Pontificia Universidad Católica del Perú

Facultad de Ciencias e Ingeniería

DISEÑO DE UN SISTEMA DE ACCESO VEHICULAR A LA PUCP BASADO EN TECNOLOGÍA RFID Y DETECCIÓN DE PLACAS VEHICULARES

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

Luis Enrique Gomero Vásquez

ASESOR: Willy Eduardo Carrera Soria

Lima, junio del 2017

Le doy gracias a Dios, mi familia y mi enamorada por haberme apoyado durante el desarrollo de mi tesis. Igualmente, agradezco mucho al profesor Willy Carrera por la ayuda y asesoría brindada durante todo este proceso.

Resumen

El desarrollo de esta tesis se centra en el rubro de los estacionamientos, particularmente al interior de la PUCP y, por ello el control de los ingresos vehiculares permitirá conocer el correcto uso de los estacionamientos y también asegurar que solo usuarios válidos puedan ingresar a la PUCP.

Por ello, en este presente trabajo de tesis se plantea un sistema de acceso vehicular a la PUCP usando principalmente dos tecnologías. En ese sentido, la inclusión de nuevos avances tecnológicos permite la posibilidad de desarrollar sistemas que cumplan con un control eficiente, cumplan los estándares de seguridad establecidos y brinden un buen servicio al usuario. Entre las tecnologías empleadas para el sistema, se propuso las tarjetas RFID, que es una tecnología de identificación personal automática que incluye información auténtica del usuario y presenta lectores que permiten leer estas etiquetas a distancias. Así mismo, el uso de programas de Procesamiento Digital de Señales (DSP) como el openALPR permitirá obtener los caracteres de las placas vehiculares de los vehículos ingresantes a la universidad mediante algoritmos de procesamiento de las imágenes capturadas.

Todas estas tecnologías fueron unificadas en una plataforma basada en lenguaje de programación Java mediante librerías de conexión y una interfaz final para la gestión de accesos, que sería utilizada por el personal de seguridad encargados del acceso vehicular.

Mediante el diseño sistemático de los sistemas y realizando pruebas físicas, se obtuvieron resultados con errores por debajo del 7% en detección de placas vehiculares, que afirman que se puede identificar correctamente a los usuarios que ingresen a la universidad con sus respectivas tarjetas RFID y placas vehiculares e ingresarlos correctamente al sistema de base de datos para su acceso a las instalaciones de la PUCP. Por ese motivo, el sistema planteado permitirá generar un mejor control de los accesos vehiculares a la universidad.

FACULTAD DE
CIENCIAS E INGENIERÍA

PONTIFICIA **UNIVERSIDAD CATÓLICA** DEL PERÚ

TEMA DE TESIS PARA OPTAR EL TÍTULO DE INGENIERO ELECTRÓNICO

Título	:	Diseño de un sistema de acceso vehicular a la PUCP basado en tecnología RFID y detección de placas vehiculares
Área	:	Circuitos y Sistemas #1324
Asesor	:	Willy Carrera Soria
Alumno	:	Luis Enrique Gomero Vásquez
Código	:	20111859
Fecha	:	22/06/16

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
FACULTAD DE CIENCIAS E INGENIERÍA
DECANO

Descripción y Objetivos

En los últimos años, se ha percibido el crecimiento exponencial de la inseguridad ciudadana en el Perú, haciendose visible en hechos delictivos como crímenes, asesinatos y robos que son cuestiones que se presentan a diario. La PUCP tampoco es ajena ante este contexto, existiendo la posibilidad de que se puedan perpetuar estos tipos de delitos dentro de sus intalaciones dado que los accesos vehiculares son registrados de manera manual y puede dar pie al error. En ese sentido, el sistema propuesto en esta tesis busca reducir la probabilidad de estos eventos y propone como solución un mecanismo para controlar los accesos vehiculares a la universidad empleando diversas tecnologías disponibles actualmente que permitan identificar a los usuarios ingresantes al campus así como reconocer el vehículo del usuario para optimizar la seguridad dentro de la universidad.

El objetivo principal de esta tesis es diseñar un sistema de acceso vehicular a la PUCP basado en tecnología RFID y detección de placas vehiculares para controlar el acceso de los alumnos, profesores, personal administrativos e invitados que intenten ingresar a la universidad y de esa manera salvaguardar la tranquilidad de la comunidad universitaria ante alguna intención que vulnere su seguridad. Dentro de los objetivos específicos se condisera en primer lugar diseñar el hardware del sistema de acceso vehicular; luego, diseñar y programar el software del sistema de control e interfaz de usuario y finalmente, realizar simulaciones del sistema de acceso vehicular

MÁXIMO 50 PÁGINAS

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
SECCIÓN ELECTRICIDAD Y ELECTRÓNICA
Ing. WILLY CARRERA SORIA
PROFESOR ASOCIADO

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
FACULTAD DE CIENCIAS E INGENIERÍA
M. Sc. Ing. MIGUEL ANGEL CATAÑO SANCHEZ
Coordinador de la Especialidad de Ingeniería Electrónica

FACULTAD DE
CIENCIAS E INGENIERÍA

PONTIFICIA **UNIVERSIDAD CATÓLICA** DEL PERÚ

TEMA DE TESIS PARA OPTAR EL TÍTULO DE INGENIERO ELECTRÓNICO

Título : Diseño de un sistema de acceso vehicular a la PUCP basado en tecnología RFID y detección de placas vehiculares

Índice

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
SECCIÓN ELECTRICIDAD Y ELECTRÓNICA

Ing. WILLY CARRERA SORIA
PROFESOR ASOCIADO

MÁXIMO 50 **PÁGINAS**

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
FACULTAD DE CIENCIAS E INGENIERÍA

M. Sc. Ing. MIGUEL ANGEL CATAÑO SÁNCHEZ
Coordinador de la Especialidad de Ingeniería Electrónica

Índice General

Capítulo 4: Ensayos y resultados

Introducción

Los innovadores avances tecnológicos en el desarrollo de nuevos sistemas para automatizar procesos cotidianos e industriales han ido generando mayor interés en los usuarios debido a la disponibilidad inmediata de información que pueden generar y la posibilidad de controlar procesos automáticamente de manera remota.

Actualmente el desarrollo de nuevos dispositivos de identificación y sensores permiten que estos sistemas sean mucho más robustos y tengas cada vez más aplicaciones diversas en distintos campos donde exista alguna problemática a automatizar. Con esta tendencia, la mayoría de empresas grandes y pequeñas buscan llevar su servicio a otro nivel y poder digitalizar la mayor parte de sus procesos, tanto para aumentar su productividad y generar mayores ganancias, así como brindar mayor conexión hacia sus clientes.

El presente trabajo de tesis busca diseñar un sistema de acceso vehicular para la PUCP usando tecnologías que están logrando actualmente cambios significativos en este tipo de sistemas. La necesidad de poder monitorear los accesos vehiculares a la universidad permite que los estacionamientos sean usados debidamente y por usuarios que pertenezcan a la universidad. Con este trabajo, se pretende iniciar una propuesta de cambio para este rubro importante que maneja la PUCP.

Capítulo 1

Análisis de sistemas de acceso vehicular en la actualidad

1.1 Presentación

En la actualidad, menos del 15% de estacionamientos dentro de la ciudad de Lima cuentan con un sistema de control automático que brinden óptimas condiciones de seguridad a los usuarios de estos establecimientos [1]. El proceso común en la mayoría de estacionamientos consta en la emisión de un ticket, impreso o no, con la hora y placa del vehículo ingresante, en el mejor de los casos, que se le entrega a cada usuario a su ingreso. Este comprobante puede ser fácilmente duplicado o hurtado por algún tercero con la finalidad de robar vehículos y sin que los sistemas de seguridad establecidos los detecte. Así mismo, son pocos los establecimientos que cuentan con algún sistema que genere reportes y/o monitoree a tiempo continuo los accesos vehiculares de estos espacios.

Según el Informe Anual de Seguridad Ciudadana publicado en el 2015 por el Instituto de Defensa Legal, en el cual se realiza un balance del gobierno del ex Presidente Ollanta Humala, se realizaron encuestas (ver Tabla 1.1) sobre cómo perciben los peruanos la inseguridad en la calle y el siguiente cuadro demuestra que existe alrededor de un 45% de la población que incluye al robo de vehículos como una amenaza frecuente en nuestra ciudad.

Tabla 1.1 Población urbana, de 15 a más años de edad, con percepción de inseguridad en un año, por tipo de delito [2].

Tipo de hecho delictivo	Enero-junio 2013	Enero-junio 2014	Enero-junio 2015
Robo de dinero, cartera, celular	78,9	77,6	77,5
Robo de vivienda	70,3	70,1	74,9
Robo de vehículo	46,4	44,3	39,1
Amenazas e intimidaciones	38,1	38,0	38,8
Extorsión	No especifica	7,9	20,3
Maltrato y ofensa sexual	14,5	13,6	13,1
Secuestro	13,2	12,8	14,1

Si bien la tasa de robo de vehículos ha ido disminuyendo durante los años, no es totalmente baja como para afirmar que esta amenaza ya no es frecuente en las calles de la capital, más bien es necesaria una cooperación bien estructurada de la policía y las municipalidades encargadas de velar también por la seguridad. En ese sentido, la presente tesis busca desarrollar un sistema capaz de poder solucionar esta constante necesidad específicamente dentro del estacionamiento del campus de la PUCP. Con más de 10 playas de estacionamiento vehicular dentro del campus [3], es muy posible que el personal de seguridad permita el acceso a terceros con vehículos que tengan una intención maliciosa y esto se pueda dar aún más en horas punta cuando el flujo y congestión vehicular aumentan en las entradas de la universidad, haciendo que sea ineficiente el control de seguridad en el campus. Por otro lado, no se realiza un monitoreo efectivo de los accesos, ya que no se tiene un control de qué usuarios o vehículos ingresan a la PUCP en determinada hora del día y ello también provoca que el uso del estacionamiento este siendo mal gestionado y no se le otorgue el servicio de parqueo vehicular a quienes realmente lo necesitan.

El propósito de este capítulo es dar a conocer la situación de los sistemas actuales de acceso vehicular y analizarlos desde un punto de vista general y organizacional hasta el punto específico que se centra en la PUCP y examinar la realidad en este centro de estudios. En ese sentido, se darán a conocer las fallas o limitantes del sistema de la universidad y la posterior declaración de la problemática que lo engloba.

1.2 Entorno General

En un ámbito general, existen diversas empresas dedicadas al rubro de la control y acceso vehicular en estacionamientos y a su vez son muy competitivas en el mercado mundial. A continuación, se describirá brevemente la situación actual de este rubro y qué normativas rigen a las empresas que se dedican a brindar este tipo de seguridad vehicular.

1.2.1 Tendencia Mundial

En la actualidad, en países en los cuales se ha dado mayor énfasis al desarrollo tecnológico en necesidad de índole urbano, se puede apreciar que el

correcto uso y administración de tecnologías en sistemas de acceso vehicular ha permitido que todos los procesos tiendan a la automatización con un mínimo porcentaje de intervención humana en los procesos.

El avance tecnológico permite que estos espacios se vuelvan menos vulnerables ante hecho delictivos y con una correcta administración y ejecución de las tecnologías del sistema hacen que el control vehicular sea viable en estos tipos de establecimientos.

1.2.2 Normas y protocolos de seguridad

Según la Ley N°29461 promulgada en el año 2009 por el Congreso de la República, los estacionamientos deben regularizarse y cumplir una serie de estándares que van desde obligaciones del titular del establecimiento hasta obligaciones del usuario del estacionamiento. Dentro de las obligaciones del titular el reglamento señala lo siguiente en el Artículo N°4: “Entregar una constancia de ingreso del vehículo y brindar el servicio de vigilancia y seguridad respecto del vehículo y sus partes accesorias durante el tiempo de ocupación del estacionamiento, conforme a los alcances de lo previsto en la ley” [4]. Así mismo, esta constancia debe de incluir, además de los datos de la empresa concesionaria del establecimiento, información básica del ingreso como la fecha, hora, placa del vehículo y, en ciertos casos, información del usuario ingresante. Al momento de la salida del usuario del estacionamiento, se debe validar la constancia generada al ingreso para poder retirarse de manera correcta del establecimiento donde estaciono su vehículo.

1.3 Entorno Específico

Dentro del análisis de los sistemas de acceso vehicular, es de gran índole reconocer cuál es la demanda del usuario final y cuáles son las oportunidades de mejora para estos sistemas. Para ello, se explicará en qué medida se han utilizado las tecnologías disponibles en este rubro en cuanto a seguridad y acceso vehicular en la PUCP y qué fabricantes permiten suplir estas necesidades a las empresas que desean mejorar o implementar un sistema de seguridad para sus establecimientos.

1.3.1 Situación actual del acceso vehicular a la PUCP

Dentro de la universidad, el sistema de acceso vehicular se encuentra vulnerable ante distintos factores que afectan el desempeño humano del personal de seguridad. La PUCP cuenta con dos ingresos vehiculares; uno ubicado en la parte delantera y otro en la parte posterior que se pueden ver representados en la Figura 1.1.

Figura 1.1 Ubicación de Puertas de Acceso Vehicular a la PUCP. Fuente: www.puntoedu.pucp.edu.pe

El control como se ve en la Figura 1.2 y Figura1.3 es realizado de forma manual y no cuenta con un sistema de control que registre debidamente los ingresos tanto de usuarios como de vehículos a la universidad. Solo es posible verificar manualmente en la base de datos de alumnos y/o docentes si el usuario pertenece a la PUCP. Es por ello que el estudio realizado es necesario para poder monitorear los ingresos de manera automática con el fin de conocer qué usuarios realmente están haciendo uso correcto de los estacionamientos de la PUCP y generar un reporte de flujo de usuarios que acceden al campus, así como fortalecer la seguridad del ingreso por las diversas puertas de la universidad.

Figura 1.2 Entrada principal PUCP

Fuente: Propia

Figura 1.3 Entrada principal PUCP

Fuente: Propia

1.3.2 Fabricantes

Actualmente, existen diversas empresas dedicas a este rubro creando y acoplando nuevas tecnologías para diseñar sistemas de seguridad cada vez más robustos. En Perú, las empresas de seguridad toman tecnologías de procedencia internacional y las acomodan a las necesidades y alcances de cada proyecto que se realice. Entre los fabricantes más destacados se encuentran SkiData, cuyos productos son administrados por la empresa IntellisoftParking en el Perú. Así mismo, la empresa Accist y ZKteco cuentan con desarrollo de accesos vehiculares en el Perú y con distintos tipos de soluciones desde controles de acceso electromecánicos hasta sensores biométricos. Dentro de la línea de soluciones de productos que son utilizados se encuentran Barreras de ingresos, sistemas de

reconocimiento de matrículas vehiculares, sistemas de abonados, sistemas de auditoría de perfiles, entre otros [5]. Por otro lado, existen otras empresas que también se ubican dentro del mercado competitivo con una gran autonomía y reconocimiento como lo es la empresa Los Portales, que administra estacionamientos de diversos centros comerciales de la ciudad con tecnologías como Portales Pass y otras que le dan mayor comodidad al usuario [6], pero que no son aplicadas en todos sus estacionamientos razón por la cual su sistema también tiene el riesgo de poder ser infiltrado para hechos delictivos.

1.4 Procesos internos del sistema actual de acceso vehicular a la PUCP

El sistema de acceso vehicular a la PUCP se ha venido realizando durante estos años de manera manual y hasta el momento no se han realizado cambios significativos en el tema de usar nuevas tecnologías para proteger la seguridad del campus. Por ejemplo, aun se cuentan con cámaras analógicas en los accesos vehiculares y tan solo una computadora para las dos entradas en la puerta principal y que en horas punta no satisface la demanda del usuario para poder ingresar rápida y seguramente a los estacionamientos de la universidad.

Los procesos internos del actual sistema se pueden explicar mejor con el siguiente diagrama de bloques en la Figura 1.4 y brindará una mejor visión del entorno por el cual los usuarios acceden actualmente a los estacionamientos del complejo universitario.

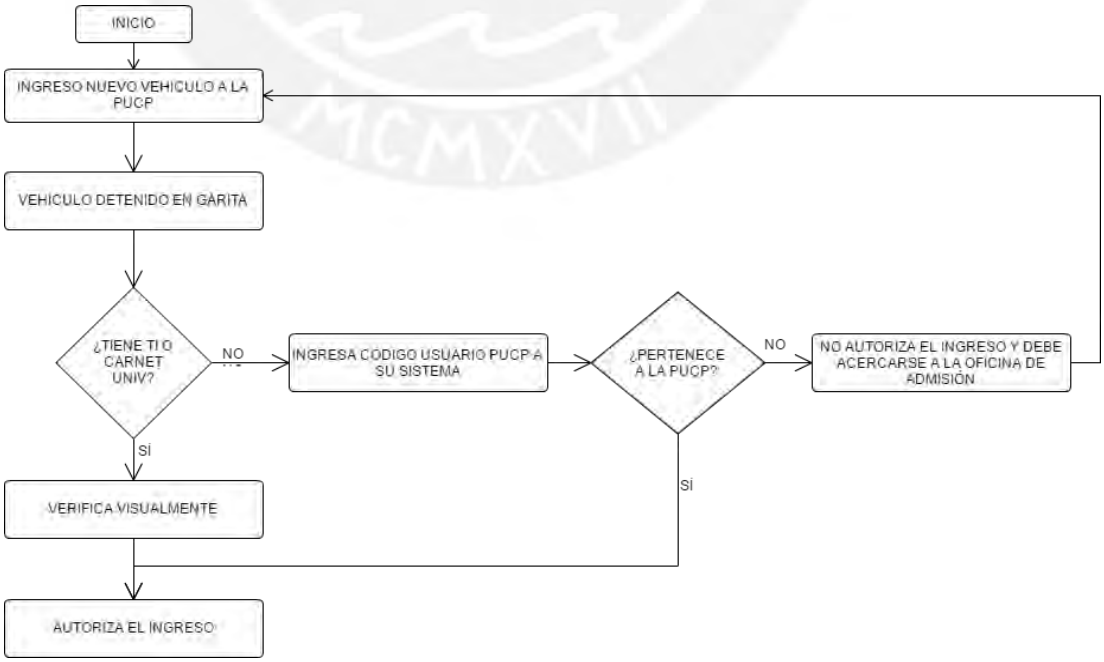

Figura 1.4 Diagrama de procesos internos en el Acceso Vehicular PUCP

Fuente: Propia

1.5 Declaración de problemática

Según el diagrama de procesos internos que se maneja actualmente en la PUCP, se puede observar que este carece un sistema óptimo de monitoreo y registro de los accesos vehiculares y de usuarios por día. Por otro lado, al no contar con un sistema de registro existe la posibilidad de que el ingreso sea vulnerable por terceros. En primer lugar, la verificación que realiza el personal de seguridad al usuario que desea ingresar se realiza visualmente, con una duración de 5 segundos, y solo se debe mostrar el documento sin dárselo a la persona de seguridad. En este bloque del sistema, tampoco se verifican los documentos de las personas que puedan acompañar al posible usuario y, por distintos factores como cansancio, fatiga, brillo solar pueden hacer que se autorice el pase a un usuario con un TI o documento falso y más aún dejar ingresar a sus acompañantes sin saber su identidad, ya que a veces se asumen que también son estudiantes y por evitar una cola de vehículos en la entrada se les permite ingresar. Por otro lado, el único bloque digital que posee este sistema es la verificación manual por computadora del código del usuario asociada a la base de datos de la universidad. Si bien es correcto realizar una verificación con una base de datos, está debe realizarse rápida y automáticamente y debe ser aplicada a todo posible usuario que desee acceder a los estacionamientos de la PUCP que tenga o no un documento de identificación. Por ese motivo, el desarrollo de esta investigación busca encontrar una solución integral que proponga un sistema viable de acceso vehicular a la universidad, con ayuda de múltiples tecnologías que se encuentran en nuestro entorno y permita monitorear los accesos que se dan diariamente a la universidad.

Capítulo 2

Fundamentos teóricos y tecnologías aplicadas en sistemas de acceso vehicular

2.1 Estado del arte

El avance tecnológico ha permitido que diversos mecanismos y herramientas sean optimizadas para tener una mejor eficiencia y cumplan más propósitos de los que cumplían antes con el fin de solucionar problemas cotidianos en la sociedad de la forma más sencilla posible y cree un lazo entre los usuarios y la nueva tecnología insertada.

La necesidad de tener un mejor control sobre los vehículos y el crecimiento del número de estacionamientos en la capital ha insertado el uso de tecnologías para automatizar el flujo de vehículos en estos recintos. Sin embargo, durante los años han surgido diversos cambios tecnológicos que en algunos casos ha sido aprovechado por empresas que se dedican a la seguridad y control en el rubro de estacionamientos.

Para comprender más de los sistemas de acceso vehicular, es necesario comprender el entorno en el cual se emplean estas tecnologías, incluyendo diferentes herramientas que trabajan en conjunto, como sensores, actuadores, controladores, indicadores y también los entornos de programación.

En las siguientes líneas se explicarán brevemente las tecnologías utilizadas en los diferentes sistemas de acceso vehicular que existen y así obtener un sustento conciso de las alternativas que se optarán para el diseño del sistema.

2.1.1 Identificación del usuario

Dentro de un sistema de acceso vehicular, el primer paso es el reconocimiento de quién es el usuario que esté intentando ingresar a las instalaciones donde se brinde el servicio de estacionamiento. Para ello se presentarán las diversas tecnologías de ingreso vehicular que se utilizan en la actualidad.

- **Ingreso por ticket con código de barras y banda magnética (Ver Figura 2.1)**:

En este medio el usuario debe detenerse en el módulo de seguridad que haya instalado la empresa a cargo del estacionamiento y debe presionar, en este caso, un pulsador que esté alojado en el panel que presenta el módulo y esperar algún comprobante para confirmar su ingreso al establecimiento. Esta es una de las primeras formas de inclusión de tecnología para iniciar un control de acceso

vehicular hacia un estacionamiento. Existen varios lugares que aún utilizan este mecanismo por simplicidad y rapidez, ya que la emisión de un ticket con hora de ingreso y un identificador por código de cada usuario es lo único que necesitan estos estacionamientos para poder hacer el cobro por las horas de brindar el servicio de parqueo. Por otro lado, las bandas magnéticas Son utilizadas por su memoria inalterable y porque presentan protección ante fallas de alimentación. Normalmente son usadas en entidades bancarias, pero también existen dispositivos utilizados en seguridad vehicular como es en el caso de este estudio. Este tipo de sistema utiliza señales electromagnéticas para poder registrar y a la vez codificar información importante del usuario en una banda que puede ser fácil y seguramente leída por una máquina de identificación instantánea [7].

Figura 2.1 Módulo Emisor de Tickets empresa Pemica.
http://www.pemica.com.do/soluciones-para-estacionamientos/

- **Detección por RFID**: La detección basada por RFID o también conocida como radiofrecuencia ha facilitado el uso y administración de las playas de estacionamiento actuales automatizando lo procesos colocando portales fijos o escáneres, asociadas a tarjetas RFID del usuario o etiquetas RFID pegadas en los parabrisas de los vehículos [1]. Este método consiste en asignar un código de información a un producto o usuario y usar esta información para acceder a información adicional al respecto. Estos sistemas cuentan con dos componentes importantes:

1. El “Transponder”, que es una etiqueta electrónica o también conocida como “tag” que consta de un pequeño micropocesador conectado a una antena de radio pequeña. Cabe resaltar que esta etiqueta contiene un único identificador que solo estaría relacionado a un único usuario o producto, por lo cual es intransferible o invulnerable ante una copia del producto.
2. El “lector”, que recibe la información que proviene del “Transponder” por medio de la antena. El lector genera un campo electromagnético constante cuya señal de

RF es captada por el receptor del “tag”, el cual activará un transmisor el cual enviará un mensaje codificado único para luego ser decodificado por el receptor y posteriormente procesado por la computadora [8].

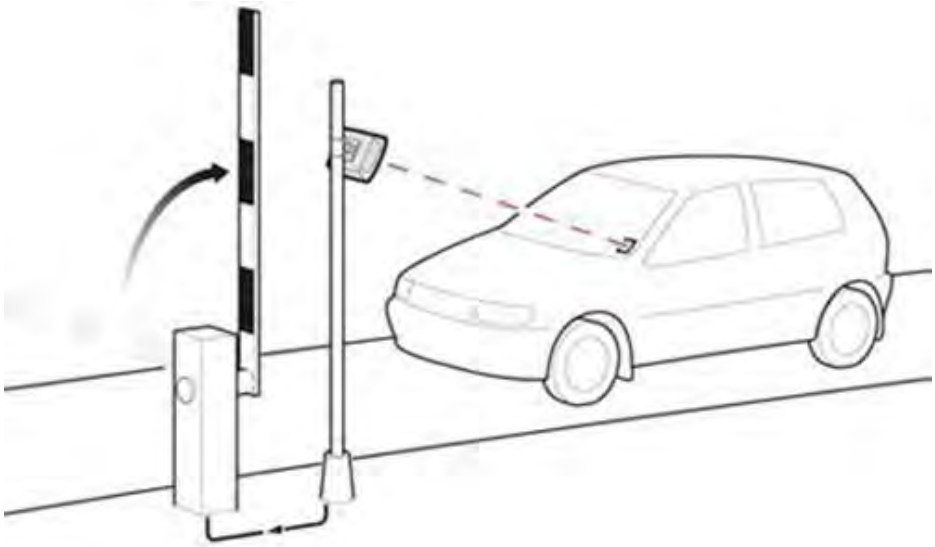

Figura 2.2. Acceso basado en una tarjeta RFID montada a un vehículo.
http://www.ipsolutions.com.pe/control-de-acceso-vehicular.html

- **Sensores Biométricos**: En este medio, el lector recibe información por parte del escaneo de alguna característica física del usuario que pueden ser ópticas, huella digital, dimensiones de la mano, patrón de la voz y/o contorno facial.

La Biometría se centra el hecho de que todas las personas, en este caso usuarios, poseen características únicas e intransferibles y por lo tanto existen métodos para poder identificarlas y ser comparadas para su verificación [9]. Dentro de las ventajas que ofrece este sistema predomina que es más fácil e intuitivo el manejo por parte del usuario; además, que ofrece pedestales personalizados para cada tipo de solución. Es importante señalar que este sistema puede escalar al punto de integrarse con todos los sistemas de seguridad que presente el establecimiento donde se ubique el sistema de acceso vehicular [10].

Dentro de los productos disponibles en esta industria, la empresa Suprema desarrolló un equipo de alta tecnología llamado BioStation A2 (ver figura 2.3), que consta en un terminal de huella IP de alto desempeño. Esta impulsado por un CPU de 1GHz iMX6 Quad-Core con la capacidad de realizar hasta 150,000 comparaciones por segundo y una velocidad de transferencia de datos de hasta 5,000 usuarios/min. Según sus especificaciones logra almacenar un máximo de

500,000 usuarios y 5,000 registros de texto. Cuenta con una pantalla táctil de 5'' IPS LCD con cristal frontal reforzado [11].

Figura 2.3 Módulo de última generación biométrico BioStation A2
Fuente: http://www.siasa.com/

Por otro lado, dentro del reconocimiento por patrón de voz y contorno facial, estos dos actúan de manera simultánea para dar un resultado confiable al encargado de gestionar los ingresos vehiculares. Para el reconocimiento facial, los algoritmos tienen dos partes principales: una es la detección del rostro y su normalización, y la segunda es la identificación de la cara del usuario. Este mecanismo es conocido como totalmente automático y los que solo toman en cuenta la segunda parte son conocidos como algoritmos parcialmente automáticos. En el primer algoritmo, se extraen las características normalizadas en un vector numérico y esto nos da una firma normalizada del individuo. Luego, el proceso a seguir es el algoritmo de coincidencia, en el cual se compara la firma normalizada con el conjunto de las firmas almacenadas en un servidor o base de datos y a partir de porcentajes de similaridad se puede llegar a decir que cierta firma le pertenece y coincide con la de la base de datos [12]. Del mismo modo, en la voz se comparan patrones únicos de la voz tales como características fisiológicas y hábitos lingüísticos; de esta manera, los factores físicos y de comportamiento de una persona se fusionan para desencadenar en un único patrón de voz para cada individuo del sistema [13].

Dentro de los equipos más destacados en el mercado se encuentra FaceAXS de EasyWay Biometrics (ver figura 2.4), que cuenta con un algoritmo de reconocimiento facial "dual sensor" que agiliza el reconocimiento facial, al mismo tiempo que asegura su exactitud. Así mismo, tiene integrado un sistema de memoria y adaptación de entrada de voz que permite atenuar el ruido proveniente

del exterior y filtrar por medio de algoritmos la secuencia de voz proveniente del usuario. La pantalla de interfaz es una pantalla TFT a color de 3.5'' con doble cámara con leds infrarrojos para el reconocimiento facial y un micrófono de alta precisión.

Figura 2.4 Módulo FaceAXS de EasyWay Biometrics. Fuente: www.siacsa.com

2.1.2 Detección de placas vehiculares

El campo de detección de placas vehiculares es diversamente amplio y contiene diversos mecanismos de detección y también existen factores que aumentan la probabilidad de que existan errores durante la captura y procesamiento de las imágenes. Por ello, es necesario establecer estándares que permitan obtener buenas imágenes y es a partir de ello que se busca procesar las imágenes obtenidas de acuerdo al protocolo de cómo se tomaron las fotos. En ese sentido, lo óptimo es obtener una imagen frontal del vehículo y evitar si es posible con algún filtro físico el reflejo de brillo sobre la placa a analizar. Esto se puede lograr estableciendo la distancia desde donde se realizarán las capturas el ángulo de giro o inclinación que tenga la cámara respecto a la placa del vehículo. Los sistemas convencionales solo hacen uso de una cámara instalada a unos metros de donde estará ubicado el vehículo y luego debe comunicarse con un procesador, ya sea el de la computadora o uno externo que permita detectar y procesar en tiempo real los caracteres de la placa del vehículo que moviliza al usuario que desee ingresar al sistema.

El proceso básico para la identificación de caracteres de la placa vehicular inicia con identificar el área de la placa vehicular. En este proceso se incluyen algoritmos para detectar el área rectangular que caracteriza a las matrículas vehiculares. Uno de los algoritmos de mayor uso es el de detección de bordes Canny y que tiene

como objetivos obtener una baja tasa de error, es decir que los bordes de la imagen no se pierdan, a su vez los puntos de los bordes detectados deben ser exactos y debe de haber solo una respuesta para cada borde. Para desarrollar este algoritmo, se debe iniciar con un filtrado de la imagen por medio de un filtro “kernel gausiano” que disminuye el ruido de la imagen y se obtiene una imagen suavizada. Luego, se debe ubicar el grosor del borde y calcular su dirección. Una vez conocida las direcciones, se aplica una supresión no máxima y finalmente se aplica un seguimiento a lo largo de los pixeles donde se halló la placa vehicular para aplicar un recorte de banda y de la placa del vehículo. El recorte de banda se utiliza para detectar y recortar el área donde se ubica la matrícula por medio de un análisis de proyección vertical de la figura y por último se realiza un recorte de la placa a través de un análisis horizontal del recorte de banda. Los siguientes pasos van luego hacia el reconocimiento de caracteres; para ello, por un algoritmo de restauración y segmentación de caracteres; y finalmente, se codifican los caracteres y se procede a reconocerlos por medio de comparación [14].

En este rubro, varias empresas han incursionado esta tecnología a sus equipos de seguridad en sistemas de acceso vehicular. Una de ellas es SKIDATA, que implementó su solución llamada PlateTech.Logic basada en la integración de sistemas LPR y de su software Parking.logic. El sistema genera un ticket de código de barras en el ingreso y que tiene escrito la placa del vehículo. Luego en la salida del estacionamiento, el sistema verifica si la placa asociada al código de barras es la misma con la que se retira el vehículo para que le otorgue el pase de salida del estacionamiento [15].

La empresa Intellisoft parking ha podido insertar esta tecnología en el Perú y ha configurado el sistema de LPR (License Plate Recognition) de SKIDATA de tal manera que se adecue a las placas de nuestro país. Para ello tomó en cuenta las siguientes indicaciones, mostradas en la figura 2.12, que dio a conocer el Ministerio de Transportes y Comunicaciones el año 2010, que ponía nuevos modelos de placas según la imagen 2.5.

Figura 2.5 Nuevo sistema de placas vehiculares en el Perú.

Fuente: http://www.intellisoftparking.com/

2.1.3 Barreras vehiculares

El uso de barreras vehiculares es indispensable dentro del sistema de acceso vehicular a espacio privados y los mecanismos de control en estos dispositivos van desde el control manual hasta la interacción de sensores y cámaras para realizar un despliego automático de este elemento de seguridad. Lo óptimo es que estas barreras cuenten con un sistema de anti-aplastamiento mediante sensores de masa o infrarrojos y puedan ser controlados mediante distintos medios como inalámbricos, por cableado serial o por botoneras o interruptores.

Dentro de las diversas empresas que ofrecen estos sistemas de acceso, la empresa DONOSTI cuenta con bloqueador de acceso con velocidades (ver Figura 2.6) de accionamiento de 1.2 segundos y con longitudes de asta variables de 3 a 6m. Además, cuentan con una entrada digital que permite generar comandos a la barrera que pueden ser conectadas a diversos controles de accesos como semáforos, sensores de masa y dispositivos que controlen tiempos de apertura [16].

Figura 2.6 Tranquera vehiculares marca DONASTI.

Fuente: http://www.donostiperu.com/parking_solutions.html

Así mismo, SKIDATA presentó un modelo de barrera vehicular, ver Figura 2.7, con un brazo que puede llegar a elevarse hasta 4.5m que tiene la capacidad de ser iluminado desde su interior y; además, permite la orientación a los usuarios mostrando diversos símbolos en su panel de led frontal [15].

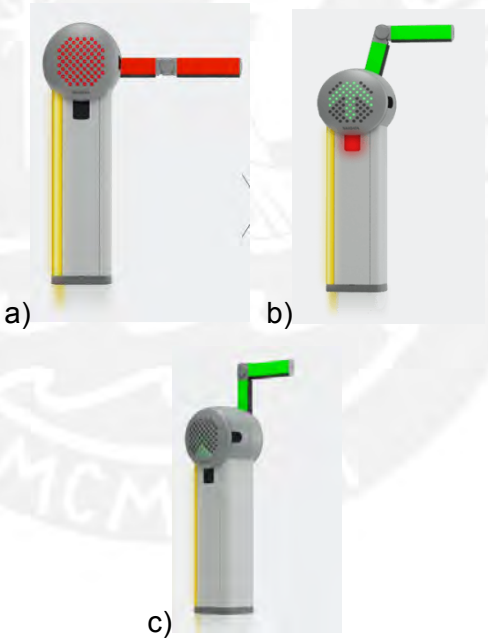

Figura 2.7 Módulo de acceso vehicular

a) En espera para una entrada de usuario. b) Abertura de la barrera e indicadores de esperar a que finalice el proceso. C) Finalización de la apertura y autorización de ingreso.

Fuente: http://www.intellisoftparking.com/

2.2 Síntesis sobre las tecnologías expuestas

Durante las últimas décadas, han surgido una gran variedad de productos destinados al control de accesos vehiculares, así como también diferentes protocolos para interconexión de los dispositivos debido a la gran demanda de seguridad que se tiene actualmente.

Según las necesidades de cada usuario se debe implementar un sistema de control de acceso de acuerdo a las prioridades de éste, prestando atención en el protocolo a usar, la cantidad de dispositivos a controlar, la robustez y escalabilidad del diseño, el tipo de arquitectura que se debería utilizar y especialmente en la relación costo – beneficio que se obtendría luego de la implementación del sistema.

El aporte que presenta la tecnología RFID en los sistemas de seguridad es de alta importancia, debido a que este sistema desplaza a los dispositivos analógicos y presenta ventajas tales como la utilización de una infraestructura económica, accesibilidad remota, escalabilidad, múltiples aplicaciones y mejor performance del sistema. Por otro lado, el coste del almacenamiento digital es inferior al analógico, al mismo tiempo que la calidad es mayor y la flexibilidad del sistema aumenta porque es posible disponer de un sistema de grabación distribuido.

Finalmente, también es importante mencionar que el éxito del diseño depende de grado de conocimiento que se tenga del contexto en donde se desarrollará dicho sistema.

Según la Tabla 2.1, se ve factible usar la tecnología RFID debido a su mejor performance a diferencia de otros sistemas costosos y que para las dimensiones y contexto del proyecto las condiciones son aceptable para el uso de esta tecnología.

Tabla 2.1 Cuadro comparativo de los sistemas de detección de usuario [8].

	Código de Barras	Banda Magnética	Memoria de Contacto	Sistemas Biométricos	RFID Pasivo	RFID activo
Modificación de la información	No Modificable	Modificable	Modificable	No Modificable	Modificable	Modificable
Seguridad de los Datos	Mínima	Media	Alta	Alta	Variable (baja a alta)	Alta
Capacidad de Almacenamiento de datos	-Lineales(8-30 caracteres) - 2D hasta 7.200 caracteres	Hasta 128 bytes	Hasta 8MB	No aplica	Hasta 64 KB	Hasta 8MB
Precio	Bajo	Medio-Bajo	Alto (cerca de US$1 por memoria)	Alto	Medio (menos de US$0.50 por tag)	Muy Alto (US$10 a US$100 por tag)
Estándares	Estables	Estables	Propietarios, no estándar	No estándar	Evolucionando hacia estándar	Propietario y en evolución hacia estándar
Ciclo de Vida	Corto	Mediano	Largo	Indefinido	Indefinido	Depende de la batería (3 a 5 años)
Distancia de Lectura	Línea de vista y (hasta 1.5m)	Requiere contacto	Requiere contacto	Depende del biométrico	No requiere línea de vista ni contacto Hasta 10m.	No requiere línea de vista ni contacto Hasta 100 m. y mayores
Interferencia Potencial	Cualquier modificación en las barras y objetos entre el código y el lector	Bloqueo del contacto	Bloqueo del contacto	Puede ser bloqueo del contacto, o bloqueo de línea de vista e inclusive el ruido.	Ambientes o campos que afecten la transmisión de radio frecuencia	La interferencia es muy limitada, debido a la potencia de transmisión.

2.3 Parámetros que establecen la calidad de la instalación de un sistema de acceso vehicular y las características operativas

- Satisfacción del usuario: Es una medida que nos interesa para tener el conocimiento de si el servicio brindado cumple con las expectativas del cliente. Se puede obtener analizando las opiniones de los usuarios.

- Calidad del servicio: Mide si se establece una velocidad apropiada de conexión para la recepción de datos y la disponibilidad de la red. Estos parámetros son los que establecen el acceso a Internet para la transmisión y recepción.
- Sistema modular: Es una medida relevante en cuanto a costos y performance. En ese sentido, si se desea integrar más componentes al sistema de acceso es posible hacerlo por medio de algún puerto disponible de conexión y permitirá integrar otros tipos de tecnologías al sistema.

2.4 Modelo Teórico

El sistema de control vehicular que se propone permitirá controlar los accesos, la detección de placa de los vehículos y la ubicación de estos datos en una base de datos para su posterior uso.

Para establecer este sistema se requiere de un conjunto de herramientas tecnológicas que funcionen de manera íntegra y segura. El sistema está compuesto básicamente por lectores, etiquetas RFID o tags, una cámara web, un módulo o interfaz informativo y un servidor con el software de administración

.

Para realizar el control de acceso, se utilizará un lector RFID a la entrada, 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 captura de imágenes, cuando se active el sensor RFID se enviará una señal al microcontrolador que activará la cámara, que ya está posicionada a la altura de la placa y luego enviará esta imagen a la computadora para su posterior procesamiento y digitalización

Todos los lectores estarán comunicados con el servidor por medio de cable UTP debido a que tiene un mayor alcance y presenta una mejor seguridad ante un posible hackeo del sistema. A través del software de administración, que tendrá el servidor, se podrá monitorear si el usuario está en la base de datos y coincide con la placa de vehículo que registró para su ingreso y así asignarle esta placa para una posterior oportunidad.

A continuación, se mostrará en la figura 2.8 el diagrama de bloques del sistema de acceso vehicular.

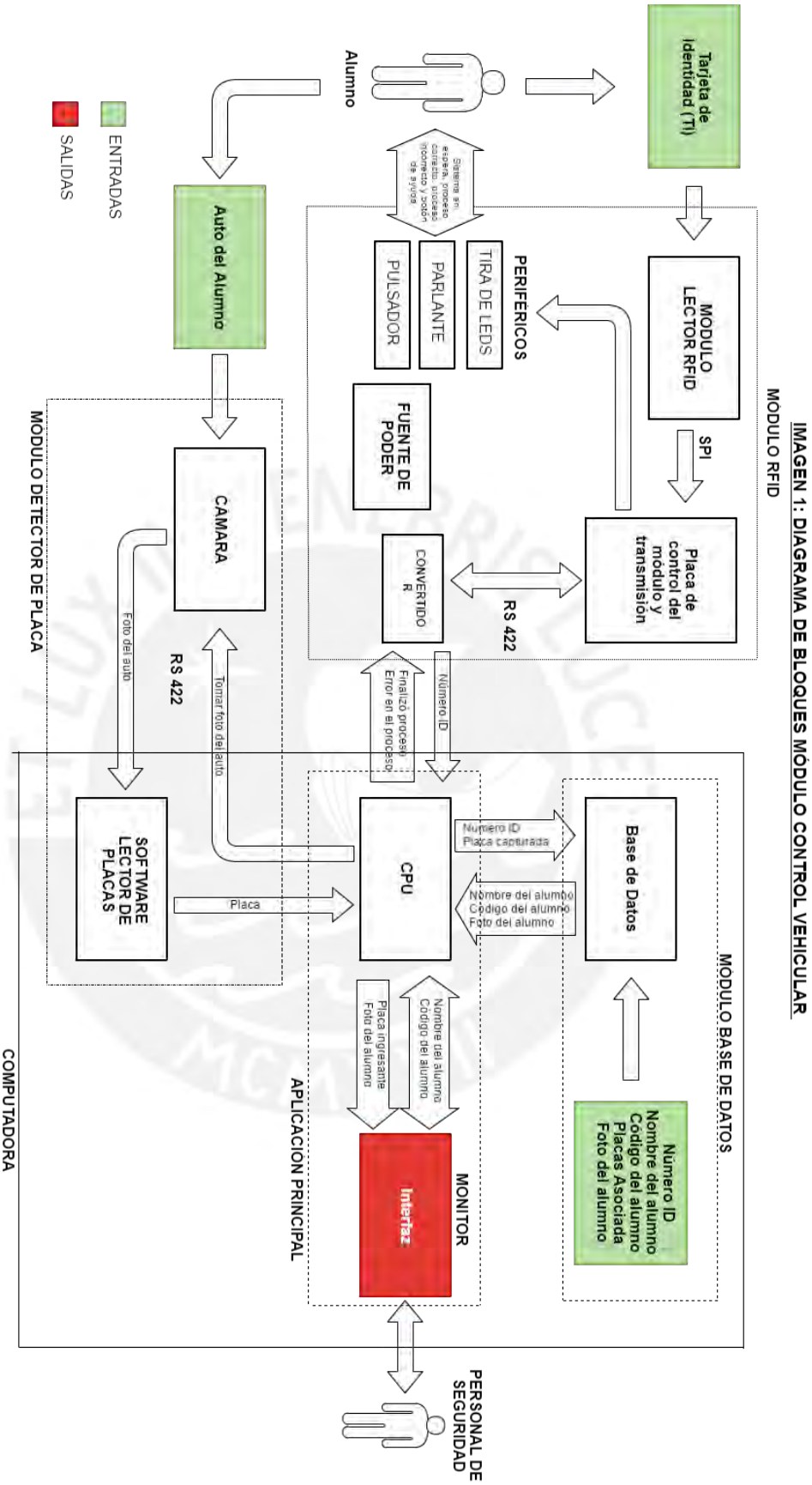

Figura 2.8 Diagrama de bloques del control del sistema

Fuente: Propia

Capítulo 3

Diseño del sistema de acceso vehicular

En las siguientes líneas de este capítulo se definirán las hipótesis y objetivos que involucran el desarrollo de la investigación. Así mismo se explicarán toda estructura del diseño relacionada al sistema de acceso vehicular que se tiene planeado aplicar en la PUCP.

3.1 Objetivo general

El objetivo principal de esta tesis es diseñar un sistema de acceso vehicular a la PUCP basado en tecnología RFID y detección de placas vehiculares, para controlar el acceso de los alumnos, profesores, personal administrativos e invitados que intenten ingresar a la universidad y de esa manera salvaguardar la tranquilidad de la comunidad universitaria ante alguna intención que vulnere su seguridad.

3.1.1 Objetivos específicos

1. Diseñar el hardware del sistema de acceso vehicular
2. Diseñar y programar el software del sistema de control e interfaz de usuario.
3. Realizar simulaciones del sistema de acceso vehicular.

3.2 Alcance

Desarrollar y proponer el diseño de un sistema de acceso vehicular a la PUCP que permita el ingreso de usuarios a la universidad, entre ellos alumnos, profesor, personal administrativo y visitas. En ese sentido, el sistema planteado será capaz de reconocer al usuario mediante su tarjeta RFID de identificación, la cual la pasará sobre el módulo detector de entrada y este permitirá reconocer al usuario y lo vinculará con la placa de su vehículo de ingreso y de ser correcto y compatibles los datos de ingreso se procederá a dar pase al usuario abriendo una tranquera vehicular y dar acceso a los estacionamientos del Campus de la universidad.

3.3 Diagrama de bloques de la solución a la problemática

A continuación, en la Figura 3.1 se mostrará el sistema de control que se pretende aplicar para dar solución a la problemática del sistema actual de acceso vehicular en la PUCP.

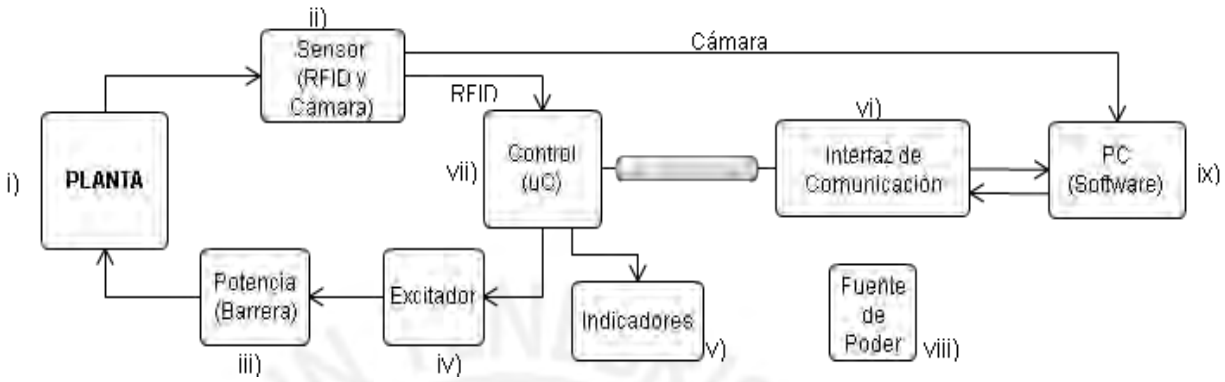

Figura 3.1 Bloques Sistema de Control

3.4 Análisis del diagrama de bloques y los protocolos usados en cada proceso

Según el sistema de control establecido anteriormente, es necesario definir los requerimientos, alternativas, criterios de selección, los circuitos diseñados y los componentes que se pretenden emplear en cada bloque del diseño expuesto. Para ello se desarrollará un análisis de cada bloque del sistema propuesto dando a conocer el porqué de cada solución diseñada.

I) Planta:

Dentro de este bloque, se considera el sistema físico que hay en sí; por lo tanto, el análisis se centra solo en las necesidades que existen en el sistema actual y la posible ubicación de los equipos que se instalarían para la automatización del sistema de acceso vehicular.

Como se observa en la Figura 3.2 las herramientas con las que cuentan la actual planta es una cámara analógica ubicada a 1.3m del fin del cruce peatonal y una barrera vehicular manual de madera ubicada al final del crucero peatonal. Como se observa solo se cuenta con una computadora que está conectada a la base de datos y se usa en el caso que el usuario no cuente con su tarjeta de identificación físicamente en el momento. Por ello, se realiza una verificación en la computadora vía intranet de la PUCP si este usuario pertenece a la universidad.

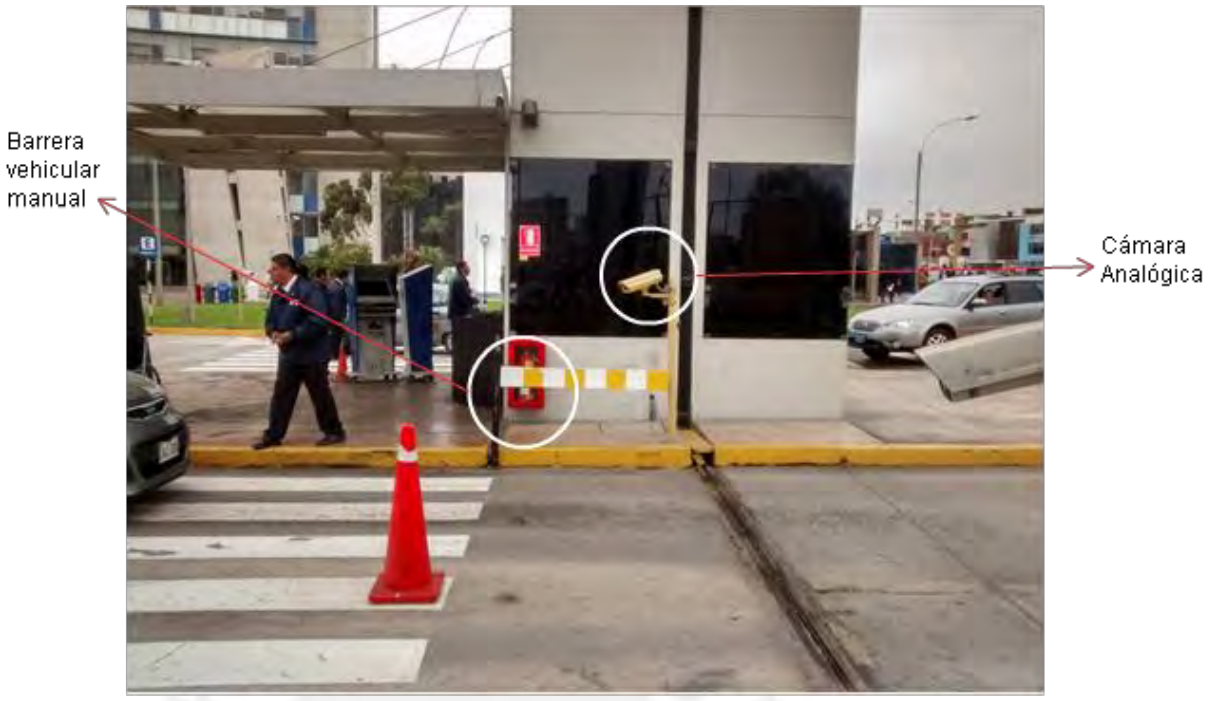

Figura 3.2 Elementos presentes en el actual sistema vehicular PUCP.

Todos estos procesos toman tiempo y son vulnerables ante la posibilidad de un engaño o filtración de algún tercero debido a fallas del factor humano durante el permiso de acceso. Es por ello, que en la Figura 3.3 se puede observar la idea de cómo podría ser la estructura del nuevo acceso vehicular aplicado a la planta o sistema que se tiene en la actualidad. Como se ve, las entradas vehiculares se mantienen iguales y también el centro de control o garita en el cual el personal de seguridad tendría un espacio con mejores condiciones para poder monitorear el proceso de acceso vehicular. En ese sentido, se dispondría de un módulo RFID (componente color azul) que interactúe con el usuario y este deba pasar su tarjeta RFID para acceder al campus. Así mismo una cámara digital (componente color amarillo) permitirá tomar las imágenes de las placas del vehículo y ser procesadas por el software de control. Todos los procesos serían supervisados por el personal de seguridad en caso suceda alguna eventualidad o una guía de cómo usar el nuevo sistema de acceso vehicular.

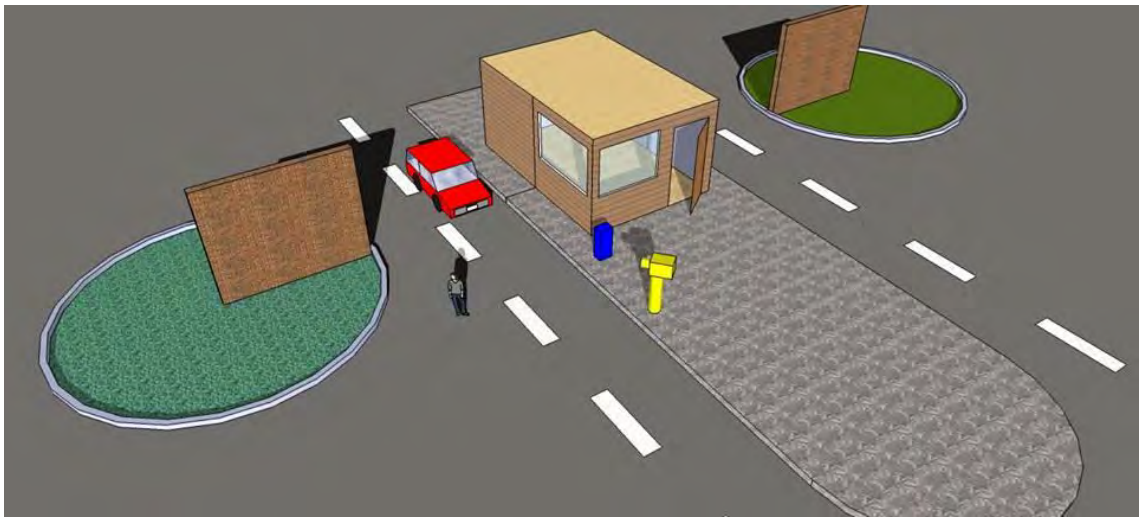

Figura 3.3 Diseño del nuevo sistema para la planta.

II) Sensor:

En esta etapa, como se apreció en la figura 3.1, la información del usuario es encriptada en un tag RFID y se envía esta información que será una variable detectada por el módulo RFID y posteriormente procesada por el bloque de control. A continuación, se analizarán las necesidades y diseño que se tiene para el sistema a aplicar.

Identificación del usuario:

Requerimientos:

Por motivos de practicidad el usuario que desee acceder a la universidad con su vehículo deberá hacerlo de manera automática y rápida, pero también necesita de una solución que sea económica en caso se realice un cobro por el servicio de implementar este nuevo sistema en la universidad. Es por ello, que la solución debe ser económica y segura de tal manera que no sea una carga para el usuario, sino un mecanismo rápido y práctico que pueda ser usado eficazmente en cualquier momento.

Alternativas:

Según lo expuesto en el capítulo 2, en la parte de identificación de usuario, se dio a conocer varios tipos de tecnologías para transmitir información del usuario. Dentro de ellas, la tecnología RFID pasiva permitía tener una mejor performance debido a que tiene un mayor tiempo de vida que las bandas magnéticas y el alcance de 10m es suficiente para el desarrollo del proyecto propuesto. Otro factor importante es el costo económico de los tags que no superan los 5 nuevos soles por tag.

De acuerdo a los requerimientos propuestos, la tecnología RFID pasiva es la escogida para el desarrollo del nuevo sistema de acceso vehicular. Sin embargo, existen muchas variedades que se acomodan al entorno propuesto y es necesario poder escoger una de ellas.

Como se sabe existen diferentes equipos RFID que se pueden clasificar por su fuente de energía y el rango de frecuencia que usan. Dentro de la fuente de energía existen 3 tipos de RFID. Uno de ellos son los pasivos que obtienen su energía del campo de radiofrecuencia generado por el lector de RFID. Otros son los activos que en su estructura ya tienen incorporado una pequeña batería que los alimenta; y, por último, los RFID semi-activos son tags que permanecen en la condición de modo pasivo hasta que el lector de tarjetas lo activa enviando una señal y es ahí donde pasa a modo activo [17]. Según la Tabla 3.5, se pueden observar los rangos de frecuencia que aceptan las normas que regulan estos dispositivos. Estas varían desde los 100 KHz hasta frecuencias que alcanzan los rangos de microondas en 30 GHz aproximadamente.

Tabla 3.1 Tipos de RFID disponibles según sus rangos de frecuencia

Banda	LF Baja frecuencia	HF Alta Frecuencia	UHF Ultra-alta frecuencia	Microondas
Rango de frec.	30-300KHz	3-30MHz	300MHz-2GHz	2-30GHz
Frecuencias RFID	125-134KHz	13.56MHz	868MHz (Europa) 915MHz (USA)	2.45GHz
Distancias (aprox) tags pasivos	<0.5m	Hasta 2m	6m	Activo: >100m No habitual pasivo
Velocidad	<1kbps	25kbps	Hasta 640kbps	
Ventajas	Buen comportamiento con metal y agua	Buena distancia, mejor velocidad y anticolisión	My alta velocidad (600 tags/s), estandarización global ePC, mayores distancias	
Inconvenientes	Corta distancia, baja velocidad, poca capacidad anticolisión	Peor comportamiento con agua y metales	Muy sensible al agua y al metal	
Uso habitual	ID Animal, coches, controles de accesos	Accesos y seguridad, smart cards, pasaporte	Logística procesos de fabricación	Activos: autopistas, contenedores
Otras caracteristicas	Campo cercano Acop. Magnético	Campo cercano Acop. Magnético	Campo lejano Acop. Eléctrico	

Fuente: http://www.iberwave.com/tiposdesistemas.html

Criterio de selección: El rango de trabajo se basará en los lectores pasivos, ya que su uso es más comercial y práctico debido a que no necesitan de cambios de batería. Por ese motivo se trabajarán en frecuencias de LF y HF, además es necesario saber que estos tags pasivos tienen la función de sólo lectura o de lectura y escritura, en la cual la información de identificación puede ser modificada por el lector [18].

Según la tabla 3.1, se establecen las diferencias principales entre los tipos de RFID que serían viables para el uso en el proyecto. En este caso, se optó por elegir el sensor RFID MFRC522.

Tabla 3.2 Comparación de lectoras RFID

Caract/Modelos	EM4102 [19]	T5577[20]	MFRC522[21]
Fuente de Energía	Pasivo	Pasivo	Pasivo
Frecuencia de trabajo	125 KHz	125 KHz	13.56 MHz
Función	Solo escritura	Lectura y escritura	Lectura y escritura
Memoria	512 bits	330 bits	1Kb
Voltaje de alimentación	-0.3 - 7.5 V	0.5 – 5 V	2.5 – 3.3 V
Fabricante	EM Microelectronic	Atmel	MIFARE
Costo (S/.) 1US$= S/. 3.29	53.00	65.00	23.00 Tag: 4.5

Debido a la capacidad suficiente y necesaria para los datos del usuario, el modelo MFRC522, Figura 3.4, es capaz de sostener el diseño del circuito del sensor y además cuenta con características que lo diferencian de otros dispositivos aún más costosos.

Figura 3.4 Lector RFID MFRC 522

Fuente: http://www.nxp.com/documents/data_sheet/MFRC522.pdf

Circuito:

El circuito interno de este tag, consta del chip MFRC 522, el cual es alimentado por una antena que es receptora del campo generado por el lector. Según la Figura 3.5 se puede observar que la antena actúa como resonante ante la emisión de ondas electromagnéticas proveniente del lector y le envía energía al circuito de memoria interna que, a su vez, responde enviando por RF un código identificador que se puede usar para validar o identificar la información del producto.

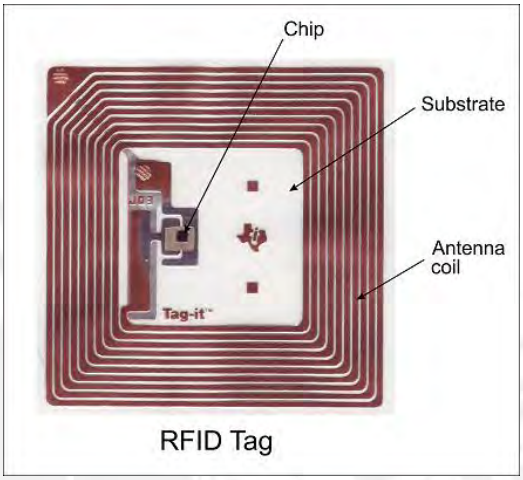

Figura 3.5 Estructura interna TAG MRFC 522

Fuente: http://www.prometec.net/arduino-rfid/

Características eléctricas:

Voltaje de alimentación: 3.3 V.

Corriente Consumida por el módulo RFID RC522A. En la Tabla 3.3 se aprecia los valores totales de corriente consumidos por este lector RFID y se tiene que el valor máximo de corriente consumida puede llegar a los 163 mA en uso continuo.

Tabla 3.3 Valores de corriente máxima consumida por RFID [21].

Pin	Descripción	Corriente máxima consumida
PVDD	Corriente de alimentación	40 mA
DVDD	Corriente de alimentación digital	9 mA
SVDD	MFIN y MFOUT	4 mA
TVDD	Corriente de transmisión	100 mA
AVDD	Corriente de alimentación analógica	10 mA
	TOTAL	163 mA

Identificación de vehículo:

Requerimientos:

Para la detección de las placas de los vehículos ingresantes, se necesita una cámara capaz de poder registrar estás imágenes con la mayor nitidez posible para el procesamiento de las placas y detección de los caracteres de la misma. Así mismo, según la Figura 3.1, deberá enviar los datos hacia la PC, por lo que necesita una conexión práctica hacia este dispositivo.

Alternativas:

Dentro de las cámaras existentes en el mercado se pueden extraer ciertos modelos que presentan cualidades únicas para diferentes propósitos. En la Tabla 3.4 se considerarán los modelos tentativos para ser usados en una futura implementación del sistema de acceso vehicular y mencionando ciertas características como modelo, resolución, conectividad, fabricante y precio.

Tabla 3.4 Comparación de cámaras digitales en el mercado

Características/ Modelo	Cámara Web pro C920[101]	Genius Eye 110[102]	DCS-3715[103]	Life-Cam HD 3000[104]
Resolución	1080p – 720p	640x480 px	Full HD 16:9	720 p
Conectividad	USB 2.0	USB 1.1	Ethernet	USB 2.0
Fabricante	Logitech	Genius	D-link	Microsoft
Precio(S/.)	369.90	70.00	1090.00	150.00

Características/ Modelo	Cámara Web pro C920	Genius Eye 110	DCS-3715	Life-Cam HD 3000
Equipo	 [3.1]	 [3.2]	 [3.3]	 [3.4]

Fuente: [3.1] http://www.falabella.com.pe/falabella-pe/product/14692452/Camara-Web-Pro-C920-HD-Gris
[3.2] http://es.specsen.com/webcam-genius/genius-eye-110/
[3.3] http://www.dlinkla.com/dcs-3715
[3.4] http://www.microsoft.com/hardware/es-es/p/lifecam-hd-3000#details

Criterio de selección y ubicación:

Según la Tabla 3.4, la cámara a escoger es la DCS-3715 de la marca DLink. Esta cámara tiene un puerto Ethernet y al mismo tiempo puede ser alimentado por este puerto mediante POE (Power Over Ethernet) lo cual facilita su instalación hacia la unidad de procesamiento de las imágenes, en este caso la PC. Así mismo, esta cámara posee un filtro IR que permite obtener mejores imágenes durante vigilancia nocturna y cuenta con una memoria SD para tener algún respaldo local que pueda almacenar las grabaciones de la cámara. La principal característica de este dispositivo es la calidad HD 16:9 que cuenta con un lente vari-focal para entornos variados, proporcionando mayor calidad a las capturas realizadas [22].

Esta cámara se ubicará en una estructura especialmente diseñada para este modelo y que se debe de encontrar a 5.25 metros del módulo RFID. Ver Figura 3.6.

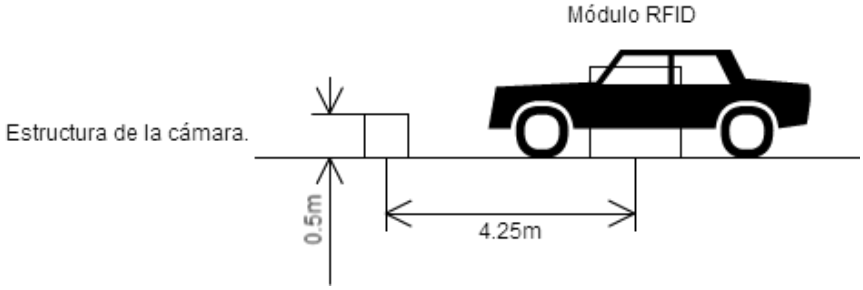

Figura 3.6 Posicionamiento de la cámara de detección vehicular.

Fuente: Propia

III) Potencia:

Requerimientos:

En esta etapa se necesita poder controlar una barrera vehicular que deberá ser seleccionada dentro de las posibilidades del mercado según su torque, voltaje y corriente consumida. El tiempo de abertura y la precisión de los sensores de fin de carrera o de obstrucción son determinantes para elegir la barrera que pueda acomodarse a las necesidades del presente proyecto. Así mismo, la conectividad de esta barrera de acceso de control con el sistema planteado debe ser práctica y de rápida respuesta a la señal de abertura y/o bloqueo proveniente de la etapa de control.

Alternativas: En el mercado existen diversas barreras automatizadas que permiten un flujo continuo de carros y uso intensivo de esta. Sin embargo, es necesario utilizar el modelo correcto que se adecúe a las necesidades del proyecto. En este caso es necesario escoger una barrera que permita un uso intensivo por las dimensiones del proyecto y así mismo que permita controlarla sin ningún problema desde un dispositivo tercero a la barrera. Así mismo, un modelo económico y de fácil instalación permitirá tener un proyecto escalable para adaptarlo a diferentes tipos de entradas de acuerdo al contexto real del problema.

A continuación, en la Tabla 3.5 se mostrarán los modelos principales de barrera vehiculares que existen en el mercado y sus características que los diferencian de otras.

Tabla 3.5 Modelos de barreras vehiculares

Característica /Modelo	LiftMaster BG770	Platinum Access PB19	LiftMaster Mega Arm	Zebra barrera Vehicular CAME Gard4
Tensión de Alimentación	220 VAC	110/220 VAC	110/220 VAC	230 VAC 50Hz, monofásica
Potencia Consumida	180 W	320 W	250 W	300W
Tiempo de apertura	4 s	6 s	2.5 s	6 s
Tipo de Motor	Motor DC – 24V – 1/2HP	Motor DC – 24V con Encoder	Motor DC – 24V – 1/2HP	Motor 230V

Longitud Brazo	4 m	5.8 m	3.6 m	4,6 Y 8 m
Control/Sensores	Remoto RF, Interruptores	Interruptores, Control Remoto, Comandos	Interruptores, cerrado con Interruptor o temporizador. Sensor de obstrucción.	Lectores de tarjeta, sensor de obstrucción,
Precio	US$1660	US$1670	US$1520	US$1990

Fuente: http://www.gatedepot.com/category/traffic-barriers_barrier-gate-operators/

Según la tabla anterior se escogerá la barrera de la marca LiftMaster de modelo Mega Arm, ya que lo diferencia de otras por su velocidad de apertura, así como las diferentes posibilidades de control que posee, haciéndolo más dinámico ante los posibles cambios de excitadores que envíen la señal hacia la barrera vehicular. Todas estas barreras encontradas en el mercado, se adaptan a la red eléctrica nacional de 220V y 60 Hz, por lo que no serían malas opciones para su uso comercial dentro de estos sistemas; sin embargo, el precio que ofrece el modelo de LiftMaster está dentro de los más bajos del mercado y al ser una marca reconocida y con gran trayectoria en su rubro permite dar robustez a la solución propuesta.

Por otro lado, el método que lo hace más robusto y práctico para el control de esta barrera vehicular es el uso de los contactos o interruptores para la abertura automática ubicado en el terminal 1 de la entrada J5 de la placa de control. Esta barrera cuenta con un temporizador regulable por medio de Interruptores DIP (ver Figura 3.7a) para el cierre automático de la barrera que se activa una vez que se haya dejado de enviar la señal de abrir la barrera (2.5 s) o se puede disponer de un segundo interruptor para cerrar la tranquera vehicular secuencialmente si se decidió deshabilitar el cerrado de la barrera por medio de un temporizador automático. Este temporizador puede ser ajustado de 1s a 16 s de acuerdo a la necesidad del cliente (por defecto el cierre se realiza a los 4s de liberarse la barrera) y es regulable por medio de 1 DIP Switch de 5 contactos ubicado en la misma tarjeta de control del dispositivo.

Según la Figura 3.7b se puede observar la conexión de los terminales para abrir o cerrar la barrera vehicular, así como las conexiones que se deben realizar para que la barrera se encuentre habilitada y funcione correctamente cuando exista algún evento de obstrucción al momento del ciclo de cierre de la barrera.

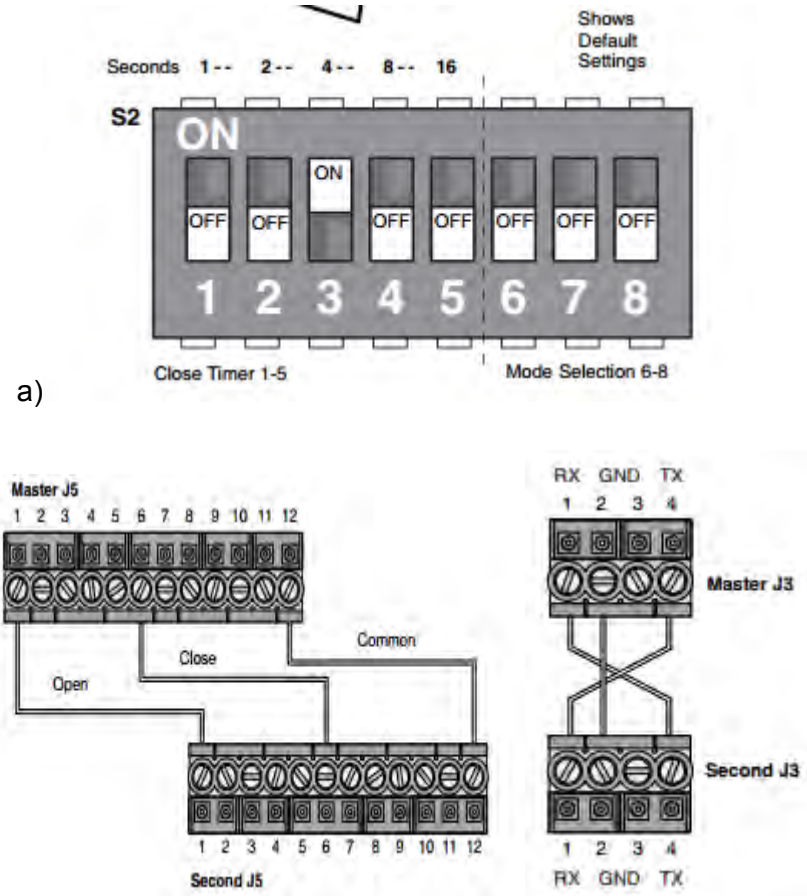

Figura 3.7. a) Interruptores (1-5) tiempo para cierre automático de la barrera. B) Conexión de los interruptores(J5) para apertura o cierre de la barrera – Activados a 0V. Conexión para el sistema automático ante obstrucción de la barrera (J3).

Fuente: http://www.gatedepot.com/get_manual_file/37620/

Así mismo, la barrera Mega Arm cuenta con un sistema de baterías cuando por algún problema en la red se corte el suministro eléctrico y tenga la posibilidad de funcionar con las baterías dispuesta de 24V tanto para el control manual de la barrera o si se desea se puede configurar que cuando exista este corte de suministro eléctrico la barrera vehicular abra el brazo y permita que se el flujo de vehículos en caso exista una emergencia y se necesite agilizar y desalojar las instalaciones en las cuales la barrera obstruya los accesos vehiculares [23].

IV) Excitador:

Requerimientos: En este caso se necesita de un mecanismo que funcione de interruptor controlado, en esta ocasión, no de forma manual, sino desde el envío de una señal de la etapa de control. En ese sentido, la barrera LiftMaster Mega Arm recibirá de su tarjeta interna de control una señal de 0v cuando la barrera necesite abrirse y esto será posible cuando un interruptor lleve esa señal a 0V y a su vez soporte la cantidad de corriente que pase por ese punto.

Criterio de selección:

La forma más efectiva de poder controlar esta señal de activación de la barrera vehicular es con la ayuda de un control de relé de acción rápida. En ese sentido, se tienen diversos tipos y modelos de relés en el mercado, pero se prefirió usar algún modelo robusto y que el control de este relé sea seguro por medio de una señal digital proveniente en este caso de la etapa de control (ATmega328).

Según la tarjeta principal de control de la barrera vehicular de marca LiftMaster, lo único que se debe realizar para abrir adecuadamente la barrera vehicular es la unión entre el terminal 1 (unido con los terminales 2 y 3) del conector J5 con el terminal de 0V (terminales 9 - 12) y así enviar esta señal para activar el mecanismo de apertura de la barrera. Ver Figura 3.8.

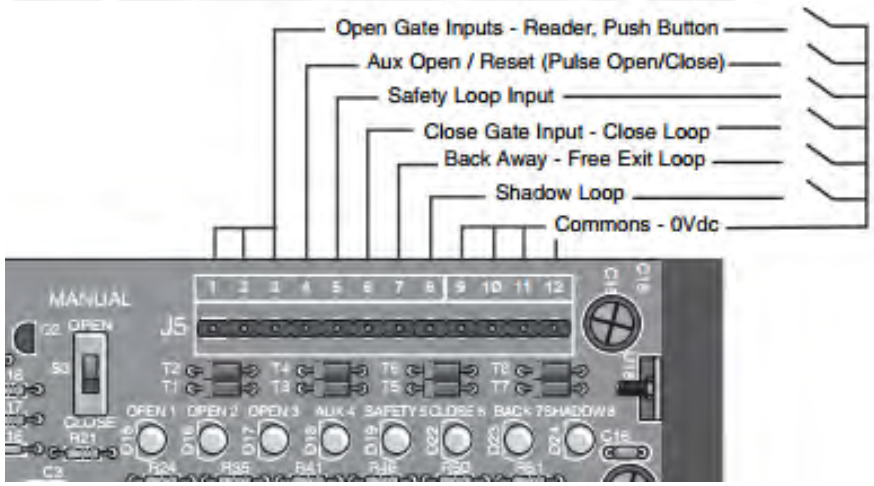

Figura 3.8 Terminales del conector J5 para activación del mecanismo de apertura de la barrera vehicular.

Fuente: http://www.gatedepot.com/get_manual_file/37620/

Teniendo en cuenta el diseño del fabricante, el control de estos pines debe hacerse de forma cuidadosa y evitar generar picos de voltaje, ya que pueden dañar el circuito de control de la barrera. En ese sentido, el uso de un relé es el indicado para asegurar los niveles de voltaje, así como soportar los niveles de corriente que pasen por estos pines. Según el fabricante de la barrera, la entrada a controlar tiene un voltaje de 24 a 30V y con una corriente de 500 a 600 mA. Dentro de las opciones del mercado existen diversos modelos de relé, pero para el caso específico de este proyecto y la necesidad de brindar robustez y efectividad a la solución se prefirió utilizar un relé de estado sólido de modelo **G3MB-202P** de la marca OMRON. Este relé puede soportar corrientes de 2 Amperios en su salida, suficiente para la activación del sistema de apertura de la barrera vehicular propuesta. Así mismo, el modelo del relé está en un empaquetado tipo "SIP" que es pequeño y robusto y se venden en módulos para este tipo de propósito ya con borneras y circuito de protección fallas eléctricas que puedan dañar al relé. Los precios en el mercado de estos módulos dependen de la cantidad de relés por módulo y en el caso de este proyecto de fin de carrera se utilizará el modelo de un solo relé que tiene un costo de US$ 4.00. En la Figura 3.9 se muestra el módulo que consta de un solo relé SSR. Como se puede apreciar es fácil de montar en un chasis o plataforma para la activación de la barrera vehicular y puede extender el cableado desde el módulo hacia los pines de control de la barrera sin ningún problema, ya que cuenta con las borneras de salida que soportan una intensidad de corriente de hasta 2 Amperios [24].

Figura 3.9 Módulo de Relé de estado sólido G3MB-202P – 1 Relé

Fuente: https://es.aliexpress.com/item/5V-1-Channel-OMRON-SSR-G3MB-202P-Solid-State-Relay-Module-240V-2A-Output-with/32235826928.html

Para comunicar este módulo de relé con el sistema de control principal y el sistema de control de la barrera solo basta con alimentar el módulo del relé con un voltaje continuo, según su hoja de fabricante, de 5V y conectado a la tierra del sistema de control principal y por medio de un pin de la etapa de control (0V o 5V) conmutar el estado del relé, que se activa en una lógica en baja mediante el pin CH, cuando se autorice el pase del usuario al campus universitario. De esta manera es posible realizar el control del sistema del relé de estado sólido y según la figura 3.10 se puede observar la conexión que tendrá la barrera vehicular con la parte de control por medio del bloque del excitador, que en este caso está compuesto por la activación del relé de estado sólido y un circuito externo de un led verde que permitirá saber cuándo está en funcionamiento el bloque excitador. Así mismo, para exigir menos al microcontrolador y tener un mejor control del relé de estado sólido que llega a consumir alrededor de 30mA cuando es alimentado a una tensión de 5v, se adicionó un circuito basado en un transistor NPN (2N222) con resistencia de protección de base de 10K ohmios que permita conectar el circuito a tierra para activar o desactivar la apertura del relé. Este circuito posee un led indicador verde con un voltaje de operación de 2V que está limitado a una corriente de 15mA [25] (dentro de sus valores permitidos) por la resistencia de 2K ohmios conectada en serie. La salida del relé como se vio en el módulo anterior debe permitir unir el contacto entre el PIN1 y 0VDC del terminal J5 en la tarjeta de control de la barrera LiftMaster Mega Arm. En ese sentido el relé estaría cumpliendo su tarea de forma rápida, silenciosa y consecutiva sin ningún problema, ya que son características de este tipo de relé. Además, las conexiones de tierras o GND estarían completamente aisladas entre la etapa de control y de potencia gracias a este bloque excitador del sistema.

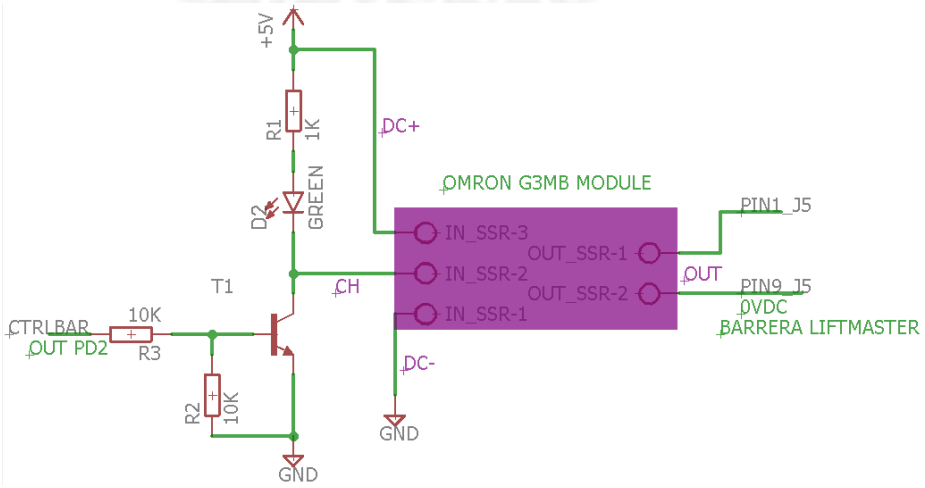

Figura 3.10 Diagrama esquemático de conexión entre la parte de control (uC) y la barrera de acceso vehicular.

V) Indicadores:

Requerimientos: Para indicar de manera tangible al usuario que desea ingresar a la PUCP se deben contar con indicadores visuales y/o auditivos que sean fácilmente reconocidos por el usuario y permitan un flujo eficaz de los vehículos en su acceso. En primer lugar, se necesitará un sistema indicador visual que dentro del entorno del proyecto los LEDs son los que se acomodan a este tipo de necesidad, teniendo la capacidad de ser visibles durante el día y la noche eso depende del nivel de luminosidad y el tipo de LED que se vaya a escoger.

Para el tema de los indicadores auditivos se debe de tomar en cuenta que el sonido a emitir debe ser totalmente audible hasta el interior del vehículo y ser capaz de alertar al personal de seguridad que se encuentre próximo al módulo de acceso en caso exista algún procedimiento erróneo.

Criterio de selección:

Para los LEDs se tiene como condición que se deben indicar con diferentes colores la situación del acceso vehicular; por lo tanto, los LEDs a utilizar debe ser los RGBs. En ese sentido, se cuentan en el mercado con diferentes modelos de empaquetamientos de estos dispositivos. Uno de ellos son las cintas de Leds RGB, ver Figura 3.11, que según sus especificaciones llega a consumir 36W por cada 5m (7.2W/1m) de esta tira de led. Por lo tanto, siendo la alimentación de estos leds 12V y por necesidades del proyecto se necesita cubrir una distancia entre 0.5 a 1 m, su consumo de corriente llegaría a ser aproximadamente 600mA (En 1 metro, 7.2W = 12V***0.6A**). Además, este tipo de cinta posee una protección IP65 que lo hace resistente ante espacios con exposición.

Figura 3.11 Cinta de Leds RGB marca SECOM.

Fuente: www.secom.es

Por otro lado, se tienen otras presentaciones de estos leds RGB, una de ellas son los displays RGBs que pueden tener forma circular, cuadrada o rectangular. Sin embargo, esta tecnología tiene una presentación rígida y no permite modificarlo al entorno donde se ubique. Otra alternativa, es poder realizar manualmente un circuito de Leds RGBs conectado en series y siguiendo la forma del módulo donde serán ubicados. Si bien estas alternativas son un poco más económicas a simple vista, no llegan a ofrecer una calidad en cuanto a su continuo uso (fabricación manual) y no son adaptables al cambio físico. Aunque el precio de las cintas RGB de marca SECOM estén entre los 50 a 65 nuevos soles, esto no lo debilita frente a otras alternativas, ya que cuenta con sistemas de adhesivo que lo hace aún más práctico y tiene una mejor adaptación al ambiente de trabajo donde se vaya a emplear. Por esa razón, se escogió esta tecnología de tiras de leds RGB y que serán controladas por un voltaje de 12V.

Parlante:

Cumplen la misma función de la tira de LEDs de indicar al conductor en qué estado se encuentra el sistema.

Características:
- Resistencia interna: 8Ω.
- Voltaje de alimentación: 5V.

La conexión de este parlante con la placa de control del módulo y transmisión se puede realizar por medio del conector existente en dicha placa. Ver Figura 3.12.

Figura 3.12 Parlante de 8 Ω – 4W

Fuente: Propia

VI) Interfaz de comunicación

Requerimientos:

En este bloque la señal enviada por el microcontrolador debe ser capaz de pasar por un cable de red de aproximadamente 8 metros para comunicar la PC y la tarjeta de control. En ese sentido, se necesita de una tecnología capaz de lidiar con problemas relacionados a caída de voltaje, ya que esto afecta directamente a la información que se desea enviar de un lado a otro.

Alternativas y criterio de selección:

Según la Tabla 3.6, se pueden ver tres tipos de protocolos posibles para usar en el sistema propuesto. El protocolo RS485 permite recorrer largas distancias y sin problemas en su eficiencia de entrega de datos. Además, posee una velocidad de transmisión relativamente alta en comparación a otros protocolos y posee una sensibilidad alta lo que lo hace más seguro ante pérdidas de voltaje en la línea de transmisión. Lo que lo hace más importante es el modo de transmisión dual de datos lo cual es lo óptimo para sincronizar tanto el módulo de detección RFID con el software principal de control.

Tabla 3.6 Alternativas de protocolos de comunicación

	RS 485 [26]	RS 232 [26]
Costo aproximado:	35 por dispositivo	15 soles por dispositivo
Número de dispositivos que permite conectar	De 32 drivers, 32 receptores	1 driver, 1 receptores
Distancia	Hasta 1.2 Km a 9600 baudios/s	150 m a 9600 baudios/s
Velocidad máxima	10Mbps	160kbits
Complejidad	Media	Baja
Modo de operación	Diferencial	Single-Ended
Niveles de voltaje	De +/- 6V a +/-1.5V	‘1’ (-3v a -25v) ‘0’ (3v a 25v)
Sensibilidad el receptor	+/- 3V	+/- 200 mV

Número de cables necesarios	3	2 (Con driver USB RS232)

Diseño:

Para el diseño de la tarjeta próxima a la PC se siguió el mismo diseño de los MAX485 en el bloque de control, solo que esta vez la recepción serán los pines de transmisión del control y los de transmisión serán los de recepción del control.

Según la Figura 3.13, se puede apreciar que los pines son los complementarios a la etapa de control, pero se mantiene aún el pin de GND. Esta norma se basa en un sistema diferencial que permite en primer lugar eliminar los errores por ruido que se filtran en el canal de comunicación. Como se observa se usan señales A o D+, que es la señal de emisión/recepción no invertida transmitida al canal de comunicaciones. Así mismo, la señal B o D- es la señal de emisión/recepción invertida transmitida al canal de comunicaciones y una referencia que es la señal GND. Es necesario mencionar que cuando la entrada “enable” tiene un ´0´, el equipo se encuentra en modo recepción y en ‘1’ cuando entra en modo transmisión [27]. Este concepto es utilizado para enviar datos a través de la red y es importante señalar que el dispositivo MAX485 hace factible la compatibilidad entre los niveles de señal TTL con las normas 485 por medio de los terminales RE y DE.

Además, se incorporó una resistencia entre cada canal de comunicación Tx y Rx para evitar problemas de debilitamiento de la señal y no existan pérdidas de potencia.

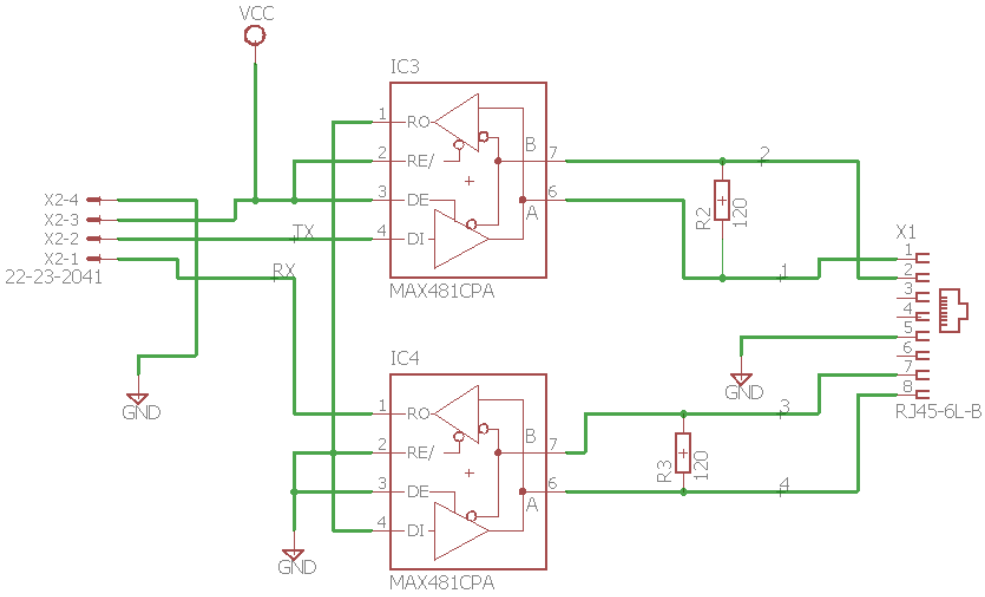

Figura 3.13 Conexión protocolo de comunicación 485, mediante MAX485

Fuente: Propia

Por otro lado, luego de que la señal que viene de la etapa de control por medio del cable de red, se convierte en niveles de voltaje TTL que es lo que envía en realidad el microcontrolador. Sin embargo, esta señal no puede ser leída directamente por la computadora, así que es necesario adecuar una manera de pasar estos datos a un formato que se pueda pasar hacia la PC y este formato es el USB. En ese sentido, se optó por usar un conversor USB- TTL disponible en el mercado que lo que hace es convertir a través de un chip FT232R la señal proveniente del TTL y pasarlo a formato USB mediante una señal de reloj [28].

VII) Control

Requerimientos:

En esta etapa, el proceso se centra en la recepción de información proveniente del lector RFID MFRC 522 y en conjunto con la verificación de información con el software del sistema se procede a realizar la acción programada para cada caso. Dentro de las respuestas, estará el enviar la información a la PC sobre la tarjeta leída y recibir la información de la PC para enviar las notificaciones al usuario si se concede o no su ingreso. Además, se requiere en este bloque administrar el bloqueo o barrera vehicular para concluir el proceso de ingreso del usuario a la PUCP. Por ello, se debe de contar con una tarjeta de control capaz de poder manipular estos datos y contar con un sistema que también permita detectar si existen fallas en la tarjeta de diseño electrónico.

Dentro del número de pines de entrada se encuentran los 6 pines de la conexión por SPI con el RFID (sin contar VCC y GND). Luego para la comunicación con la PC se necesitan dos pines (Tx y Rx) y finalmente se necesitarán otros dos pines para el control del excitador de la barrera automática. En ese sentido, se tienen 10 pines que son de entrada y salida para los otros bloques. Luego se tendrán que usar 6 pines más para el control de los indicadores (3 de leds, 1 del parlante, 1 del botón de ayuda y 1 de Reset del sistema).

Por último, el almacenamiento que se necesita para alojar el programa en la memoria del controlador será de aproximadamente 350 KB.

Alternativas:

Según la Tabla 3.7 se buscó una lista de microcontroladores que podrían facilitar y acomodarse al propósito del control de estos datos. Entre ellos se pueden ver datos importantes como la capacidad de estos dispositivos, así como los pines que manejan, ya que el proyecto demandará una cierta cantidad de pines que permitan controlar los datos de entrada y salida del sistema.

Tabla 3.7 Lista de microcontroladores ATmega disponibles en el mercado y clasificados por características funcionales.

Device	ATmega8	ATmega168	ATmega328
Flash	8192	16384	32768
SRAM	1024	1024	2048
EEPROM	512	512	1024
Max Freq (MHz)	16	20	20
Touch Chnls	12	16	16
Ext Interrupts	2	24	24
SPI	1	2	2
Temp	N	N	Y
picoPower	N	N	N
Vcc	2.7 to 5.5	1.8 to 5.5	1.8 to 5.5
In Compare	0	1	1
Out Compare	0	6	6
PWM	3	6	6
Price($)	2.61	3.11	**2.06**

Fuente: http://avrprogrammers.com/articles/atmega8-vs-atmega328

Criterio de selección:

Según la tabla 3.2 propuesta anteriormente, se pueden analizar varios tipos de soluciones disponibles en el mercado. Sin embargo, dentro de las posibles alternativas, se vio factible el uso del microcontrolador ATmega328, esto debido a su bajo costo y también que cumple con los estándares que demanda el proyecto, entre ellos la cantidad de pines disponibles, los dos puertos SPI, y el almacenamiento disponible para la programación del sistema. Además, este chip viene integrado en plataformas como las de Arduino que presentan practicidad en

cuanto el uso de sensores como es el caso del MFRC 522 en el cual no existen problemas de compatibilidad y trabajan correctamente.

Circuito y diseño:

Para el diseño del circuito se tomaron en cuenta los requerimientos de este bloque del sistema, el cual contará con los datos de la detección del sensor RFID y luego procederá a comparar estos valores con la base de datos de la computadora que le enviará una letra "O" por protocolo serial en caso sea correcta la comparación de los datos, en ese caso se mostrarán por medio de los indicadores propuestos (Leds RGB, parlante y señal de barrera vehicular) el ingreso del usuario y se prenderá la tira de leds en color verde, un sonido corto de 880 Hz y duración 1s y finalmente se abrirá la barrera vehicular hasta que el vehículo termine de ingresar. En caso, la verificación de los datos del usuario y la información en la computadora sea incorrecta, se retornará una letra "F" por el canal serial y esto será traducido en un parpadeo de lo leds en color rojo cada 100 ms y una frecuencia de 880 Hz y no se enviará señal para abrir la tranquera vehicular. Estos indicadores se desactivarán una vez que el personal de seguridad haya podido solucionar el problema del ingreso del usuario manualmente debido a factores como no estar registrado en la base de datos, error en la detección de la placa u otros factores externos. La desactivación de los indicadores de error será por medio del software de la computadora y permitirá seguir con el proceso de manera normal. Cabe mencionar que cuando el sistema se encuentre en modo de espera tendrá los leds encendidos en color azul y estará a la espera de ingreso de un nuevo usuario a la PUCP.

Para el diseño del circuito se usó la herramienta de desarrollo Eagle y se comenzará detallando la etapa de recibir los datos por el sensor RFID. En este diseño se utilizó el protocolo SPI usando los pines de 1, 2, 3, 4 y 5 del puerto B del microcontrolador que son OC1A, SS, MOSI, MISO y SCK respectivamente. El cableado es directo al microcontrolador ATmega328 y en este caso el dispositivo maestro es el microcontrolador y el esclavo sería el módulo RFID. La alimentación del módulo RFID es 3.3V

Igualmente siguiendo esa misma lógica de activación de un circuito para encender un led, se utilizó un circuito para la activación de los leds indicadores de ingreso por medio de transistores BJT NPN BC848, con resistencia de Base de 10KΩ, resistencia de colector de 4.7KΩ y resistencia de protección de 100KΩ. Luego la señal de activación pasará al pin Gate del Mosfet de activación IRF530. La lógica

de este circuito es poder disminuir el ruido generado y también poder exigir el mínimo de corriente al microcontrolador, ya que cada pin de este puede emitir a lo máximo 40mA [29]. En la Figura 3.14 se aprecia el modelo que se empleó para el diseño del modelo de encendido de leds RGB.

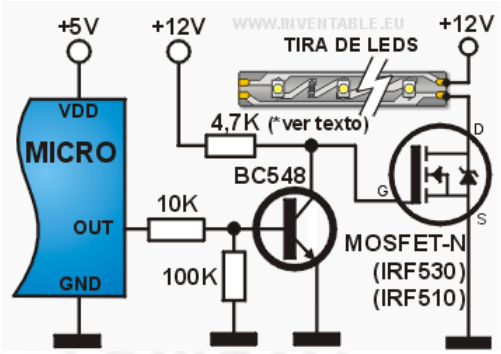

Figura 3.14 Circuito Activación de LEDs [29]

Fuente: www.inventable.eu

El parlante de 8Ω que emitirá los sonidos para reafirmar si el proceso de acceso es válido o no contará con un Mosfet de activación de canal N IRF 530. El circuito se activa en lógica alta y cuenta con una resistencia de protección de 10KΩ y otra de 620Ω para evitar un excesivo consumo de corriente en el pin PD3 del microcontrolador. Por medidas de protección del circuito debido a que el parlante puede generar corrientes de fuga, se consideró agregar un diodo de carrera libre 1N4004 entre los bornes del parlante. En la Figura 3.15 se puede apreciar los elementos utilizados representados por sus símbolos en el software de diseño de placas electrónicas.

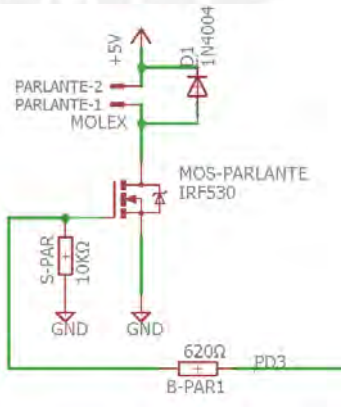

Figura 3.15 Circuito Activación parlante

Fuente: Propia

Para la etapa de recepción y envío de datos a la computadora se usaron 2 MAX485 que son los encargados de poder realizar la comunicación full dúplex entre el microcontrolador y la computadora por un principio de diferencia de voltaje. Esta etapa será detallada en el acondicionamiento de la señal enviada. En este caso el mismo circuito aplicado en la tarjeta de control será aplicado en el terminal de la computadora para poder conocer la información exacta que envió el microcontrolador y sin pérdidas de información importante. Se dispuso de LEDs SMD de color rojo y verde que permitirán saber si la comunicación serial que se está enviando se da de manera correcta entre ambos dispositivos. Se configuró uno como emisor y otro como receptor para que se pueda realizar la emisión y transmisión de datos de manera correcta. Esta información viajará a través de un cable de red y se dispondrán, según la Figura 3.16, en el conector RJ45 usando los pines 1 y 2 para la recepción y el 7 y 8 para transmisión, teniendo como tierra común el pin 5. Adicionalmente, añadieron unos jumpers en las líneas de comunicación en caso se desee verificar manualmente con una computadora si el envío de datos desde el microcontrolador se está haciendo de manera correcta y poder depurarlo en ese momento.

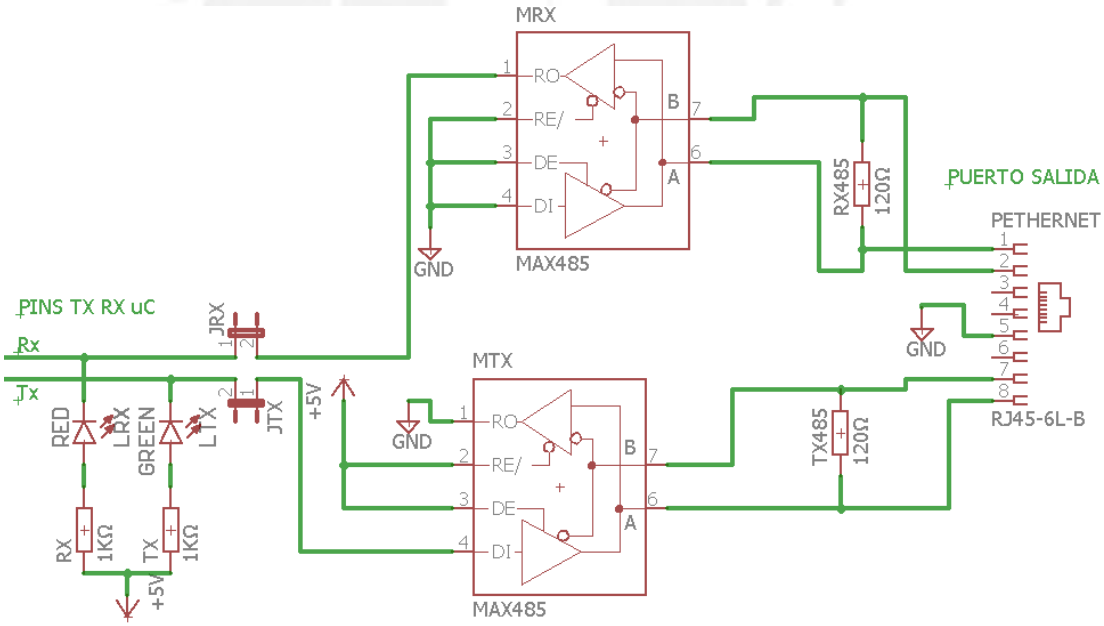

Figura3.16 Circuito de envío y detección de datos con la PC

Fuente: Propia.

VIII) Fuente de poder

Requerimientos: Dentro de los consumos de los bloques del sistema de acceso están incluidos todos los bloques menos el de potencia, que tiene un sistema de alimentación aparte y con protecciones a tierra, y el sistema PC que cuenta con su propia fuente de computadora próxima a ella. En ese sentido, se centrará el análisis en buscar fuentes disponibles en el mercado que sean capaces de suministrar la corriente que demanda el uso en conjunto de los bloques ya mencionados anteriormente.

La siguiente Tabla 3.8 muestra las corrientes consumidas por bloques considerando el funcionamiento correcto de cada etapa según las especificaciones de cada fabricante en su hoja de datos.

Tabla 3.8 Corriente consumida por bloque del sistema

Bloque	Voltaje	Corriente Consumida (mA)
Sensor (RFID MFRC 522)	3.3 V	163 mA
Control (ATMega328)	5V	18 mA
Circuito indicador (LEDs, Parlante)	Leds 12V Parlante 5V	1107 mA
Transmisión (Max 485)	5V	61.8 mA
Excitador	5V	31.5 mA
Total		1 443.3 mA

Fuente: Propia

Según la corriente total consumida por el sistema, se tomará una fuente de poder de 2.5 A capaz de poder suministrar la potencia a los circuitos previamente

establecidos. Además, esta debe ser capaz de entregar voltajes de 3.3 V, 5V y 12V para los circuitos diseñados en la etapa de control.

Se escogió la fuente real de 2.5 A de marca Thermaltake, ver Figura 3.17, que cumplen con los requisitos del sistema. Cuenta con las salidas de voltaje de 3.3, 5 y 12 V. El costo es de S/. 100.00 [30].

Especificaciones: Voltaje de Entrada: 115V/230 V ~, Corriente de entrada: 8A/4A, Frecuencia: 47Hz – 63 Hz

Figura 3.17 Fuente de poder Thermaltake 2.5 A

Fuente: www.himarkcomputers.com

IX) PC (Software)

Requerimientos: Para la creación de la plataforma virtual que permita gestionar los accesos vehiculares a la PUCP se tomó en cuenta que la información enviada por el puerto USB sea la que se encargue controlar los envíos de confirmación sobre el acceso del usuario. Es necesario que en la plataforma se pueda visualizar en tiempo real el estado de las entradas vehiculares y que se genere una lista de los accesos vehiculares, así como el usuario ingresante a una hora determinada. Esta interfaz debe ser entendible fácilmente para el personal de seguridad que esté monitoreando los accesos a la PUCP.

Esta PC debe contar con puertos USB accesibles y en correcto funcionamiento para poder programar los microcontroladores y recibir los datos provenientes de interfaz de comunicación. Así mismo, debe contar con la herramienta JDK de Java, que es capaz de ejecutar el programa descrito en lenguaje Java, por ello la tarjeta

de procesamiento RAM debe ser mayor a 2 GB para poder interactuar tanto con la cámara en streaming como el envío de datos hacia el controlador.

Diseño: Para el desarrollo de la plataforma se usó el entorno de desarrollo Netbeans a través del lenguaje de programación de JAVA en el cual se comenzó por crear un JFrame o ventana de diseño el cual está dividido en tres zonas. La primera es relacionada a los datos del usuario ingresante, de donde se extraerá de una base de datos ya creada la información relacionada al TAG RFID que se procesó en la etapa de control. En la base de datos, que en este caso fue creada en SQL Server se crearon 3 tablas relacionables entre sí. La primera tabla "Usuarios" contiene la información de los tags RFID disponibles y los datos del usuario (Código PUCP, nombres y apellidos). La segunda tabla "Vehiculos" se irán añadiendo registros cada vez que un usuario ingrese con un tag RFID y la base de datos esta creada para no repetir la misma placa de vehículo.

Con ello ya se tendrían registrados los usuarios y vehículos que están ingresando a la PUCP, pero es necesario conocer el detalle de los ingresos; es decir qué vehículo ingreso a tal hora y con qué usuario como conductor. Para ello, se creó la tabla "Ingresos" que registrará detalladamente los ingresos durante el día a la universidad y servirá para poder mostrarlo dentro de una lista histórica de ingresos que sería la segunda zona de la interfaz para el usuario final.

La tercera zona mostrará en tiempo real la cámara que detecta los vehículos que se acercan al módulo y es aquí donde se realiza el procesamiento de las imágenes por medio de la herramienta de OpenCV que es una librería en el cuál se pueden desarrollar programas para detección de objetos y en especial existen algoritmos que pueden detectar los caracteres de las placas vehiculares [31]. En esta etapa se captura uno de los fotogramas del vehículo ingresante durante el streaming de la cámara y se aplica un recorte al área de interés de la placa y es enviada a la aplicación openALPR para obtener, finalmente, la matrícula vehicular.

Finalmente, luego de verificar estos datos de ingreso y almacenarlos en la base de datos, se procede a enviar una señal serial "O" de ingreso correcto si el código RFID leído se encuentra en la base de datos. En caso contrario, se envía un caracter serial "F" para indicar que el acceso no le es permitido al usuario que desea ingresar a la universidad. Si existiera alguna falla en la placa procesada, el personal de seguridad tiene la opción de poder ingresar correctamente la placa vehicular manualmente y continuar con el proceso de ingreso.

A continuación, en la Figura 3.18 se mostrará el diagrama de flujo del proceso general que realiza el programa principal de control en Java y en la Figura 3.19 se detallará el diagrama de flujo del control del ATmega328 del bloque de control.

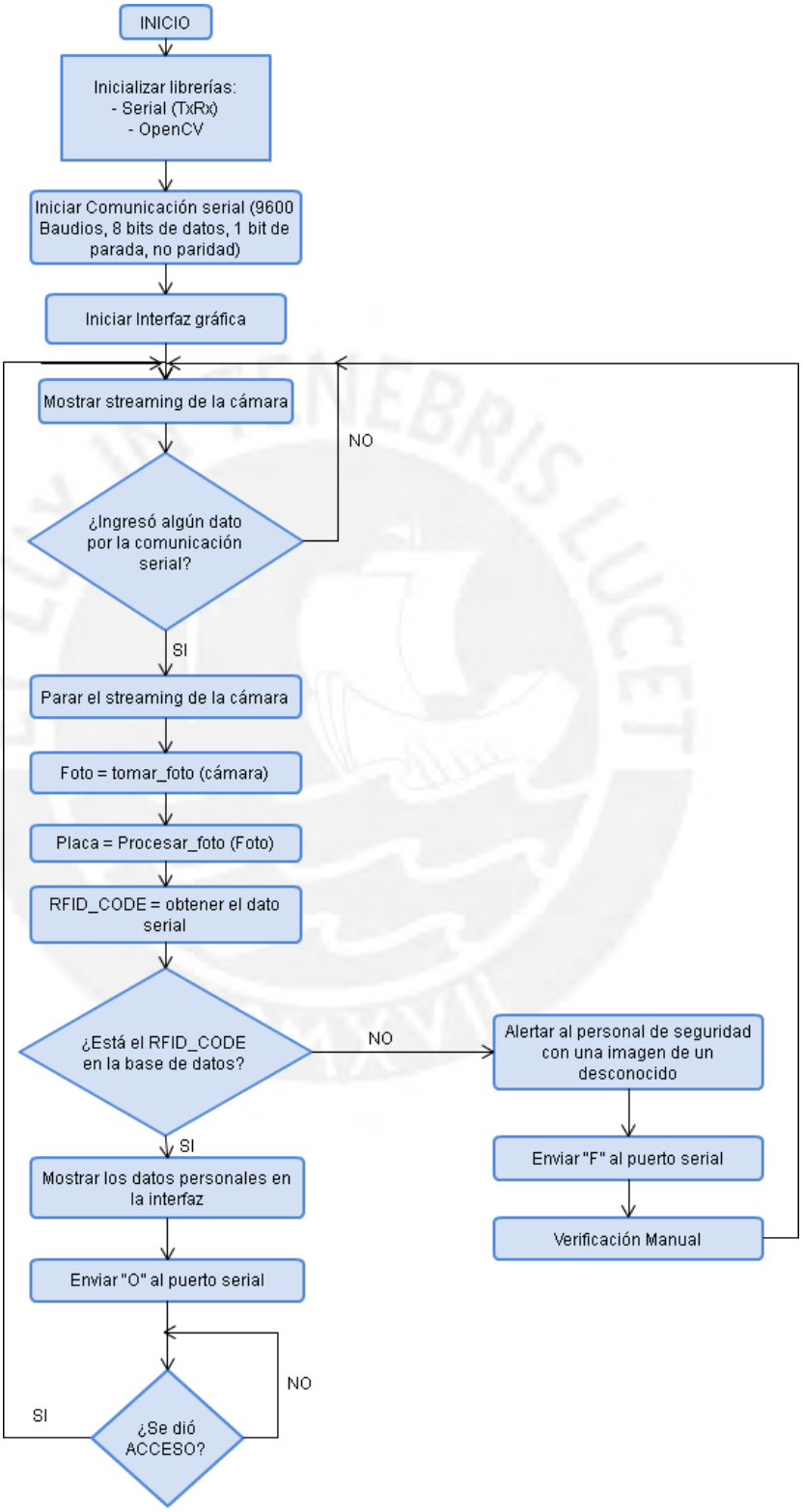

Figura 3.18 Diagrama de flujo Interfaz Java

Fuente: Propia

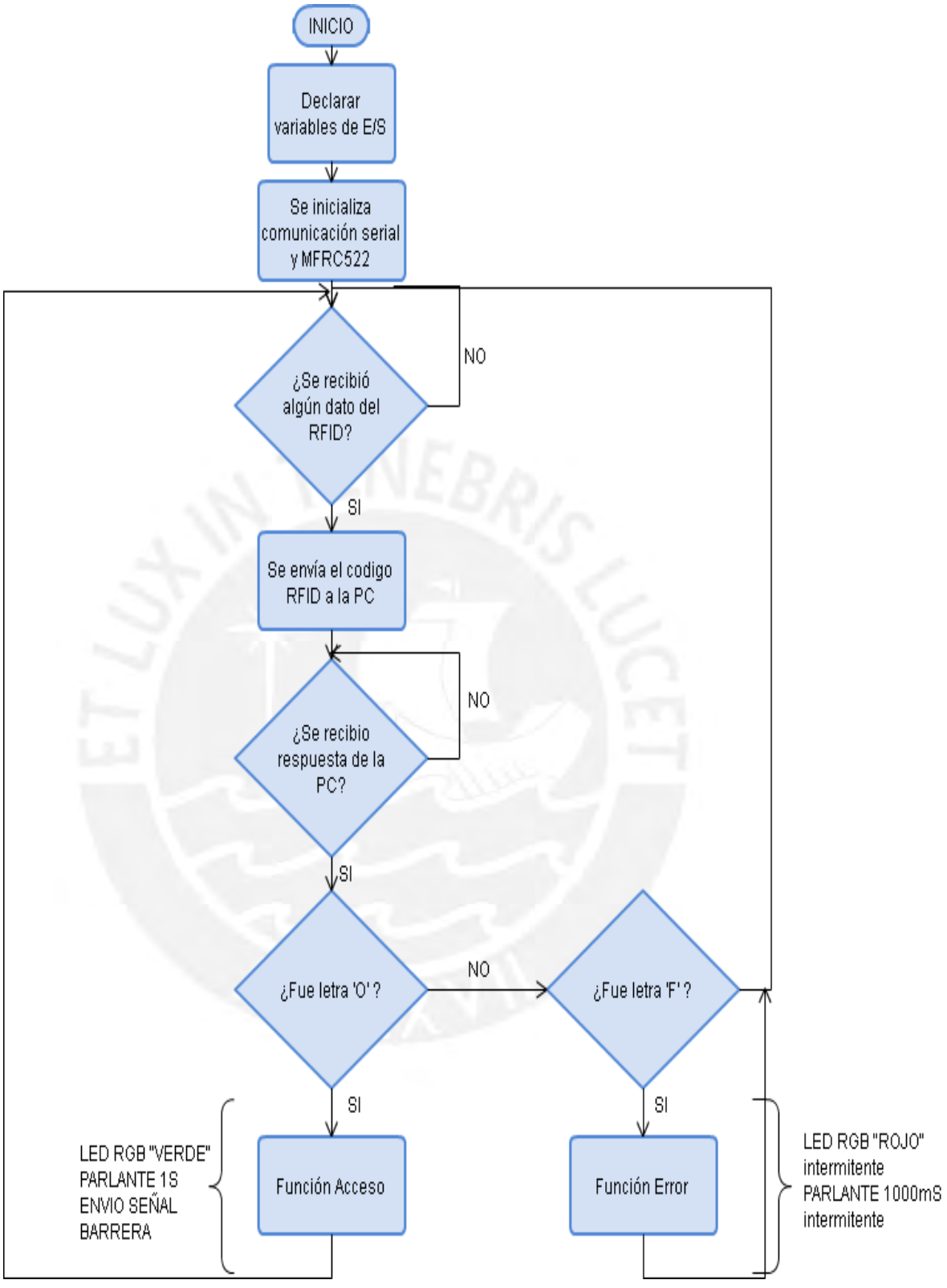

Figura 3.19 Diagrama de flujo ATmega328, bloque de control.

Fuente: propia

Capítulo 4

Ensayos y resultados

En el presente capítulo se detallarán las pruebas y/o ensayos realizados para la comprobación de los diferentes bloques del sistema de acceso vehicular, para finalmente hacer simulaciones de la interfaz final que se propone para el proyecto.

Dentro de los ensayos se consideran los siguientes:

- Pruebas RFID- ARDUINO

- Pruebas interfaz final y control de accesos (detección de placas vehiculares).

4.1 Prueba RFID-Arduino:

Se realizaron pruebas con el Hiperterminal de la PC para detectar los códigos de siete tags RFID a diferentes distancias del lector MFRC522. Se tomó una línea base de referencia de nivel 0cm y la base del lector a 0.5 cm de la línea base como se muestra en la Figura 4.1.

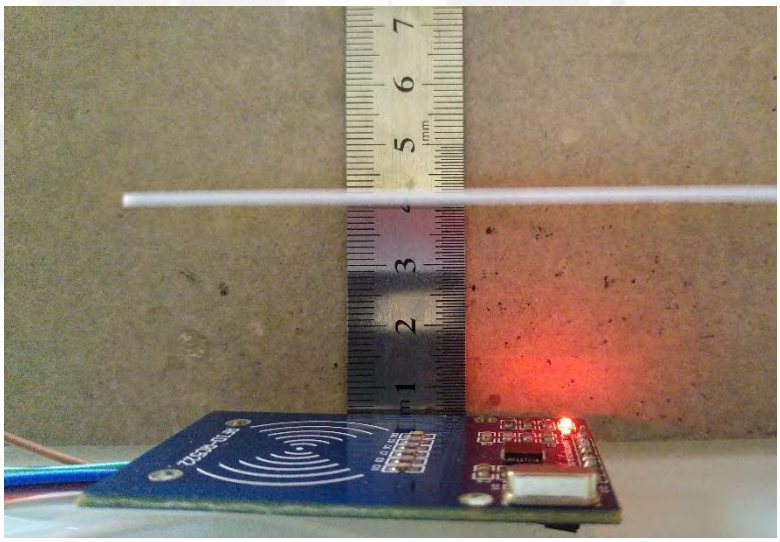

Figura 4.1 Entorno de prueba de lectura de tags RFID.

Se obtuvieron resultados similares realizados en cuatro pruebas con las mismas condiciones de lectura (ver Figura 4.2) y se obtuvo que el punto promedio de lectura recomendado de los tags RFID se encuentran entre los 3.5 cm y 4 cm entre la base del lector y el tag que se desee identificar.

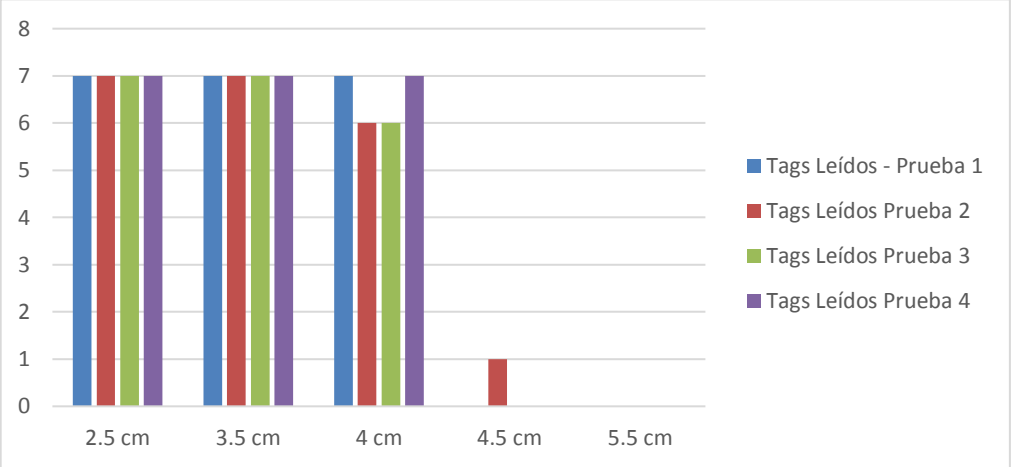

Figura 4.1 Estadística de pruebas de lectura de Tags RFID

Fuente: Propia

4.2 Prueba interfaz final y control de accesos

Finalmente usando la herramienta de desarrollo Netbeans y el lenguaje de programación Java, se ejecutaron 3 pruebas del programa final usando la tarjeta diseñada en la etapa de control y con la interfaz de comunicación mediante el protocolo RS485. Así mismo la posición de la cámara se dispuso según el protocolo propuesto en el capítulo 2, que proponía tener la cámara a una altura de 0.5 m del piso y a una distancia de alrededor de 4 m del vehículo considerando un ángulo de giro de la cámara de 20 a 30 grados con respecto al eje paralelo al vehículo. Se realizó pruebas de 66 a 70 vehículos ingresantes con 7 tags RFID que representaban a los usuarios ingresantes. En la Figura 4.3 se observan las estadísticas de las pruebas realizadas y se observa que el error promedio del reconocimiento de placas vehiculares se encuentra alrededor del 8% del total de pruebas realizadas.

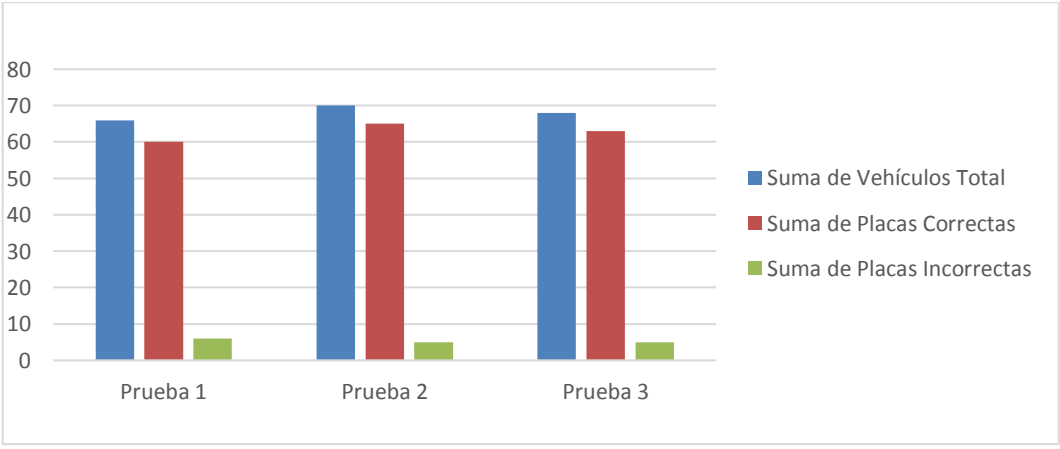

Figura 4.3 Estadística de pruebas de la plataforma con usuarios y vehículos.

CONCLUSIONES

Al realizar las pruebas de conexión y pruebas de la lectura de los tags RFID se observó que la distancia promedio para obtener una buena lectura debería estar entre los 3 a 4 cm de la base del lector MFRC522. Por lo tanto, cuando se elabore un módulo de ingreso para el lector de los tags, se debe tomar en cuenta que el lector debe estar lo más próximo posible a la superficie de lectura. Puede estar cubierto por una tapa de material acrílico o madera, ya que no afectan a la lectura de los tags.

Se concluyó que la aplicación de detección de placas vehiculares openALPR presenta fallas cuando el ángulo focal de la cámara con respecto al carro supera los 30 grados y que existen equivocaciones con placas que contienen letras como “Y” o “Q” que son reconocidas como “V “y “O” respectivamente. Por ello, la posición establecida de la cámara no debe tener un ángulo mayor a 30 grados respecto al vehículo ingresante.

El uso de los leds y parlantes son útiles para dar a conocer el ingreso de los usuarios de manera automática. Esto permite que los procesos de ingreso sean manejados desde una caseta de control por el personal de seguridad sin que se estén realizando verificaciones presenciales de los usuarios ingresantes a la PUCP.

Finalmente, estos diseños serán útiles cuando se proponga realizar una mejora del sistema de acceso vehicular actual, ya que han sido previamente simulados y puestos en pruebas física respondiendo correctamente ante distintos escenarios. Con este trabajo de fin de carrera se busca incentivar y proponer una mejora en los procesos de ingreso a la universidad y que estos puedan ser replicados en algún futuro momento en las instalaciones de la PUCP.

RECOMENDACIONES

- Una alternativa para poder controlar la etapa de potencia, que consta en liberar la barrera vehicular para concluir el ingreso vehicular, se puede dar por medio de una transmisión inalámbrica. En esta alternativa se debería contar con un transmisor que recibe la señal de la PC y un dispositivo receptor inalámbrico que reciba la señal proveniente de la etapa del software de control. Para ello, también sería necesario incluir un procesador que reciba esta señal inalámbrica que podría realizarse adicionando otro Atmega328 a la parte receptora para que procese las señales de apertura de la barrera vehicular.
- El uso de tags RFID activos permiten tener un mayor rango de lectura y por ello se recomendaría poder adquirir un tag activo junto a un lector de su misma frecuencia de funcionamiento para poder obtener lecturas desde un punto más lejano o incluso poder adicionar este tag al vehículo ingresante que se convertiría en una variable más del sistema para el monitoreo de los accesos vehiculares.
- El uso de plataformas web en el campo de programación permitiría obtener una plataforma con una mejor experiencia de usuario y también llevaría a que toda la información de los accesos se encuentre monitoreada desde la red de la PUCP. Por ello, la migración de este diseño hacia una red sería un punto importante a tratar en una posterior implementación.
- Finalmente, desde el punto de vista del software, se recomienda poder realizar un manejo de la información proveniente de las entradas vehiculares, como por ejemplo reportes de cuantos vehículos ingresan en intervalos de tiempo, conocer la demanda del parqueo vehicular, entre otros reportes de explotación de información. Por ello, si se dispondría de la base de datos de la universidad sería posible tener mayores datos estadísticos y mejorar la seguridad del campus universitario.

BIBLIOGRAFÍA

[1] GS1 PERU
2011 Estacionamientos automatizados con RFID
[en línea][consultado 18/03/16]
<http://innovasupplychain.pe/articulos/1136-estacionamientos-automatizados-con-rfid>

[2] Instituto de Defensa Legal (IDL). (2015). "Seguridad Ciudadana: Informe Anual 2015" pp. 19-23. Recuperado de: http://www.idl.org.pe/%C3%A1rea/seguridad-ciudadana

[3] Descubre PUCP
2013 Estacionamientos
[en linea][consultado 10/04/16]
<http://descubre.pucp.edu.pe/poi/index/filtro/estacionamientos>

[4] Ley N° 29461. Diario Oficial El Peruano, Lima, Perú, 27 de noviembre de 2009.

[5] IntellisoftPaarking
2013 PRODUCTOS - SKIDATA
[en línea] [consultado 15/04/2016]
<http://www.intellisoftparking.com/cms/index.php/productos/skidata>

[6] LOS PORTALES
2015 Estacionamientos
[en línea] [consultado 20/04/2016]
<http://www.losportales.com.pe/estacionamientos>

[7] IDgalimi S.A
2013 Componentes para control de accesos
[en línea] [consultado 15/04/2016]
http://www.idgalimi.com.ar/componentes-para-control-de-accesos.html

[8] 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.

[9] SIASA
2011 Productos-biometría
[en línea] [consultado 17/04/2016]
< http://www.siasa.com/biometria.php>

[10] DOINTECH
2015 Control de Acceso vehicular
[en línea] [consultado 17/04/2016]
http://www.dointech.com.co/control-acceso-vehicular.html#biometrico

[11] SIASA
2011 Productos
[en línea] [consultado 17/04/2016]
http://www.siasa.com/producto.php?prod=0100059

[12] Smowl
2016 Tech
[en línea] [consultado 20/04/2016]
http://smowltech.com/es/technology

[13] Certicámara
2012 Biometría de reconocimiento de voz, rostro y de iris.
[en línea] [consultado 21/04/2016]
https://web.certicamara.com/media/49428/certivoz-rostroiris.pdf

[14] José Delgado. (2010). Reconocimiento de placas vehiculares. Tesis de maestría en Ciencias de Ingeniería Mecatrónica. Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional. México.

[15] SKIDATA
2016 Parking Management
[en línea][consultado 16/04/2016]
http://www.skidata.com/en/parking-management/barrierscolumns/barrier-system-barriergate.html

[16] DONOSTI
2016 Parking Solutions
[en línea][consultado 15/05/2017]
http://www.donostiperu.com/parking_solutions.html
[17] Iberwave Ingeniería
2008 RFID
[en línea][consultado 18/04/2016]
http://www.iberwave.com/tiposdesistemas.html
[18] Enzocard
2009 Concepto RFID
[en línea][consultado 10/04/2016]
http://blog.enzocard.eu/2012/09/28/principales-modelos-rfid/
[19] E. M. Microelectronic
2002 EM4102 – Read Only Contactless Identification Device
[en línea][consultado 11/04/2016]
http://www.nesweb.ch/downloads/X400RFID.pdf
[20] Atmel
2014 ATA5577C – Read/Write LF RFID IDIC 100 to 150 kHz
[en línea][consultado 11/04/2016]
http://www.atmel.com/images/Atmel-9187-RFID-ATA5577C_Datasheet.pdf
[21] N. X. P. Semiconductors
2016 MFRC522 Standard performance MIFARE and NTAG frontend
[en línea][consultado 11/04/2016]
https://www.nxp.com/documents/data_sheet/MFRC522.pdf
[22] D-Link
2014 Soluciones Empresariales
[en línea][consultado 11/05/2016]
http://www.dlinkla.com/dcs-3715
[23] LiftMaster Professional
2007 Mega Arm Gate Operator
[en línea][consultado 12/02/2017]
http://www.gatedepot.com/get_manual_file/37622/
[24] OMRON
2012 Solid State Relay G3MB
[en línea][consultado 20/02/2017]
http://datasheet.octopart.com/G3MB-202PEG-4-DC20MA-Omron-datasheet-111010.pdf
[25] Sparkfun
2011 Shop – Products – Led Basic Green 5mm
[en línea][consultado 12/06/2017]
https://www.sparkfun.com/products/9592
[26] National Instruments
2011 Notas técnicas
[en línea][consultado 08/03/2017]
http://digital.ni.com/public.nsf/allkb/2CABB3FD5CAF2F8686256F1D005AD0CD
[27] Maxim Integrated
2016 Interface Circuits
[en línea][consultado 23/04/2017]
https://www.maximintegrated.com/en/app-notes/index.mvp/id/367
[28] FTDI Chip
2014 FT232R
[en línea][consultado 04/05/2016]
http://www.ftdichip.com/Products/ICs/FT232R.htm

[29] Inventable
2015 Guía - Mosfet
[en línea][consultado 10/05/2016]
https://www.inventable.eu/como-conectar-un-mosfet-a-un-microcontrolador/
[30] MercadoLibre Perú
2016 Fuente de Poder
[en línea][consultado 20/05/2016]
http://articulo.mercadolibre.com.pe/MPE-419897541-fuente-de-poder-thermaltake-de-450w-reales- JM
[31] OpenCV
2016 OpenCV
[en línea][consultado 08/05/2016]
http://opencv.org/