

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA



PONTIFICIA
UNIVERSIDAD
CATÓLICA
DEL PERÚ

DISEÑO DE UN SISTEMA DE CONTROL VEHICULAR BASADO EN EL ACCESO DE ESPACIOS LIBRES Y UBICACIÓN EN ESTACIONAMIENTOS USANDO RFID

Tesis para optar el Título de **Ingeniero Electrónico**, que presenta el bachiller:

Jorge Martin Rios Vidalón

ASESOR: Ing. Luis Angelo Velarde Criado

Lima, Julio del 2011

RESUMEN

La realidad de los estacionamientos en nuestro país indica que la atención y el servicio prestados son mínimos ya que la mayoría de estacionamientos opera bajo un control manual, es decir, una persona realiza el control de ingreso y salida de vehículos, con lo cual se genera una dependencia en el personal para obtener un control vehicular eficiente y brindar un buen servicio. Aunque algunas empresas han tratado de mejorar la administración de su estacionamiento con sistemas automáticos, estos les han generado mayores problemas e incomodidades a los usuarios.

Los avances tecnológicos de hoy en día, dan la posibilidad de desarrollar sistemas que cumplan un eficiente control, brinden facilidades y den buen servicio a los usuarios, obteniendo así, una buena administración del estacionamiento. Para ello es necesario utilizar la tecnología más adecuada para poder desarrollar un sistema con las características mencionadas.

La tecnología RFID es un sistema de autoidentificación inalámbrica que consiste en etiquetas que almacenan información y lectores que puedan leer estas etiquetas a distancia. La solución planteada establece el diseño de un sistema de control vehicular basado en esta tecnología, que tomará en cuenta controlar los accesos, los espacios libres y la ubicación de los autos en un estacionamiento.

Con las pruebas realizadas, se puede concluir que el sistema de control vehicular basado en la tecnología RFID permitió cumplir con las expectativas del caso. Este sistema pudo identificar a los usuarios automáticamente, mostrar la cantidad de espacios libres en el estacionamiento en un determinado momento, obtener una referencia de la ubicación de los vehículos y supervisar las actividades del estacionamiento desde una computadora. Por ende, el sistema podrá ofrecer un mejor control y administración del lugar, dando comodidades y un mejor trato al usuario durante su estadía en el estacionamiento.

Gracias a todas las personas que contribuyeron en que pueda terminar mi carrera y convertirme en ingeniero, gracias Mary, mi hermana, que fuiste un ejemplo para mi con tu responsabilidad y perseverancia; a mi abuelita Loli, gracias por tu preocupación, tus oraciones y por todas las veces que me despertabas para que no llegar a tarde a mis clases, a Cinthya, mi enamorada, que con tus consejos, amor y apoyo ayudaron a ser de mi una mejor persona, a mi padre, muchas gracias por tu apoyo, confianza y sobretodo por tu gran ejemplo como hombre, y en especial a mi madre, la gran gestora de este logro, gracias por tu preocupación, amor, apoyo y por estar siempre pendiente de mi, sin ustedes no hubiese podido terminar lo que me propuse como meta hace ya varios años, muchas gracias por todo.

ÍNDICE

INTRODUCCIÓN	08
CAPÍTULO 1: PROBLEMÁTICA DEL SISTEMA DE CONTROL VEHICULAR USADO EN LOS ESTACIONAMIENTOS	
1.1 Variables globales	09
1.1.1 Tendencia mundial	09
1.1.2 Normalización	09
1.1.3 Economía.....	10
1.2 Oportunidades y amenazas.....	10
1.2.1 Proveedores	10
1.2.3 Tecnologías	10
1.3 Variables internas.....	10
1.3.1 Infraestructura.....	10
1.3.2 Recursos humanos.....	10
1.4 Proceso que se analiza	11
1.4.1 Descripción del proceso	11
1.4.2 Análisis	11
1.5 Declaración del marco problemático	12
1.6 Fundamentación	12
CAPÍTULO 2: FUNDAMENTOS TEÓRICOS Y TECNOLOGÍAS USADAS PARA CONTROL VEHICULAR	
2.1 Estado del arte.....	13
2.1.1 Presentación del asunto de estudio.....	13
2.1.2 Estado de la investigación.....	14
2.1.3 Conclusiones sobre las tecnologías vistas	18
2.2 Control vehicular.....	19
2.2.1 Control de acceso.....	19
2.2.2 Control de espacios libres	19
2.2.3 Control de ubicación	19
2.3 RFID	19
2.3.1 Componentes	20
2.3.2 Funcionamiento	20
2.3.3 Frecuencias	21

2.3.4 Estándares.....	21
2.4 Modelo teórico	22
CAPÍTULO 3: DISEÑO DEL SISTEMA DE CONTROL VEHICULAR USANDO RFID	
3.1 Hipótesis de la investigación	24
3.1.1 Hipótesis secundarias.....	24
3.2 Objetivo de la investigación	25
3.2.1 Objetivos Específicos	25
3.3 Diseño del sistema	25
3.3.1 Sistema RFID	25
3.3.1.1 Kit RFID	25
3.3.1.2 Instalación de equipos RFID.....	26
3.3.2 Diseño del Sistema indicador de espacios libres	28
3.3.2.1 Hardware	28
3.3.2.2 Software.....	30
3.3.3 Comunicación inalámbrica.....	31
3.3.3.1 Secure Socket iWifi.....	31
3.3.3.2 Tarjeta de configuración y comunicación	32
3.3.3.3 Programación del módulo.....	33
3.3.4 Diseño del Software de Administración	38
CAPÍTULO 4: PRUEBAS DEL SISTEMA Y ANÁLISIS DE RESULTADOS	
4.1 Desarrollo de pruebas	42
4.1.1 Prueba con el Sistema RFID	42
4.1.2 Prueba con el Secure Socket iWifi	43
4.1.2.1 Tarjeta de configuración y comunicación del Secure Socket	43
4.1.2.2 Configuración del Secure Socket	44
4.1.2.3 Prueba de comunicación	45
4.1.3 Prueba con el Software y el Sistema indicador de espacios libres	49
4.1.3.1 Tarjeta del sistema indicador de espacios libres	49
4.1.3.2 Aplicación Cliente: Lectores RFID	49
4.1.3.3 Prueba de comunicación	50
4.2 Presupuesto.....	61
CONCLUSIONES.....	63
RECOMENDACIONES	64
BIBLIOGRAFÍA.....	65
ANEXOS	

INTRODUCCIÓN

Con el desarrollo de la tesis, se busca encontrar la mejor solución a los actuales problemas que tienen los sistemas de control vehicular en los estacionamientos. A través de la automatización de algunos procesos, se pretende obtener un sistema que brinde un mejor servicio al usuario.

El presente documento está estructurado en cuatro capítulos, donde cada uno de los cuales desarrollará temas trascendentales y diversos con el fin de contribuir en la realización de la tesis.

El primer capítulo presenta el marco problemático del sistema de control vehicular que se utiliza en los estacionamientos, con lo que se podrán identificar los verdaderos problemas de los actuales sistemas.

El segundo, abarca las actuales tecnologías usadas en los sistemas de control vehicular y, además, se desarrollarán algunos conceptos teóricos. Con esto se busca conocer las ventajas y desventajas que resultarían de aplicar esta tecnología al sistema deseado.

En la tercera parte, se explicará el diseño del sistema de control vehicular que se plantea. Para lo cual se presentará la hipótesis y objetivos correspondientes a la tesis, los que permitirán entender que es lo que se busca solucionar con este diseño.

En el cuarto capítulo se desarrollarán las pruebas con los equipos y componentes del sistema propuesto, para luego realizar el análisis de las respuestas obtenidas por cada elemento de sistema.

Al final del documento, se encuentran las conclusiones extraídas de la tesis desarrollada, así como algunas recomendaciones sobre futuros proyectos o pruebas que se puedan realizar con este sistema.

CAPÍTULO 1

PROBLEMÁTICA DEL SISTEMA DE CONTROL VEHICULAR USADO EN LOS ESTACIONAMIENTOS

En el presente capítulo se desarrollan diferentes aspectos y variables que abarcan el marco problemático del sistema de control utilizado en los estacionamientos. Estos ayudarán a identificar los aspectos favorables y los inconvenientes del actual sistema.

1.1 Variables globales

Los siguientes puntos a tratar, abarcan los aspectos ligados a temas de carácter general, posibles condiciones o tendencias favorables en el desarrollo del asunto de estudio.

1.1.1 Tendencia mundial

La realidad en la que vivimos se proyecta a que todos los procesos realizados por el hombre sean ahora hechos por equipos en base a tecnología. Esto optimiza los resultados antes obtenidos, brindando un mejor producto o servicio.

La tendencia en diferentes lugares como Europa, Asia y Estados Unidos es hacia la completa automatización de los servicios prestados en los estacionamientos. Lamentablemente, en nuestro país, el desarrollo tecnológico en esta área es mínimo, llevándose a cabo el control vehicular de forma manual.

1.1.2 Normalización

Debido a que los equipos utilizados en los sistemas vehiculares van a interactuar con personas, estos deben de cumplir con estándares internacionales para que regulen su funcionamiento y no haya ningún tipo de problema en su utilización, asegurando el bienestar de las personas.

1.1.3 Economía

Los estacionamientos cuentan con una inversión de dinero muy pobre, aunque existan empresas dedicadas a la administración de estos lugares. Los administradores buscan invertir lo menos posible, dejando de lado la tecnología ya que los equipos son caros y no ofrecen mucha variedad. Por ello se opta por el trabajo del hombre como solución al problema [1].

1.2 Oportunidades y amenazas

Los siguientes puntos a desarrollar abarcarán aspectos sobre el actual mercado global en relación al sistema estudiado.

1.2.1 Proveedores

Actualmente existen empresas nacionales e internacionales que fabrican o importan equipos para control vehicular. Estas cuentan con todo tipo de instrumentos y materiales que pueden ser utilizados en la formación de cualquier sistema de control.

1.2.3 Tecnologías

Debido al desarrollo de diversas tecnologías se han podido crear diferentes equipos basados en estas. Hoy en día, se desarrollan tecnologías como código de barras, banda magnética, proximidad, biométrica, radio frecuencia, etc., que logran hacer posible el desarrollo de un sistema de control vehicular adecuado.

1.3 Variables internas

Los puntos a tratar serán aspectos internos al asunto de estudio.

1.3.1 Infraestructura

Algunos estacionamientos cumplen con las medidas y requerimientos estándares para que un auto pueda ingresar, estacionarse y salir del lugar sin problema. Además, colocan señales que permiten al usuario orientarse dentro del estacionamiento.

1.3.2 Recursos humanos

La mayoría de estacionamientos al realizar un control manual sobre los autos, es necesario que cuenten con personal a cargo de esta labor. Dependiendo del tamaño y del número de accesos del estacionamiento se necesitará mayor o menor cantidad de personal.

1.4 Proceso que se analiza

1.4.1 Descripción del proceso

El tipo de sistema de control vehicular empleado en los estacionamientos obliga al usuario a realizar los siguientes procesos:

- El usuario, para entrar estacionamiento, deberá dirigirse a cualquiera de los ingresos del local, donde el personal a cargo le entregará algún tipo de identificación (boleto).
- Dentro de las instalaciones, el conductor debe buscar un lugar donde dejar su auto. Al encontrar un espacio disponible, el usuario estacionará su vehículo. Caso contrario, el usuario pasará a retirarse del estacionamiento.
- Al momento de retirarse, el usuario deberá dirigirse a la salida para dejar la identificación dada en el ingreso y salir del estacionamiento.

1.4.2 Análisis

Según el proceso planteado anteriormente, este presenta los siguientes problemas.

1. Al funcionar de forma manual, existe mucha dependencia en el personal para que se realice un buen control y se preste un buen servicio al usuario. Además, se debe tomar en cuenta que para que una persona realice bien su labor depende de variables externas, como, por ejemplo, su estado de ánimo. Por ello, su trabajo puede ser realizado de manera ineficiente, perjudicando al usuario.
2. Otro punto importante que no se toma en cuenta es brindar algún tipo de facilidad o servicio al usuario dentro del estacionamiento. Es decir, el mismo usuario debe buscar y encontrar un sitio libre para dejar su auto, lo cual puede causarle demoras y malestar al no hallar el espacio requerido.
3. También se debe tomar en cuenta que en los estacionamientos nadie se hace responsable por la seguridad del auto, aunque se encuentre dentro de este local. Inclusive las empresas administradoras colocan en los tickets que se les da a los usuarios, mensajes donde se les indica que nadie se hace responsable por pérdida o daño al vehículo.
4. Por último, al momento de salir de los estacionamientos se requiere de personal simplemente para la recepción de los pases brindados en la entrada, lo cual genera una mayor inversión en contratación de empleados.

1.5 Declaración del marco problemático

La actual situación de los estacionamientos en el Perú indica que la atención al usuario, dentro de estos lugares, es mínima. Sin embargo, algunos estacionamientos pretenden mejorar su servicio a través de sistemas automáticos, sin tomar en cuenta que originan más dificultades al usuario al momento de usarlos. Por otro lado, el sistema de control al llevarse a cabo en forma manual, genera que se dependa de una persona para funcionar y brindar un buen servicio. Además, se debe tomar en cuenta que el personal, al estar presente solo en los accesos, ocasiona que el usuario no recibe ningún tipo de facilidad dentro del local para estacionarse, y que tampoco existe ningún tipo de respaldo en cuanto a la seguridad del auto. Por lo tanto, los estacionamientos no cuentan con un adecuado sistema que les permita mejorar su atención y servicio al usuario.

1.6 Fundamentación

Las tecnologías modernas permiten desarrollar un sistema de control vehicular que logre brindar un adecuado servicio en el estacionamiento. Para ello se deberá analizar diversas tecnologías con las que se pueda establecer el sistema que cumpla con estos requerimientos. En el siguiente capítulo se hará referencia de algunos ejemplos de sistemas reales implementados con diferentes tecnologías, que ayudarán a determinar la mejor opción para el sistema de control vehicular.

CAPÍTULO 2

FUNDAMENTOS TEÓRICOS Y TECNOLOGÍAS USADAS PARA CONTROL

VEHICULAR

En este segundo capítulo se tratará sobre las tecnologías usadas en los sistemas de control vehicular. Para esto se revisarán algunos ejemplos de sistemas basados en diferentes tecnologías y, además, se explicarán algunos conceptos básicos sobre el sistema que se plantea.

2.1 Estado del arte

2.1.1 Presentación del asunto de estudio

La necesidad de mantener un control y una buena administración sobre un estacionamiento ha dado paso a la creación de sistemas que cumplan con estos requerimientos. Los sistemas de automatización y control de estacionamientos permiten brindar mejoras y facilidades al estacionamiento que beneficiarán tanto a los administradores como a los usuarios del lugar [2].

Estos sistemas solucionan diferentes necesidades y, por lo tanto, funcionan de diversas formas. Sin embargo, cualquier sistema que permita administrar correctamente un estacionamiento, debe controlar los recursos más importantes de este. Por lo mismo, para que un auto no tenga ningún inconveniente, el sistema debe funcionar en la entrada, en la salida y dentro de la playa.

Por ello, se analizarán los actuales avances tecnológicos desarrollados en sistemas de control vehicular y, además, se verán ejemplos de sistemas aplicados en diferentes lugares para que se pueda evaluar las ventajas y desventajas de estos, con lo cual se podrá definir la tecnología a utilizar.

Esta deberá solucionar los diversos problemas e ineficiencias presentados actualmente en un estacionamiento. Por lo tanto, con esta tecnología se obtendrá un

sistema que trabaje eficientemente, mejore la seguridad y optimice los recursos del estacionamiento.

2.1.2 Estado de la investigación

Los sistemas automáticos de control vehicular requieren de tecnologías que les permita de alguna forma identificar al usuario del estacionamiento. Se pueden encontrar diversas tecnologías como: códigos de barras, banda magnética, proximidad y RFID.

El Código de barras es una tecnología muy conocida y usada, que permite, de una manera rápida y precisa, codificar información. Las ventajas que presenta son que se imprime a bajos costos, permite porcentajes muy bajos de error y tiene rapidez en la captura de datos. Sin embargo, presentan desventajas como que son fáciles de duplicar, su vida útil es corta y necesitan de mantenimiento para poder funcionar sin problemas [3].

La Banda magnética es otra tecnología importante actualmente ya que es utilizada en diferentes actividades. Esta es grabada o leída mediante contacto físico, pasándola a través de una cabeza lectora/escritora, gracias al fenómeno de la inducción magnética [4]. Las ventajas y desventajas de esta tecnología son similares a las de código de barras, ya que también son baratas, tienen rapidez para captar datos, necesitan de mantenimiento y su vida útil es corta [3].

Otra posible tecnología es la proximidad, es decir, utilizar lectores de proximidad y tarjetas de acceso. Esta, respecto a las vistas anteriormente, presenta ventajas como no requerir de mantenimiento, son poco susceptibles a la interferencia, es imposible duplicar las tarjetas y su vida útil es larga, aproximadamente cinco años. Sin embargo, una clara desventaja, estaría en relación a la distancia que el usuario debe pasar la tarjeta para poder identificarse en la lectora, entre 8 y 62 cm. [3]. Debido a esto, este tipo de aplicaciones con distancias relativamente cortas, podría limitar las facilidades y ventajas que se le quiera brindar al usuario.

Otra de las actuales tecnologías con las que se puede contar para implementar este sistema, es la identificación por radio frecuencia (RFID). Esta técnica inalámbrica se basa en el almacenamiento y recuperación remota de datos usando transpondedores [5]. Tiene como propósito fundamental transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.

Los sistemas RFID presentan ciertas desventajas respecto a las tecnologías anteriormente vistas:

- Las tarjetas RFID son más caras con respecto, por ejemplo, al código de barras.
- Estos sistemas no presentan un estándar mundial, con lo cual las frecuencias usadas por RFID son incompatibles en diferentes lugares. Por ejemplo, las frecuencias usadas en USA son incompatibles en Europa y Japón.
- Debido al tráfico ilícito de etiquetas RFID existen preocupaciones por la seguridad y privacidad empresarial y personal.

Sin embargo, en respuesta a estas desventajas, se presenta lo siguiente:

- Las tarjetas RFID son más caras pero a largo plazo duran más ya que estas no se desgastan.
- Se puede tener sistemas RFID con un rango de frecuencias que respeten los requisitos locales de cada país.
- Además, la invulnerabilidad que se puede lograr en los sistemas RFID es tal que no se puede lograr ningún tipo de falsificación ni fraude, ya que la transferencia de información entre la antena y el TAG podrá estar altamente codificada.

A continuación, se presentan aplicaciones de algunas de estas tecnologías en sistemas de control vehicular.

Automatización del estacionamiento del Aeropuerto Internacional Jorge Chávez:

Federal Signal Corporation es un fabricante y proveedor mundial de seguridad pública, equipos de señalización y comunicaciones. Actualmente, es el mayor fabricante estadounidense de sistemas avanzados automáticos de control de estacionamiento, accesos e ingresos, y tiene una amplia red de distribución mundial [6].

Debido a la necesidad de tener una mejor administración del estacionamiento, LAP, operador del aeropuerto, adquirió en el 2002 una solución integral de equipos y sistemas Federal APD.

El sistema instalado tiene destinado para el control de usuarios eventuales, tickets de banda magnética. Con lo cual, el sistema debía contar con equipos que se encarguen de expender los tickets para cada vehículo y, además, otros equipos que se encarguen de verificar la salida del auto del estacionamiento.

A pesar de ser una buena solución al problema presentado, este tipo de sistema presenta ciertos inconvenientes:

- El usuario no sabe manipular el expendedor de tickets.
- El expendedor de tickets se atasca.
- Pérdida de ticket por parte del usuario.
- El ticket es maltratado (doblado, arrugado), lo que ocasiona que, el lector del verificador de salida, tenga problemas para leer la banda magnética.

Todos estos inconvenientes, durante el uso del sistema, ocasionan que el control vehicular tenga muchos problemas.



FIGURA 01: Ingreso de vehículos Aeropuerto Internacional Jorge Chávez
Fuente: Intellisoft S.A.

La figura nº 1 muestra la entrada para usuarios eventuales del estacionamiento, donde se aprecia también a una persona, encargada de ayudar en caso haya algún problema con el equipo.

Además del sistema para usuarios eventuales, se instaló un sistema de control de usuarios regulares (abonados). Este sistema funciona a través de lectores de proximidad y tarjetas de acceso. La distancia a la que funciona el lector es de aproximadamente 5 cm. Al igual que el sistema anterior, este también presenta ciertos inconvenientes, pero con la diferencia que estos están más orientados a la facilidad y comodidad en el uso del sistema. Así, por ejemplo, muchas veces los usuarios tienen que abrir la ventanilla del auto, sacarse el cinturón de seguridad para poder estirarse y alcanzar una distancia corta con respecto al lector, para poder pasar la tarjeta y habilitar su acceso. Además, hay usuarios que no saben utilizar el sistema, es decir, no saben cómo pasar la tarjeta por el lector.

En la figura nº 2 se muestra la posible ubicación de un lector de proximidad en un sistema de control vehicular.



FIGURA 02: Lector de proximidad
Fuente: Federal APD

Telepeaje de Argentina:

Uno de los sistemas de control vehicular que más se está utilizando hoy en día en los peajes de diferentes países es conocido con el nombre de Telepeaje. Sic TransCore Latinoamérica (SICSA) es una empresa con base en Argentina, dedicada al desarrollo de sistemas para el control vehicular. “En 1995, SICSA diseñó e instaló el primer sistema de acceso dinámico de Sudamérica, denominado TELEPEAJE, empleando la tecnología de identificación por radio frecuencia (RFID) [7].

En relación al funcionamiento del sistema, cuando el vehículo se acerca a la vía, las antenas con las que cuenta el sistema, leen la información de las etiquetas RFID y permiten el paso del vehículo. No existe intervención de una persona para realizar la operación. Solamente pueden circular por las vías de Telepeaje aquellas personas que tengan estas etiquetas en el parabrisas de su vehículo [7]. En la figura nº 3 se muestra como trabajaría este sistema.

Por lo tanto, el sistema ayuda a disminuir el entorpecimiento del tráfico causado por las cabinas de peaje, ya que el proceso se realiza con sólo una disminución de la velocidad del vehículo, es decir que el mismo circula prácticamente sin detenerse.

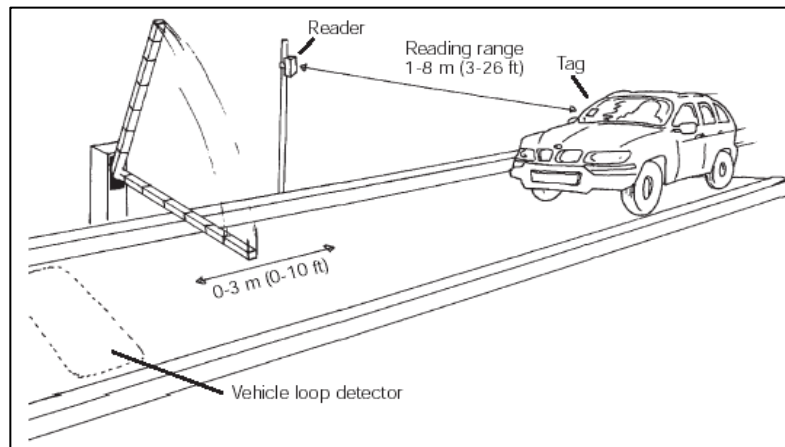


FIGURA 03: Funcionamiento del sistema RFID
Fuente: Federal APD

Las ventajas de trabajar con un sistema como el presentado son:

- “Operación manos libres, sin detención, con lo que se reduce el tráfico en entradas y salidas.
- No hace falta bajar la ventanilla, con lo cual hay mayor seguridad personal.
- Accesible en precio, fácil de instalar y mantener.
- No hay equipos en la vía que puedan ser dañados por los vehículos.
- No requiere tarjetas ni tickets, los cuales suelen perderse o gastarse.
- Procesamiento automático en puertas remotas.
- Acceso cómodo para discapacitados.
- Sistema flexible que se adecua a los requerimientos del cliente en cuanto a distancia, velocidad y presupuesto” [7].

2.1.3 Conclusiones sobre las tecnologías vistas

De acuerdo a las tecnologías desarrolladas y a los casos relacionados con sistemas de control vehicular, se puede obtener la síntesis siguiente:

- Las tecnologías de código de barras o banda magnética, si bien son tecnologías con las que se puede desarrollar un sistema de control vehicular, las desventajas y los inconvenientes que presentan al trabajar, no hacen de este un sistema eficiente y confiable.
- Por el lado de la tecnología de proximidad, si bien presenta mayores ventajas respecto a las mencionadas anteriormente, su funcionamiento, para un sistema vehicular significa limitar las facilidades y comodidades que se le quiere brindar al conductor para su identificación.

- En cambio, con respecto a la tecnología RFID, se puede llegar a implementar un sistema que no necesite de ninguna actividad por parte del conductor, más que la de manejar, para que pueda realizar su identificación sin problemas. Con este tipo de sistema, se pueden dar ventajas y facilidades que con los otros no se podría.

Los siguientes puntos presentan definiciones y conceptos sobre los sistemas automáticos de control vehicular.

2.2 Control vehicular

Se puede definir como la regulación de las actividades de un vehículo con el fin de lograr un funcionamiento predeterminado, de modo que se reduzcan las probabilidades de fallos y se obtengan los resultados buscados [8].

El sistema de control vehicular que se propone presenta tres mecanismos de control: de acceso, de ubicación y de espacios libres.

2.2.1 Control de acceso

Se define como una medida de seguridad que permite limitar o restringir el acceso a determinados lugares [3]. Esto implica que se deba contar con algún tipo de identificación para validar el acceso.

2.2.2 Control de espacios libres

Consiste en determinar los lugares no ocupados dentro de la capacidad de un terreno o sitio [9]. Con lo cual, se podrá controlar la información referente a la cantidad de espacios libres que hay en el estacionamiento.

2.2.3 Control de ubicación

Permite precisar la posición de un vehículo en un espacio o lugar determinado [9]. Con esto, se obtiene información acerca de en qué lugar se encuentra el auto en un momento dado.

2.3 RFID

Es un término genérico utilizado para describir a los sistemas que transmiten la identidad de un objeto o persona de manera inalámbrica, utilizando ondas de radio. Así pues, RFID es una tecnología de identificación automática” [10].

2.3.1 Componentes

Un sistema RFID tiene dos componentes básicos: lector y etiqueta RFID o tag.

a) Lector

Es un dispositivo que puede leer y escribir datos hacia etiquetas RFID compatibles usando ondas de radio [11].

b) Etiqueta RFID

Es un objeto que puede ser aplicado o incorporado a cualquier elemento con el propósito de identificarlo al transmitir el código que posee hacia el lector mediante ondas de radio.

Tipos

Los tags o etiquetas RFID se pueden clasificar según su alimentación [12]. Se pueden distinguir tres tipos:

- Tag Pasivos: “Este tipo de tags RFID no tienen fuente de alimentación (batería) integrada, utilizan la energía emitida por el lector para autoalimentarse y transmitir su información almacenada al lector” [12].
- Tag Activos: “Es aquel que tiene una fuente de alimentación incorporada, como una batería o un panel solar, y tiene circuitería específica para realizar una tarea en concreto” [12].
- Tag Semi-activos: “Poseen una fuente de energía interna, una batería, y unos circuitos para realizar tareas específicas. La batería se limita a proporcionar energía a estos circuitos ya que la emisión de los datos se hace mediante la energía que manda el lector” [12].

2.3.2 Funcionamiento

Las etiquetas electrónicas llevan un microchip incorporado que almacena el código único identificativo del elemento al que están adheridas. El lector envía una serie de ondas de radiofrecuencia al tag, que éste capta a través de una pequeña antena. Estas ondas activan el microchip, que, mediante la microantena y la radiofrecuencia, transmite al lector cual es el código del elemento [13].

2.3.3 Frecuencias

Las frecuencias de RFID pueden ser divididas en 4 rangos:

- a) **Baja Frecuencia (9-135 KHz).** Los sistemas que utilizan este rango de frecuencia tienen la desventaja de una distancia de lectura de sólo unos cuantos centímetros. Sólo pueden leer un elemento a la vez [11].
- b) **Alta Frecuencia (13.56 MHz).** Esta frecuencia es muy popular y cubre distancias de 1cm a 1.5 m. Típicamente las etiquetas que trabajan en esta frecuencia son de tipo pasivo [11].
- c) **Ultra High Frequency (0.3-1.2GHz).** Este rango se utiliza para tener una mayor distancia entre la etiqueta y el lector (hasta 6 metros, dependiendo del fabricante y del ambiente). Estas frecuencias no pueden penetrar el metal ni los líquidos a diferencia de las bajas frecuencias pero pueden transmitir a mayor velocidad y por lo tanto son buenos para leer más de una etiqueta a la vez [11].
- d) **Microondas (2.45-5.8GHz).** La ventaja de utilizar un intervalo tan amplio de frecuencias es su resistencia a los fuertes campos electromagnéticos, producidos por motores eléctricos, por lo tanto, estos sistemas son utilizados en líneas de producción de automóviles. Sin embargo, estas etiquetas requieren de mayor potencia y son más costosas, pero es posible lograr lecturas a distancias de hasta 8 metros. [11]

2.3.4 Estándares

La tecnología RFID debe cumplir con estándares creados por organizaciones como ISO y EPC.

- a) **ISO:** ISO tiene 3 estándares para RFID: ISO 14443 (para sistemas sin contacto), ISO15693 (para sistema de proximidad) e ISO 18000 (para especificar la interfaz aérea para una variedad de aplicaciones) [11].
- b) **EPC:** EPC global es una organización sin fines de lucro que ha desarrollado una amplia gama de estándares para la identificación de productos. Las funciones de EPC o Código Electrónico de Producto son similares a las de UPC o Código de Producto Universal encontrado en la tecnología de código de barras. EPC es un esquema de identificación para identificar objetos físicos de manera universal por medio de etiquetas RFID. El código EPC en una etiqueta RFID puede identificar al fabricante, producto, versión y número de serie, y adicionalmente provee un grupo de dígitos extra para identificar objetos únicos [11].

Gen 2: EPCglobal ha trabajado con un estándar internacional para el uso de RFID y EPC, en la identificación de cualquier artículo, en la

cadena de suministro para las compañías de cualquier tipo de industria. El estándar gen 2 de EPCglobal es probable que llegue a formar la espina dorsal de los estándares en etiquetas RFID. EPC Gen2 es la abreviatura de “EPCglobal UHF Generation 2” [11].

2.4 Modelo teórico

El sistema de control vehicular que se propone permitirá controlar los accesos, los espacios libres y la ubicación de los autos dentro del estacionamiento.

Para formar este sistema se requiere de un conjunto de equipos que funcionen de manera integrada. Está compuesto básicamente por lectores, etiquetas RFID o tags, un display informativo y un servidor con el software de administración.

Para realizar el control de acceso, se utilizará un lector RFID a la entrada y otro a la salida, para poder realizar la identificación de los autos a través de los tags. Estos lectores permitirán automatizar de alguna forma el control antes realizado por un personal.

Para el control de la ubicación, se colocarán lectores RFID dentro del estacionamiento que permitan obtener la información necesaria para tener una referencia de donde se encuentra el vehículo. Todos los lectores estarán comunicados con el servidor inalámbricamente.

A través del software de administración, que tendrá el servidor, se podrá calcular los espacios libres y la ubicación de los autos. Para mostrar los espacios libres, se utilizará un display que también estará comunicado inalámbricamente con el servidor. Además, este software permitirá también registrar toda la actividad del estacionamiento.

En la figura nº 4 se presenta el sistema de control vehicular planteado.

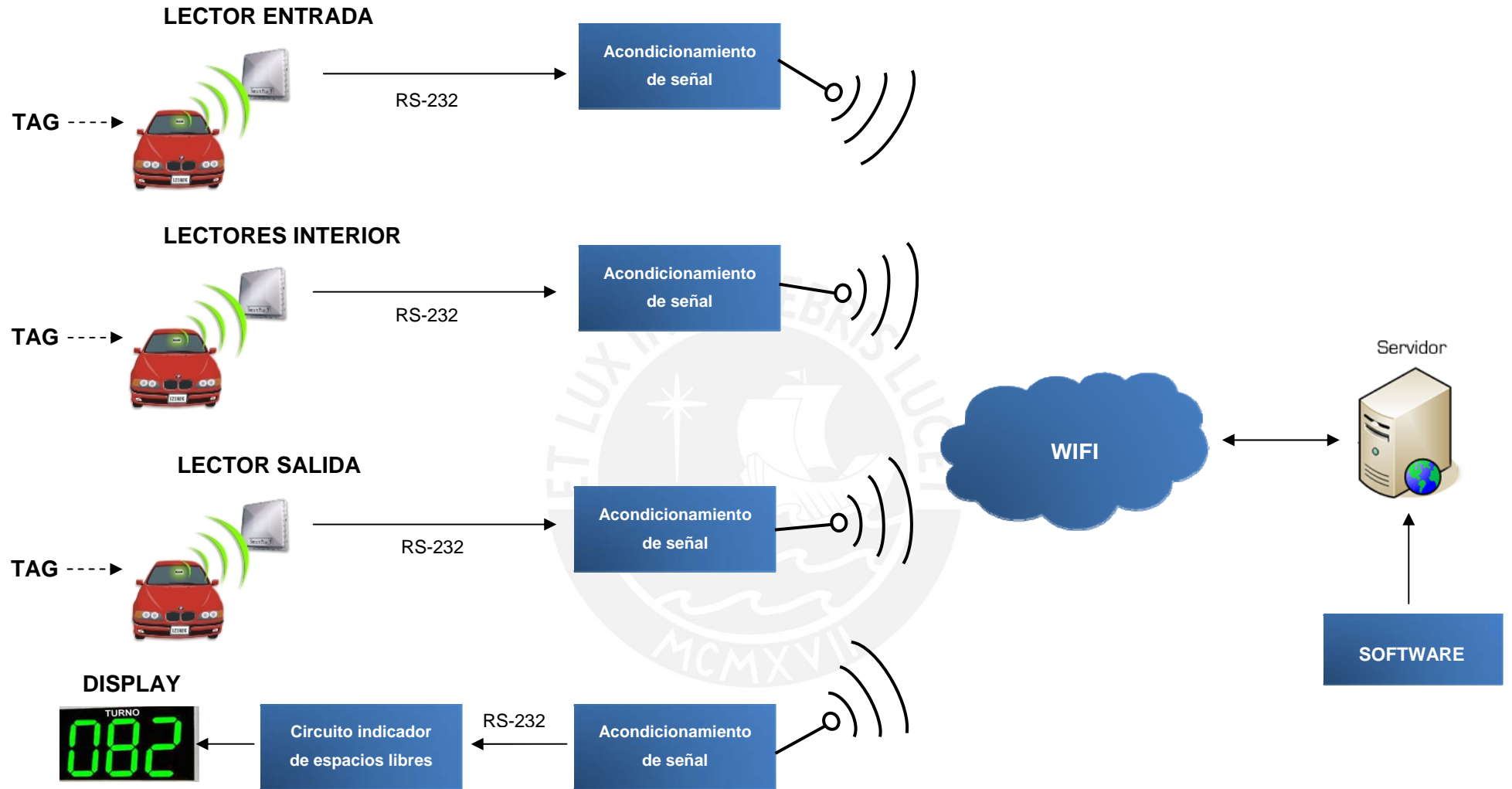


FIGURA 04: Modelo Teórico
Fuente: Elaboración propia

CAPÍTULO 3

DISEÑO DEL SISTEMA DE CONTROL VEHICULAR USANDO RFID

Este capítulo desarrollará la hipótesis y los objetivos de la tesis con el fin de comprender el diseño realizado. Además, se indicarán las herramientas, equipos, hardware y software necesarios para probar este diseño.

3.1 Hipótesis de la investigación

Dado que el sistema de control vehicular usado en los estacionamientos opera de forma manual, es decir, un persona realiza el control del lugar, generando problemas en el trato al usuario, falta de seguridad y facilidades con las personas que hacen uso de las instalaciones, entonces un sistema de control vehicular que permita controlar el acceso, los espacios libres y la ubicación de los autos basado en la tecnología RFID permitirá obtener un sistema que pueda brindar mayores ventajas y facilidades a los usuarios del estacionamiento.

3.1.1 Hipótesis secundarias

- 1) Debido a que el control manual que se usa en los estacionamientos ocasiona colas y congestión en los accesos, un sistema que automatice este proceso mejorará la rapidez en los ingresos y salidas de estos locales.

- 2) Para que el usuario pueda estacionarse sin problemas, una alternativa sería tener un sistema que logre brindar información sobre los espacios disponibles y la posición de los vehículos.

- 3) Para mejorar la administración del estacionamiento, debe contarse con un software que muestre las actividades de los autos dentro de la playa de estacionamiento, permitiendo así que el estacionamiento pueda ser monitoreado desde este equipo.

3.2 Objetivo de la investigación

El objetivo del presente trabajo de tesis es diseñar un sistema de control vehicular que permita controlar el acceso, los espacios libres y la ubicación de los autos en un estacionamiento usando la tecnología RFID.

3.2.1 Objetivos Específicos

- 1) Diseñar un sistema que automatice el control vehicular de los accesos.
- 2) Diseñar un sistema que muestre los espacios libres y obtenga una referencia de la ubicación de los vehículos.
- 3) Diseñar un software de administración desde donde se monitoree las actividades de los autos en el estacionamiento.

3.3 Diseño del sistema

El sistema que se plantea se puede dividir en cuatro partes: Sistema RFID, Sistema indicador de espacios libres, Comunicación inalámbrica, y el Software de administración. Estos se explicarán en forma detallada en los siguientes puntos a tratar.

3.3.1 Sistema RFID

Al ser la tecnología RFID la base del sistema de control vehicular, es necesario tener equipos RFID que permitan cumplir con las necesidades del sistema.

Para definir correctamente las especificaciones de los equipos, se debe analizar las necesidades del sistema propuesto. Según lo cual, estos deben responder a la necesidad de mayor importancia: ***La distancia de trabajo de los equipos debe ser grande, es decir, que el alcance del lector sea tal que pueda leer los datos del tag sin ocasionar la detención del vehículo, y haya el tiempo necesario para el procesamiento de datos.*** Por lo mismo, las distancias generalmente usadas en control vehicular con RFID son entre 2 y 7 metros.

3.3.1.1 Kit RFID

De acuerdo a las investigaciones realizadas, los equipos RFID que permiten alcanzar largas distancias trabajan a frecuencias entre 300 y 1200 MHz. Con estas se podrían alcanzar distancias de hasta 6 metros, suficientes para lo que se requiere.

Por otro lado, era necesario que los equipos RFID cumplan con alguno de los estándares conocidos: ISO o EPC, tal que trabajen con las normas y regulaciones del caso.

Por tanto, tomando como referencia las necesidades mencionadas anteriormente, se adquirió un Kit RFID, que incluye un lector (figura nº 5), una antena y algunos tags, con las características mostradas en la tabla nº 1.

Parámetro	Valor/Tipo	Unidad
Frecuencia	860 - 960	MHz
Interface	UART (TTL): 9.6 - 115.2	Kbps
Protocolo	EPC C1G2 / ISO 18000-6C	
Corriente consumo	1.5	Amperios
Voltaje	3.3	Voltios
Rango Lectura	2 - 5	Metros
Antena	50	Ohmios

TABLA 1: Características Kit RFID
Fuente: Skyetek



FIGURA 05 : SkyModule M10
Fuente: Skyetek

3.3.1.2 Instalación de equipos RFID

Con estos equipos se podrá formar la parte del sistema que permite identificar a cada usuario del estacionamiento. Para ello deberá seguirse el esquema de instalación que muestra la figura nº 6:

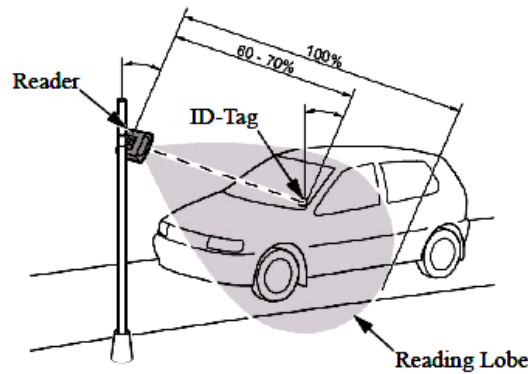


FIGURA 06: Sistema RFID vehicular
Fuente: Federal APD

Como se puede apreciar, el lector emitirá ondas de radio de acuerdo a su rango de alcance y cuando el tag entre en contacto con estas ondas, este responderá enviando su código, con lo cual se realizará la identificación del usuario.

Para favorecer a la identificación del tag, se debe instalar en el parabrisas del vehículo, en la esquina superior o inferior, en el lado del piloto, para así evitar algún tipo de incomodidad u obstrucción visual.

Además, se debe instalar el lector en el lado izquierdo del carril, sobre algún tipo de poste o soporte que le permita alcanzar una altura tal que esté por encima de la altura que tiene el tag. También hay que tomar en cuenta que al estar el lector a un lado del carril, este requiere una inclinación que le permita apuntar en la dirección por donde pasará el tag. En la figura nº 7 se puede apreciar mejor como se instalaría el sistema RFID.

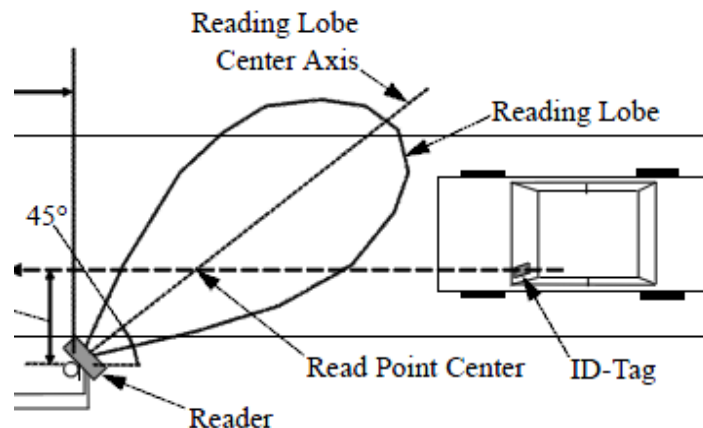


FIGURA 07: Sistema RFID vehicular
Fuente: Federal APD

Como se ve en la figura, el tag estará un tiempo dentro del rango de lectura del lector, donde se realizará la comunicación entre ambos. Este sistema RFID se utilizará para recolectar los datos necesarios del estacionamiento.

Por lo mismo, para realizar el control de acceso se necesitará lectores tanto en la entrada como en la salida. Si el estacionamiento es grande, es decir cuenta con varias divisiones o pisos se puede colocar lectores dentro del estacionamiento que permitan obtener la información necesaria para saber la posición relativa de los autos al interior del estacionamiento. Por lo tanto, con este sistema RFID se obtendrán los datos de los vehículos, los cuales se trasladarán hacia un servidor para su posterior procesamiento.

3.3.2 Diseño del Sistema indicador de espacios libres

El sistema indicador de espacios libres deberá comunicarse con el servidor para procesar la información enviada por este y actualizar la información del display. Por ello es necesario utilizar elementos que me permitan procesar los datos enviados y mostrar la información sobre la cantidad de espacios libres en el estacionamiento.

3.3.2.1 Hardware

Los componentes que fueron seleccionados para el desarrollo del Sistema indicador se detallan en los siguientes puntos.

a) Microcontrolador

Es el dispositivo programable con el cual se puede procesar la información y que debe poder comunicarse con el servidor. Además, debe ser de fácil acceso en el mercado local y, las herramientas necesarias para trabajar con él, como son el grabador y su entorno de programación, deben poder adquirirse sin problema.

Tomando en cuenta estas referencias, se prefirió trabajar con el microcontrolador ATmega8 sobre otros dispositivos, ya que, al tener experiencia en su manejo, contar con las herramientas necesarias y cumplir con las características como, tener el puerto necesario para la comunicación con el servidor y ser de fácil acceso en el mercado local, generaron una notoria diferencia sobre el resto de controladores.

b) Display

Este dispositivo es necesario para poder visualizar la cantidad de espacios libres dentro del estacionamiento en un determinado momento. Para ello, se deben mostrar

básicamente los dígitos del 0 al 9, en números que podrían llegar hasta las 3 ó 4 cifras. Al igual que el microcontrolador, este dispositivo debe ser cómodo económicamente y fácil de conseguir, además de poder mostrar los valores antes mencionados.

Tomando en cuenta estos requerimientos y realizando las comparaciones con las diferentes opciones presentadas, se optó por utilizar un display de 7 segmentos, ya que es de fácil acceso al mercado, no tiene un costo elevado y principalmente, puede mostrar fácilmente los dígitos del 0 al 9 y la cantidad de cifras dependería únicamente del número de displays usados. Las otras opciones, como un LCD o un display alfanumérico, si bien pueden mostrar las cantidades deseadas, son mucho más caros y no son tan fáciles de conseguir como el producto escogido.

Debido a que las cantidades a mostrar, en el display de 7 segmentos, son altas, ya que un estacionamiento puede contar con muchos lugares, se utiliza un display de 7 segmentos de 4 dígitos, tal como lo muestra la figura n° 8.

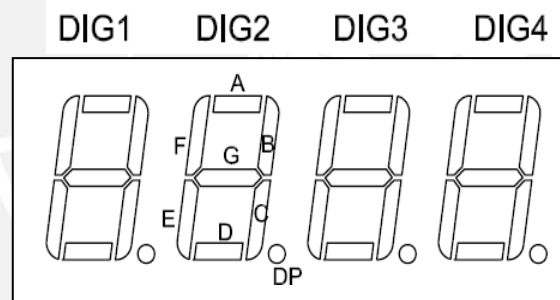


FIGURA 08: Display 7 segmentos de 4 dígitos
Fuente: Bond-led

Las dimensiones del display que se está usando, al ser un prototipo, son pequeñas, de aproximadamente 19 cm de alto por 50 cm de largo. Sin embargo, si se desea implementar el sistema, se debe contar con un display de dimensiones mayores.

Este dispositivo funciona a través de leds rectangulares, llamados cada uno segmento, que se encienden o apagan para formar los números que se desee al polarizarlos correctamente. Estos pueden ser de dos tipos: Ánodo común y Cátodo común. Como su nombre lo indica, para el primer tipo, los leds están unidos por el ánodo, y en el otro caso, por el cátodo. Se diseñó el circuito indicador utilizando un display cátodo común ya que al trabajar con este tipo de display, se puede utilizar una lógica positiva para encender los segmentos.

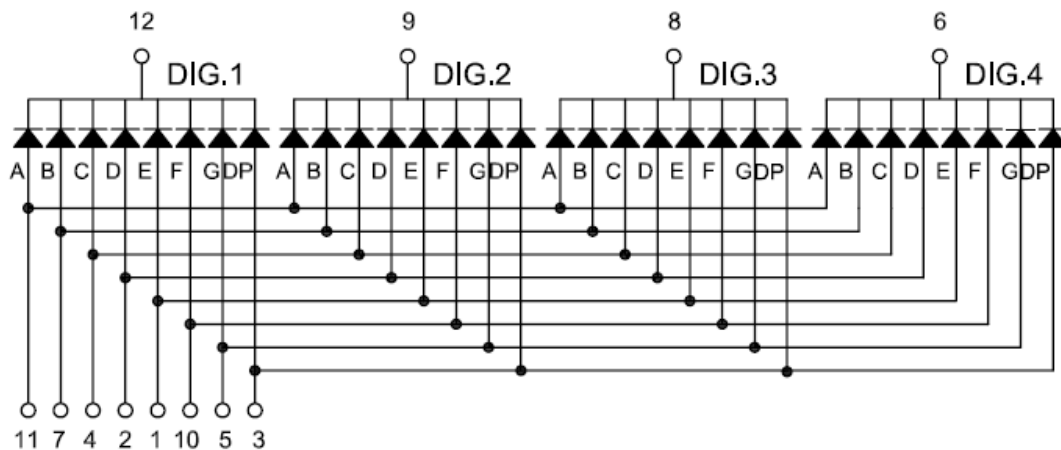


FIGURA 09: Diagrama circuito interno - Display 7 segmentos de 4 dígitos
Fuente: Bond-led

Con el microcontrolador y con la ayuda del diagrama anterior del display, figura nº 9, se obtuvo el circuito que se encargará de mostrar la cantidad de autos. Para visualizar el circuito resultante “**Véase Anexo 4**”.

En este se puede apreciar que, algunos pines del display de 7 segmentos están conectados a resistencias ya que se requiere regular la corriente de los segmentos a encender. Se usaron resistencias de 330 ohmios para que regulen la corriente a 15 mA. El otro pin de las resistencias está conectado al microcontrolador para que este ordene cuando se deban prender o pagar los segmentos.

La bornera de comunicación, es para conectar los pines Rx, Tx y GND del dispositivo con el que se quiera realizar la comunicación serial, el cual será el Secure Socket iWifi.

3.3.2.2 Software

El microcontrolador ATmega8 se programó según las características del display seleccionado. Por ello, se utilizó el puerto B para controlar los segmentos a encender o apagar, siendo la referencia el PB0 con la letra A hasta el PB6 con la letra G. Además se necesitó del puerto C para controlar el encendido o pagado los dígitos del display, usando el PC0, como la referencia, para habilitar el dígito 4 hasta el PC4 para habilitar el dígito 1.

Básicamente, el programa muestra los 4 dígitos encendidos a la vez, mientras espera la llegada de un nuevo dato para actualizar la información mostrada. Sin embargo, para encender los 4 dígitos al mismo tiempo se usa un algoritmo que encienda un dígito a la vez, pero funciona a una frecuencia tan alta que no es posible detectarlo con los ojos y genera el efecto de que todos estuvieran encendidos al mismo tiempo. Debido a ello se usa, una interrupción por USART en la recepción para poder realizar los otros procesos mientras se espera la llegada de un dato nuevo. Para revisar los diagramas de flujo y el programa realizado “**Véase Anexo 2**”.

Con la grabación de este software en el microcontrolador y la implementación de la tarjeta se podrá obtener el sistema que permita mostrar la cantidad de espacios libres en el estacionamiento.

3.3.3 Comunicación inalámbrica

Los equipos a comunicar con el servidor son los lectores RFID y el sistema indicador de espacios libres, que poseen un puerto serial para su comunicación. Sin embargo, al tener restricciones en cuanto a las distancia de la comunicación serial entre equipos, máximo 15 metros, según el estándar RS-232, y tomando en cuenta que los estacionamientos tienen áreas amplias, se requiere trabajar con un dispositivo que comunique los equipos inalámbricamente a través de una red wifi. Con esto se evitará cablear los puntos en los cuales se encontrarán los equipos y también se reducirán los gastos de instalación.

3.3.3.1 Secure Socket iWifi

Debido a la necesidad de contar con un elemento que funcione como puente entre equipos seriales y redes inalámbricas, se adquirió el Secure Socket iWifi, que se muestra en la figura nº 10. Este dispositivo posee un modo de trabajo, llamado modo Serial Net, en el cual puede funcionar como se necesita para lograr comunicar los lectores RFID y el sistema indicador, a través de su puerto serial, con una red wifi. La tabla nº 2 muestra las características de este dispositivo:

Parámetro	Valor	Unidad
Voltaje operación	3.3	V
Frecuencia	2.4	GHz
Corriente consumo	290	mA
Interface	TTL serial	

TABLA 2: Características Secure Socket iWifi
Fuente: Connect One

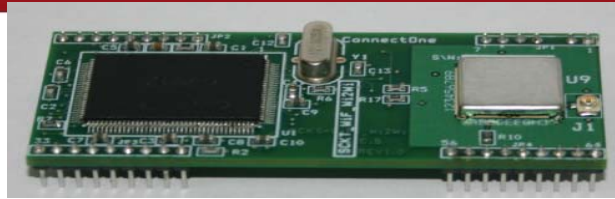


FIGURA 10: Secure Socket iWifi
Fuente: Connect One

Si bien las características eléctricas presentadas en la tabla anterior, no son requerimientos indispensables del sistema, el requisito principal para el dispositivo a elegir era cumplir con la comunicación de los equipos. Es por ello que, al cumplir con las necesidades de comunicación, se escogió este elemento como base del sistema inalámbrico.

3.3.3.2 Tarjeta de configuración y comunicación

Este dispositivo wifi se debe configurar previamente para que funcione de acuerdo a las necesidades del sistema. Para ello se requiere del programa iChip Config, el cual permitirá configurar los parámetros necesarios.

Sin embargo, primero se debe establecer la comunicación entre el dispositivo wifi y el equipo, ya sea una computadora o laptop, donde se instalará el software iChip Config. Tomando en cuenta que actualmente la mayoría de equipos de cómputo utiliza un puerto USB para comunicación, se diseñó una interfaz que permita comunicar ambos dispositivos, el Secure Socket y la computadora, a través de este puerto. Para ello, la interfaz trabaja con el chip FT232R que permite la conversión, de los datos del dispositivo wifi, de serial a USB.

El FT232R se alimenta a través de la energía recibida por el conector USB, 5v. Los datos de la computadora se envían a los pines 15 y 16 del chip FT232R, que son los pines de datos USB. Además, este chip posee un pin denominado VCCIO que permite controlar los niveles de voltaje de las entradas y salidas seriales, según el nivel de voltaje que reciba. Tomando en cuenta que las entradas y salidas seriales del Secure Socket trabajan a 3,3v, fue necesario colocar el VCCIO a este nivel de energía para que las entradas y salidas seriales del FT232R tengan este mismo nivel. Para esto se usó el pin 17 del FT232R que entrega este nivel de voltaje.

El Secure Socket iWifi se alimenta a través de una fuente externa. Debido a que este requiere 3.3v, se usa un regulador de voltaje para obtener este nivel. No se pudo

conectar el pin 17 del FT232R, que también posee este nivel de energía, al pin de alimentación del Secure Socket, porque este pin no entrega la corriente que requiere el dispositivo wifi. El pin del FT232R entrega un máximo de 50 mA, siendo el nivel máximo requerido por el módulo wifi, durante la transmisión, de 290 mA. Por ello se utilizó el convertor de voltaje LM 1117, que entrega como mínimo 800 mA. Además, se colocó un led, en el pin 58 del módulo wifi, que permitirá indicar cuando el dispositivo está escaneando una red wifi o cuando realiza un enlace con el equipo que posee el software. Para ello se usó un led de 3mm y una resistencia de 330 ohmios para regular su corriente a 10 mA.

Posteriormente, se unieron los pines de transmisión y recepción de datos del FT232R (pines 34 y 35, respectivamente) con los del Secure Socket (pines 1 y 5, respectivamente). Además, también se unieron los pines de control de datos, CTS y RTS, del FT232R (pines 33 y 38, respectivamente) con los del Secure Socket (pines 3 y 11, respectivamente). Los pines de control de datos aseguran que la comunicación se realice sin problemas, ya que a través de estos se coordina la transmisión y recepción de datos. Para realizar la conexión anterior, hay que tomar en cuenta que el pin de transmisión de uno va al pin de recepción del otro y viceversa. Del mismo modo con los pines de control, es decir, el pin CTS de uno va al pin RTS del otro y viceversa. Para visualizar el diseño de la tarjeta con los requerimientos antes mencionados “**Véase Anexo 4**”.

Las borneras y los jumpers permitirán, luego de configurar el dispositivo wifi, comunicar serialmente el Secure Socket iWifi con otros equipos. Para ello se colocaron jumpers en las conexiones de los pines de transmisión, recepción, CTS y RTS. Con esto, los jumpers permitirán que en la posición 1-2 se comuniquen el dispositivo wifi con el FT232R y en la posición 2-3, se comunique el Secure Socket con otro equipo. Debido a esto, esta tarjeta servirá para configurar el Secure Socket y para comunicarlo serialmente con algún dispositivo que necesite conectarse inalámbricamente a una red wifi. Para visualizar las figuras que muestran las distribuciones de los pines del Secure Socket y del FT232R “**Véase Anexo 4**”.

3.3.3.3 Programación del módulo

El Secure Socket iWifi se programa a través del software iChip Config. Este software permite programar al controlador del dispositivo wifi, el chip CO2128, con comandos AT+i. Una línea de comando AT + i es una cadena de caracteres que se envían desde el host al iChip del Secure Socket, mientras se encuentre en estado de comandos. La

línea de comandos tiene un prefijo, cuerpo y terminador. Cada comando debe comenzar con la secuencia de caracteres de AT + i, y terminado por un <CR>, retorno de carro. Los comandos se pueden introducir tanto en mayúsculas como en minúsculas.

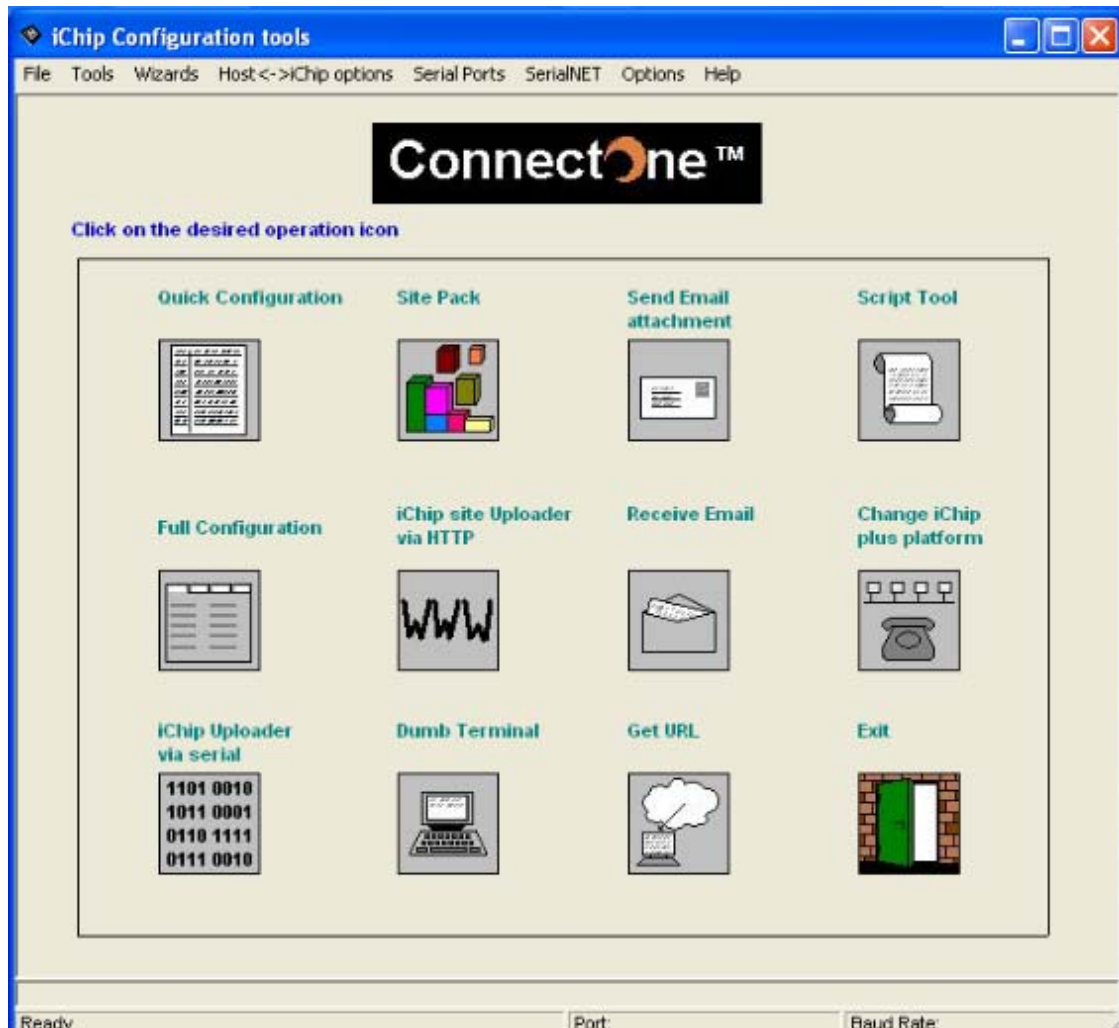


FIGURA 11: Software iChip Config
Fuente: Connect One

En la figura nº 11, se muestra la pantalla principal del software. En la parte superior, tiene algunas pestañas con las que se pueden realizar configuraciones. Con una de estas, llamada Serial Port, se debe configurar el puerto donde está conectado el Secure Socket y la velocidad con la que trabajará. La figura nº 12 ilustra esta primera configuración.

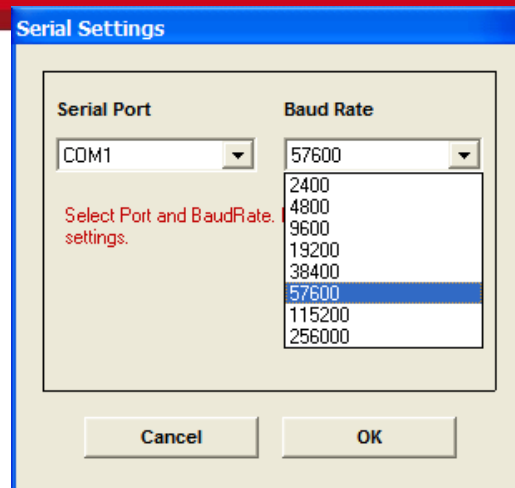


FIGURA 12: Ventana Serial Port
Fuente: Connect One

Posteriormente, para programar el Secure socket se debe ingresar al ícono de nombre Dumb Terminal que se encuentra en la parte central de la pantalla principal, donde se procederá escribir los comandos AT+i.

Los comandos que permitirán configurar al Secure Socket iWifi, para conectarse a un determinado Access Point, son los siguientes:

- AT+iFD, restaura todos los valores de fábrica del chip, para realizar un nuevo comienzo.
- AT+iBDRF= <n>, configura los baudios en la conexión serial. Donde:
 - ✓ n=a, Configuración automática
 - ✓ n=3, Configura los baudios a 2400
 - ✓ n=4, Configura los baudios a 4800
 - ✓ n=5, Configura los baudios a 9600
 - ✓ n=6, Configura los baudios a 19200
 - ✓ n=7, Configura los baudios a 38400
 - ✓ n=8, Configura los baudios a 57600
 - ✓ n=9, Configura los baudios a 115200
 - ✓ n=h, Configura los baudios a 230400
- AT+iRP20, retorna una lista de todas las visibles Access Point y redes Ad-Hoc captadas por el Secure Socket.
- AT+iWLSI= <ssid>, configura el SSID (Service Set Identifier) que tiene cada Access Point. Este parámetro identifica al Access Point al que el iChip se va a conectar. Se puede interpretar como el nombre de la red.
- AT+iWSTn= <sec>, configura el tipo de seguridad para cada red a la que se conecte el Secure Socket. Donde:

- ✓ “n” toma valores del 0 al 9, que corresponde al número de cada red a la que se haya conectado
 - ✓ sec=0, No tiene seguridad
 - ✓ sec=1, WEP-64
 - ✓ sec=2, WEP-128
 - ✓ sec=3, WPA-TKIP
 - ✓ sec=4, WPA2-EAPS
- AT+iWKYn= <clave>, configura la clave de cada red a la que se conecte el Secure Socket. Donde:
 - ✓ “n” toma valores del 0 al 9, que corresponde al número de cada red a la que se haya conectado
 - ✓ clave, caracteres representados hexadecimalmente.
 - AT+iDOWN: reinicia la configuración realizada en el Secure Socket.

Con estos comandos se podrá realizar la conexión a una determinada red y obtener una dirección IP. Sin embargo, se deben realizar otras configuraciones para poder establecer comunicación entre el Secure Socket iWifi y un procesador remoto.

Para ello se utilizará el modo Serial Net del Secure Socket, el cual permite establecer una conexión serial asíncrona entre un socket TCP o UDP a través de una LAN o Internet. Tiene el propósito principal de permitir que los dispositivos que trabajan sobre una línea serial se puedan comunicar a través de una red con otros dispositivos, ya que en modo Serial Net, el iChip CO2128 actúa con una Router entre el puerto serie del dispositivo y la Red. Para ello, es necesario realizar otras configuraciones a las mencionadas anteriormente.

Los dispositivos que se comunican en una red pueden ser clientes o servidores. En general, los clientes suelen iniciar la comunicación mediante el envío de demandas de servicios a un servidor, mientras que los servidores responden a las demandas de los clientes. El Modo de SerialNET incluye componentes para ser tanto de servidor como cliente de dispositivos locales.

Según los requerimientos de la tesis, se configuró el Secure Socket como cliente ya que se necesita que este envíe información a un servidor en determinados momentos. Por ello, el servidor estará esperando que algún cliente se conecte para establecer la comunicación.

Los comandos AT+i que permiten configurar el Secure Socket como cliente y en modo Serial Net son los siguientes:

- AT+IHSRV= <nombre del servidor: puerto>, configura el nombre y el puerto del servidor a ser usados en el modo Serial Net.
- AT+IFCHR= <flush_character>, configura el carácter que indicará el momento en el cual se transmitirán los datos. Donde:
flush_character: 'a'-'z' / 'A'-'Z' / '0'-'9', character hexadecimal.
- AT+ISNSI= <settings strings>, configura algunos parámetros para el modo Serial Net.

settings strings: <baudios>, <cantidad de bits>,<paridad>,<bits de parada>,<flujo>. Donde:

- ✓ baudios: toma valores del 0 al 9 o el valor de "h"

Código Baudio	Baudios	Código Baudio	Baudios
0	Ver Nota1	6	19200
1	600	7	38400
2	1200	8	57600
3	2400	9	115200
4	4800	h	230400
5	9600		

TABLA 3: Valores de Baudios
Fuente: Connect One

Nota1: cuando baudios=0, se determina el valor de los baudios según el valor del comando BDRD, anteriormente definido.

- ✓ cantidad de bits: 7 - 8
- ✓ paridad: N(ninguna) - E(par) - O(impar)
- ✓ bits de parada: 1 (1 bit de parada)
- ✓ flujo: 0(no hay control de flujo) - 1(si hay control de flujo)

Por defecto, los valores que se tiene son: 5, 8, N, 1, 0 – 9600 baudios, 8bits, No paridad, 1 bit de parada, no hay control de flujo.

- AT+IHIF=n, especifica la interfaz de comunicación a ser usada entre el iChip y el otro procesador. Donde:
 - ✓ n=0: Interface automatic
 - ✓ n=1: USART0
 - ✓ n=2: USART1

- ✓ n=3: USART2
- ✓ n=4: USB Device
- ✓ n=5: USB Host
- AT+ISNMD: Activa el modo Serial.

Con todos estos comandos se podrá configurar el Secure Socket en modo Serial Net, donde será cliente en una determinada red. Con esto, un dispositivo con interfaz serial se podrá comunicar inalámbricamente con una red a través de este dispositivo wifi.

Sin embargo, además de estos comandos se puede necesitar del uso de otros para verificar el estado de la actual configuración que se está realizando:

- AT+IRP10, reporta el contenido de la actual conexión. La respuesta contiene valores de acuerdo a la siguiente sintaxis:
I/(<estado del puerto>, <rango de transferencia>, <nivel de la señal >, <calidad del enlace>), donde:
 - ✓ Estado del puerto:
 - 0: Adaptador del Wireless LAN no presente
 - 1: Adaptador del Wireless LAN deshabilitado
 - 2: Buscando para iniciar la conexión
 - 4: Conectado
 - 5: Fuera del rango
 - ✓ Rango de transferencia: 1 a 54 Mbps
 - ✓ Nivel de la señal (%): rango de 0 a 100
 - ✓ Calidad del enlace (%): rango de 0 a 100
- AT+IIPA?, reporta la actual dirección IP que posee el Secure Socket

La ejecución de estos comandos podrán ayudar a entender de una mejor manera como se va configurando el Secure Socket iWifi.

3.3.4 Diseño del Software de Administración

Para obtener un sistema integrado que permita registrar todas las actividades realizadas en el estacionamiento, se requiere de un Software de Administración. Este software debe tener una interfaz amigable para que la persona que lo utilice tenga todas las comodidades y facilidades para manejarlo sin problemas.

Además, debe poder realizar algunos procesos básicos como registrar la información de los tags, enviada inalámbricamente por cada lector RFID. Con esto se tendrá la

información correspondiente a cada vehículo. También se debe enviar inalámbricamente información al display sobre la cantidad de espacios libres en el estacionamiento. Por otro lado, este software, que será instalado en una computadora, debe permitir que esta computadora funcione como servidor y que pueda recibir conexiones de los distintos clientes, es este caso de los lectores y del display informativo.

Debido a estos requerimientos, se utiliza el programa Visual Basic 6.0, como base para el desarrollo del software. Este programa utiliza un ambiente de desarrollo completamente gráfico, lo cual permitirá obtener la interfaz amigable que se desea.

Además, cuenta con una herramienta de trabajo, llamada Winsock, que realiza conexiones Cliente/Servidor a través de protocolos TCP y UDP. Este único componente puede trabajar de dos formas, como Cliente (Conecta a un servidor) y como Servidor (Recibe conexiones). Además, se puede trabajar con vectores de Winsock, lo que permitiría administrar varias conexiones con un mismo código en común. Este tipo de funcionamiento, tipo arreglo, es el requerido por el sistema ya que se conectarán varios equipos al servidor.

Con el programa definido, se pasó a la conformación de la interfaz y programación en Visual Basic utilizando el componente Winsock como base, con el fin de obtener el Software que permita cumplir con los requerimientos del sistema. Para revisar el diagrama de flujo y el programa realizado "**Véase Anexo 1**". El resultado obtenido se muestra en la figura nº 13.

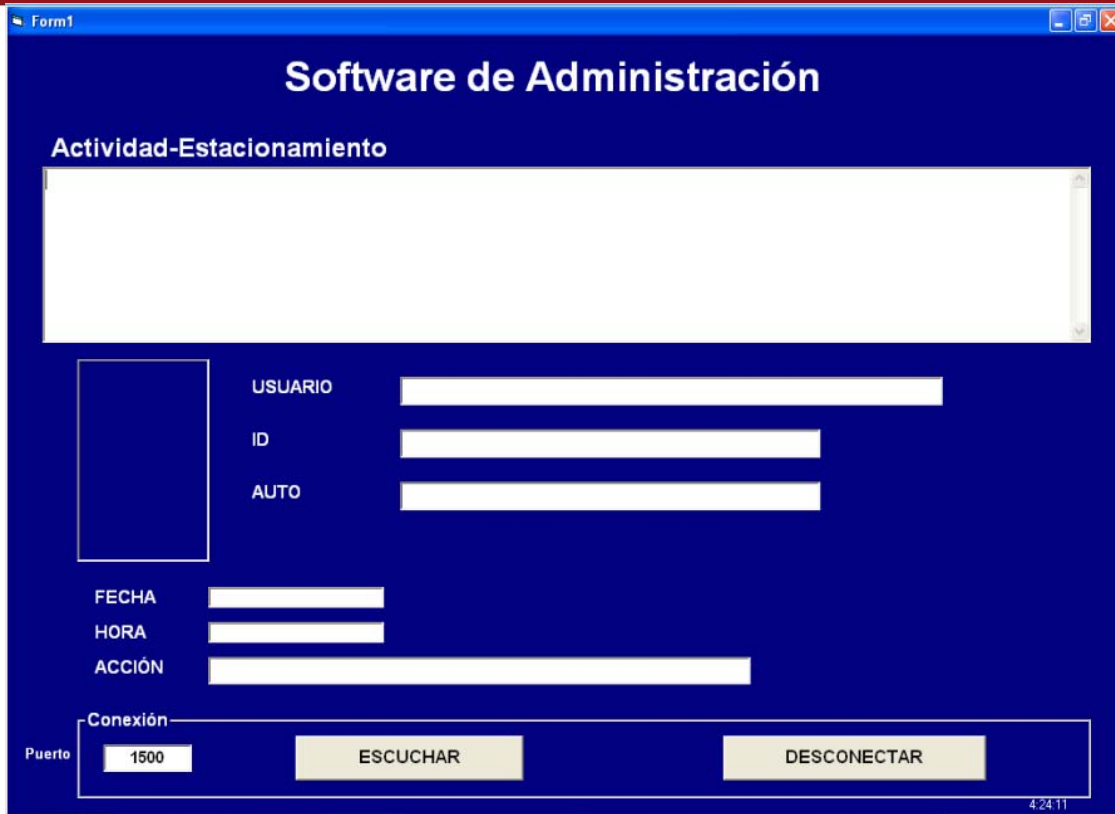


FIGURA 13: Interfaz usuario - Software de administración
Fuente: Elaboración propia

Para poder empezar a trabajar con esta interfaz se debe colocar el número del puerto en la casilla correspondiente, por el cual se establecerán las comunicaciones. Sin embargo, este valor será colocado desde el programa. Por lo tanto, el primer paso será presionar el botón “Escuchar” para habilitar la recepción de conexiones por parte de los clientes. Luego de esto, los clientes podrán establecer la comunicación con el servidor.

A medida que se vayan conectando los lectores, se podrá observar la información captada por estos en la interfaz. Todo lo realizado por los vehículos se registrará en el cuadro superior blanco, y para dar una mayor facilidad, la información específica correspondiente a cada usuario se podrá visualizar en las casillas ubicadas al medio de la interfaz. Estas indicarán el nombre de la persona, su código, que tipo de auto tiene, la fecha y hora de la acción realizada y la acción realizada. Esta acción podría hacer referencia a la salida, ingreso del estacionamiento u otra actividad hecha por el usuario.

Además de mostrar un resultado en la pantalla, el Software también envía información al Sistema indicador de espacios libres para actualizar la información del display. Para ello se envía un comando para indicar que se debe aumentar la cuenta del display, y otro comando para disminuirla.

Con el acople de todas las partes diseñadas, es decir, el Sistema RFID, la comunicación inalámbrica, el Sistema indicador de espacios libres y el Software de Administración, se pasarán a realizar las pruebas correspondientes para evaluar su funcionamiento.



CAPÍTULO 4

PRUEBAS DEL SISTEMA Y ANÁLISIS DE RESULTADOS

En el presente capítulo se explicarán las pruebas realizadas con los elementos del sistema para analizar su funcionamiento individual. Posteriormente, se desarrollará una prueba con el sistema completo, es decir, con los elementos acoplados para simular el sistema de control diseñado.

Al final, dependiendo de los resultados obtenidos, se podrá concluir si el sistema de control vehicular cumple con las expectativas establecidas al inicio de la tesis.

4.1 Desarrollo de pruebas

Las pruebas de comunicación se realizaron sobre una red de área local, LAN, con dirección IP 192.168.1.0 y máscara de subred 255.255.255.0.

4.1.1 Prueba con el Sistema RFID

El Kit RFID adquirido debe permitir la adquisición de datos de los vehículos que poseen etiquetas RFID adheridos a los parabrisas. Para ello fue necesario probar el Kit y verificar que cumpla con los requerimientos dados anteriormente.

Para realizar la prueba fue necesario conectar algunos elementos para formar el sistema RFID, instalar el software del Kit en una computadora que tenga puerto serial y contar con los Tags. La figura n° 14 muestra la disposición de los equipos durante la prueba.

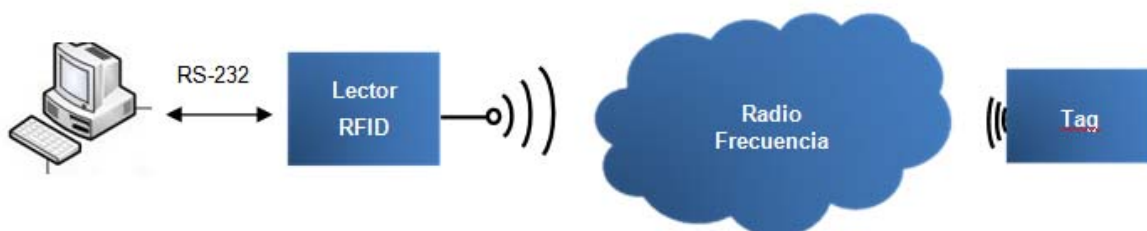


FIGURA 14: Sistema RFID - Prueba1
Fuente: Elaboración propia

Luego de la prueba, se pudo estimar que el rango de alcance del lector RFID es de aproximadamente 3 metros y que para velocidades mayores a 30 km/h el lector tiene problemas para captar los datos del tag.

En conclusión, se pudo verificar el funcionamiento del sistema RFID aunque este trabaja correctamente respetando ciertos límites: la distancia de alcance se encuentran entre 2 y 2.5 metros y la velocidad entre 20 a 25 km/h. Para estos valores, el sistema RFID puede desempeñar eficientemente su trabajo.

4.1.2 Prueba con el Secure Socket iWifi

Todas las configuraciones y herramientas usadas para probar el funcionamiento del dispositivo wifi se desarrollan en los siguientes puntos. Al final se realiza una prueba que permitirá analizar si el dispositivo wifi, luego de su configuración, logra comunicar inalámbricamente dos equipos que pertenecen a una misma red pero usando la interfaz serial de una de ellos.

4.1.2.1 Tarjeta de configuración y comunicación del Secure Socket

Para llevar a cabo las pruebas con el Secure Socket se tuvo que implementar la tarjeta de configuración y comunicación de este dispositivo. El diseño de esta tarjeta fue explicado anteriormente en el punto 3.3.2.2. Para visualizar la tarjeta final con la que se realizaron las pruebas “**Véase Anexo 4**”.

En esta tarjeta se encuentra montado el Secure Socket iWifi sobre sus unos sockets. Los jumpers son componentes importantes dentro del diseño de la tarjeta ya que permiten, en una posición, realizar la configuración del dispositivo wifi y, en la otra, la comunicación serial, a través de las borneras, con otros equipos.

Un punto importante a tomar en cuenta en la utilización de esta tarjeta es que, la comunicación, requiere de 3.3 voltios. Tomando como referencia que los equipos usan 5 voltios, fue necesario regular la entrada de la comunicación de esta tarjeta a este nivel de energía. Debido a esto se trabajó con un divisor de voltaje en la línea de recepción de la tarjeta. La figura nº 15 ilustra el circuito utilizado para obtener al nivel adecuado en la entrada de la comunicación de esta tarjeta.

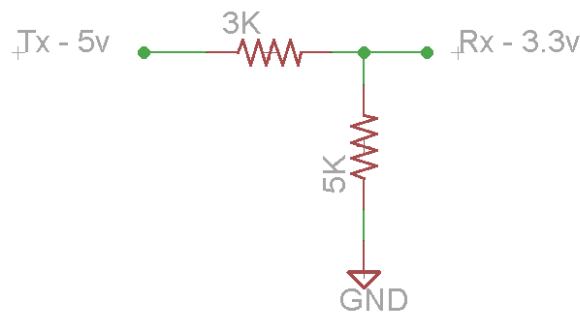


FIGURA 15: Circuito divisor de voltaje
Fuente: Elaboración propia

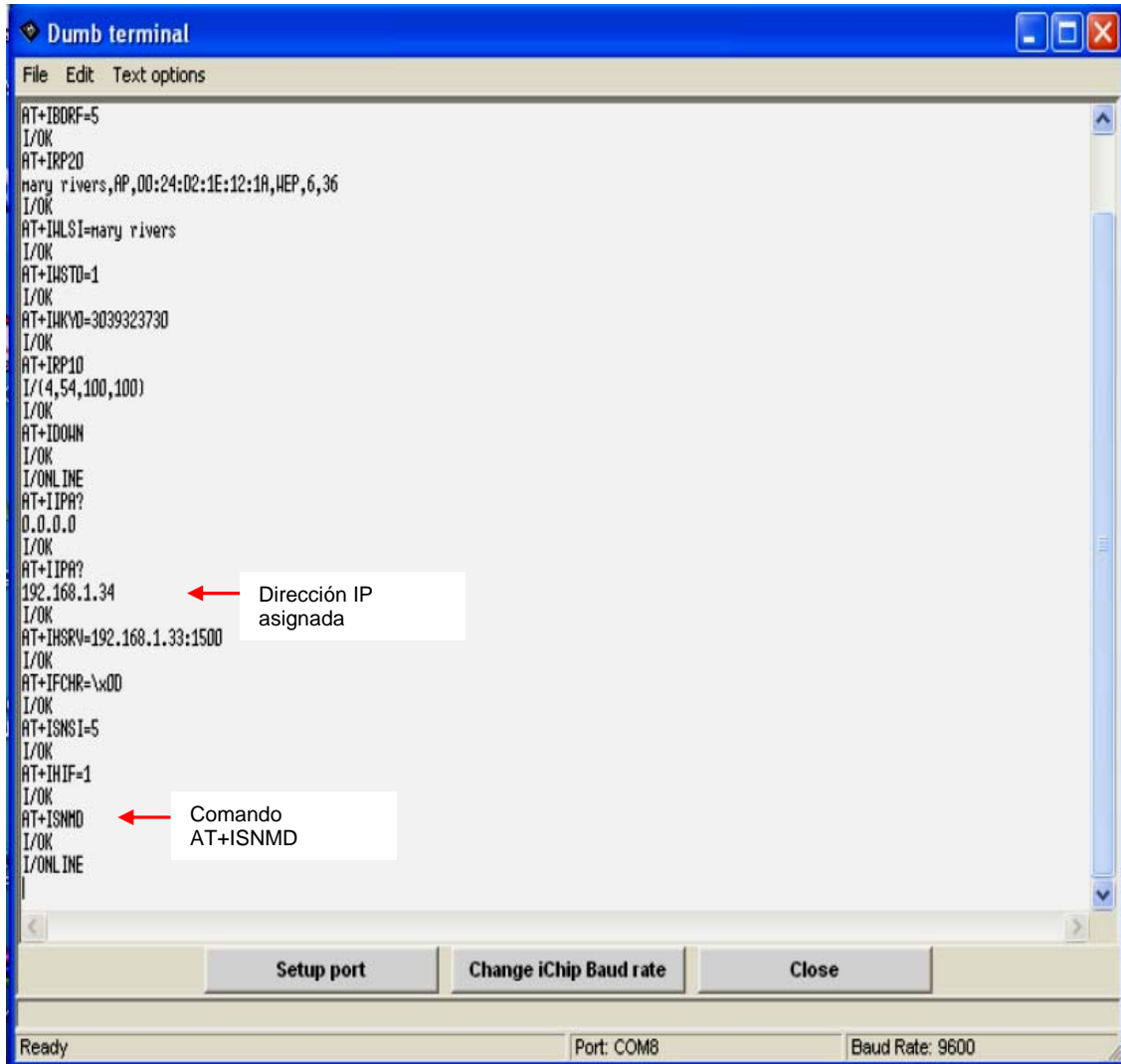
Entonces, la transmisión del equipo que maneja 5 voltios debe ir conectada al pin “Tx-5v” del diagrama anterior, para que la recepción de la tarjeta del Secure Socket sea conectada al pin “Rx-3.3v”, y le llegue el nivel de voltaje adecuado. Para la Transmisión de la tarjeta del Secure Socket no fue necesario modificarle el voltaje, ya que al trabajar con niveles TTL, el equipo que maneja 5 voltios, al recibir 3.3 voltios como entrada, interpreta el valor como nivel alto, por lo que se logra la comunicación correcta.

Por tanto, solo será necesario colocar este divisor en la Recepción de la tarjeta para que se pueda comunicar sin problemas con equipos que manejan 5 voltios. Con esta tarjeta implementada y la utilización del divisor de voltaje se pudieron realizar todas las pruebas necesarias para verificar el funcionamiento del Secure Socket.

4.1.2.2 Configuración del Secure Socket

Este transmisor-receptor wifi comunica a los dispositivos seriales, como son los lectores RFID y el sistema indicador de espacios libres, con el servidor a través de una red inalámbrica. Los equipos seriales serán los clientes en la red, por lo cual se configuró el Secure Socket de esta forma. Para revisar la configuración realizada “Véase Anexo 3”.

En la figura nº 16 se muestra la configuración realizada en el DUMB TERMINAL del programa de configuración del Secure Socket iWifi.



```

AT+IBDRF=5
I/OK
AT+IRP20
nary rivers, AP, 00:24:D2:1E:12:1A, WEP, 6, 36
I/OK
AT+IHLSSI=nary rivers
I/OK
AT+IHWSTO=1
I/OK
AT+IHWYD=3039323730
I/OK
AT+IRP10
I/(4,54,100,100)
I/OK
AT+IDOWN
I/OK
I/ONLINE
AT+IIPR?
0.0.0.0
I/OK
AT+IIPR?
192.168.1.34
I/OK
AT+IHSRV=192.168.1.33:1500
I/OK
AT+IFCHR=\x00
I/OK
AT+ISNSI=5
I/OK
AT+IHIF=1
I/OK
AT+ISNMD
I/OK
I/ONLINE
  
```

FIGURA 16: Configuración Secure Socket - Dumb Terminal
Fuente: Connect One

A partir de la ejecución del comando, `AT+ISNMD`, y la respuesta positiva del dispositivo wifi, el Secure Socket queda listo para recibir información serialmente y transmitirla hacia el servidor a través de la red wifi.

4.1.2.3 Prueba de comunicación

Para realizar esta prueba fue necesario contar con el Software de Administración, la tarjeta de configuración y comunicación del Secure Socket, el Hyperterminal de una computadora, un cable serial y un circuito basado en el chip MAXIM 232, que adecue los valores de los voltajes de la computadora y del Secure Socket. Antes de conectar

cualquier elemento, primero se debió cambiar la posición de los jumpers de la tarjeta, para habilitar las borneras y desde ahí comunicar a los equipos seriales.

Posteriormente se realizaron las conexiones correspondientes entre la tarjeta del Secure Socket, el circuito con el MAXIM 232 y el cable serial. El cable serial comunicaría al Hyperterminal de la computadora con la tarjeta del dispositivo wifi, teniendo, al circuito basado en el MAXIM 232, como enlace entre ambos. El Software de Administración se instaló en una laptop con el objetivo de verificar que se puede realizar la comunicación de un equipo que utiliza una interfaz serial, con otro que se encuentra conectado a una red inalámbrica. La figura n° 17 muestra la disposición de los equipos en la prueba realizada.



FIGURA 17: Disposición de equipos - Prueba 2
Fuente: Elaboración propia

Luego de realizar todas las instalaciones y conexiones, se procedió a configurar el Hyperterminal, como lo muestra la figura n° 18:

- 9600 bps
- 8 bits de datos
- Sin paridad
- 1 bit de parada
- Sin control de flujo

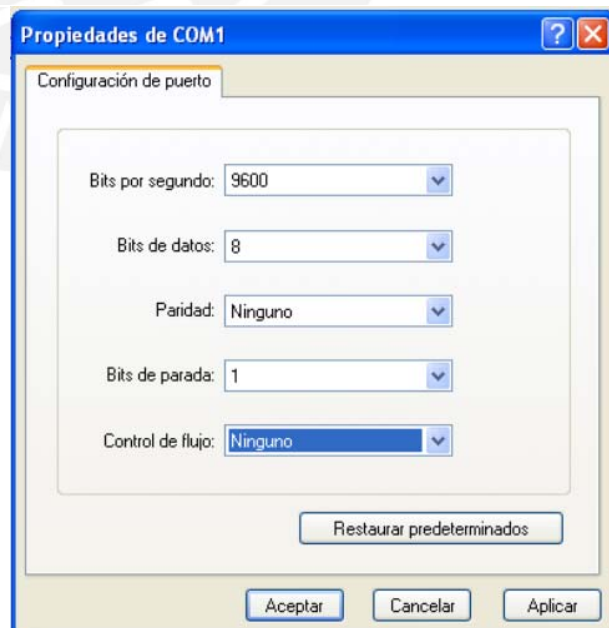



FIGURA 18: Configuración Hyperterminal
Fuente: Connect One

En la laptop, con el Software de Administración instalado, se habilitaron las peticiones de conexión de clientes, presionando el botón “Escuchar”. Desde el Hiperteminal de la computadora se realizó la conexión con el Software, al enviar cualquier caracter.

En el cuadro superior de texto del Software, llamado Actividad-Estacionamiento, se puede ver, en las líneas 2 y 3, que el cliente, llamado CLIENTE1, con dirección IP 192.168.1.34 se ha conectado. Esta dirección IP es la que le fue asignada al Secure Socket en la configuración inicial.

Una vez establecida la conexión, en la ventana del Hyperterminal se escribió la siguiente trama: 010010. Esta fue recepcionada automáticamente por el software, el cual arrojó el resultado que se observa en la figura nº 19.



The screenshot shows a software window titled "Form1" with a dark blue background. The main title is "Software de Administración". Below it, a section titled "Actividad-Estacionamiento" contains a text area with the following text: "Escuchando conexiones.", "DIRECCION-IP(0) :192.168.1.34", "Cliente1: Conexión aceptada", "Cliente 1: ID - Auto : 010010", "INGRESO: PUERTA N°1", "DISPLAY: Entrada Auto > 0", "USUARIO: Carmen Vidalon", "ID: 010010". Below this, there is a profile picture of a woman and a form with fields for "USUARIO" (Carmen Vidalon), "ID" (010010), and "AUTO" (Combi Placa : HIJ789). Further down, there are fields for "FECHA" (14/11/2009) and "HORA" (14:11:18). A large green button labeled "ACCIÓN" displays "INGRESO : PUERTA N°1". At the bottom, a "Conexión" section includes a "Puerto" field with the value "1500" and two buttons: "ESCUCCHAR" and "DESCONECTAR". The system clock in the bottom right corner shows "14:12:13".

FIGURA 19: Software de Administración – Respuesta a código
Fuente: Elaboración propia

En la cuarta línea del cuadro Actividad-Estacionamiento, se puede ver que la trama 010010 fue enviado por CLIENTE1, que identifica al Secure Socket. Este código, según el resultado de la figura n° 19, corresponde a la persona que se muestra en pantalla, con sus respectivos datos. Además de la respuesta mostrada, el Software envió la siguiente información al cliente que le envió la trama, confirmando la llegada de los datos sin problema. Esta información se pudo visualizar en el Hyperterminal.

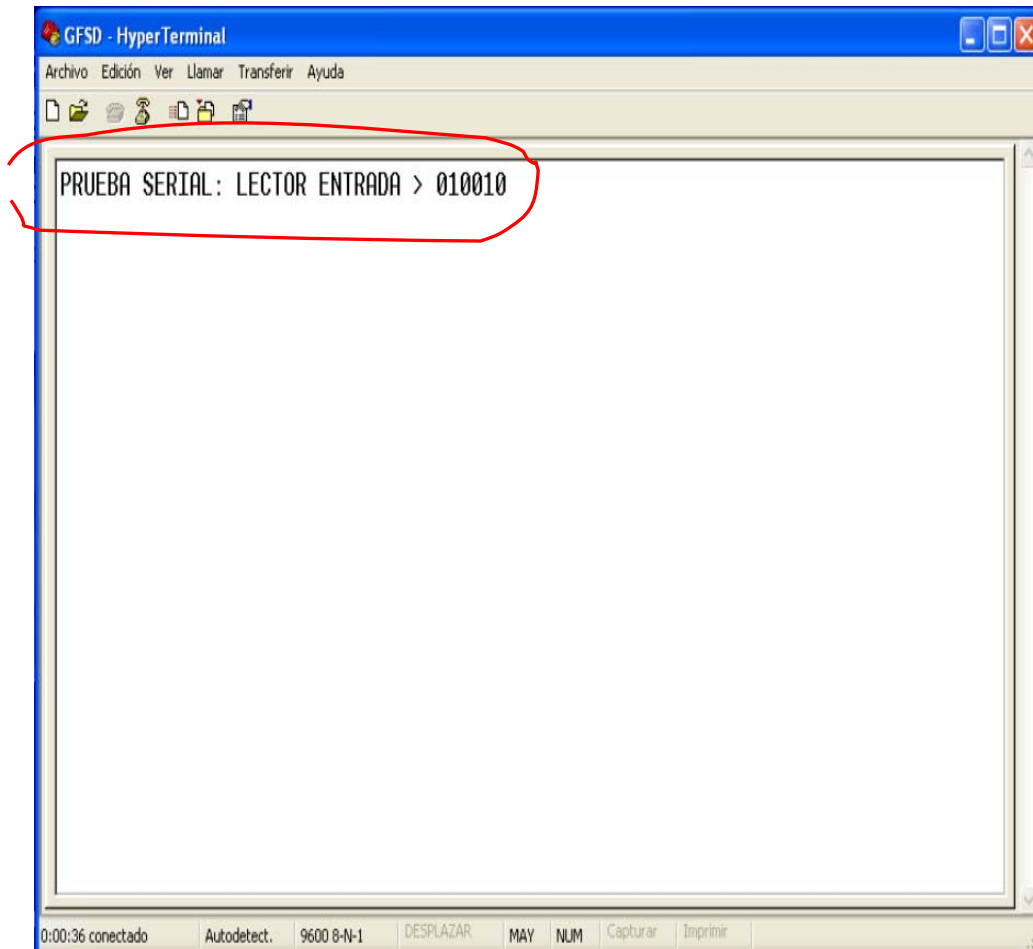


FIGURA 20: Hyperterminal: Respuesta del Software
Fuente: Hyperterminal

Esta respuesta enviada por el software se debe a los datos enviados desde el Hyperterminal al inicio de la prueba.

Con esta prueba de comunicación entre el Hyperterminal de una computadora y una laptop, se puede concluir que el Secure Socket iWifi está listo para comunicar cualquier equipo serial con una red wifi.

4.1.3 Prueba con el Software y el Sistema indicador de espacios libres

La prueba realizada básicamente intenta simular el funcionamiento del Sistema de control vehicular en un estacionamiento. Para ello, fue necesario contar con todas las partes del sistema. La conclusión a la que se llegará dependerá de los resultados obtenidos durante el desarrollo de la prueba. Los elementos y componentes que ayudaron en el desarrollo de la actividad en mención, se explican en los siguientes puntos.

4.1.3.1 Tarjeta del sistema indicador de espacios libres

La implementación de la tarjeta del Sistema indicador de espacios libres permite tener mayor facilidad en la realización de las pruebas y obtener un mejor análisis del diseño de la tarjeta. Para visualizar la tarjeta con la que se realizaron las pruebas “**Véase Anexo 4**”.

La comunicación serial se hará por la bornera ubicada sobre el lado izquierdo de la tarjeta. Por este componente se realizará la conexión entre esta tarjeta y la tarjeta del Secure Socket iWifi. Tener en cuenta que para conectar ambas es necesario colocar el circuito divisor de voltaje, explicado en el punto 4.1.2.1.

4.1.3.2 Aplicación Cliente: Lectores RFID

El software de administración se instaló en una computadora que cumplirá la función de servidor del sistema. Este software procesa la información mandada por los lectores RFID y muestra los resultados en la pantalla de la computadora. Además, automáticamente manda información al sistema indicador de espacios libres para actualizar su información.

Para realizar las pruebas, los equipos deben estar conectados a una misma red para poder comunicarse. Los datos que deben ser recolectados por los lectores RFID en el estacionamiento y enviados al servidor fueron simulados con una aplicación en Visual Basic, llamada aplicación Cliente. La aplicación permite enviar información, como cliente, a un servidor en una red cualquiera. Esta se instaló en dos laptops para que una desarrolle la función del lector de entrada y la otra, del lector de salida. En la figura nº 21 se muestra la aplicación utilizada para simular el funcionamiento de los lectores RFID.



Form1

CLIENTE

Actividad

Enviar

Conexión Servidor 192.168.1.33 Conectar

Puerto 1500 Desconectar

FIGURA 21: Aplicación cliente
Fuente: Elaboración propia

Únicamente se debe presionar el botón “Conectar” para que el servidor acepte a este cliente y puedan intercambiar información. La dirección IP y el puerto de comunicación se colocaron por defecto en la programación de la aplicación.

4.1.3.3 Prueba de comunicación

Teniendo la tarjeta del Sistema indicador de espacios libres conectada a la tarjeta de configuración y comunicación del Secure Socket iWifi, la aplicación Cliente, que simulará los lectores RFID, instalada en cada laptop y con el Software de Administración instalado en el servidor, se realizó la prueba comunicación entre todos los elementos. La figura nº 22 muestra la disposición de los equipos en la prueba realizada.

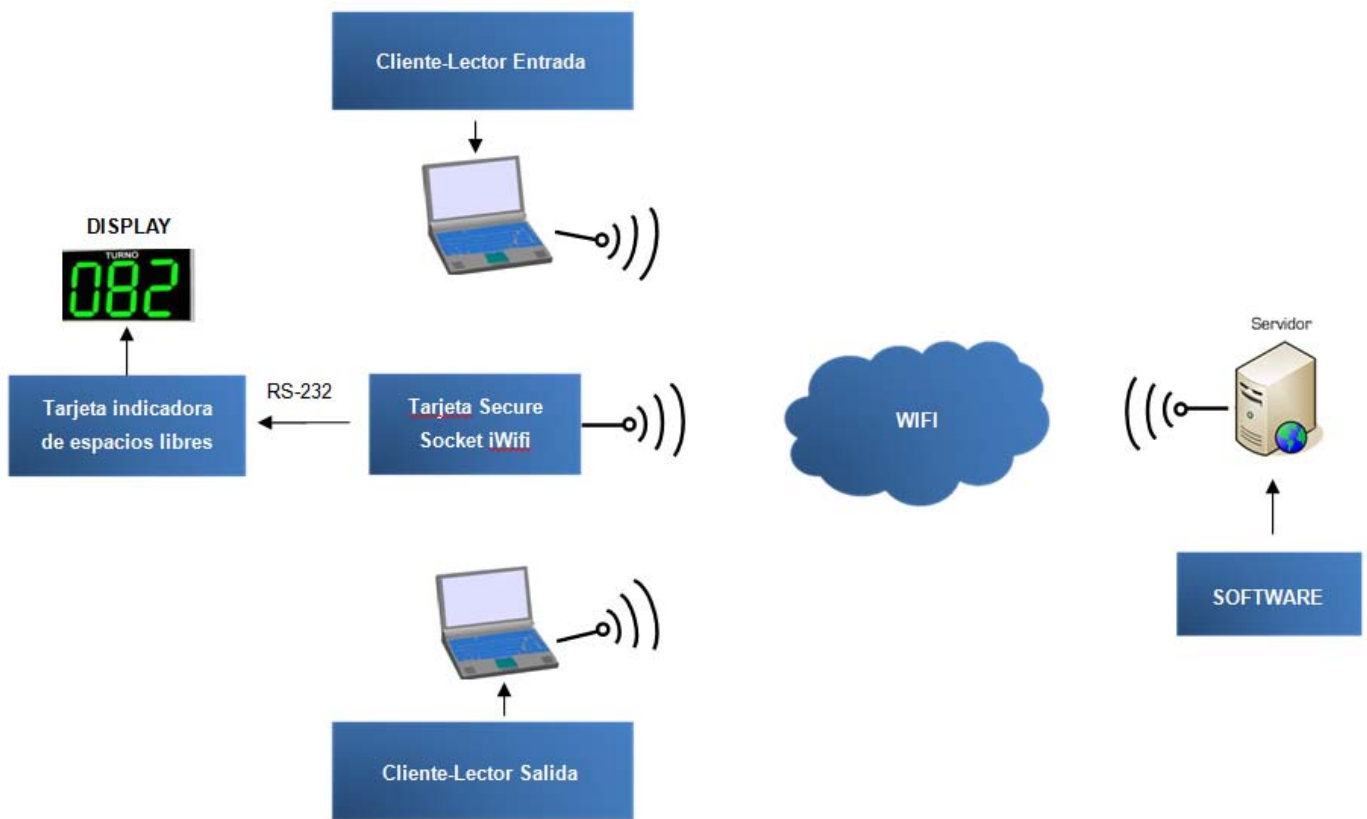


FIGURA 22: Disposición de equipos - Prueba 3
Fuente: Elaboración propia

Primero se habilitaron, en el Software de Administración, las peticiones de conexión para permitir a los clientes comunicarse con el servidor. Esto se realiza al presionar el botón “Escuchar”, que se encuentra en la parte inferior de la pantalla. Automáticamente, luego de presionar este botón, aparece en el cuadro Actividad-Estacionamiento, la frase “Escuchando conexiones”, lo cual verifica que se habilitaron las conexiones para los clientes. Esto se muestra en la primera línea del cuadro Actividad – Estacionamiento de la figura n° 23.

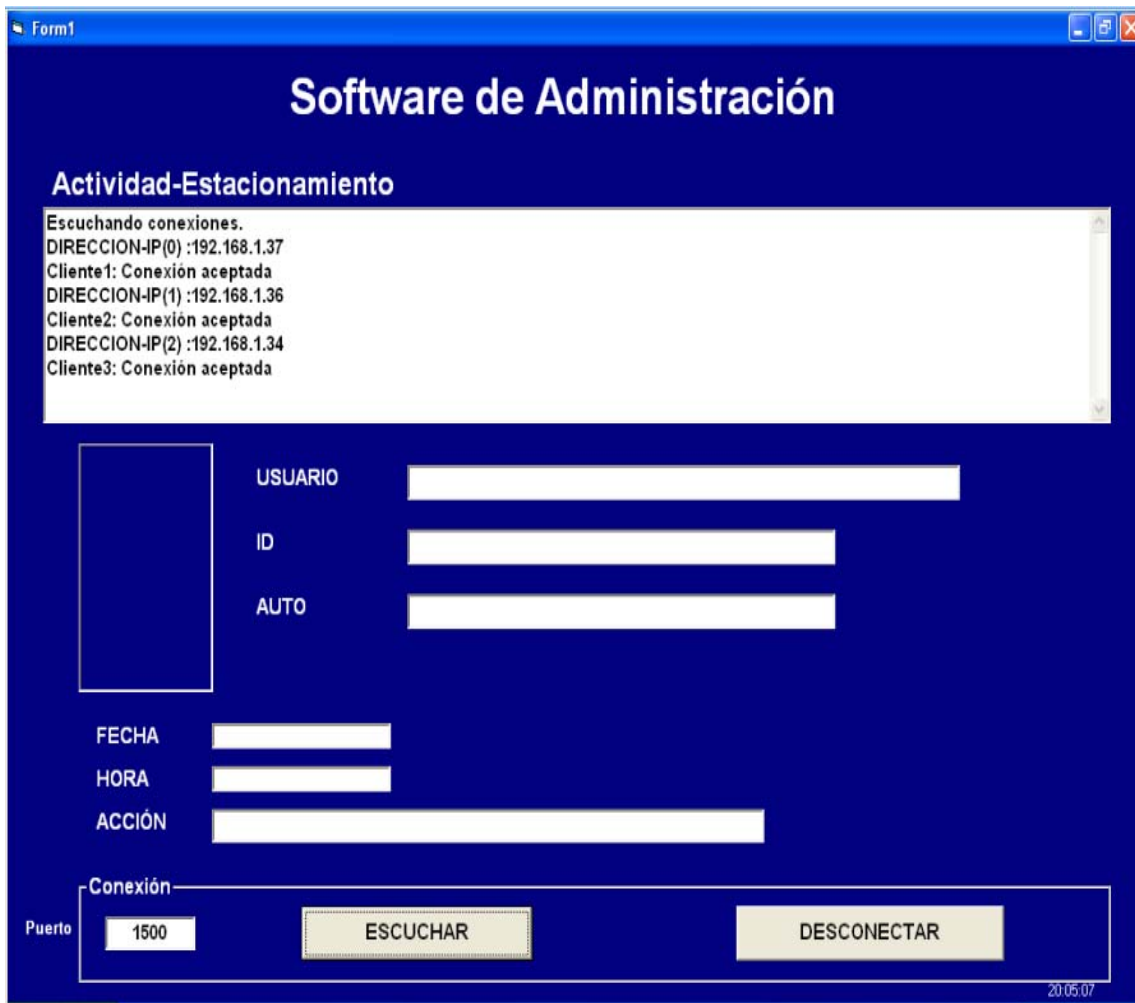


FIGURA 23: Software de Administración - Conexión clientes
Fuente: Elaboración propia

Posteriormente, los clientes deberán conectarse al servidor. Para ello, en las aplicaciones Cliente, que simulan los lectores RFID, deberá presionarse el botón “Conectar” para establecer la comunicación con el servidor. En el caso del Sistema indicador de espacios libres, dentro de su programación está configurado para que desde el inicio envíe un comando para conectarse al servidor.

Como se puede observar en la figura nº 23, en el cuadro Actividad-Estacionamiento, todos los clientes se lograron conectar sin problema al servidor, estableciéndose correctamente la comunicación entre todos. Las direcciones IP 192.168.1.36 y 192.168.1.37 pertenecen a los lectores RFID. El primero corresponde al lector de salida, identificado por el software como CLIENTE 2, y el segundo al lector de entrada,

identificado como CLIENTE1. La otra dirección IP, 192.168.1.34 pertenece al sistema indicador de espacios libres, identificado por el software como CLIENTE3.

Como ya se mencionó anteriormente, esta dirección IP le fue asignada al Secure Socket durante su configuración inicial. Todas las conexiones se realizaron en un tiempo promedio de 1 segundo, sin ninguna dificultad.

Luego de verificar el establecimiento de comunicación entre todos, se debía probar el funcionamiento del Software de Administración y del Sistema indicador de espacios libres a los datos enviados por los lectores RFID. Como condición inicial, se colocó en el display 114 espacios disponibles. A partir de este valor se analizaría la respuesta del Sistema indicador de espacios libres.


Se empezó la prueba enviando datos a través del lector de salida. Para ello, en la aplicación Cliente - Lector Salida, se envió la siguiente trama: 000000. Esta representa el código de un tag RFID captado por el lector al salir un auto del estacionamiento.



FIGURA 24: Aplicación Cliente - Lector de Salida: Envío de datos
Fuente: Elaboración propia

Como se puede observar en la figura n° 24, en el cuadro Actividad, se muestra la trama enviada desde esta aplicación. La respuesta del Software, al dato enviado, es

lo que se muestra en la figura nº 25. En el cuadro Actividad-Estacionamiento del Software se puede verificar, en la última línea, que el dato fue enviado por el lector de salida, CLIENTE2.



The screenshot shows a software window titled 'Form1' with the main heading 'Software de Administración'. Below this is a section titled 'Actividad-Estacionamiento' containing a log of events:

```

Escuchando conexiones.
DIRECCION-IP(0) :192.168.1.37
Cliente1: Conexión aceptada
DIRECCION-IP(1) :192.168.1.36
Cliente2: Conexión aceptada
DIRECCION-IP(2) :192.168.1.34
Cliente3: Conexión aceptada
Cliente 2: ID - Auto : 000000
  
```

Below the log is a user profile section with a photo of a man and the following fields:

- USUARIO: Martin Rios
- ID: 000000
- AUTO: Volkswagen Gol - Placa: ABC-123
- FECHA: 14/11/2009
- HORA: 20:05:35
- ACCIÓN: SALIDA : PUERTA N°2 (text in green)

At the bottom, there is a 'Conexión' section with a 'Puerto' field set to '1500' and two buttons: 'ESCUCHAR' and 'DESCONECTAR'. A timestamp '2006.17' is visible in the bottom right corner.

FIGURA 25: Software de Administración – Respuesta al Lector de salida
Fuente: Elaboración propia

Como se puede observar en la figura nº 25, la respuesta del Software indica que el código mandado corresponde a la foto de la persona que se muestra, con sus respectivos datos. Con letras verdes se indica que esta persona se retiró del estacionamiento por la Puerta 2.

La figura nº 26 muestra la actualización del display del Sistema indicador de espacios libres, luego de recibir datos del Software de Administración,

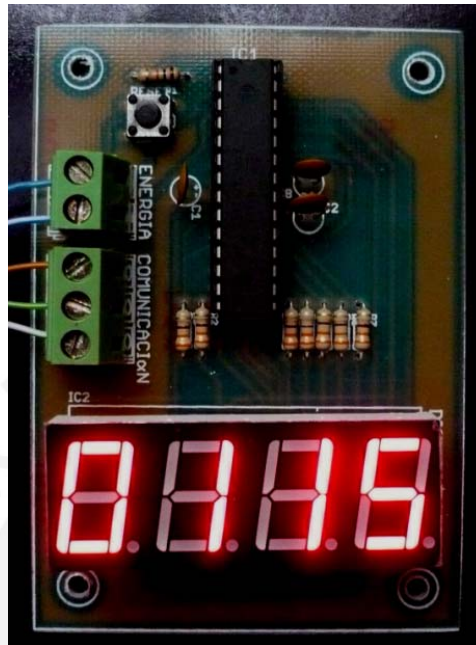


FIGURA 26: Tarjeta Sistema indicador de espacios libres: Actualización display
Fuente: Elaboración propia

La actualización mostrada en el display, hecha por el Sistema indicador de espacios libres, es correcta ya que al retirarse un vehículo del estacionamiento, debe aumentar en uno los espacios disponibles.

Desde el envío de datos desde la aplicación Cliente – Lector Salida, hasta obtener la respuesta del Software de Administración y la actualización del valor del display, transcurrió aproximadamente 0.5 segundos. Con esto se puede concluir que la respuesta de ambos, a los datos enviados por el lector de salida, fue instantánea.

Para continuar con la prueba, se envió de la aplicación Cliente - Lector Entrada la trama: 000100. La trama enviada representa el código captado por el lector de entrada cuando un vehículo ingresa al estacionamiento. La figura nº 27 ilustra este proceso.



FIGURA 27: Aplicación Cliente – Lector Entrada: Envío de datos
Fuente: Elaboración propia

Como se puede observar en la figura nº 27, en el cuadro Actividad se muestra el dato enviado desde esta aplicación.

La respuesta del Software a este código se puede observar en la figura nº 28. En el cuadro Actividad-Estacionamiento se puede verificar, en la primera línea, que el dato fue enviado por el lector de entrada, CLIENTE1.



Form1

Software de Administración

Actividad-Estacionamiento

Cliente 1: ID - Auto : 000100
 INGRESO: PUERTA N°1
 DISPLAY: Entrada Auto > 0
 USUARIO: Angelo Velarde
 ID: 000100
 AUTO: Volkswagen Escarabajo - Placa : NOP-586
 20:06:49
 14/11/2009

	USUARIO	Angelo Velarde
	ID	000100
	AUTO	Volkswagen Escarabajo - Placa : NOP-586

FECHA: 14/11/2009
 HORA: 20:06:49
 ACCIÓN: **INGRESO : PUERTA N°1**

Conexión
 Puerto: 1500

2007.09

FIGURA 28: Software de Administración – Respuesta al Lector de entrada
 Fuente: Elaboración propia

La figura nº 28 muestra que la respuesta del Software al código enviado por el lector de entrada identifica a la persona que se muestra en la foto, con sus datos correspondientes. En letras verdes se indica que el vehículo ha ingresado al estacionamiento por la Puerta 1.

La respuesta del sistema indicador de espacios libres luego de recibir los datos del Software, se observa en la figura nº 29.

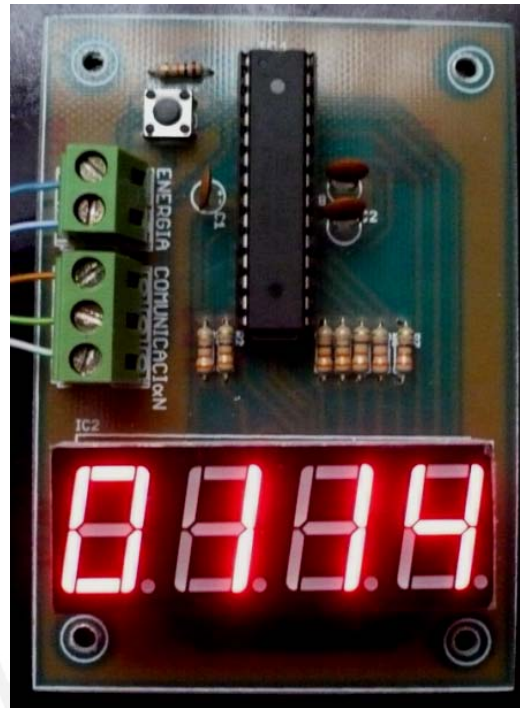


FIGURA 29: Tarjeta Sistema indicador de espacios libres: Actualización display
Fuente: Elaboración propia

La actualización, hecha por el sistema indicador de espacios libres, en el display es correcta ya que al entrar un vehículo al estacionamiento, se debe disminuir en uno la cantidad de espacios disponibles. Al igual que la trama anteriormente enviada, todas las respuestas de los equipos tuvieron un tiempo promedio de 0,5 segundos.

Para terminar la prueba, se envió un código que no pertenece a la base de datos que maneja el Software de Administración desde la aplicación Cliente – Lector Entrada. El código enviado fue: 010101. La figura nº 30 ilustra este proceso.



Form1

CLIENTE

Actividad

Conexion establecida.
Cliente >000100
Cliente >010101

Enviar

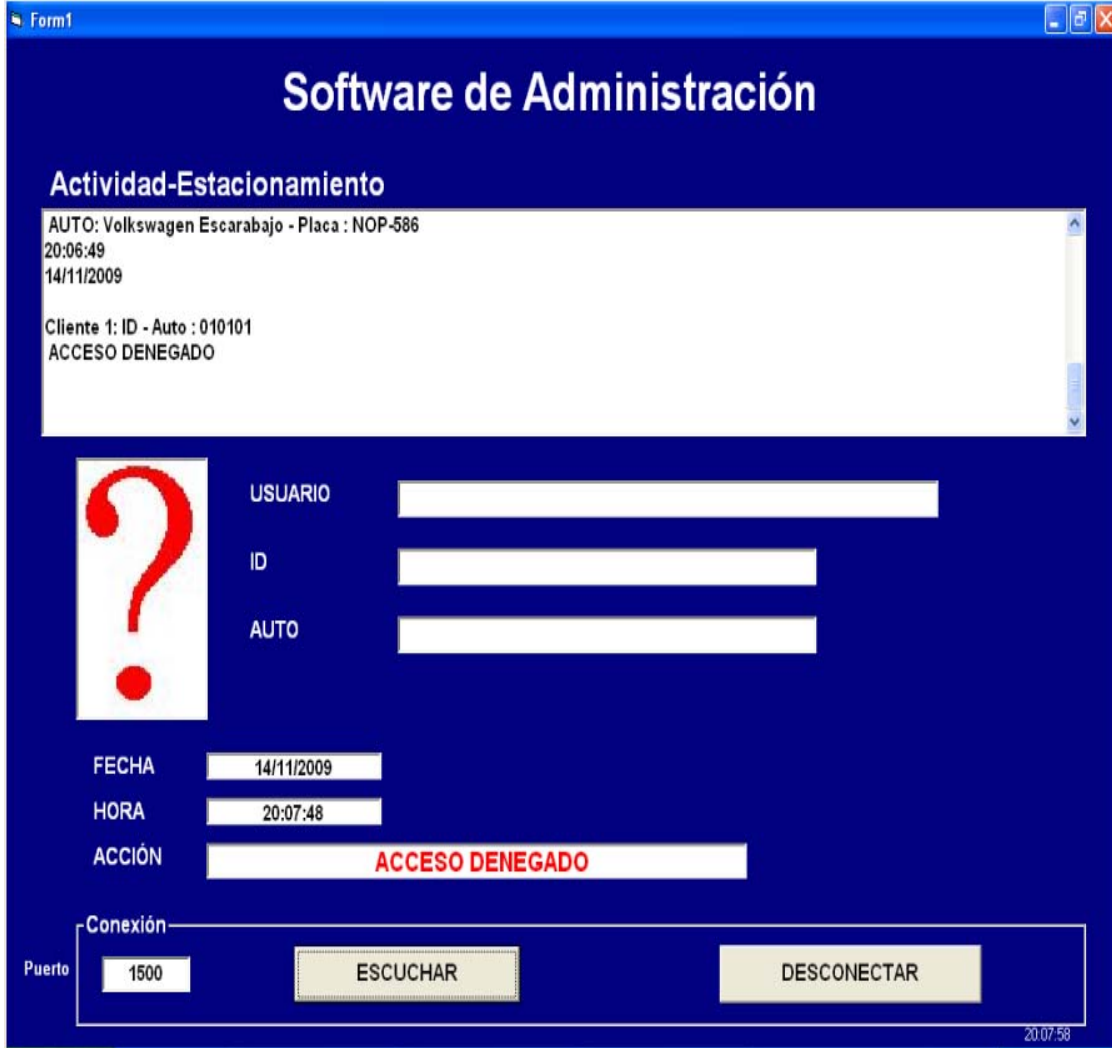
Conexión Servidor Conectar

Puerto Desconectar

FIGURA 30: Aplicación Cliente - Lector Entrada: Envío Código no autorizado
Fuente. Elaboración propia

En el cuadro Actividad, en la tercera línea, se puede apreciar que el código enviado desde esta aplicación fue 010101.

La respuesta del Software es la que se muestra en la figura nº 31. Al no tener almacenado en su base de datos el código enviado, no se le autoriza al vehículo a ingresar al estacionamiento. En letras rojas se indica que se le ha denegado el acceso a este auto.



The screenshot shows a software interface titled "Software de Administración". It features a section for "Actividad-Estacionamiento" with a log of activity. Below this is a login form with fields for "USUARIO", "ID", and "AUTO". A large red question mark icon is positioned to the left of these fields. At the bottom, there is a "Conexión" section with a "Puerto" field set to "1500" and buttons for "ESCUCHAR" and "DESCONECTAR".

Software de Administración

Actividad-Estacionamiento

AUTO: Volkswagen Escarabajo - Placa : NOP-586
20:06:49
14/11/2009

Cliente 1: ID - Auto : 010101
ACCESO DENEGADO

USUARIO:

ID:

AUTO:

FECHA: 14/11/2009

HORA: 20:07:48

ACCIÓN: **ACCESO DENEGADO**

Conexión

Puerto: 1500

ESCUCHAR

DESCONECTAR

20.07.58

FIGURA 31: Software de Administración – Respuesta al código no autorizado
Fuente: Elaboración propia

En el cuadro Actividad-Estacionamiento se puede apreciar que el código 010101 fue enviado por el lector de entrada, CLIENTE1. Al igual que en los procesos anteriores, la respuesta del Software fue inmediata, aproximadamente 0.5 segundos en mostrar en pantalla el resultado al código enviado.

De la prueba realizada:

Lector	Dato enviado	Dato recibido Software	Tiempo respuesta Software (s)	Tipo respuesta Software	Tiempo respuesta Display (s)	Tipo respuesta Display	Error
Salida	000000	000000	0.5	Correcta	0.5	Correcta	Ninguno
Entrada	000100	000100	0.5	Correcta	0.5	Correcta	Ninguno
Entrada	010101	010101	0.5	Correcta	0.5	Correcta	Ninguno

TABLA 4: Datos de la prueba
Fuente: Elaboración propia

Los resultados de la prueba indican que la comunicación entre todos los equipos a través de la red wifi fue correctamente realizada ya que no se tuvo ningún error al recibir los datos enviados y tampoco se presentó ninguna falla ni error al observar las respuestas del Software de Administración y del Sistema indicador de espacios libres.

Por lo tanto, todos los equipos funcionaron de acuerdo a lo establecido según sus propias configuraciones, con lo cual se puede concluir que el Sistema de control vehicular, según la solución diseñada, funciona eficazmente.

4.2 Presupuesto

El presupuesto que se presenta en la tabla nº 5 toma en cuenta todos los gastos en la adquisición de componentes y equipos, la realización de las tarjetas y el diseño de la solución.

Item	Descripción	Cant.	Precio Unitario (S/.)	Precio Total (S/.)
01	Kit RFID	01	8,500.00	8,500.00
02	Secure Socket iWifi	01	120.00	120.00
03	FTDI 232R: Conversor Serial-USB	01	27.00	27.00
04	Socket 2mm separación	02	5.50	10.00
05	Microcontrolador ATmega8	01	12.00	12.00
06	Socket 28 pines (ATmega8)	01	0.50	0.50
07	Tarjeta wifi-configuración y comunicación	01	30.00	30.00
08	Tarjeta indicadora espacios libres (cátodo común)	01	24.00	24.00
09	Display 7 segmentos 4 dígitos	01	4.00	4.00

10	Socket Display	01	0.50	0.50
11	Conector USB tipo b	01	1.00	1.00
12	Conector Jack DC	01	0.50	0.50
13	Regulador LM117	01	4.50	4.50
14	Borneras(2 y 3)	04	1.00	4.00
15	Jumpers	04	0.50	2.00
16	Condensador 100nF, 10nF, 10uF, 4.7uF	09	0.20	1.80
17	Resistencia 330, 10k ohmios ¼ vatio	09	0.10	0.90
18	Pulsador	01	0.50	0.50
19	Led 3mm	01	0.30	0.30
20	Mano de obra	01	2,000.00	2,000.00
			TOTAL (S/.)	10,743.50

TABLA 5: Presupuesto
 Fuente: Elaboración propia



CONCLUSIONES

1. El diseño propuesto logra automatizar el acceso, al identificar a los usuarios a través de los tags; puede obtener la ubicación de un vehículo, a través de los datos de un determinado lector; muestra la cantidad de espacios disponibles en un momento dado, y, a través del Software de Administración, se pueden supervisar las actividades del estacionamiento.
2. El dispositivo RFID permite la identificación del auto sin causar molestias al usuario, confirmando su adecuada elección sobre otras tecnologías.
3. La comunicación inalámbrica, basada en el componente Secure Socket iWifi, logró transferir cada bit de información de un extremo al otro sin distorsión alguna. Tanto en la prueba 2 como en la prueba 3 se pudo comprobar la comunicación dentro de la red inalámbrica.
4. El Software de Administración desarrollado puede conectar múltiples clientes sin perder o alterar la información que debe mandar o recibir de cada uno, es decir, puede atender a varios lectores o displays y lograr una comunicación exitosa entre cada uno de ellos . Se puede tomar como referencia la prueba realizada en la que se conectó a tres clientes y no se tuvo ningún inconveniente para relacionar los datos recibidos con el equipo correspondiente.

RECOMENDACIONES

1. Al utilizar la tarjeta de configuración y comunicación, se deben tomar en cuenta los voltajes que llegan a la tarjeta ya que es necesario utilizar un circuito divisor de voltaje, tal como lo muestra la figura nº 15.
2. Para que el presente diseño se pueda implementar a escala real, se debe considerar cambiar el display del sistema indicador de espacios libres por uno más grande dependiendo de la posición final del dispositivo.
3. Al trabajar sobre una red Lan exclusiva para los equipos del sistema de control vehicular, se garantiza una mejor velocidad de transmisión de los datos, ya que si el sistema se monta sobre una red existente, puede causar demoras en la comunicación de los dispositivos.
4. El Kit RFID debe ser probado en condiciones normales de trabajo, es decir en un estacionamiento con los Tags pegados en los parabrisas de diferentes autos, para evaluar la correcta comunicación con el servidor.

BIBLIOGRAFÍA

[1] I. Crisólogo. (2009). Diseño de un sistema electrónico para el aviso automático de disponibilidad en estacionamientos vehiculares. Tesis en Ingeniería Electrónica. Pontificia Universidad Católica del Perú. Consulta: 20 de Agosto de 2009.

<http://www.tesispuccp.com.pe>

[2] Intellisoft SA. (2007). Aeropuerto Internacional Jorge Chávez. Consulta: 17 de Setiembre de 2009.

http://intellisoftparking.com/cms/index.php?option=com_content&task=blogsection&id=6&Itemid=45

[3] SYSCOM. (2008). Introducción a los sistemas de control de acceso. Consulta: 17 de Septiembre de 2009.

<http://dvr.syscom.com.mx/documentos/syscom/presentaciones/presentacion-control-acceso.ppt>

[4] C. Galvis. (2007). Introducción a la tarjeta con banda magnética. Consulta: 25 de Octubre de 2009.

<http://www.monografias.com/trabajos43/banda-magnetica/banda-magnetica.shtml>

[5] P. Sweeney. (2005). RFID for dummies. (Primera Edición). Estados Unidos: For Dummies. Consulta: 20 de Agosto de 2009.

http://www.12manage.com/methods_rfid_technology.html

[6] Federal APD. (2009). Tag Master Long Range RFID. Consulta: 28 de Septiembre de 2009.

http://www.federalapd.com/PRODUCTS/Access/tagmaster_prods.pdf

[7] Sic Transcore. (2003). Sistema de Gestión y Administración para Peaje-Telepeaje. Consulta: 20 de Septiembre de 2009.

<http://www.sictranscore.com.ar/Peaje.html>

- [8] S. Robbins y M. Coulter. (1996). Administración. (Quinta Edición). México.
Consulta: 24 de Octubre de 2009.
<http://books.google.com.pe/books?id=YP1-InmORdgC&pg=PP1&dq=ROBBINS,+Stephen+y+COULTER,+Mary.+Administraci%C3%B3n.#v=onepage&q=&f=false>
- [9] Diccionario de la Real Academia Española. (2001). Estacionamiento. Consulta: 10 de Septiembre de 2009.
http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=estacionamiento
- [10] B. Sabater. (2009). Marketing RFID. Tesis de maestría en Ingeniería de las Telecomunicaciones. Universidad Politécnica de Cataluña. Consulta: 26 de Agosto de 2009.
<http://upcommons.upc.edu/pfc/bitstream/2099.1/7340/1/M%C3%A1rketing%20RFID.pdf>
- [11] J. Alvarado. (2008). Sistema de control de acceso con RFID. Tesis de maestría en Ciencias. Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional. México.
- [12] D. Contreras. y Lacasa. (2007). Definición RFID. Consulta: 17 Septiembre de 2009.
<http://www.gii.upv.es/.../RFID%20Por%20Diego%20Contreas%20Jimenez%20y%20Anton>
- [13] Information Highway Group. (2004). Tecnología RFID. Consulta: 25 de Octubre de 2009.
<http://www.ihg.net/java/X?cqi=lateral.rfid.Introduccion.pattern>
- [14] SKYETECK. (2006). SkyeModule M10. Consulta: 20 de Agosto de 2009.
<http://www.skyetek.com/Portals/0/Documents/Products/M-10%20Datasheet.pdf>
- [15] Bond led. (2008). “0.56” Four Digit 7–Segment display. Consulta: 18 de Octubre de 2009.
<http://www.bond-led.com/specification/led-numericdisplay/0.56%20four%20digit%20numeric.pdf>

[16] Connect One. (2009). Ichip Config User Manual. Consulta: 23 de Octubre de 2009.

http://www.connectone.com/media/upload/iChip_Config_UTILITY_Manual.pdf

