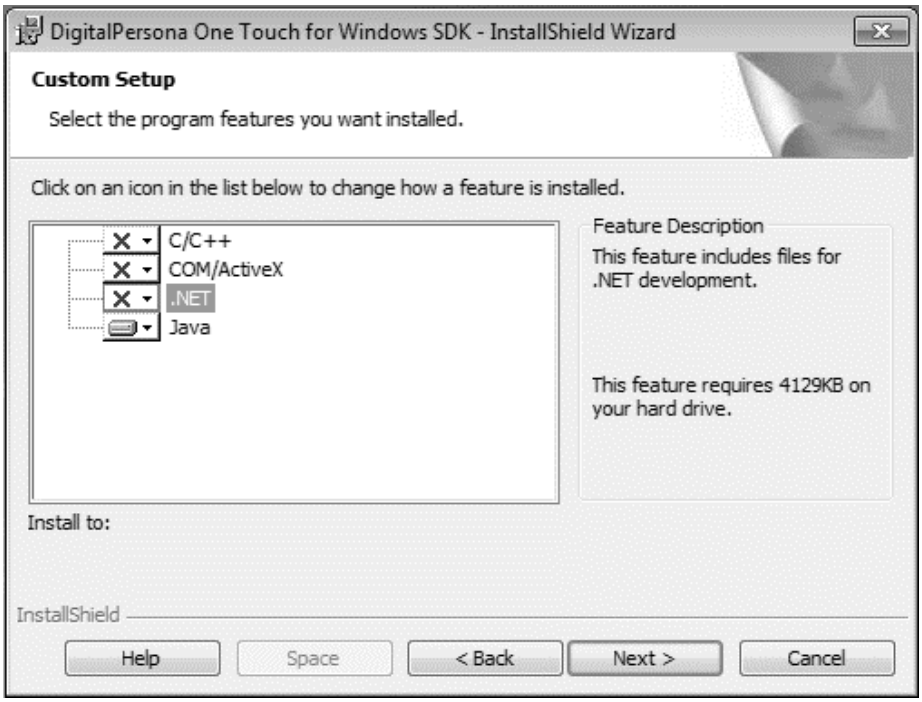


Figura 5.19. Selección de librerías

Finalmente se procede a instalar el SDK, al terminar es necesario reiniciar el equipo.

c) Driver Phidget

Ahora debemos instalar el driver para el lector de RFID, el cual se descarga de la página del proveedor:

http://www.phidgets.com/docs/Operating_System_Support

Este software le permite al ordenador reconocer el Lector de RFID, en la página se puede encontrar disponible para Windows, Linux y MAC OS.

Una vez descargado el archivo phidget_installer.exe, se ejecuta y se siguen las instrucciones del instalador.
Se elige la siguiente ruta para su instalación:

C:|Program Files|Phidgets|

Es necesario dar clic en Next, y esperar unos minutos mientras el producto es instalado.

d) NetBeans.

Por último se instala un IDE (Integrates Development Enviroment), es un entorno gratuito y se puede descargar de la página siguiente:

https://netbeans.org/downloads/

Se utiliza Java SE version 7.0.1. Una vez descargado el software se ejecuta, y seleccionamos la siguiente ruta de instalación:

C:\Program Files\Net Beans 7.0.1\

Se aceptan los términos de licencia y se espera a que el software se instale, al terminar se reinicia el ordenador.

5.7.-Implementación del sistema

Para la elección del hardware y software se tomaron en cuenta aspectos de compatibilidad, no solo en el sistema operativo, también para el desarrollo de código. Las bibliotecas de java del dispositivo RFID, del sensor biométrico y cámara web permitieron construir un código de acuerdo a los objetivos del proyecto. (Véase figura 5.20.)

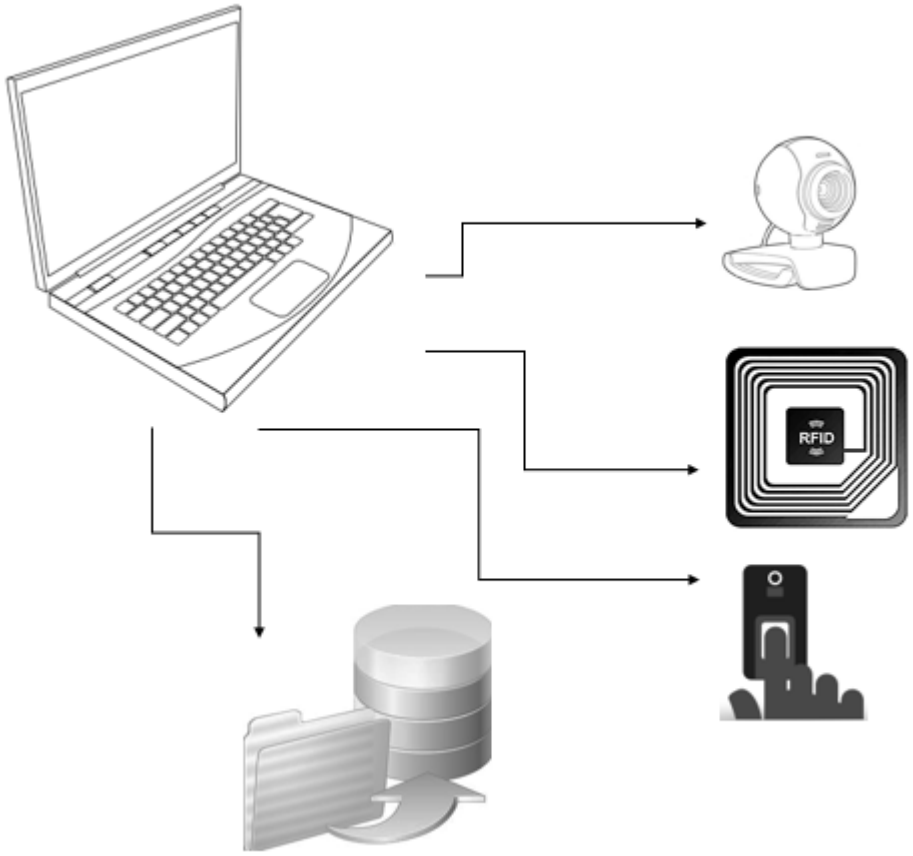


Figura 5.20. Aspectos de compatibilidad

5.7.1.-Interfaz de Usuario

La interfaz gráfica se compone de 5 paquetes que contienen las clases que integran el código para interactuar con el hardware y la base de datos, también contiene el código de cada una de las ventanas gráficas para el registro, monitoreo y búsqueda de usuarios en la aplicación. (Figura 5.21.)

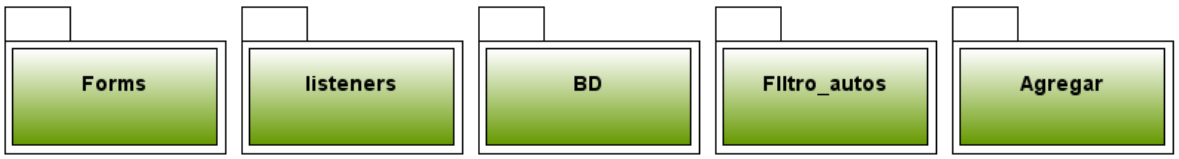


Figura 5.21. Interfaz gráfica

Forms

La clase usuarios, es la clase principal de la interfaz gráfica, contiene el monitoreo de la salida y entrada de automóviles al estacionamiento por lo que debe estar activa para permitir el acceso o denegar la salida, ésta contiene un menú con las opciones para agregar un nuevo usuario, agregar un usuario a un auto existente, agregar un auto a un usuario existente y buscar registros en la base de datos. (Véase figura 5.22.)

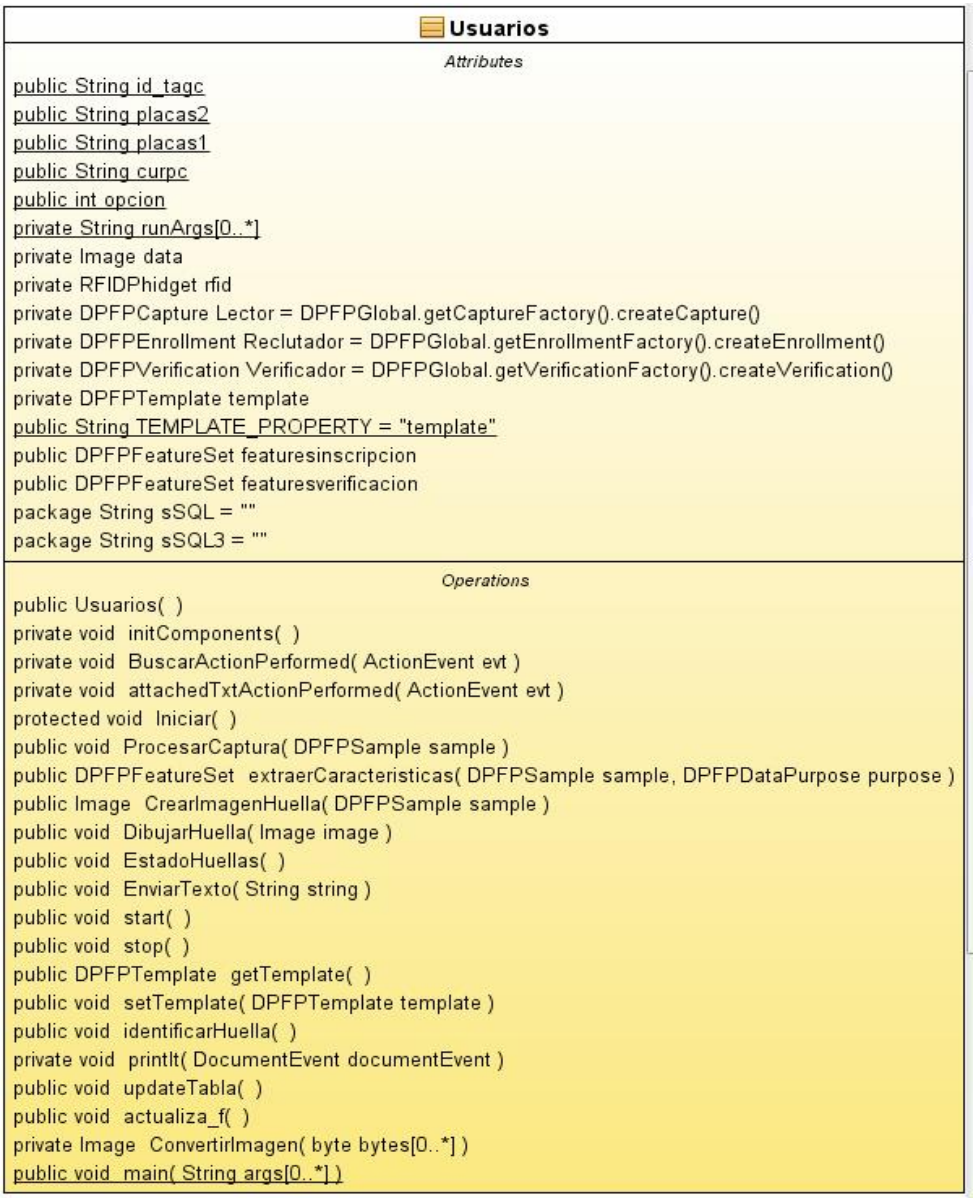


Figura 5.22. Clase de usuarios

La clase dispositivos permitirá reconocer la cámara web y capturar la imagen del usuario que se registre por primera vez en la base de datos. (Véase figura 5.23.)

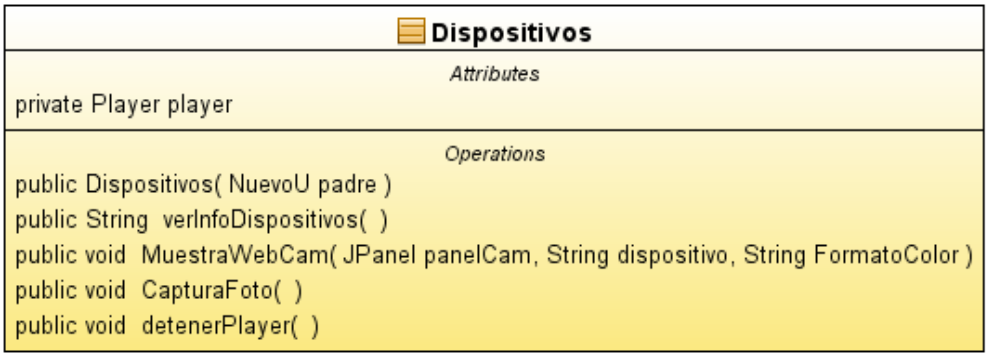


Figura 5.23. Clase de dispositivos

La clase RFIDTagGainLis_hist permite mediante el dispositivo RFID reconocer los tags que se aproximan de los automóviles, es llamada por la clase usuarios para monitorear la entrada y salida de los vehículos y guardar el estado actual del automóvil en la base de datos. (Véase figura 5.24.)

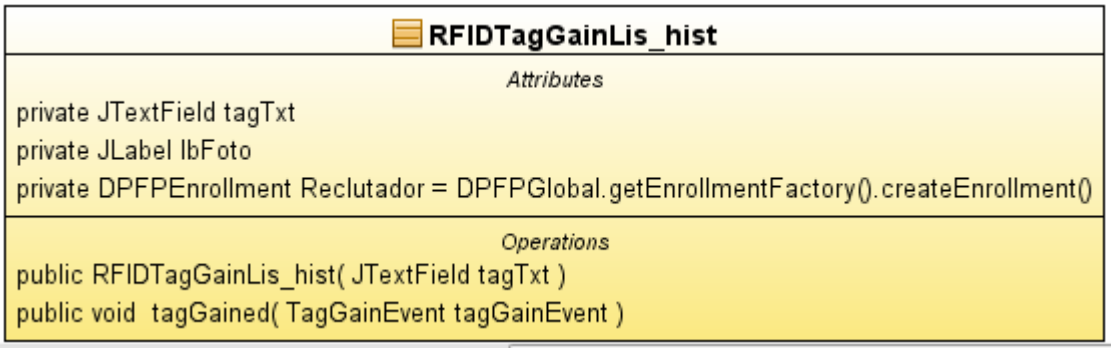


Figura 5.24. Clase RFIDTagGainLis_hist

La clase Odatos es usada por la clase usuarios para mostrar en la aplicación mediante una tabla, el historial de la entrada y salida de automóviles. (Véase figura 5.25.)

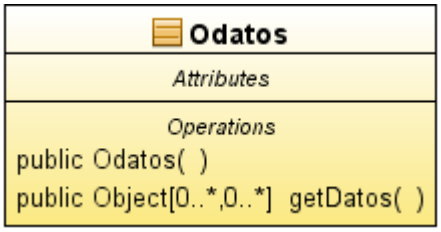


Figura 5.25. Clase Odatos

La clase búsqueda, realiza una conexión a la base de datos y por medio de opciones filtra consultas a la base de datos. (Véase figura 5.26.)

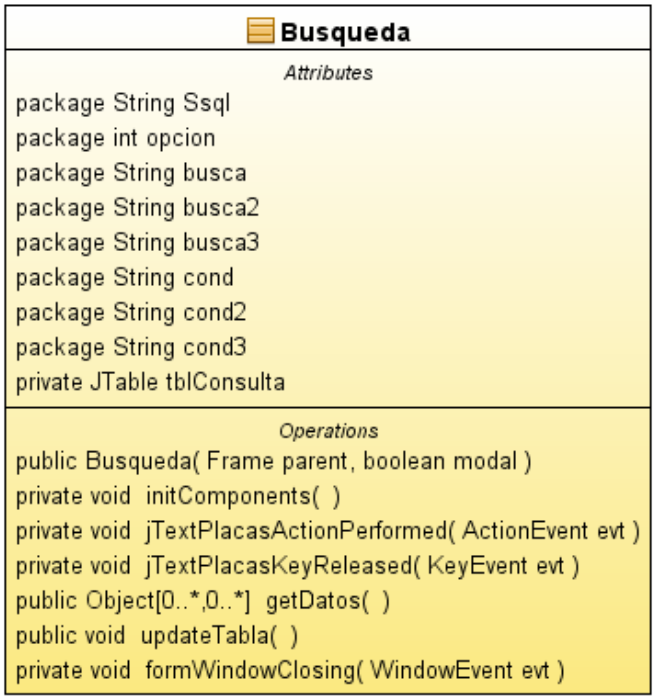


Figura 5.26. Clase búsqueda

Agregar

La clase NuevoU se encarga de registrar usuarios en la base de datos, realiza un llamado a los métodos y clases del RFID, sensor biométrico y de la cámara web para capturar los datos del usuario y del auto. (Véase figura 5.27.)

Figura 5.27. Clase NuevoU

La clase verifica como su nombre lo indica, es la encargada de verificar que en la base de datos exista el registro de un usuario mediante el reconocimiento de la huella dactilar. Esta clase es empleada cuando se agrega un auto a un usuario existente o se agrega un usuario a un auto existente. (Véase figura 5.28.)

Figura 5.28. Clase Verifica

La clase NuevoAu permite agregar a la base de datos un nuevo automóvil a un usuario que ya existe en la base de datos. (Véase figura 5.29.)

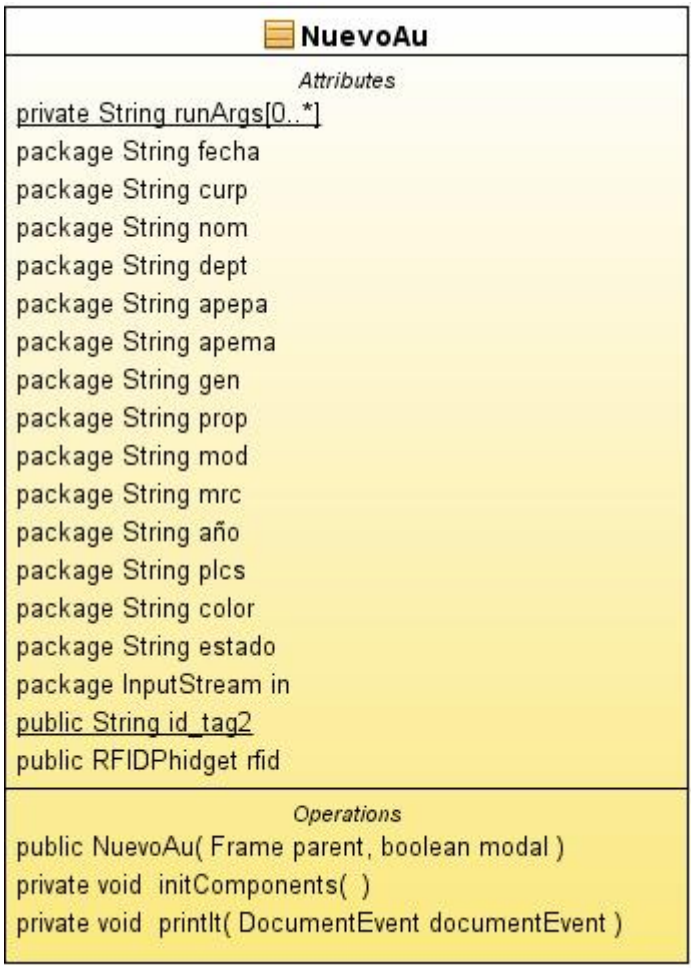


Figura 5.29. Clase NuevoAu

NuevoUa se encarga de asociar a nivel base de datos un usuario a un automóvil que ya fue registrado previamente. (Véase figura 5.30.)

Figura 5.30. Clase NuevoUa

La clase opciones es requerida cuando se agrega un usuario a un auto existente, muestra los automóviles que pueden ser compartidos al nuevo usuario. (Véase figura 5.31.)

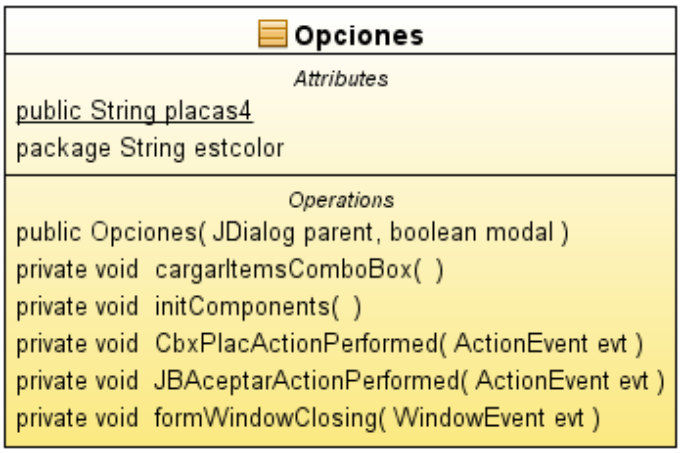


Figura 5.31. Clase de opciones

Listeners

Este conjunto de clases son esenciales para el reconocimiento del id del tag que se aproxima al dispositivo RFID. Los métodos de estas clases abren y cierran procesos hilos que evitan el encolamiento con los procesos del sensor biométrico, también atrapan excepciones en caso de error. (Véase imagen 5.32.)

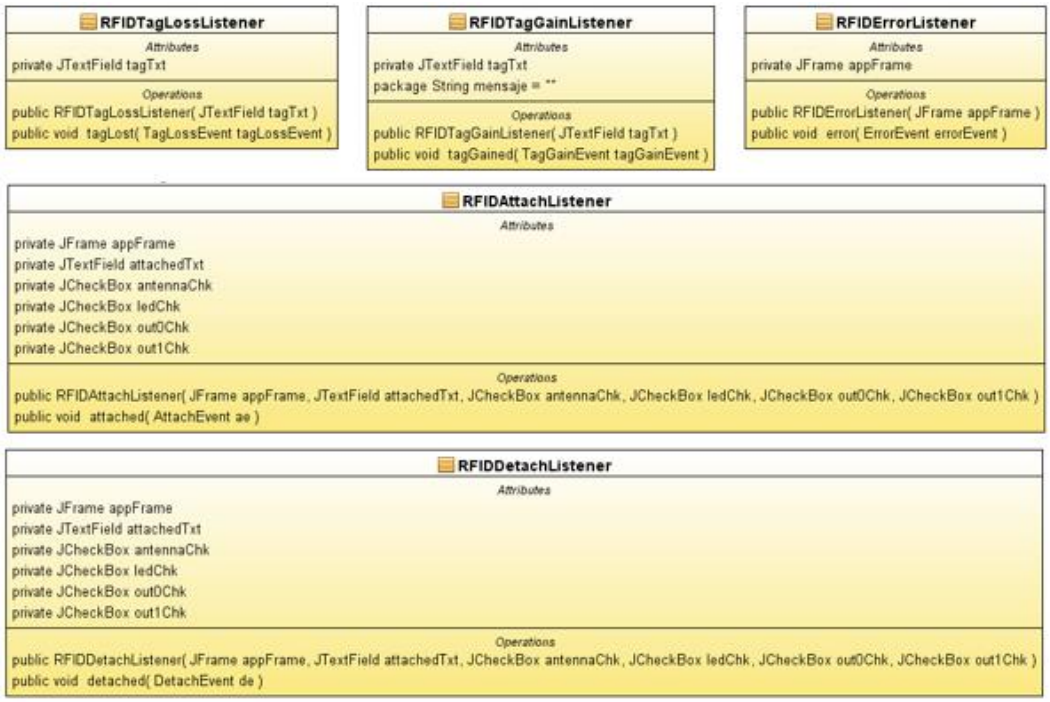


Figura 5.32. Listeners

BD

Contiene las conexiones a la base de datos que son utilizadas por las clases que insertan y actualizan registros. (Véase figura 5.33.)

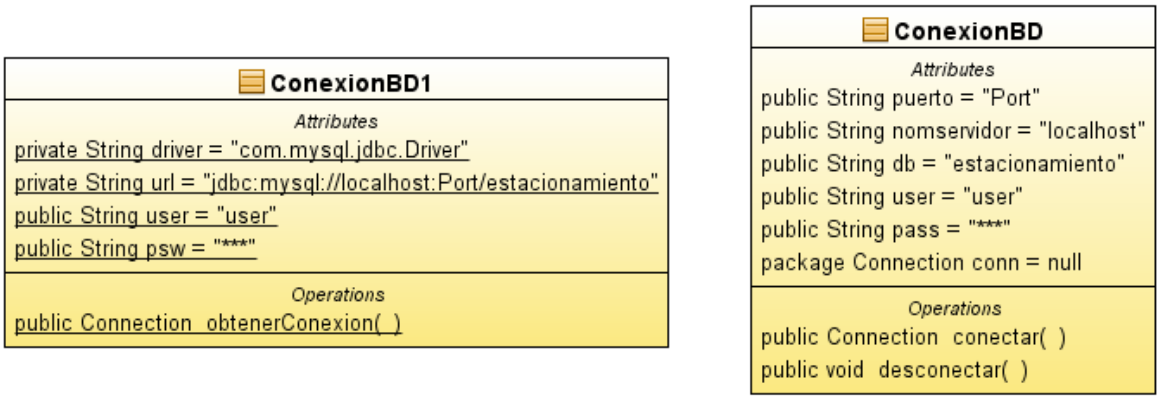


Figura 5.33. BD

Filtro Autos

Las clases que conforman este grupo son utilizadas por la clase opciones, su función principal es devolver los autos que posee un usuario. (Véase figura 5.34.)

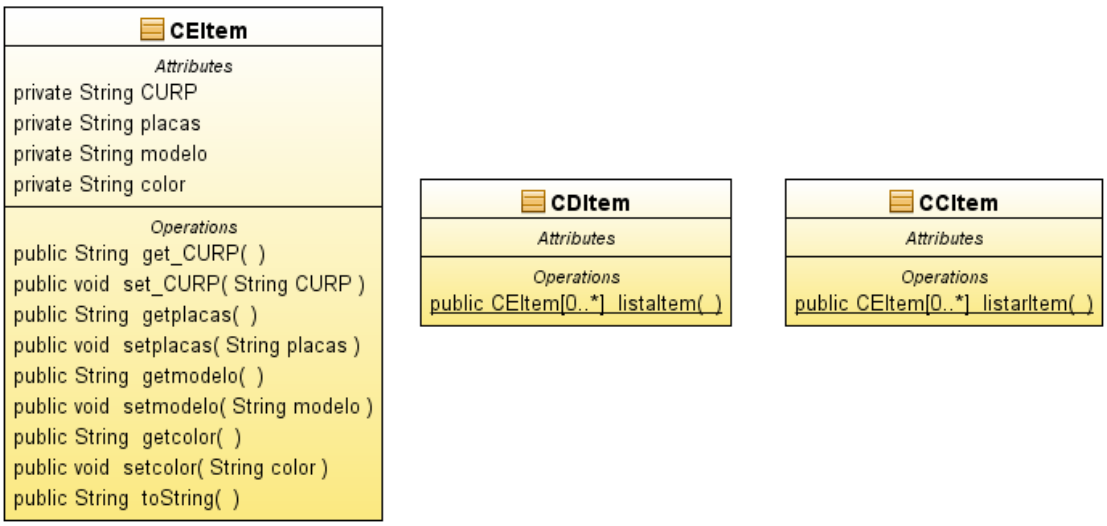


Figura 5.34. Filtro Auto

Conclusiones

La implementación de nuevas tecnologías como las tarjetas de RFID y los dispositivos biométricos ha ido en aumento, esto debido a su alta eficiencia y a su bajo costo, sin embargo existe aún un amplio campo de desarrollo en los que se pueden implementar medidas como ésta, uno de ellos son los estacionamientos que como ya hemos mencionado sus medidas de seguridad se han quedado muy limitadas, es por ello que en el presente proyecto se desarrolló un sistema de alta eficiencia, para lo cual se tomaron en cuenta factores como los siguientes:

1- La necesidad de mejorar los sistemas de seguridad en los estacionamientos haciendo uso de nuevas tecnologías como lo son el RFID y los dispositivos biométricos, es este caso el sensor de huella digital.
2- La relación entre el costo de la implementación del sistema y el valor de los automóviles resguardados.
3- La confiabilidad de los dispositivos utilizados.
4- La agilidad con la que los autos pueden entrar y salir del estacionamiento.
5- El riesgo de que los vehículos sean sustraídos de los estacionamientos debido a la falta de seguridad en ellos.

Los sistemas de seguridad en los estacionamientos de nuestra ciudad, y en general de nuestro país se han rezagado y no han echado mano de la creciente diversidad de dispositivos tecnológicos que pueden ayudar a mejorar en gran medida la seguridad de los vehículos.

Actualmente el uso de etiquetas RFID se ha limitado al cobro de peajes pues ha demostrado ser una tecnología confiable y ágil, igualmente el uso de los sensores de huella digital ha alcanzado tan alto nivel de confiabilidad que se usa en bancos para la autenticación de los usuarios. Además resultan ser tecnologías relativamente económicas, y en conjunto representan un nivel de seguridad muy alto en comparación con los sistemas actuales.

En este proyecto se logró desarrollar un sistema que integra la tecnología RFID para la autenticación del automóvil y el uso de un sistema biométrico de huella digital, que junto con una base de datos y una interfaz de usuario logró encontrar una alternativa para mejorar la seguridad en los estacionamientos a un costo razonable

y sin perder de vista la agilidad de la mayoría de los sistemas actuales. Los costos de desarrollo e implementación así como del material a utilizar es realmente bajo, sin embargo el costo está en función del nivel de seguridad, ya que se puede incrementar el nivel de seguridad en el sistema si es que el valor de los activos así lo requieren.

Se demostró que ambas tecnologías se pueden complementar de manera adecuada, abriendo las posibilidades a ser utilizadas en conjunto para la mejora de cualquier sistema de seguridad que lo amerite.

Además, este proyecto representa un avance en la seguridad en los estacionamientos, incluso es un sistema escalable, es decir, que se ajusta a las necesidades y posibilidades de los usuarios, quienes al hacer uso de este sistema pueden tener la seguridad de que su patrimonio está a salvo.

Se espera que en un futuro este proyecto forme parte de la tecnología aplicada en estacionamientos privados de nuestro país, como método de prevención de robo de vehículos, e incluso en versiones posteriores el sistema podría enviar notificaciones a dispositivos móviles, siendo parte del boom de la tecnología móvil en el mundo, entre otros.

Glosario

A

AMIS: Asociación Mexicana de Instituciones de Seguros.

Antropometría: Se refiere al estudio de las dimensiones y medidas humanas con el propósito de valorar los cambios físicos del hombre.

API: Interfaz de programación de aplicaciones, del inglés Application programming interface.

Aplicación: Es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos.

Atributos: Son las características de las clases.

B

Bandera: Se refiere a uno o más bits que se utilizan para almacenar un valor binario o código que tiene asignado un significado.

Biblioteca: En programación un conjunto de implementaciones funcionales, codificadas en un lenguaje de programación, que ofrece una interfaz bien definida para la funcionalidad que se invoca.

Biométrico: Referente a Biometría, la biometría es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o rasgos físicos.

Broadcast: Es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Byte: Es la unidad fundamental de datos en una computadora, un byte son ocho bits contiguos. El byte es también la unidad de medida básica para memoria.

C

Campo: En una base de datos es la unidad mínima de almacenamiento.

CD: Disco compacto, del inglés Compact disc.

Circuito Integrado: También conocido como chip o microchip, es una estructura de pequeñas dimensiones de material semiconductor, sobre la que se fabrican circuitos electrónicos generalmente mediante fotolitografía y que está protegida dentro de un encapsulado de plástico o cerámica. El encapsulado posee conductores metálicos apropiados para hacer conexión entre el chip y un circuito impreso.

Clase: En java, es una descripción generalizada de una colección de objetos similares una clase se compone de métodos y atributos.

Clave primaria: Es un campo o a una combinación de campos que identifica de forma única a cada fila de una tabla.

Clave foránea: es un campo que se usa en una tabla secundaria y que coincide con la clave primaria en una tabla relacionada.

D

Decodificador: Es un dispositivo que acepta una entrada digital codificada en binario y activa una salida. Este dispositivo tiene varias salidas, y se activará aquella que establezca el código aplicado a la entrada.

DPI: Puntos por pulgada, del inglés Dot per inch. Es una unidad de medida para resoluciones de impresión.

Driver: Un controlador de dispositivo o manejador de dispositivo.

E

EER: Tasa de error igual, del inglés Equal error rate. Es cuando se da un ajuste entre la tasa de FAR y la tasa de FRR de manera que estos sean iguales.

EPC: Corresponde a las siglas en inglés de Código Electrónico de Producto y se refiere a una clave de identificación unívoca de cualquier objeto, permite detallar información sobre el mismo, facilita el seguimiento de los productos a lo largo de una cadena de abastecimiento.

Etiquetas RFID: Elemento de un sistema RFID, pueden ser activas, semi-activas o pasivas.

F

FAR: Tasa de falso positivo, del inglés False Acceptance Rate. En un sistema de control de accesos el FAR se refiere a aceptar a alguien que no es quien aparenta ser.

FNMR: Tasa de falso negativo, del inglés False non match rate. En un sistema de control de accesos el FNMR se refiere a no aceptar a alguien que sí es quien aparenta ser.

H

Hardware: Se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

I

ID: Identificador único.

IDE: Entorno de desarrollo integrado, del inglés Integrated development environment. Es un entorno de programación que ha sido empaquetado como un programa de aplicación; es decir, que consiste en un editor de código, un compilador, un depurador y un constructor de interfaz gráfica.

IFF: Por sus siglas en inglés (Identification Friend or Foe), identificador amigo-enemigo es es un sistema de identificación criptográfica. Dentro del campo militar, sirve para distinguir a aeronaves o a vehículos enemigos de los que no lo son. Fue desarrollado en Alemania en 1940 y usaba frecuencias de radar de 125 MHz y 550-580 MHz.

Interfaz: Se utiliza para nombrar a la conexión física y funcional entre dos sistemas o dispositivos de cualquier tipo dando una comunicación entre distintos niveles

ITV: Término acuñado por el Departamento de Defensa de Estados Unidos, se define como
la capacidad de hacer el seguimiento de la identidad, el estado y la ubicación del inventario y los envíos desde el origen hasta el consignatario o destino, ofreciendo una verdadera transparencia a la cadena de suministros.

J

JDK: Kit de desarrollo Java, del inglés Java development kit. Es un software que provee herramientas de desarrollo para la creación de programas en Java.

JMF: Del inglés Java media framework. Es una librería de Java desarrollada por Sun Microsystems para facilitar el desarrollo de aplicaciones multimedia en este lenguaje de programación.

JRE: Entorno de ejecución de Java, del inglés Java Runtime environment. Es un conjunto de utilidades que permite la ejecución de programas Java.

L

Librería: Es un conjunto de implementaciones funcionales, codificadas en un lenguaje de programación, que ofrece una interfaz bien definida para la funcionalidad que se invoca.

Llave:

Linux: Sistema operativo libre, basado en Unix.

M

MB: Mega bytes.

Método: Se entiende como el comportamiento que se define en una clase.

Middleware: Es un software que asiste a una aplicación para interactuar o comunicarse con otras aplicaciones, o paquetes de programas, redes, hardware y/o sistemas operativos.

Morfología: Rama de la biología que estudia la forma o estructura de los seres vivos.

Multithreaded: Las unidades centrales de procesamiento con capacidad para multihilo(*multithreading* en inglés) tienen soporte en hardware para ejecutar eficientemente múltiples subprocesos de ejecución.

MySQL: Es un sistema de gestión de bases de datos relacional, multihilo y multiusuario.

N

Números binarios: Es un sistema de numeración en el que los números se representan utilizando solamente las cifras cero y uno (*0* y *1*). Es uno de los que se utiliza en las computadoras, debido a que trabajan internamente con dos niveles de voltaje, por lo cual su sistema de numeración natural es el sistema binario (encendido *1*, apagado *0*).

P

Paquete: En Java es un contenedor de clases que permite agrupar las distintas partes de un programa cuya funcionalidad tienen elementos comunes.

Proceso hilo: También hilo de ejecución, hebra o subproceso es la unidad de procesamiento más pequeña que puede ser planificada por un programa o sistema operativo.

Programación orientada a objetos: es un paradigma de programación que usa los objetos en sus interacciones, para diseñar aplicaciones y programas informáticos.

R

Relación: En una base de datos es una asociación, vinculación o correspondencia entre entidades.

Registro: un conjunto de campos relacionados.

Retina: Es un tejido sensible a la luz situado en la superficie interior del ojo.
Voiceprint: Gráficas del tono y volumen de voz.

RFID: Identificación por Radiofrecuencia, las siglas vienen del inglés Radio Frequency Identification.

S

SDK: Kit de desarrollo de software, del inglés Software development kit.

Sensor: Es un dispositivo capaz de detectar magnitudes físicas o químicas, llamadas variables de instrumentación, y transformarlas en variables eléctricas.

Software: Equipamiento lógico o soporte lógico de un sistema informático.

T

Tag: Se refiere a una etiqueta RFID.

TCP/IP: La familia más importante de protocolos en Internet. Protocolo de control de transmisión del inglés Transmission control protocol y protocolo de Internet del inglés Internet protocol.

U

UHF: Frecuencia ultra alta, del inglés Ultra high frecuency.

USB: Bus serial universal, del inglés Universal serial bus. Es un bus estándar industrial que define los cables, conectores y protocolos usados en un bus para conectar, comunicar y proveer de alimentación eléctrica entre computadoras, periféricos y dispositivos electrónicos.

W

Windows: Microsoft Windows (conocido generalmente como Windows o MS Windows), es el nombre de una familia de distribuciones para PC, smartphone, servidores y sistemas empotrados, desarrollados y vendidos por Microsoft.

Wizard: Programa de instalación de software.

Bibliografía

CAPITULO 1

1.- El Economista. Póliza obligatoria aumentará a 50% el nivel de autos asegurados: ***http://eleconomista.com.mx/finanzas-personales/2013/05/29/poliza-obligatoria-aumentara-50-nivel-autos-asegurados*** *(Ilse Santa Rita, 2013).*

2.- La Jornada AMIS: Bajo la recuperación de autos robados *http://www.jornada.unam.mx/2013/08/01/economia/023n2eco (Susana González, 2013).*

3.- Comercityus, Soluciones RFID para acceso a edificios y control de estacionamientos. *http://www.comercyti.us/servicios/rfid-para-estacionamientos/ (Comercityus, 2012).*

4.- Lectores RFID-Tags http://www.sictranscore.com.ar/Lector%20RFID.html (Sictranscore, 2013).

CAPITULO 2

1.-KOELLE, A. R., S. W. Deep, y R. W. Freyman, (1975) "Short-Range Radio Telemetry for Electronic Identification, Using Modulated RF Backscatter," Proceedings of the IEEE, pp. 1260-1261.

2.-KOELLE, A. R., (1988) "Short-Range UHF Telemetry System Using Passive Transponders for Vehicle ID and Status Information," IEEE Workshop on Automotive Applications of Electronics, pp.34-38.

3.-WANT, R. (2006) "An Introduction to RFID Technology," IEEE Pervasive Computing, pp. 25-33.

4.- Radio Frequency Identification Ready to Deliver, Signal Magazine January 2005, Armed Forces Communications and Electronics Association (AFCEA), http://www.afcea.org/

5.- At Delta, tracking bags with radio tags, Ron Coates, CNET News, 1 July 2004, http://news.com.com/2102-1012_3-5254118.html

6.- SWEENEY Patrick, (2005), *RFID for dummies,* 111 River Street Hoboken, NJ 07030-5774: Wiley Publishing.

7.- Products for USB Sensing and Control, Phidgets Inc. (2012). http://www.phidgets.com

8.- HUNT Daniel, PUGLIA Albert, "RFID A guide to Radio Frecuency Identification", WILEY (2007), N.J. Estados Unidos.

CAPITULO 3

1.- MATEOS, Marino. (2005), *"Tecnologías biométricas aplicadas a la seguridad",* RA-MA, pp.28-35.

2.- ROYER, Jean-Marc, (2004) *"Seguridad en la informática de empresas. Riesgos, amenazas, prevención y soluciones"*, eni. pp 125-128.

3.- BIOMETRIKA, Introduction to biometric systems, Ivan Drakic 2011. http://drakic.org/2011/12/15/introduction-to-biometric-systems/

4. - NICHOLS Ellis, "Biometrics, Theory, Applications and Issues", Nova Biomedical, (2011) N.Y. Estados Unidos.

5.- SILVEYRA Jorge, "Investigación del delito, sistemas de identificación humana", La Rocca, (2006), B.A. Argentina.

CAPITULO 4

1.- CEBALLOS, Javier, (2011), *"JAVA 2. Curso de programación"*, Alfaomega-RA-MA.

2.- LOPEZ, José, (2007), *"Domine PHP y MySQL. Programación dinámica en el lado del servidor"*, Alfaomega-RA-MA.

3.- SZNAJDLEDER Pablo, "JAVA a fondo. Estudio del lenguaje y desarrollo de aplicaciones", Alfaomega, 2010, B.A. Argentina.

4.- MELTON Jim, EISENBERG Andrew, "SQL y JAVA. Guia para SQLJ, JDBC y tecnologías relacionadas", Alfaomega RA-MA, 2002, D.F. México.-