UNIVERSIDAD TÉCNICA FEDERICO SANTA MARIA

DEPARTAMENTO DE ELECTRÓNICA

VALPARAÍSO – CHILE

“SOLUCIONES PARA MEJORAR LA PERCEPCIÓN DE SEGURIDAD EN PROYECTOS HABITACIONALES DE ALTA ENVERGADURA”

HEINRICH KARL REINKING ESTAY

MEMORIA DE TITULACIÓN PARA OPTAR AL TÍTULO DE INGENIERO CIVIL ELECTRÓNICO MENCIÓN COMPUTADORES

PROFESOR GUÍA: DANIEL ERRAZ L.

PROFESOR CORREFERENTE: MARCOS ZUÑIGA B.

MARZO - 2017

Dedicatoria

En agradecimiento a mis padres Carlos Reinking V. y María Nelly Estay por convertirme en lo que soy, tanto en mi educación académica como en la vida, por su incondicional apoyo a lo largo de toda mi existencia y por nunca perder la fe en mí.

Han sido y seguirán siendo un pilar fundamental y nada de esto hubiese sido posible sin ustedes. Además de mis agradecimientos, les debo la vida.

Con amor, su hijo.

Agradecimientos

Primero que todo agradezco a mis padres por todo el apoyo brindado durante toda mi carrera, por financiarme todos mis estudios y estar conmigo hasta en las últimas instancias.

Agradezco a mi Profesor Guía Daniel Erraz por brindarme todo el apoyo emocional, intelectual, técnico y pedagógico; como también por la paciencia, los conocimientos y por estar ahí siempre que lo necesité a lo largo de todo este trayecto y nunca perder la fuerza ni la esperanza.

También agradecer a el Centro Integrado de Aprendizaje en Ciencias Básicas CIAC por facilitar las dependencias y materiales para el desarrollo del prototipo funcional del proyecto.

Además, agradecer a mi compañera de equipo Macarena Gallardo por su paciencia, amistad y sus conocimientos, los cuales son responsables de haber logrado completar y concretar este proyecto.

Por último, agradecer a aquellos que me han acompañado en el transcurso de mi carrera universitaria y que se han mantenido fuertes y leales como hermanos; su amistad y compañía fueron claves para conseguir terminar mi carrera universitaria.

Resumen

Hoy en día, se vive inmerso en una sociedad resignada a la delincuencia, al temor y a la necesidad de protegerse. Con el pasar de los años, las fuerzas policiales han ido perdiendo territorio, mientras que los victimarios aumentan.

Por otra parte, existe una sobre oferta en la industria inmobiliaria, debido a que se han generado proyectos apuntados al mismo segmento de mercado. He ahí donde nace la necesidad de diferenciarse entre ellos para poder acaparar la clientela y nada mejor para ello que acudir al uso de la tecnología.

En base a los dos enfoques señalados, se propone el desafío de diseñar una solución que permita la distinción del cliente por medio de la percepción de seguridad. Para esto se genera un sistema de seguridad inalámbrico compuesto por dos directrices: Servidor y Aplicación/Cliente. La aplicación permitirá el control de los accesos al recinto – tales como puertas, ascensores, portón del estacionamiento – dándole así al usuario poder de abrir puertas o portones por medio de su *Smartphone.*

Por otra parte, el Servidor genera una base de datos de todos los habitantes, visitas y trabajadores del recinto, en donde se ingresan los datos de su cédula de identidad a través de la lectura del código QR, el departamento y piso en donde vive o visita, y la *Bluetooth MAC Address*. La base de datos generada ha de ser completada por el encargado de la vigilancia del *Lobby* del edificio.

Luego, solo los usuarios que se encuentren registrados en la base de datos podrán hacer uso de la aplicación; el pedido del ascensor a través de la aplicación será solamente al primer piso o *Lobby* y hacia el piso que esté registrado el usuario.

En vista y considerando que el proyecto se generó en el marco de Memorias Multidisciplinarias, el desafío se elaboró en equipo. Es por esto que la temática se abordará bajo las perspectivas de Cliente y Servidor.

El presente documento refiere a todo lo que es el desarrollo e implementación del Servidor del sistema de seguridad.

Abstract

Now a day, we live in a society who has surrender himself to delinquency, fear and necessity to protect themselves. Years go by, the police enforcements have been losing fighting ground, meanwhile the criminals gain more and more.

In a different topic, the real estate has experience an exponential growth at the point of glut, due to numerous projects pointing the same market segment. Here appears the need to differentiate from each other, so they can hoard the customers, and nothing fits better than incorporating cutting edge technology to their projects.

Based on the previous points, it arises the challenge to designed a solution that allows the distinction of the client through security perception. To approach this, we created a wireless security system build by two guidelines: Server and Client/Application. The Application runs over Android Smartphones, and allows the user to control the different access to the building – such as parking lot gateway, Lobby access door, elevator control – through their devices. Regarding to the Server, it generates a data base of all the inhabitants, visitors and workers of the compound, based on the QR from their Identification Document, the department's number in which they live or are visiting, and the Bluetooth MAC Address of the device previously paired to the system. The data base filled up lays on the person in charge of the building's access. There by, only the users that have been registered into the data base can use the Smartphone Application; either way the user can request the elevator only to the floor they have been register on or the ground level.

The project has been built under de new Multidisciplinary Program, which is why the thematic will be approach by two angles: Server and Client.

This document refers to the development and elaboration of the Security System's Server.

Glosario

Bluetooth MAC Address	Identificador único de cada dispositivo, compuesto de 12 caracteres hexadecimales.
NFC	Near Field Communication.
Half-Duplex	El mismo canal es utilizado para transmitir y recibir.
SSL	Secure Socket Layer, protocolo criptográfico que proporciona seguridad en redes informáticas.
RFID	Radio Frecuency Identification (Identificación por radio frecuencia).
Contactless	Tipo de tecnología la cual permite utilizar credenciales de seguridad sin la necesidad de presentarlas o hacer contacto en identificadores.
GUI	Graphical User Interface, Interfaz Gráfica de Usuario.
CCTV	Closed Circuit Television.
DVR	Digital Video Recorder: es una computadora especializada en capturar y almacenar video digital
Ataque Middle-Man	Tipo de ataque informático en donde un tercero adquiere la capacidad de leer, insertar y modificar el flujo de información entre dos partes.
Red PAND **(1)**	Private Area Network Daemon, es una red tipo demonio que permite a los usuarios verse entre sí, pero son invisibles a agentes externos.
CPU	Central Process Unit, Unidad del dispositivo encargado de tomar entradas y procesarlos.
Emparejamiento	Proceso en el cual dos dispositivos se interconectan mediante un código aleatorio que ambas partes deben aceptar.
mySQL	Sistema de control y gestión de base de datos
RFCOMM	Radio Frequency Communication (Comunicación por radio frecuencia)
Adhoc	Red de comunicación entre 2 usuarios sin la participación de un enrutador o *switch*
BR/EDR	Bit Rate/Enhanced Data Rate, tipo de transmisión en donde se hace el mayor esfuerzo (gasto energético) en conseguir que la tasa de transferencia se mantenga alta.
Streaming	Transmisión digital de contenido multimedia.
Broadcast	Un emisor transmite información a múltiples receptores.
Hash	Función que convierte los datos en números binarios o hexadecimales, de tal manera que si se inserta el mismo dato se convierte en el mismo número, pero prácticamente imposible a base del número obtener el dato
superusuario	Usuario con privilegios de editar cualquier archivo del sistema, incluso si son parte del registro de arranque o si son de vital importancia.
Open Source	Tipo de código que forman parte del dominio público bajo licencia Open Source Definition
APK	Aplicación empaquetada de Android, archivo comprimido para la instalación de una aplicación en Smartphone Android

Tabla de Contenido

Tabla de Ilustraciones

Marco General del Proyecto

1. Análisis del desafío y alternativas de problemas específicos a resolver

El desafío consiste en implementar un sistema de seguridad en edificios de más de 100 departamentos. En la actualidad existe una amplia gama de sistemas, los cuales varían tanto en torno a su complejidad como a su costo de implementación. Pero en el desafío propuesto, se solicita uno "no invasivo", lo cual acota las medidas a implementar.

De acuerdo a lo conversado con el cliente, el término "no invasivo" va enfocado a la retención de la visita o residente por periodos prolongados (más allá del agrado de este). Al hablar de edificios de más de 100 departamentos, implica un alto flujo de personas diario que se traduce en nueva información todos los días. También señala que, de acuerdo a la experiencia de la inmobiliaria, se sabe que, en los sistemas de seguridad hasta la fecha implementados, la causa común de falla o fracaso ha sido el vigilante. Esto se debe a que en el perfil de contrato no se busca a un experto en programación o redes de computadores, sino que alguien que haga presencia en el *Lobby* del edificio. Cabe destacar que buscar un trabajador que tenga conocimientos avanzados de redes difícilmente estaría de acuerdo en tomar el trabajo a no ser por un sueldo considerable.

Luego, el desafío se plantea como un sistema de seguridad difícil de vulnerar, que no sea invasivo y que sea capaz de controlar altos flujos de personas, las cuales pasarán a ser un problema a resolver, tanto de manera individual como al juntarlas.

En base a lo planteado, inicialmente se debe buscar aquellas modalidades de sistemas que cumplan una relación beneficio vs costo favorable para ser instada. Se deben generar requerimientos básicos y asegurarse que el modelo de seguridad propuesto cumpla con ellas. Adicionalmente, se debe determinar si la solución es viable de implementar en los espacios definidos y con la discreción necesaria. Por último, generar e implementar una versión preliminar y probarla.

2. Definición del problema

Se requiere un sistema de seguridad robusto, vale decir, difícil de vulnerar. La principal amenaza consiste en el vigilante. Históricamente, los sistemas de seguridad activos - siendo activo a todos aquellos sistemas que no pasan desapercibidos e impiden el paso de aquel que no tenga autorización - más comunes han sido vulnerados debido a irresponsabilidad de los usuarios o del vigilante. Este fenómeno ocurre en dos situaciones: Los sistemas son controlados por una persona por medio de un interruptor maestro, o son automáticos - operan de manera autónoma - pero des activables por el personal, con lo que se deja a juicio si utilizar o no el sistema.

Luego, los sistemas no invasivos más comunes y populares son fáciles de vulnerar. Tómese como ejemplo un sistema en que la persona deba autentificarse al ingreso de manera voluntaria: si la persona tiene malas intenciones y quiere eludir este control, basta con buscar las circunstancias adecuadas.

Por otro lado, los sistemas invasivos - aquellos que retienen a la persona por un tiempo considerable - tienden a ser deshabilitados por el cliente al poco tiempo de implementarlos, dado que, si por ejemplo se implementa un sistema por retención -como las barras de acceso tipo molinete – y se presenta un usuario con discapacidad o simplemente un adulto mayor que desconoce cómo utilizar el sistema, estos se verían impedidos a ingresar al recinto lo que nuevamente recae en otorgarles a los vigilantes el poder de decidir quién entra y quién no.

En consecuencia, si el sistema no cumple con los requisitos planteados, de alguna u otra manera el usuario buscará maneras de eludirlo o sabotearlo, lo que conllevará al cliente a deshabilitar el sistema y volver a lo antiguo.

3. Soluciones Existentes / Estado del Arte

En el mundo de la seguridad, existe una amplia gama de soluciones las cuales varían de acuerdo a su precisión, robustez, percepción de seguridad, eficiencia energética, eficacia y cuan invasivo sea, cuyos valores varían dependiendo del nivel exigido para cada uno de estos. En la actualidad, se han implementado una gran diversidad de sistemas de seguridad, los cuales se analizarán como *Inputs* y *Outputs*, los cuales serán definidos más adelante.

3.1 Inputs

3.1.1 Teclado Numérico

Los sistemas de seguridad por código son de los más populares y económicos del mercado. A grandes rasgos, cada usuario maneja su propio código: para activar el sistema, ingresa su código y obtiene el acceso. Este tipo de sistema es poco invasivo y es capaz de controlar flujos moderados de personas. Su implementación va desde solo control de acceso hasta nivel de privilegios. Este último le entrega al usuario una restricción de movimiento dentro del recinto, permitiéndole acceder a determinados sectores, como también negarles acceso a otras.

La ventaja que posee este sistema es la simplicidad para el usuario: no requiere portar ningún objeto adicional, requiere pocos conocimientos previos para su uso y en su gran mayoría un individuo es capaz de memorizar entre 4 a 8 dígitos.

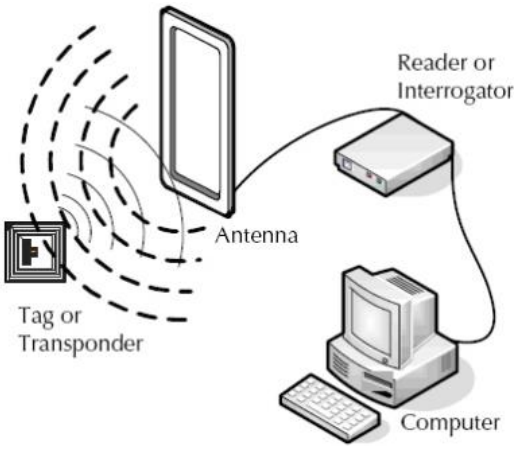
Por otra parte, la vulnerabilidad de del sistema recae en la autentificación de usuario. No hay ningún tipo de procedimiento que permita al sistema saber si la persona que está ingresando el código es el legítimo dueño o no. Si un usuario revela de manera voluntaria o involuntaria su código de seguridad, obtendrá todos los beneficios y restricciones de aquel código, vulnerando así la seguridad del edificio.

En la actualidad, el teclado numérico está siendo utilizado de forma complementaria con otros sistemas: la mayoría de las empresas de seguridad privada ofrecen la activación y desactivación del sistema por medio de un código, pero el sistema en si está gobernada por un micro controlador que se programa y configura en respuesta sensores – tanto de proximidad como de laser – de tal forma que, si un intruso cruza el perímetro, se activa una respuesta, como una sirena, aviso a la empresa o policía.

3.1.2 RFID (2)

La identificación por radio-frecuencia es un sistema que puede ser visto como “un código de barra inalámbrico”. Un RFID *tag* - etiqueta RFID - es un pequeño chip con una antena que emite un número único de identificación, el cual solo puede ser leído por un Lector RFID.Existen dos tipos de etiquetas RFID, las pasivas y las activas, teniendo cada cual sus ventajas y desventajas.

Los RFID pasivos operan en el rango de frecuencias de hasta 960 [MHz] y funcionan por inducción de energía emitida desde el lector, lo cual disminuye significativamente su valor de adquisición, pero a su vez una menor distancia de operación.



Los RFID activos usan una fuente de poder dedicada para emitir una señal con su código de identificación, operan en el rango de frecuencia de los 433[MHz] hasta los 5,8[GHz], por lo cual le permite un mayor rango operación (3,3 metros). La desventaja que presentan los sistemas activos a los pasivos son el precio de adquisición y el mantenimiento de la fuente de alimentación - por lo general baterías - y, por otro lado, la desventaja de los pasivos frente a los activos son que están sujeto a perturbaciones debido al rango de frecuencia en la que operan, por lo que generalmente funcionan estando casi en contacto con el lector RFID.

Los sistemas de seguridad por RFID están en su apogeo, encontrándose en la actualidad como uno de los más económicos y eficientes. La desventaja de este sistema frente a otros, es que al ser una antena emitiendo una señal, muchos investigadores afirman que es factible vulnerar estos sistemas. En particular, investigadores de la Universidad Johns Hopkins consiguieron penetrar al RFID Digital Signature Transponder de Texas Instruments (3).

Para ensamblar el sistema, se utiliza un dispositivo – generalmente un micro controlador - hacia un terminal de lectura RFID. En el dispositivo se crea un programa que gestione los códigos RFID de los usuarios – por lo general se asocian a una base de datos – pudiendo así incorporar usuarios al sistema.

Otra forma de implementarlo, es a través de un micro computador – como Raspberry Pi – y aprovechar los GPIO para generar una respuesta del sistema en base a las lecturas de los códigos RFID. De esta forma, se pueden conectar hacia cerraduras electrónicas o actuadores, y, dependiendo de los privilegios que tenga el usuario, permitirle o restringirles el acceso a diversas secciones del recinto. La particular ventaja de utilizar RFID activo, es que los usuarios no requieren establecer un contacto físico con el lector, sino que solo portarlo; de esta manera, el usuario pasa a tener un radio de activación – podría llamarse un aura – que lo rodea y que active el sistema.

3.1.3 NFC (4)

Tecnología de comunicación inalámbrica de corto alcance y alta frecuencia que permite el intercambio de datos. Opera en la banda de frecuencia de los 13.56 [MHz] y su tasa de transferencia puede alcanzar los 424 [Kbits/s], por lo que es utilizada para comunicaciones instantáneas, es decir, para identificación y validación.

La ventaja es que su uso es transparente - el usuario no percibe los procesos internos - por lo que pasa desapercibido, *Half-Duplex*, las transmisiones pueden utilizar encriptaciones de seguridad como SSL y al trabajar con distancias reducidas hace que sea difícil que un dispositivo interfiera la comunicación.

Como desventaja es que su tecnología no permite distancias mayores a los 20 [cm] lo que la categoriza en los medios de corto alcance.

La tecnología NFC utiliza dos modos para establecer la comunicación:

- Modo pasivo: el dispositivo emisor genera una señal modulada y el dispositivo receptor es excitado por esta señal, de donde obtiene la energía para operar.
- Modo activo: tanto el dispositivo emisor como receptor se comunican generando su propia señal, por lo que ambos necesitan una fuente de alimentación para funcionar.

Los celulares inteligentes o Smartphone con NFC pueden operar en modo de emulación NFC card, el cual permite al dispositivo actuar como una Smartcard. Las Smartcard son circuitos electrónicos de pequeñas dimensiones empotrados en dispositivos portátiles – por lo general en tarjetas o credenciales – los cuales son construidos con propósitos exclusivos, por lo general con fines de seguridad.

Ambas tecnologías – RFID y NFC – operan a base de ondas de radio frecuencia, pero NFC opera a campo cercano. En base a esto, se puede hacer una implementación similar a la de RFID, conectando un lector NFC en un terminal de un dispositivo – micro controlador, computador o micro computador – y almacenar los códigos identificadores NFC en una base de datos; de esta manera se les puede conceder o denegar acceso a secciones del recinto a los usuarios.

3.1.4 Huella Dactilar (5)

La identificación por huella dactilar es una de las biométricas más conocidas. Gracias a su unicidad y constancia en el tiempo, las huellas dactilares han sido usada para autentificar individuos desde hace ya muchos años.

El sistema electrónico captador de huellas está compuesto por una variedad de tipos de sensores ópticos, capacitivos, ultrasónicos y térmicos, los cuales son utilizados para tomar la información de imágenes digitales de la superficie de una huella dactilar. Existen diversas técnicas de coincidencia de huellas basadas en minucias o patrones: La coincidencia de patrones compara dos imágenes para ver qué tan similares son, mientras que las basadas en minucias comparan específicamente la ubicación y dirección de cada punto

Algunos inconvenientes es que existen usuarios que puedan rechazar la biometría en su conjunto, viéndola como una invasión a la privacidad. Además, los dispositivos que capturan la huella requieren de un constante mantenimiento, dado a que permanentemente está en contacto dedos, las cuales por lo general están sucios, sudorosos o simplemente con grasa por sudoración.

El uso de la huella digital se ha expandido de tal forma, en que se incorpora en dispositivos como Computadores Portátiles o Smartphones. La primera empresa de fabricación de teléfonos inteligentes en incorporar la lectura de huella digital fue Apple, la cual integró en el botón de inicio una lectura a base de patrones de la huella dactilar. Después de eso, las otras marcas lo han incorporado como estándar.

Pero existen detractores al uso de la huella, que afirman que más que seguridad aportan vulnerabilidad. Se han conocido casos que afirman que en menos de 5 minutos se ha conseguido vulnerar el sistema (6) – esto es contando con el consentimiento del usuario, vale decir su huella – pero afirman que reconstruyendo la huella a base de residuos en diversas partes, se puede ensamblar un dedo con la huella del usuario a través de una impresora 3D.

3.1.5 Banda magnética (7)

La primera persona en adherir la banda magnética a una tarjeta plástica fue el ingeniero Forrest Parry de la IBM en la década de los 60'. La banda está compuesta por una delgada película de partículas fierro-magnéticas. Opera de forma similar a la banda del casete: se puede escribir en la banda debido a que los pequeños imanes son polarizados en dirección Norte o Sur, pudiéndose traducirse así en números. (8)

Es uno de sistemas de acceso más utilizados. La banda contiene toda la información que necesita el sistema para poder autentificar al usuario. Para su implementación es necesario contar con la tarjeta y un lector de banda magnética. Es fundamental que mientras se desliza la tarjeta a través del lector debe permanecer en contacto durante toda la lectura; no se requiere una velocidad constante.

La desventaja de utilizar este sistema es la escasa implementación de métodos de criptografía, lo cual las vuelven vulnerables a la clonación. Además, se conocen diversos casos en que la información contenida en la banda magnética ha sido eliminada debido al campo magnético emitido del Smartphone (9).

Dada su simplicidad de uso y lo bien que ha sido adoptada por los usuarios, en lugar de reemplazar el sistema, se han buscado formas de fortalecerlo. Una de ellas ha sido la codificación por coercitividad de la información contenida en ellas (10). La coercitividad consiste en cuan intenso tiene que ser campo magnético para afectar la información codificada. Esta se mide en *Oersteds* y señalan que tan difícil es codificar la información. Se dividen en dos tipos:

- HiCo: Abreviación de *High Coercivity* – Alta Coercitividad – y provee el nivel más alto de inmunidad al daño por campos estáticos. Las bandas HiCo son ligeramente más caras que las LoCo, debido a que se requiere mayor potencia para vulnerarlas.
- LoCo: Abreviación de *Low Coercivity* – Baja Coercitividad – es más sencilla de implementar, pero más fácil de vulnerar que HiCo.

La mejor manera para distinguirlas entre ellas es por el color: Las HiCo son de banda negra, mientras que las LoCo son de un café claro.

Otro término utilizado a menudo es el de *Struipe-up* y *Stripe-down*. *Stripe-up* significa que la banda magnética se encuentra al frente de la tarjeta y *Stripe-down* por detrás. Esta información es relevante a la hora de utilizar la impresora, ya que la codificación para ambas es distinta

3.1.6 Reconocimiento Facial (11)

El Sistema de reconocimiento facial tiene la ventaja de ser un método no intrusivo, es decir, los datos pueden ser obtenidos incluso sin que el sujeto se percate de ello. Este sistema tiene las dificultades de reconocimiento cuando la variación entre las imágenes de distintos sujetos es muy pequeña o cuando la variación entre imágenes de una misma persona es muy amplia; esto puede ser provocado e intensificado cuando dichas imágenes hayan sido adquiridas en diferentes condiciones ya sea de iluminación, posición o calidad. Otra dificultad del reconocimiento facial es la base de datos. Esta debe ser implementada en condiciones equivalentes para todos los individuos y con cada nuevo usuario ésta aumenta, lo que implica un aumento en el procesamiento computacional. Además, a largo plazo los rasgos faciales varían, por lo que la implementación del algoritmo de reconocimiento se vuelve más complejo, ya que debe interpretar el paso de los años.

Como sistema de seguridad en edificios se trabaja con cámaras y con un software de detección de rostros. Opera en dos modalidades: por identificación y por verificación

El modo de identificación compara el rostro capturado a través de las cámaras con una serie de imágenes guardadas en la base de datos. Por el contrario, el modo de verificación compara la imagen o rostro capturado por la cámara de la persona que haya utilizado algún tipo de identificador de identidad para el acceso a través de un torniquete o puerta electrónica con la foto del titular del identificador.

El funcionamiento como sistema de seguridad para acceso sigue los siguientes pasos:

- Obtención de la imagen: el sistema a través de cámaras detecta un rostro y captura la imagen.
- Escala el rostro: determina el tamaño del rostro en la imagen y la escala al tamaño y posición predeterminados para procesar.
- Procesa la imagen: una vez obtenida la imagen en tamaño y posición preestablecidas, se localiza los componentes del rostro, se normaliza a través de componentes geométricos como la distancia entre ojos, distancia en comisura de los labios, posición de la nariz o medición de ángulos de la cara, también se pueden aplicar filtros y/o histogramas sobre la imagen con el fin de mejorarla.
- Extracción de características: entrega información para distinguir entre los rostros de diferentes personas.
- Reconocimiento: compara los vectores obtenidos de la extracción de características con los guardados en la base de datos, si cumple con el porcentaje de reconocimiento establecido se concede el acceso, de lo contrario se niega.

3.1.7 Cámaras de Seguridad con Acceso Remoto (12)

Se encuentran presente en casi la totalidad de los edificios, tanto empresariales como habitacionales. Constan de cámaras - por cable o inalámbricas - que transmiten sus capturas de imágenes a un DVR. Pero la preferencia de los usuarios por los CCTV ha migrado a la necesidad de acceso remoto, por lo que la mayoría de los sistemas ofrecidos en el mercado, permiten el acceso vía internet al DVR, pudiendo así observar en vivo lo que está ocurriendo en su domicilio o edificio, sin tener que pagar mensualmente por el servicio a una empresa de seguridad. Gracias a esto, el usuario puede no solo ver en tiempo real, sino también ver lo que ha ocurrido en los últimos días, semanas o incluso meses (varia en torno a la configuración de calidad de imagen y capacidad de almacenamiento).

Los DVR son ampliamente configurables, permitiendo así:

- Definir un "evento", los cuales pueden ir desde registrar si es que hubo movimiento en un lugar que debería estar deshabitado o si el sistema está siendo atacado, en cuyo caso pueden generar una alerta y notificar al usuario por el medio que se haya predefinido.
- Ajustar la calidad de la imagen, pudiendo disminuirla para generar más espacio en disco o aumentarla para obtener un mayor grado de detalle.
- Emitir a múltiples pantallas las transmisiones en vivo o dividir los cuadros y enviar un grupo de cámaras a una pantalla y el resto a otras.
- Respaldo en nube de la información, dando así protección en caso de robo del DVR.

En la actualidad, hay sistemas CCTV con DVR que ya ofrecen acceso remoto por medio de los Smartphone, como lo ha hecho la empresa KGuard Security, en donde por medio de una aplicación multiplataforma llamada KViewQR permite el acceso vía 3G o 4G hacia el DVR y tener visión en tiempo real de lo que sucede en el inmueble e incluso acceso a los videos almacenados en él.

A pesar de todas las buenas cualidades que posee este tipo de sistema (bajo costo, fácil de montar y configurar, poco invasivo), es un sistema vulnerable por intercepción cuando las cámaras son por cables, lo cual hace que el sistema se convierta en un arma de doble filo: si un intruso logra obtener acceso a las cámaras, esto le facilitará el robo.

Empresas como Linksys y DLink han lanzado al mercado cámaras por acceso inalámbrico denominadas IP Cameras, en las cuales se les vincula por medio de una dirección IP y cifran la información de manera de no poder sufrir ataques tipo middle-man. Bajo esta última medida, solo resulta vulnerable el sistema si es que el Router Gateway logra ser vulnerado, otorgándole al intruso acceso a la red local, lo que conlleva al acceso al DVR y a todo el sistema de Cámaras.

3.1.8 Aplicación por Smartphone

El uso de los Smartphone cada día se vuelve más indispensable. Por esto, utilizar un sistema de control de acceso a través de una aplicación vía Smartphone se vuelve una opción cada vez más atractiva. En la actualidad existen ya diversas aplicaciones para llevar a cabo esta tarea, tanto en iOS como Android.

Dentro de las más utilizadas se encuentra:

- Sicon Mobile: Realiza un control de entrada y/o salida, identificando a los usuarios a través de tarjetas de acceso desarrolladas por Construred Servicios (empresa creadora de Sicon Mobile). Las tarjetas son virtuales y cuentan con un código QR que es el leído por dispositivos ubicados en las vías de acceso. Trabaja de manera Online y Offline.

- Safecard: Aplicación similar a la anterior, pero que adicionalmente cuenta con un servicio de invitaciones que poseen una validez durante el día y la hora indicados, éstas se envían a través de un SMS, recibiendo un código número el cual se debe ingresar manualmente, o vía la app, recibiendo un código QR el cual se debe mostrar en los dispositivos de entrada.

La desventaja del uso de los Smartphone radica en la segmentación con respecto a personas mayores o niños, que no tienen el conocimiento necesario o ni siquiera cuentan con un Smartphone para acceder al servicio.

La programación de las aplicaciones para Smartphone ha cursado por varios lenguajes de programación. En un inicio, se requería de un lenguaje distinto para cada sistema operativo – iOS, Android, Windows, entre otros – pero en la actualidad se ha generado un lenguaje en común para las aplicaciones de Android e iOS llamado Swift (13). Este fue creado con la intención de reemplazar lenguajes basados en c - como c++ u Objective-c – por lo que puede ser comparado a estos lenguajes en desempeño de tareas. Todo el lenguaje de Switf, las librerías, compiladores y gestor de paquetes están publicados bajo *Apache 2.0 license with Runtime Library Exception* y el código fuente se encuentra alojado en GitHub por su naturaleza *Open Source*.

3.1.9 Bluetooth (14)

Más que un sistema de seguridad, Bluetooth es una tecnología de transmisión de datos que opera en la banda de los 2.4 [MHz]. Ha sido utilizada en dispositivos de seguridad tales como cerraduras, luces – para ahuyentar posibles ladrones – y manejo de sensores a distancia.

Actualmente, se utilizan y existen 2 versiones de la tecnología Bluetooth: BR/EDR y BLE.

La versión BR/EDR está optimizada para el uso más común que se le da a Bluetooth: La transmisión vía *streamming* en alta calidad, con un uso energético eficiente.

El BLE (Bluetooth Smart or Low Energy) permite la creación de pequeños sensores; utilizan tan poca energía que permiten disminuir su tamaño al de una moneda durante, cpn lo que duran meses y en algunos casos, durante años.

Las dos versiones sirven propósitos a diferentes. El BLE está creado en un nuevo *framework* usando GATT (Generic Atributes). GATT es muy flexible del punto de vista del desarrollador y puede ser utilizado casi en cualquier escenario. En consecuencia, permite a Bluetooth interconectar dispositivos o sensores. Por otra el BR/EDR – Bluetooth tradicional – es ampliamente explotado por aplicaciones para transmitir archivos, juegos en línea, entre otros.

Una empresa llamada Estimote, creo lo que se conoce como Beacons y Stickers (Ilustración 1). Estos son pequeños sensores, capaces de adherirse a un objeto o colocarse en un lugar. Emiten una señal de *broadcast* por medio de *BLE (Bluetooth Low Energy o Smart)* que pueden ser capturadas e interpretarlas por un *Smartphone*, desbloqueando contenido dependiendo de si es una ubicación o desplegar un menú conceptual. Por medio del Estimote *SDK (Software Development Kit)*, las aplicaciones en el *Smartphone* son capaces de entender su proximidad, pudiendo así reconocer objetos, su dueño, su ubicación, de que está compuesto, su temperatura y movimiento. Con esta información se puede generar una nueva generación de aplicaciones en el mundo real con un dispositivo inteligente.

Ilustración 1: Se despliega la información al Estimote más cercano

3.2 Procesamiento

3.2.1 Servidores dedicados o por rack (15)

Los servidores dedicados son utilizados única y exclusivamente por el cliente que lo contrata, disponiendo del 100% de su capacidad sin restricciones. La palabra Rack hace referencia a una especie de estante especialmente dedicado para colocar todo tipo de equipos de redes, tales como enrutadores, *switchs* y servidores.

La configuración del servidor pueda estar completamente adaptada a las necesidades del cliente y también existe un control sobre las aplicaciones que operan sobre el servidor. De manera opuesta, éstos tienen un costo mensual fijo y la capacidad siempre será la contratada.

Los principales vendedores de servidores por rack son HP, Cisco y Dell. Estos permiten personalizar el servidor a las necesidades, permitiendo poner servidores adicionales en el rack para redundar la información o dividir la tarea de procesamiento.

La utilización de estos dispositivos está principalmente enfocado a las medianas y grandes empresas, que requieren manejar y procesar grandes flujos de información, por lo que sus costos de adquisición son elevados. Además, requiere mantener una persona en planta a cargo de todos los servicios asociados.

3.2.2 Cloud Server (16)

Consisten en el arrendamiento de un servidor virtual o servidor “en nube”. De esta manera, no se requiere dispositivo físico en las dependencias, solo de una conexión estable a internet. Si se desea determinar el resultado de una operación matemática compleja, al hacerlo en papel y lápiz tomaría mucho tiempo y recurso, en cambio al ingresar los datos a una calculadora, se obtiene el resultado al instante. Análogamente, los *Cloud Server* reciben todos los datos, prestan el servicio que se requiera – procesamiento, almacenamiento – y entrega el resultado necesitado.

Este sistema fomenta escalar los recursos computacionales, ajustándolos según la demanda: la demanda de servicio puede crecer o disminuir de acuerdo a las necesidades del cliente. Además, para una empresa que está emprendiendo o partiendo con un negocio, le permite una significativa reducción de costos, pues no se requiere la inversión inicial en equipamiento.

Las principales desventajas son la dependencia a los proveedores del servicio, pues toda la información se encuentra almacenada en la nube, la necesidad de una conexión a internet potente y estable, y el pago mensual por el servicio de *hosting*.

Dentro de los *Cloud Hosting* – servidores que alojan la información desplegada en la nube – mejor evaluados se encuentra InMotion Hosting, Arvixe y Just Host (17). Estos se juzgaron en base a cantidad de sitios web que aloja simultáneamente, número de dominios y subdominio por cuenta, espacio dedicado y memoria disponible, y por último la ayuda y soporte que prestan al usuario.

3.2.3 Servidores locales

Se entiende como un computador o dispositivo que se adapta para ser utilizado como un servidor. Tomar un computador tradicional y convertirlo en un servidor tiene la desventaja de los costos de mantención, ya que no son equipos destinados a estar las 24 horas encendidos y no están optimizados para un bajo consumo energético.

En la actualidad han ido apareciendo los denominados Micro-Computadores, los cuales corresponden a pequeñas placas de circuito – como una placa madre de pequeñas dimensiones – con todas sus prestaciones reducidas, tales como RAM, procesador y memoria física. Debido a esto, es que son relativamente lentos al momento de cargar demasiadas tareas, por lo que solo se recomiendan para proyectos de pequeña o mediana envergadura.

Cuentan con lo justo y necesario para desempeñar las tareas requeridas, de manera de optimizar el rendimiento, uso de recursos y reducir sus dimensiones. Se les puede montar sistemas operativos tradicionales, pero se recomiendan versiones especiales, más livianas.

Los principales fabricantes de Micro-PC son Raspberry y Arduino. Tienen un costo inferior a la décima parte de un servidor por rack. Son de código libre y existen numerosas comunidades dedicadas a la ayuda y colaboración para su uso.

La diferencia entre estos dispositivos y un computador tradicional los denominados Input/Output. Estos son pines ubicados en la placa que permiten, mediante programación, destinar acciones hacia circuitos externos y actuar con respecto a estímulos externos.

3.2.4 Micro Controladores (18)

Son circuitos integrados que en su interior contienen una unidad central de procesamiento, unidades de memoria – RAM y ROM – y al igual que los micro computadores contienen puertos *Input/Output*, de tal forma que el sistema recibe estímulos del exterior y genera respuesta en base a estos. Estas partes están interconectadas dentro del micro controlador, y en su conjunto forman lo que se conoce como micro computador. Se puede decir que un micro controlador es una micro computadora encapsulada en un circuito integrado.

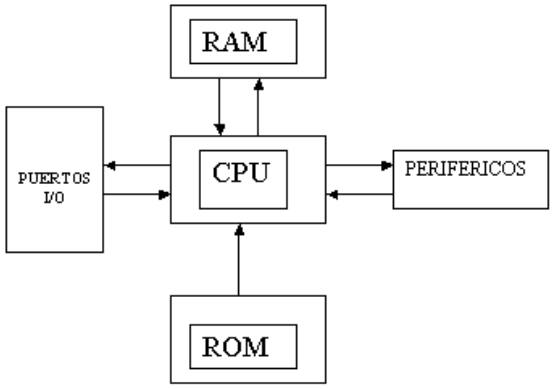


Ilustración 2: Esquema básico de un Micro Controlador

A diferencia de los micro computadores, los micro controladores requieren de un programa para que realice una función específica y carecen de un sistema operativo. Generalmente se carga el programa desde un computador vía serial o USB hacia el micro controlador para luego ser almacenado en la memoria ROM de este.

Los micro controladores son el núcleo casi la totalidad de los sistemas de alarma provistos por las empresas de seguridad privada: se configura un teclado numérico como entrada, a la par de los sensores de proximidad, de rayo o de temperatura, y se configuran usualmente dos salidas, la primera hacia una sirena para disuadir y la segunda hacia la compañía de seguridad.

El principal fabricante y proveedor de micro controladores es Texas Instruments con la MSP430, seguido por Microchip Company con una variedad de configuraciones como PIC18, PIC16 y PIC12 – familia de micro controladores de 8 bits – y en tercer lugar se encuentra Silicon Labs con los productos de la familia C8051F (19).

4. Marco Conceptual

En el desafío propuesto, hay una variedad de restricciones que imponen requerimientos mínimos en el sistema de seguridad a implementar. Es por ello que, dentro de todas las soluciones actuales existentes, hay solo algunas que son viables de utilizar. Este debe ser capaz de:

- Autentificar altos caudales de personas, dentro de los cuales se debe considerar usuarios que son propietarios del inmueble, empleados (conserjes, personal de aseo, jardineros, entre otros), inquilinos tanto de estadía breve o prolongada y aquellos externos al edificio. Estos últimos se descomponen en subcategorías, dependiendo del tipo de usuario (visitas, personal de servicios, repartidores) y/o tasa de frecuencia: frecuentes, esporádicas y casuales.

- Controlar flujos de personas, tanto acceso por *Lobby* como por vehículo, de manera segura y no invasiva. Acorde a lo planteado, un sistema se considera invasivo si este dificulta el transito regular de los usuarios. El nivel de seguridad debe ser lo suficiente robusto como para que los usuarios no se sientan vulnerables y transiten de forma tranquila sin temor a ser víctimas de un delito en su mismo condominio.

- Ser supervisado y utilizado por una persona con bajo nivel de conocimientos informáticos. Al mismo tiempo el sistema debe ser lo más autónomo posible de manera que no dependa de la constante intervención de personal especializado.

Conforme a los problemas e hipótesis planteadas anteriormente, se pueden establecer los requerimientos básicos del sistema:

- Una base de datos que contengan un catastro de todos los usuarios, albergando a los diversos tipos de usuarios con sus respectivas tasas de frecuencia.

- Control de flujo *Contactless* para fomentar el libre tránsito, sin poner en riesgo la robustez del mismo.

- Una *GUI* fácil de usar, estable y autodidacta para el usuario.

5. Alternativas de Solución:

En referencia a las problemáticas del desafío y las conclusiones en el Marco Conceptual, se acotan las tecnologías viables a utilizar. De esta manera, se separa y se define la solución bajo la perspectiva de los Inputs y el Servidor:

5.1. Input

Se define como la primera interacción con el sistema. Estos corresponden a todas las entradas del sistema, vale decir, a todo lo que concierne la captura de datos hacia el servidor.

Corresponde a la parte visible del sistema hacia el usuario, sea tanto el conserje a través del sitio web de gestión de usuarios o como los habitantes y visitas a través de la aplicación por Smartphone. Estos interactuaran con el sistema para poder hacer ingreso al edificio.

Dada las restricciones y requerimientos básicos establecidos, se filtran, de las soluciones para las entradas mencionadas en el Estado del Arte, aquellas que requieran contacto con el usuario – como por Huella Digital o Código Alfanumérico -debido a que estas representarían una invasividad del punto de vista de la movilidad del usuario a través del recinto. Además, se descarta el uso de tarjeta con banda magnética por los riesgos asociados.

Por otra parte, resultan viables soluciones del tipo *contact* less – no requieren contacto- como lo son NFC, RFID, Reconocimiento Facial y el uso de aplicación por *Smartphone*. Dentro de estas, se descarta el uso de Reconocimiento Facial, ya que, como se mencionó en el Estado del Arte, el pasar del tiempo afecta drásticamente el rostro de las personas y se requeriría que el usuario permaneciera inmóvil por dos o tres segundos frente a una cámara tridimensional – capaz de medir profundidad – y esto, de acuerdo a la definición dada por el cliente, pasaría a ser invasivo.

5.2. Servidor

Se define como el lado oculto del sistema. Corresponde a todo el procesamiento de datos capturados desde los *inputs* para luego generar una respuesta o acción del sistema.

Esta es la segunda etapa del sistema – siendo la primera la captura de datos – y no tiene una forma directa de interacción. El servidor se programa para ser aquel que toma las decisiones en lugar de una persona. Estas decisiones van desde el control hasta la restricción de acceso de los usuarios.

Dado que uno de los requerimientos del sistema es la implementación de una base de datos, se descarta inicialmente el uso de un micro controlador. Se descarta también servidor por *rack*, ya que se requiere un sistema que pase desapercibido y que se mimetice en el ambiente; además los servicios que debe desempeñar son pocos en comparación a la capacidad de procesamiento de estos.

Luego, queda como soluciones viables el uso de *Cloud Hosting* y un servidor local, teniendo cada uno ventajas y desventajas. Los servidores locales tienen un costo de inversión inicial medio y un costo fijo de mantención bajo, mientras que los *Cloud Server* no requieren de una inversión inicial, pero si de un costo de mantención mensual. Además, si se deja de pagar por el servicio, se pierde el acceso a la información, lo que genera una gran dependencia al proveedor de *Hosting*. Por otra parte, los servidores locales son vulnerables a hurto o a ataques informáticos.

6. Acercamiento a la Solución

Bajo los requerimientos del sistema de seguridad, una solución para el sistema de entrada de información es el *active RFID tag*. Al poseer un código de identificación único, es aplicable para un gran grupo de personas lo que a su vez facilita el control de flujo de estos. Se elige el activo sobre el pasivo porque el primero permite que la persona se desplace con libertad, sin tener que mostrar o buscar entre sus cosas por el *tag*. Esta última mejora considerablemente el aspecto no invasivo del sistema, consiguiendo mantener la robustez del mismo. Además, en el espectro de frecuencia que opera el sistema pasivo existen muchas perturbaciones en el ambiente que pueden dificultar la autentificación.

El sistema de seguridad a implementar por medio de *RFID* se descompone en:

- Dispositivos *RFID tag* activos, los cuales serán entregados como llaveros con la respectiva llave del departamento. Cada usuario dispondrá de un dispositivo con un identificador único, lo que le permitirá desplazarse por el recinto con el solo hecho de portarlo consigo.

- *RFID Reader* (lectores *RFID*) ubicados en cada acceso de ascensor y en las puertas de emergencia. Los primeros intervendrán los pulsadores del ascensor, de manera que solo si la persona posee un ID valido podrá desplazarse entre pisos. De no contar con el dispositivo cuando va de subida, no podrá pedir el ascensor, lo que lo deja obligado a ir donde el vigilante para solicitar acceso y dejar registro de porque no porta su dispositivo. Por otra parte, una persona podrá transitar libremente por las escaleras de emergencias, solo si lleva consigo su identificador. En caso de emergencia (suena la alarma de incendio u ocurre una catástrofe natural) el vigilante tendrá el poder de liberar todas las puertas.

- Cuando llega una visita se le solicita su Cédula de Identidad, a la cual se extrae la información por medio del lector de código de barra bidimensional. Se ingresa a la base de datos el código del *RFID* que se le pasará, conjunto con los datos extraídos de la Cédula y una captura facial para constancia. Conjunto a lo anterior, se fija el tiempo estimado que estará (medio día, un día, una semana, etc.) de manera que el registro en la base de datos caduque una vez finalizado plazo.

En cuanto a la vulnerabilidad de los sistemas *RFID* a riesgos inminentes de *hackeo,* se piensa aumentar el nivel de seguridad por medio de una codificación del *RFID tag,* lo cual generará un mayor grado de dificultad a la hora de vulnerar el sistema. Como medida complementaria se deberá implementar un software que utilizará un lector de código de barra bidimensional para la lectura de la Cédula de Identidad, información la cual será añadida de manera simultánea con el *RFID tag* y una captura facial de la persona.

Por otra parte, en lo que concierne al procesamiento de la información resulta más eficiente el uso de un servidor local que uno alojado en Nube. Esto se debe a que en principio los *Cloud Server* tienen un costo por mantención y de igual manera se debe tener un equipo de manera local para poder operarlo. A su vez no es necesario un servidor de gabinete para la implementación del sistema ni tampoco un gran nivel de recursos (procesador, RAM, memoria física, alimentación).

Para implementar lo requerido se utilizará una Raspberry Pi de tercera generación, en la cual se montará un servidor con una base de datos que posea toda la información de los residentes del edificio e ir aumentándola por medio de los registros diarios.

Al presentarle al cliente esta solución, este señala que tienen una necesidad intrínseca y no negociable de utilizar la tecnología Bluetooth para la comunicación; además de la utilización de una Aplicación por Smartphone como medio de uso para el usuario. Se le hace llegar un reporte en el cual se señala las razones de la inviabilidad de esto, entre ellas, que el sistema será demasiado invasivo y que automáticamente segmenta el mercado, pues, como fue señalado en el Estado del Arte del Smartphone, la gente mayor no está familiarizada con el uso de estos a lo que señalan que el mercado objetivo va de los 25 a los 45 años y que es intrínseco el uso de lo solicitado. En vista y considerando lo anterior se replantea la solución del sistema:

- Se diseñará un sitio web que permitirá al conserje agregar a un nuevo usuario por medio de una captura fotográfica al código QR de su cédula de identidad y una captura facial; además en el mismo formulario se deberá señalar un correo electrónico, el departamento y piso de destino, y por último la *Bluetooth MAC Address* del dispositivo con el que hará uso de la aplicación. Toda esta información será alojada en una base de datos.

- Posterior al registro, se realizará un emparejamiento del Smartphone del usuario con el servidor a través de Bluetooth.

- Por último, el usuario registrado y emparejado podrá utilizar la Aplicación para abrir la puerta de acceso al *Lobby*, llamar al ascensor y acceder al estacionamiento remotamente.

7. Contribución

De acuerdo a los perfiles del equipo se ha dividido el proyecto en lo que respecta al Servidor y la Aplicación. La contribución que se tratará en el presente documento corresponde a la configuración, programación e implementación de todo lo que concierne al Servidor.

En base a los conocimientos en redes de computadores, programación y sistemas operativos, se montará un sistema operativo Ubuntu Mate 16.04 LTS - basado en UNIX – en un Micro-PC Raspberry Pi versión 3. A este se le instalarán todos los paquetes necesarios - paquetes como apache, php5, librerías, entre otros - para la implementación de un sitio web. El sitio contará con un algoritmo de lectura de código QR y un vínculo hacia una base de datos en mySQL, gestionada a través de phpMyAdmin. En su conjunto, permitirán al conserje realizar el registro de los usuarios hacia la base de datos y permitirle a la aplicación filtrar a los usuarios que la utilicen, a solo aquellos que se encuentran registrados en la base de datos.

Para otorgarle al conserje la libertad de movimiento, se llevará a cabo una red PAND – red local privada – la cual le permitirá acceder al sitio web por medio de un Tablet a través del enlace Bluetooth.

Dada la naturaleza Multidisciplinaria de la memoria, Macarena Gallardo, alumna memorista de Ingeniería Civil Telemática y compañera de equipo en el desafío propuesto por el cliente, Inmobiliaria Fundamenta, se encargará de la creación y configuración de una aplicación para Smartphone con sistema operativo Android, que será capaz de otorgarles a los usuarios – tanto habitantes como visitas – la capacidad de abrir remotamente puertas de acceso, solicitar el ascensor y abrir el portón. La aplicación será capaz de contactar la base de datos alojada en la Raspberry Pi y consultar si el usuario que está intentando acceder a las dependencias pertenece o no al registro; de no pertenecer se le denegará el acceso a pesar de tener la aplicación. De forma adicional, la aplicación podrá consultar el piso el cual visita o reside el usuario y delimitar su solicitud del ascensor a solo los pisos de planta – niveles de estacionamiento y *lobby* – y al de destino.

8. Objetivos

Se establece como objetivo general la creación de un sistema de seguridad robusto capaz de controlar caudales variables de transito de gente, tanto peatonal como vehicular, que a su vez no dificulte el libre tránsito de las personas en proyectos habitacionales de gran envergadura, siendo estos edificios de más de 100 departamentos.

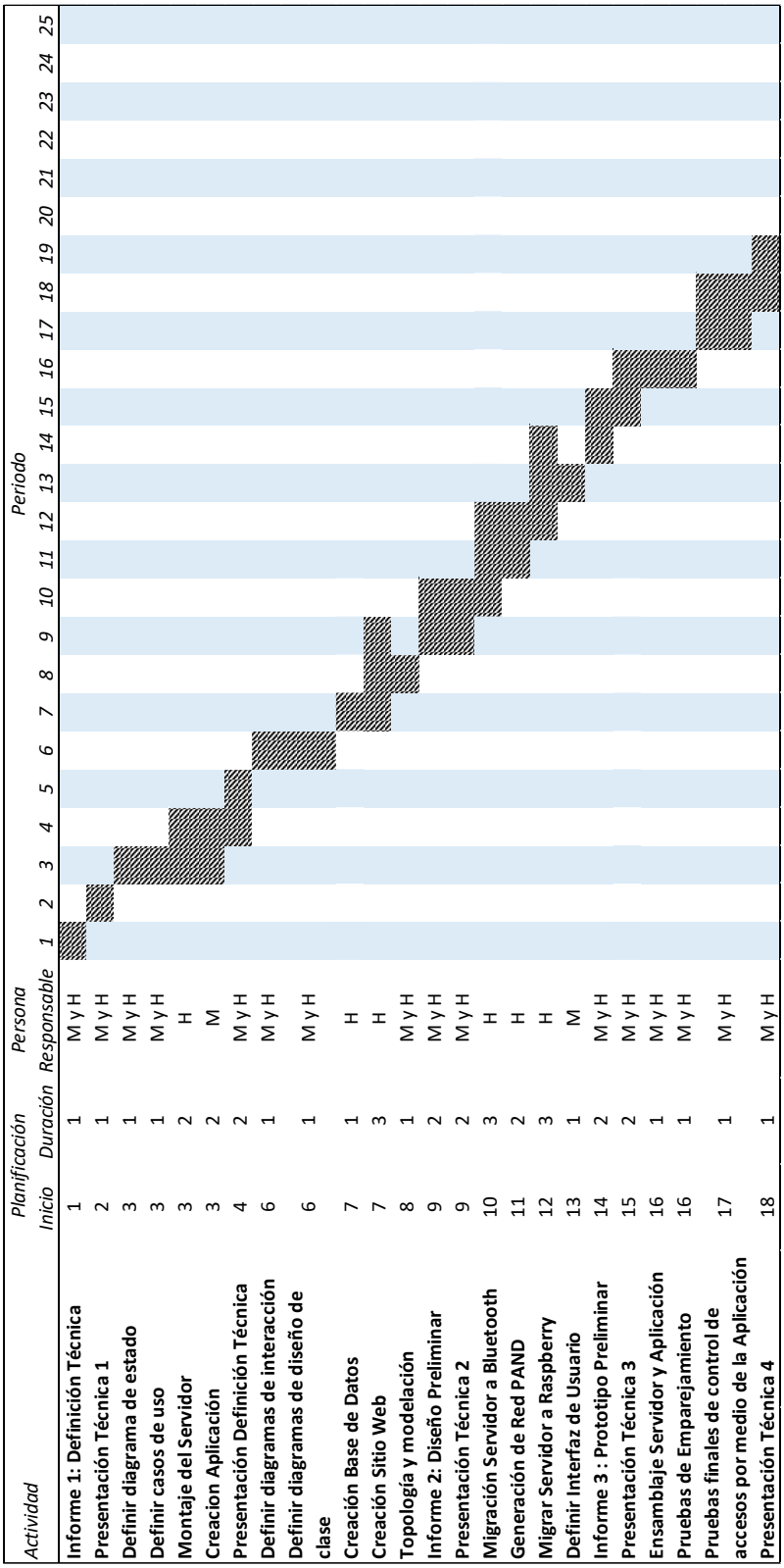
Se incorporará el requisito solicitado por el cliente, de realizar el enlace a través de Bluetooth hacia una aplicación en un Smartphone y sumado a eso se generará una interfaz para el conserje hacia un sitio web a ser utilizada en un Tablet, que se enlazará al servidor por medio de Bluetooth.

Para conseguir el acceso a una red local con Bluetooth se creará una Red PAND – red de área privada, vale decir, es invisible desde el exterior – en base al servicio denominado *Blueman*. Este corresponde a la abreviación de *Bluetooth Manager* y es una herramienta capaz de crear un punto de acceso a la red por medio de Bluetooth.

Se diseñará e implementará un servidor capaz de albergar toda la información de las entradas en una base de datos. Esta contará con todos los datos desprendidos de la cédula de identidad del usuario, la dirección MAC del dispositivo con el cual desea hacer uso del sistema y el piso y departamento al cual se dirige o habita.

Además, se diseñará y creará una Aplicación que se encargue de consultar la base de datos para saber si el usuario que desea hacer uso de esta se encuentra o no registrado en ella. La aplicación le permitirá al usuario utilizar los accesos del edificio de forma remota y controlar el portón de la zona vehicular.

9. Programación de actividades y/o plan de trabajo – Carta Gantt



Actividad	Planificación		Persona	Periodo																					
	Inicio	Duración	Responsable	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Informe 1: Definición Técnica	1	1	M y H																									
Presentación Técnica 1	2	1	M y H																									
Definir diagrama de estado	3	1	M y H																									
Definir casos de uso	3	1	M y H																									
Montaje del Servidor	3	2	H																									
Creacion Aplicación	3	2	M																									
Presentación Definición Técnica	4	2	M y H																									
Definir diagramas de interacción	6	1	M y H																									
Definir diagramas de diseño de clase	6	1	M y H																									
Creación Base de Datos	7	1	H																									
Creación Sitio Web	7	3	H																									
Topología y modelación	8	1	M y H																									
Informe 2: Diseño Preliminar	9	2	M y H																									
Presentación Técnica 2	9	2	M y H																									
Migración Servidor a Bluetooth	10	3	H																									
Generación de Red PAND	11	2	H																									
Migrar Servidor a Raspberry	12	3	H																									
Definir Interfaz de Usuario	13	1	M																									
Informe 3 : Prototipo Preliminar	14	2	M y H																									
Presentación Técnica 3	15	2	M y H																									
Ensamblaje Servidor y Aplicación	16	1	M y H																									
Pruebas de Emparejamiento	16	1	M y H																									
Pruebas finales de control de accesos por medio de la Aplicación	17	1	M y H																									
Presentación Técnica 4	18	1	M y H																									

Perfil Técnico del Proyecto

1. Requisitos del Sistema

1.1. Requerimientos Funcionales

- El sistema deberá ser robusto, vale decir, que resista ataques informáticos, altos caudales de tráfico de información y múltiples solicitudes de forma simultánea.
- No Invasivo, que de acuerdo a la definición expuesta por él cliente, no retenga al usuario por periodos prolongados, siendo prolongado, más allá del agrado del mismo.
- Permitir que los usuarios se desplacen con facilidad a lo largo de las instalaciones.
- Registrar nuevos usuarios, sean residentes, visitas o trabajadores.
- Buscar dentro del registro si un usuario se encuentra o no registrado.
- Eliminación de usuarios del registro de forma permanente.
- Controlar el acceso a los pisos, limitando el desplazamiento a solo el piso que le corresponda.

1.2. Requerimientos de Interfaces

- Sencilla de utilizar; de no poderse, al menos que sea lo suficientemente auto explicativa.
- Contar con dos interfaces: una para el usuario y una para el conserje. La primera será por medio de la aplicación por Smartphone, mientras que la del conserje será a través del sitio web y un Tablet.
- Amigable para el usuario básico
- La interfaz del sitio web debe ser sencilla de utilizar solo después de haber capacitado al encargado. Esto se debe a que, si una persona externa al recinto hurta o toma posesión del Tablet o consigue acceso al servidor, no le sería sencillo saber con precisión como proceder.

1.3. Requerimientos de Ambiente

- Debe ser de pequeñas dimensiones, capaz de mimetizarse con el ambiente, así pasará desapercibido a terceros y será más sencillo proteger el sistema a riesgos externos.

2. Arquitectura del Sistema.

2.1. Esquema General del Sistema

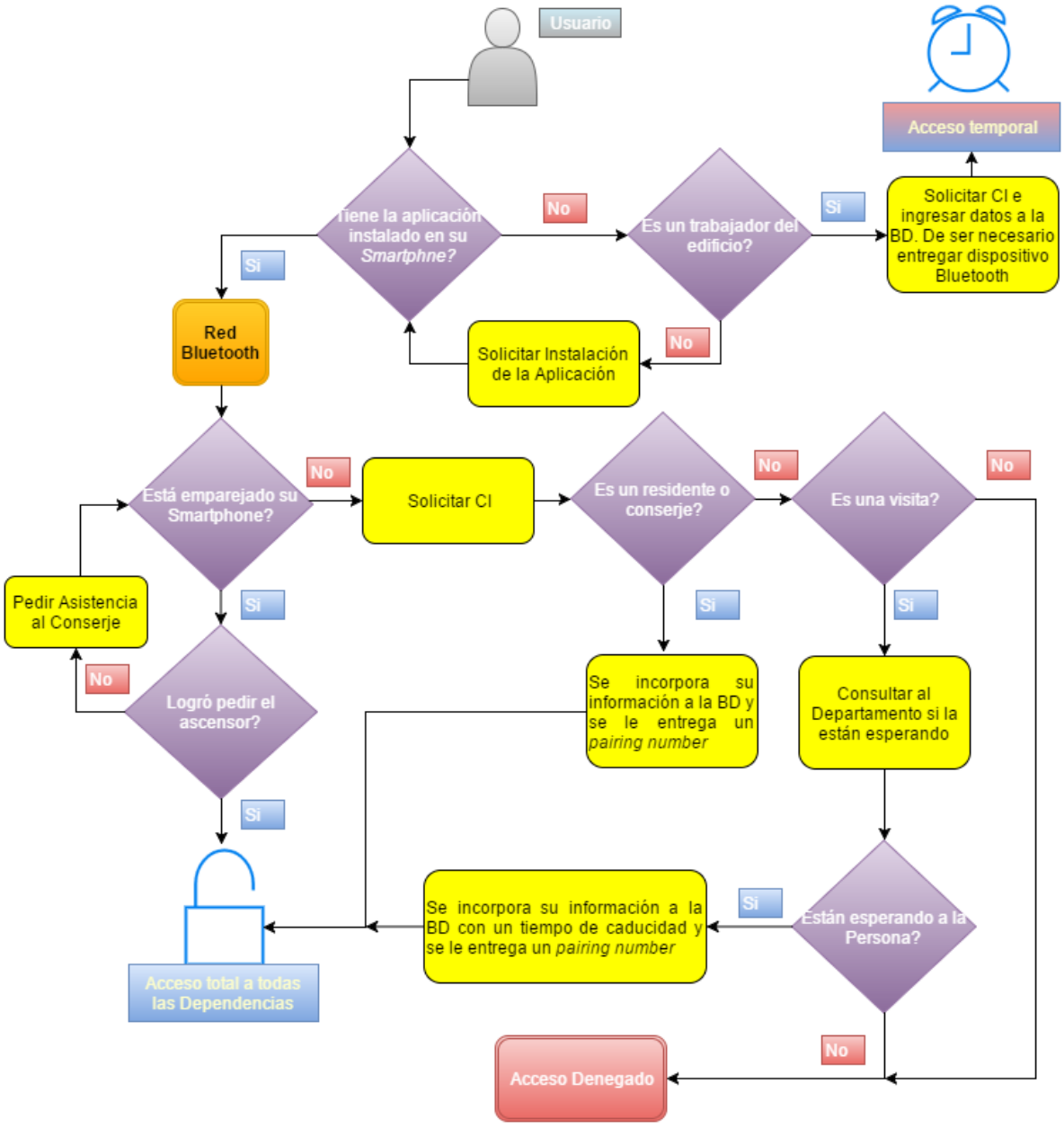


Ilustración 3: Diagrama de Flujo de funcionamiento del sistema

2.2. Descripción de Componentes

2.2.1. Android Tablet:

Por medio de este dispositivo el conserje se encargará de hacer el registro de los usuarios a través del sitio web montado en el servidor. La idea es desprenderlo de la mesa de acceso y poder hacer el registro de los usuarios, aunque se encuentre realizando otras labores al interior o exterior del edificio. Lo que concierne al prototipo se ha utilizado un Tablet Lenovo (ver Anexo), pero los requisitos fundamentales son la Cámara frontal y la conexión por Bluetooth.

2.2.2. Android Smartphone:

A través de la aplicación, los usuarios podrán tener control sobre el ascensor, puerta de acceso y portón. Estos deben encontrarse previamente registrados en la base de datos.

2.2.3. Raspberry Pi

Es un computador de placa reducida, del tamaño de una tarjeta de crédito, que se conecta a un monitor o televisor, y utiliza teclado y mouse. Este pequeño dispositivo es capaz de hacer cualquier trabajo que un computador de escritorio realice, desde navegar por internet y reproducir video en *HD*, hasta crear hojas de datos.

2.2.4. Teclado y Mouse:

Dado que la Raspberry cuenta con solo cuatro puertos USB, se utilizará un teclado con Mouse integrado. Por medio de este el conserje podrá emparejar los dispositivos con la Raspberry.

2.2.5. Monitor:

Será la interfaz de acceso directo del conserje o administrador hacia el sistema montado en la Raspberry. De esta manera, aunque falle la conexión del Tablet hacia el servidor, de igual manera podrá hacerse el registro de usuarios.

2.3. Matriz de Requisitos Funcionales y Componentes

Requicitos Funcionales	Tablet	Smart Phone	Teclado y mouse	Raspberr y Pi
Recidente		X		
Trabajador Edificio	X		X	X
Visita Registrada		X		
Visita No Registrada				

Ilustración 4: Matriz de Requisitos Funcionales y Componentes

3. Gestión de Riesgos

3.1. Supuestos

- No todos los habitantes estarán de acuerdo en implementar el sistema.
- El conserje se reusará a utilizarlo y lo usará de manera manual.
- Con la debida planeación, el sistema puede ser vulnerado por un ataque informático.
- Se deberá capacitar a la persona que opere el sistema.
- La gente de edad tendrá problemas para entrar y salir del recinto.

3.2. Dependencias

- El sistema es excluyente, impide el paso a aquel que no porte su identificación. Por lo que recaerá en los usuarios la responsabilidad mantener su teléfono cargado y avisar en caso de pérdida o hurto.
- En caso de fuerza mayor, el conserje podrá anular el sistema y podrá dejar el sistema en manual.
- El sistema debe configurarse respetando las legislaciones actuales, como el libre tránsito por las escaleras de emergencias y una salida de emergencia habilitada en caso de catástrofes.

3.3. Restricciones

- Al ser edificios de más de 100 departamentos, suponiendo un habitante permanente por departamento, se habla de una densidad de 100 personas, de las cuales, en términos estadísticos en Chile el 15% de la población es mayor de edad. (20)
- El conserje tiene la capacidad de hacer o no uso del sistema, dándole el poder de anularlo.
- El sistema debe ser capaz de no retener a los usuarios por tiempos prolongados y de agilizar la entrada y salida de estos.
- Además de fomentar un tránsito expedito, no debe ser vulnerable.
- El servidor debe quedar posicionado de tal manera que sea difícil de robar o vulnerar.

3.4. Riesgos

- Ataques informáticos para obtener información de la base de datos.
- Fallas frente a una catástrofe natural, como tormentas eléctricas, sismos, apagones.
- Predicción de comportamiento frente a cambios abruptos en las condiciones atmosféricas.
- Mala manipulación de los dispositivos instalados, como por ejemplo limpiar el servidor con un agente corrosivo, rociarlo con agua o desconectarlo.
- Falla de comunicación con los sistemas de entrada producto de interferencia o saturación de la banda de frecuencia en la que se opera.
- El robo o hurto del Smartphone de un cliente le impide al mismo acceder al recinto y al mismo tiempo le permite al perpetrador acceder con libertad a las instalaciones

4. Arquitectura revisada del sistema

4.1. Diagrama de contexto

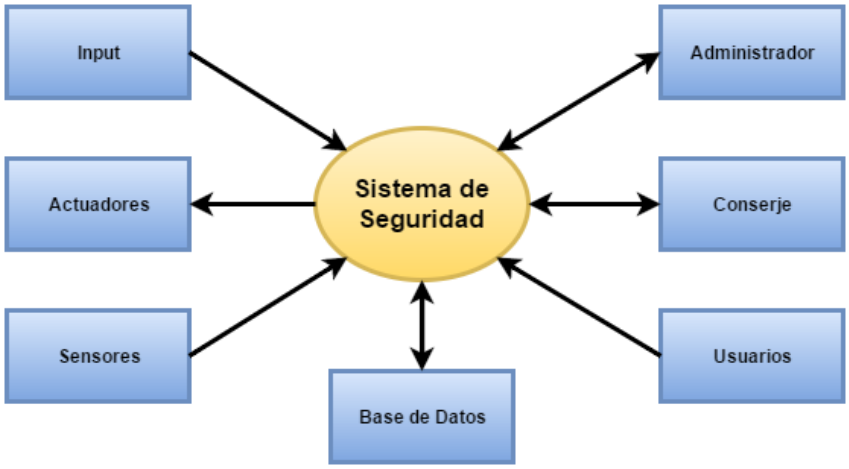


Ilustración 5: Diagrama de Contexto del sistema de seguridad

4.2. Diagrama de arquitectura

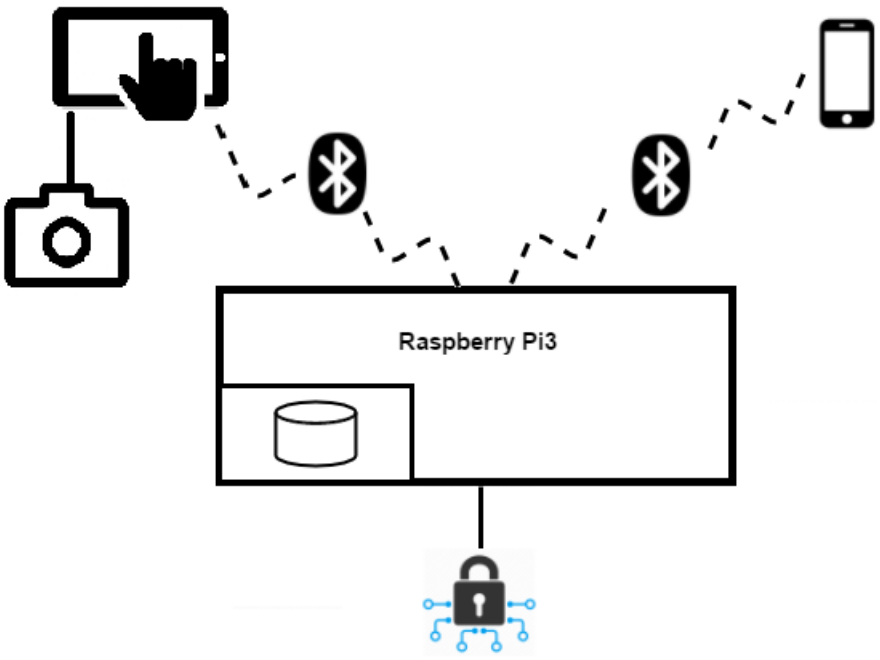


Ilustración 6: Diagrama de Arquitectura del Sistema

4.3. Descripción general de los módulos

4.3.1. Módulo input

Corresponde a todo lo que concierne las entradas, vale decir, todo aquello que aporte información al sistema para que posteriormente la procese. Dentro de esta categoría recae el formulario de registro del sitio web, los datos enviados por los usuarios a través de la aplicación y el teclado y mouse.

4.3.2. Módulo Bluetooth

Este módulo trabajará a través de una aplicación móvil, la que permitirá al usuario solicitar el ascensor al piso deseado o solicitar desbloqueo de una puerta. La primera vez de uso, todo usuario deberá emparejar su dispositivo con el servidor, autentificando esta operación por medio de un código, concediéndole así acceso a futuro. La aplicación operará sobre la plataforma *Android* y estará disponible solo dentro del rango de cobertura de la red Bluetooth.

4.3.3. Módulo output

Abarca las respuestas y/o acciones del sistema a los procesos que ha llevado a cabo con respecto a las entradas. En esta categoría entran los GPIO – General Purpose Input Output, entradas y salidas de propósito general – de la Raspberry, la cual genera la respuesta hacia los interruptores electrónicos y el monitor del sistema.

4.3.4. Módulo Micro-Computador

Para el procesamiento de datos, se utilizará un Raspberry Pi (21). Tal y como el fabricante (21) lo describe, este es una *CPU* de tamaño reducido, que permite su interconexión con diversos dispositivos tipo *Plug-and-Play*, como teclados, cámaras o cualquiera con conexión por USB o HDMI (en el caso de salida de video).

En base a sus cualidades, es que se planea utilizar como un servidor, montando en él una base de datos y ejecutando un servidor web, el cual se encargará de capturar todos los datos provenientes de las fuentes de comunicación, procesarlos y responder con una actuación en los interruptores electrónicos.

4.4. Matriz de requisitos funcionales y módulos

	Módulo Input	Módulo Output	Módulo Bluetooth	Módulo µPC
RF1			x	x
RF2	x			
RF3				x
RF4		x		x
RF5				x
RF6				x
RF7			x	

Ilustración 7: Matriz de Requisitos Funcionales por Módulo

Requisitos Funcionales:

Estos definen el comportamiento del sistema por medio del funcionamiento de cada una de sus partes. Cada función es descrita como un conjunto de entradas, salidas y comportamientos.

- ***RF1***: El Smartphone del usuario debe ser capaz de emparejarse al sistema.
- ***RF2***: El sistema debe ser capaz de obtener información de los usuarios nuevos desde el teclado, sitio web y a través de una captura de imagen.
- ***RF3***: El sistema debe guardar los datos obtenidos de los nuevos usuarios en la base de datos.
- ***RF4***: Debe ser capaz de permitir o denegar acceso.
- ***RF5***: Debe ser capaz de eliminar a usuarios del sistema.
- ***RF6***: El sistema debe interpretar los datos obtenidos desde la aplicación del Smartphone.
- ***RF7***: La aplicación del Smartphone debe lograr enviar datos a través de Bluetooth.

5. Diseño de módulos del sistema

5.1. Diseño de módulo input

Ilustración 8: Diseño del Módulo de Input

5.2. Diseño de módulo output

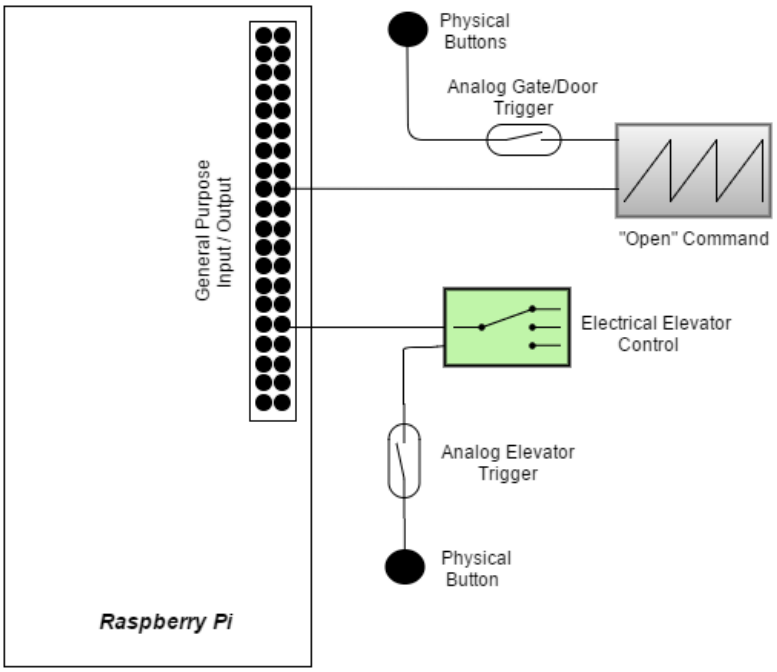


Ilustración 9: Diseño del Módulo de Output

6. Diseño de las interfaces

6.1. Modelo de navegación y diseño de interfaces usuarias

6.1.1. Interfaz conserje

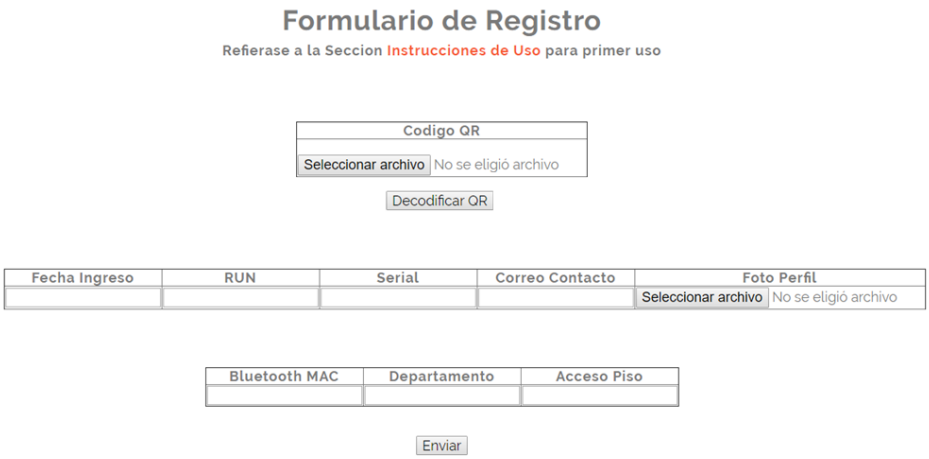


Ilustración 10: Registrar nuevo usuario

A través del sitio web, el conserje podrá gestionar la base de datos. Este podrá registrar nuevos usuarios (Ilustración 10).

Ilustración 11: Buscar usuarios en la Base de Datos

También puede buscar un usuario en particular dentro del sistema (Ilustración 11). Para eliminar un usuario (Ilustración 12), este deberá ingresar el RUN de la persona a la cual desea eliminar del sistema; además deberá ingresar credenciales de autentificación. Una vez realizado se eliminará toda información asociada a ese RUN.

Ilustración 12: Eliminar usuarios en sistema

3.1.2. Interfaz usuario

La interfaz del usuario tiene a su disposición tres opciones de peticiones: desbloquear puerta principal, solicitar ascensor o abrir portón vehicular.

Una vez escogida la opción de solicitud de ascensor, se procede a una segunda vista en la cual debe seleccionar el piso de origen.

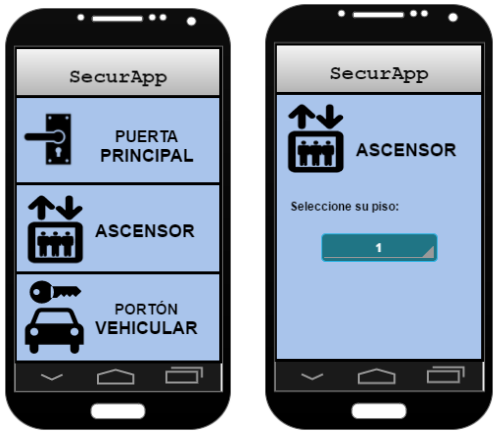


Ilustración 13: Vista desde el Smartphone a la pantalla principal y de opciones de piso

Marco General

1. Hitos Principales del Proyecto

a. Servidor

Número	Hito
1	Instalación y configuración del sistema operativo Ubuntu 16.04 Lts en Notebook.
2	Inicialización de Aplicaciones Requeridas (Apache2, PHP, mySql, gedit, phpMyAdmin, entre otras)
3	Configuración del sitio web en *localhost*
4	Creación y configuración de la base de datos (beta1, try1)
5	Pruebas iniciales de comunicación del sitio web con la base de datos
6	Agregar usuarios a través del sitio web hacia mySQL
7	Modificación de Registros por el sitio web hacia mySQL
8	Eliminación de Registro por el sitio web hacia mySQL
9	Buscador de usuarios por el sitio web hacia mySQL
10	Incorporación de Imagen de usuario a registro
11	Lectura de código QR para autocompletar datos de Carnet de Identidad
12	Agregar, modificar y eliminar usuarios vía código QR hacia mySQL
13	Creación de Tutorial para primer uso
14	Migración desde Notebook hacia Raspberry

b. Cliente

Número	Hito
1	Instalación Sistema Operativo Raspberry Pi 3.
2	Instalación de módulos necesarios para realizar conexión vía Bluetooth.
3	Creación servidor Bluetooth en Raspberry Pi 3.
4	Obtención desde el servidor de MAC Bluetooth.
5	Creación aplicación Android en IDE Android Studio.
6	Entablar comunicación directa vía Bluetooth entre Smartphone y Raspberry Pi 3.
7	Creación circuito Raspberry Pi 3 y Leds.
8	Creación de módulo en Python encargado de la comunicación con leds.
9	Interacción de leds vía Bluetooth a través de la aplicación en Smartphone.

2. Revisión de Requerimientos

Los requerimientos iniciales demandaban que el sistema fuese capaz de permitir el libre tránsito - no invasivo – y controlar - para más de 100 personas - grandes caudales.

Luego, a pedidos del cliente, estos migraron a utilización de Smartphone, uso a través de aplicación móvil a través de Bluetooth y datos estadísticos de la Energía.

En base a lo anterior:

Requerimientos	**Medición de Cumplimiento**
Uso de Smartphone	Se crea una aplicación Android, bajo el IDE Android Studio, con la cual es posible la transferencia de datos vía Bluetooth.
Comunicación vía Bluetooth	Se crea un servidor *LAMP* sobre *PAND* por Bluetooth para permitir que los dispositivos se conecten al servidor a través de Bluetooth. De ésta manera todo dispositivo, en la primera conexión, debe hacer la "negociación" con el servidor para poder establecer la comunicación. Es allí donde queda almacenado en la Base de Datos con su respectivo registro.
Servidor Bluetooth en Raspberry	Se crea y configura un servidor Bluetooth en la Raspberry Pi 3, el cual es el encargado de la creación de un canal de radio frecuencia que se encuentra recibiendo los datos enviados desde la aplicación y los procesa con el fin de realizar la interacción con los leds. Los leds se encienden por cada petición realizada desde la aplicación.

3. Revisión del Diseño

Al igual que en los requerimientos, a lo largo del camino se fueron planteando modificaciones para la utilización más óptima de los recursos:

Módulo	Diseño
Inputs	Se crea una aplicación Android para Smartphone, la cual es la encargada de realizar las peticiones de acceso, solicitud de ascensor y dar aviso de una emergencia (botón de pánico).
Actuadores	A través de la creación de un servidor Bluetooth en la Raspberry Pi 3, se emiten respuestas a las peticiones realizadas por la aplicación, las cuales se traducen a encender leds conectados a ésta y a un mensaje por pantalla al dispositivo del usuario con la confirmación o denegación de la petición.
Servidor	Se sustituye la utilización de una cámara IDE a utilizar la cámara de cada dispositivo inteligente; de esta manera, el conserje queda con un Tablet en lugar de operar directamente desde el servidor. Al mismo tiempo, por medio de la cámara de los dispositivos, se reemplaza el Lector de Código de Barra a un procesamiento de los Códigos QR de los Carnet de Identidad a través de PHP.

4. Entorno de Soporte y Desarrollo

Módulo	Soporte y Desarrollo
Servidor	El servidor se encuentra montado sobre una Raspberry Pi, la cual es capaz de atender todas las solicitudes y procesar los datos requeridos. Se programa (desarrolla) en PHP todos los códigos, incluyendo el soporte de procesamiento de imágenes QR, *Upload* de fotos de perfil, procesamiento de formularios hacia base de datos, entre otros.
Aplicación	La aplicación se desarrolla en el entorno Android Studio con programación Java y se aloja para su funcionamiento en un Smartphone y/o Tablet con Android 4.0.3 (IceCreamSandwich) o superior.

Revisión de Prototipo

1. Contexto General del Prototipo

a. Servidor

El servidor LAMP opera por medio de un sitio web, el cual le permite al conserje agregar, modificar o eliminar usuarios conectados vía Bluetooth (Ilustración 14). Para facilitar la navegación a través del sitio se le permite desplegar los distintos enlaces por medio de un menú.

LAMP proviene del acrónimo Linux, Apache MySQL y PHP. Es un tipo de programación de un servidor en la que se utiliza un sistema operativo Linux, un servidor web montado en Apache, mySQL para la gestión de base de datos y PHP para la configuración de las funcionalidades del sitio web.

La idea principal yace en la utilización del Código QR (ver Anexo) de los Carnet de Identidad para autocompletar los datos en el formulario (Imagen 2). A su vez, para los usuarios que no estén familiarizados con el sistema, se incorpora dentro del mismo sitio un tutorial paso a paso para que se pueda hacer uso de este.

Ilustración 14: Portada del sitio web

En el menú de navegación del sitio web - esquina superior derecha - se disponen las alternativas:

i. Home: Vínculo para volver al inicio de la página web

ii. Registro: Permite la incorporación de nuevos usuarios a la base de datos de manera manual o a través del código QR. Además, se debe subir una foto de perfil del usuario asociado al RUN.

iii. Buscar Usuarios: A través del buscador - por medio del RUN - permite leer todos los datos asociados a ese RUN, como el serial, foto perfil, entre otros.

iv. Instrucciones de Uso: Se le explica al usuario (conserje o administrador) como utilizar el sistema por primera vez: pasos iniciales, como subir imágenes, etapas a seguir, entre otros.

v. Eliminar Usuarios: Por medio del RUN y autenticación de credencial de administrador (o conserje) permite eliminar toda la información asociada a ese usuario y su foto de perfil.

De manera alternativa, para aquellos usuarios que no posean el nuevo Carnet de Identidad - posee código QR al reverso - se deja la alternativa del ingreso manual de datos (Ilustración 15) debido a que la cédula de identidad antigua sigue en circulación hasta el año 2020. Para este tipo de usuarios, se tendrá que escribir uno a uno los datos requeridos en el formulario - la imagen del código QR no sería necesaria - además de la foto de perfil.

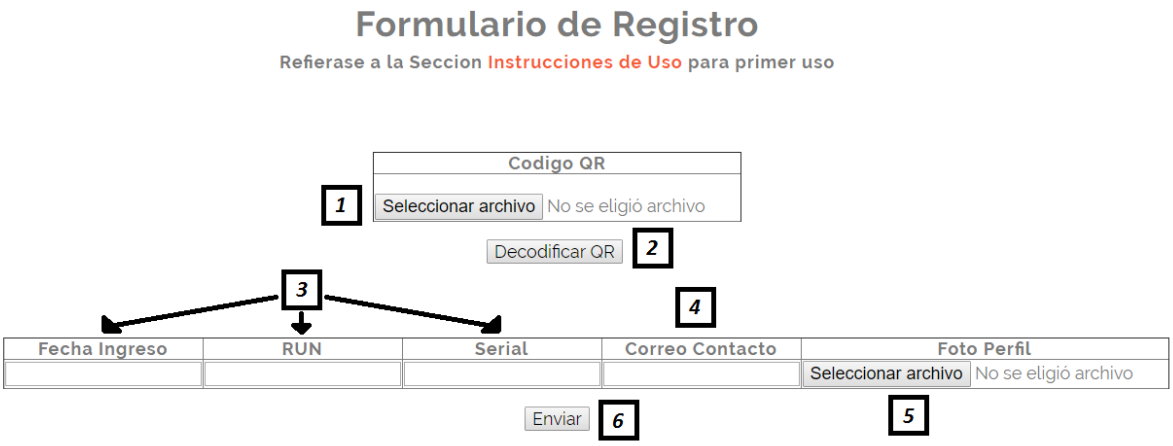


Ilustración 15: Registro de usuario, se rellenan los datos de manera automática (QR) o manual

b. Aplicación

La aplicación Android para Smartphone y Tablet es la encargada de realizar las peticiones al servidor a través de una conexión Bluetooth.

Las peticiones pueden ser:

- Acceso a la puerta principal.
- Acceso al portón vehicular.
- Solicitud de ascensor a un piso determinado.
- Dar aviso de emergencia, botón de pánico.

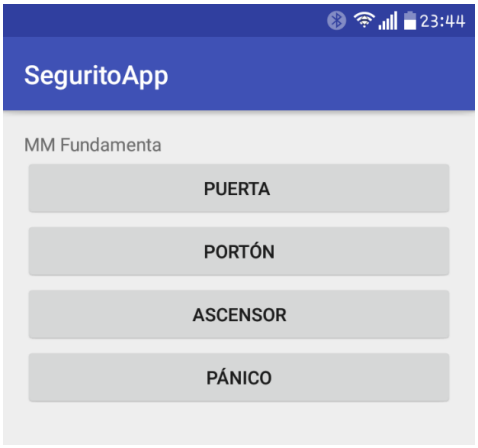


Ilustración 16: Vista principal aplicación.

La aplicación posee dos vistas, la primera (Ilustración 16) con cuatro botones principales: Puerta, Portón, Ascensor y Pánico. La segunda (Ilustración 17) vista se despliega una vez accionado el botón ascensor, la cual permite la elección del piso a solicitar el envío.

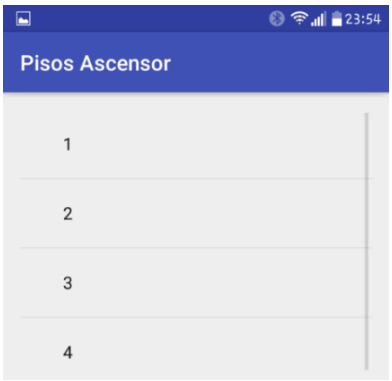


Ilustración 17: Segunda vista, pisos ascensor.

Para la lectura de los datos enviados por la aplicación se crea un programa en Python, el cual actúa de servidor Bluetooth bajo el protocolo RFCOMM (ver Anexo), creando un canal de radio frecuencia que se encuentra permanente escuchando (Ilustración 18), al llegar peticiones (Ilustraciones 19, 20, 21 y 22) desde la aplicación – del usuario - genera una salida encendiendo leds y retornando un mensaje emergente a la aplicación del estado de la solicitud "denegado" o "permitido" el cual puede ser leído por el usuario desde su dispositivo.

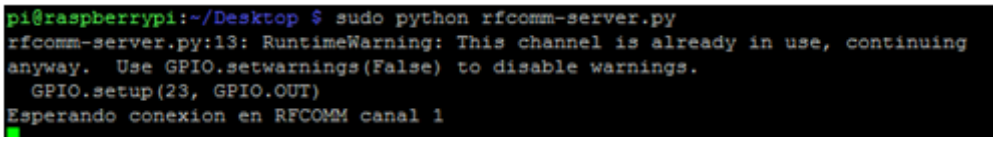


Ilustración 18: Servidor Bluetooth en ejecución.

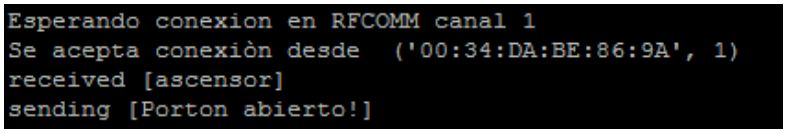


Ilustración 19: Petición de ascensor.

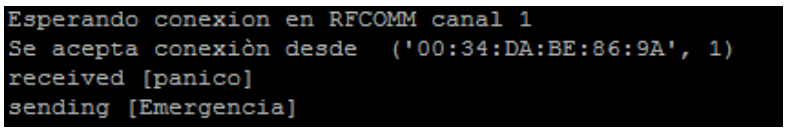


Ilustración 20: Petición de emergencia.

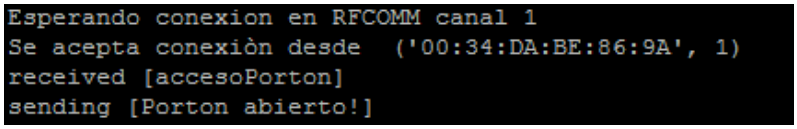


Ilustración 21: Petición de portón.

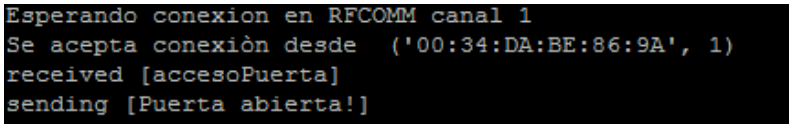


Ilustración 22: Petición de puerta principal.

2. Esquema General de Componentes del Prototipo

a. Servidor

El diseño general de la interacción usuario/servidor se ha visto simplificada de la versión inicial. Ahora, el servidor interactúa con los conserjes por medio de un sitio web a través de su Tablet (Ilustración 23). Por medio de esta interfaz, el conserje será capaz de agregar nuevos usuarios al sistema, buscar usuarios ya incorporados o eliminar registros.

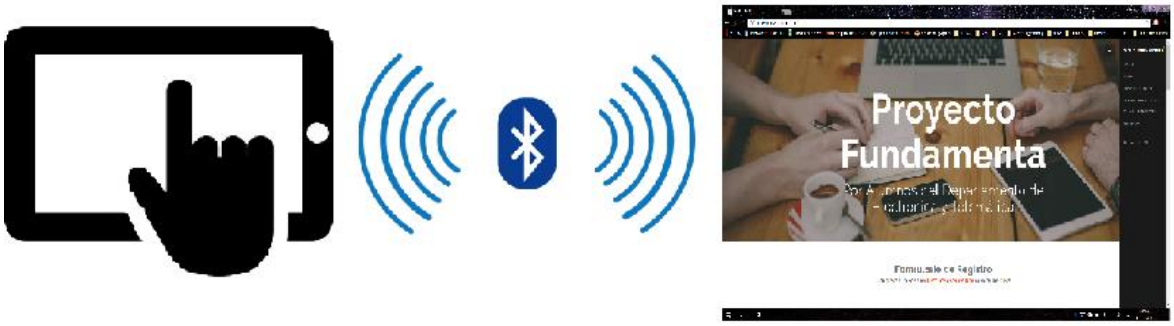


Ilustración 23: Diagrama de interacción entre Raspberry y Tablet de Conserje

El Tablet opera de manera desligada - sin conexión por cable, sino que por Bluetooth - al servidor, permitiéndole así operar de manera remota al *Lobby* del recinto. De esta manera el conserje tiene la libertad de registrar a usuarios en cualquier ubicación.

Se considera la alternativa de en una versión futura, cambiar el llamado por citófono tradicional hacia una notificación hacia el Tablet del conserje.

b. Aplicación

La aplicación interactúa con la Raspberry por medio de una conexión inalámbrica Bluetooth. Una vez iniciada en algún dispositivo - Smartphone o Tablet - comienza la comunicación de datos. Cada botón seleccionado por el usuario genera una petición al servidor, el cual responde con un mensaje emergente en la aplicación y al mismo tiempo el servidor genera una respuesta hacia los *GPIO*.

Ilustración 24: Diagrama de interacción entre Raspberry y aplicación usuarios.

c. Actuador

Una vez realizada la petición desde la aplicación al servidor, éste reacciona encendiendo leds según corresponda: led verde corresponder a la puerta, portón y ascensor y led rojo corresponde a pánico, éste último enciende de manera intermitente.

Para el prototipo funcional, se implementa un ascensor a escala, en el cual los mismos comandos que gobiernan los LED por medio de los *GPIO* de la Raspberry Pi, controlan los pisos: de esta manera por medio de la aplicación es posible controlar los pisos del ascensor en el modelo (ver Anexo).

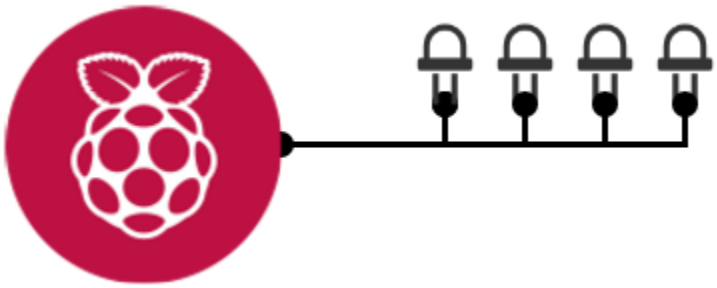


Ilustración 25: Diagrama de interacción entre Raspberry y Outputs

3. Descripción de Componentes

a. Servidor

El servidor es montado en una Raspberry Pi, con un sistema operativo Ubuntu 16.04 LTS, que consta de diversos módulos o componentes. Estos le permiten interactuar con los dispositivos de una manera eficiente y completa:

i. Servidor Web

El sitio web del servidor permite la interacción directa con el cliente: esta es la cara visible del servidor. Esto se encuentra programado en PHP, lo cual le permite al usuario utilizar códigos de alto nivel y transformarlos a bajo nivel, para luego estos ser interpretados por el servidor. De esta manera, el cliente solo ve imágenes o formularios y el código queda enmascarado.

ii. Base de Datos

Esta se encuentra desarrollada en mySQL, código y software de programación que permite la interacción directa al sitio web por medio de PHP y almacenar así, toda la información enviada. De esta manera, por medio del formulario dispuesto en el sitio web, la base de datos recoge y almacena información tales como RUN, serial, mail, fecha de ingreso al sistema y foto de perfil.

iii. Autentificación

Para impedir que un agente externo irrumpa en el sitio web y borre o extraiga los datos de la base de datos, se implementa un sistema de autentificación basado en las credenciales requeridas para PHPmyAdmin. Esta última es una interfaz web para el control, manejo y modificación de tablas y datos almacenadas en mySQL.

iv. PAND Bluetooth (22)

El concepto de PAND está elaborado bajo el enfoque de una interconexión de usuarios en un área determinado bajo el control de un dispositivo. Vale decir, es una "pequeña red" dentro de una LAN (Red de área Local). Luego, una de las tecnologías de comunicación que mejor le asienta es Bluetooth, ya que está diseñada para redes *Adhoc* en un rango no superior a 10 metros. Con estas dos tecnologías se forma lo que es una Bluetooth PAND lo que permite generar redes con tráfico de datos entre diversos dispositivos por medio de Bluetooth, dándoles la capacidad de acceder a sus respectivos servicios de red.

b. Cliente

i. Sistema operativo

La aplicación se ejecuta bajo el sistema operativo Android 4.0.3 o superior. La elección de éste se realiza considerando que abarca el 97,4% de los Smartphones y Tablet Android.

ii. Librerías en Android Studio

- Bluetooth: para la creación de Adapter, Device y Socket.
- Java: para la implementación de UUID del puerto serial de Bluetooth de la Raspberry, con tal de lograr comunicación desde la aplicación al servidor.

iii. Librerías Python

Se importan la librería GPIO para la interacción con los pines de salidas de la Raspberry Pi 3, con el fin de lograr que se enciendan los leds.

iv. Módulos Raspbian

Para lograr la comunicación directa entre la Raspberry Pi 3 y la aplicación móvil, fue necesario la instalación de los módulos Bluez y GPIO sobre el OS.

4. Interfaces Implementadas en el Prototipo

a. Servidor

Ilustración 26: Portada

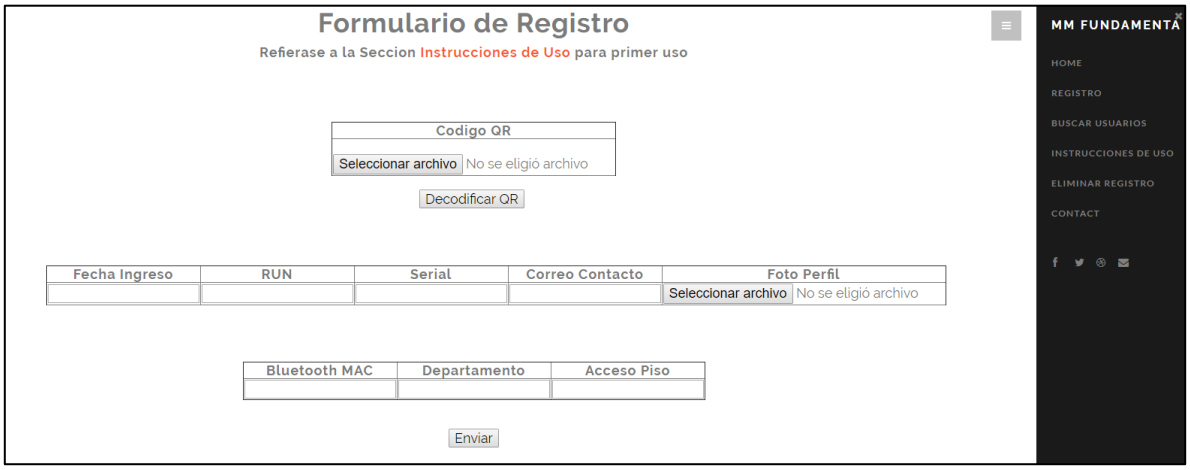


Ilustración 27: Formulario de Registro de Usuarios

Ilustración 28: Buscar Usuarios

Ilustración 29: Instrucciones de Uso

Ilustración 30: Eliminación de Usuarios. Su registro en la base de datos y foto de perfil serán eliminados

b. Aplicación

La primera imagen corresponde a la solicitud de permiso para el uso del Bluetooth, una vez aceptado, la aplicación de forma automática enciende el Bluetooth del dispositivo.

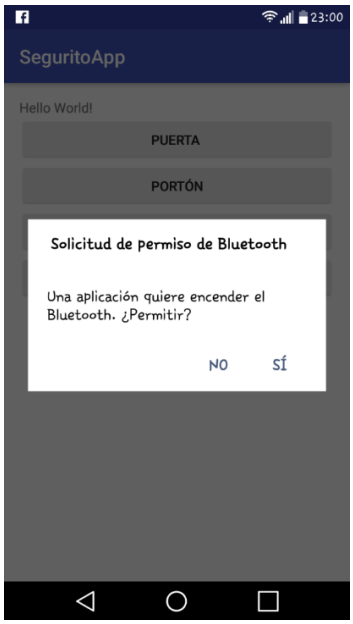


Ilustración 31: Solicitud de acceso Bluetooth.

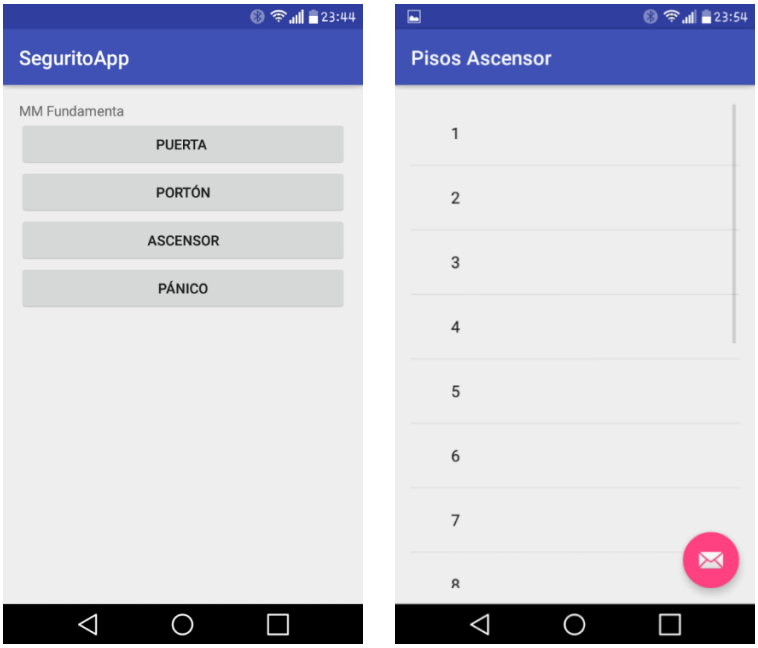


Ilustración 32: Vista principal y vista de pisos.

Verificación y Validación

1. Verificación

a. Servidor

El rol que desempeña un servidor en un sistema es vital, y es por ello que las etapas de verificación y validación son fundamentales. En lo que concierne a verificación:

Elemento	Verificación
Base de Datos	El servidor permite la creación, modificación y eliminación de datos, tablas y usuarios de PHPmyAdmin.
Web Server	Posee un sitio web al cual acceder por medio de la red local.
Bluetooth	Gestiona conexiones entre servidor y dispositivos móviles, controlando el emparejamiento y los privilegios.
Cámara	Permite subir a los formularios imágenes directas desde la cámara del dispositivo móvil.

b. Cliente

Elemento	Verificación
Código aplicación	El código compila sin errores ni *warnings*.
Dispositivos diversos	La aplicación funciona correctamente en distintos celulares, probados LG y Motorola.
Solicitud Bluetooth	La aplicación solicita el acceso de Bluetooth y en caso de confirmación lo activa automáticamente si éste se encuentra desactivado.
Vistas aplicación	La aplicación cuenta con dos vistas que funcionan correctamente.
Estado	La aplicación mantiene al usuario informado sobre el estado de su petición a través de mensajes emergentes y una pequeña ventana de diálogo.
Servidor RFCOM	El servidor RFCOMM se encuentra escuchando permanentemente en busca de peticiones.
Interacción led	Los leds se encuentran correctamente configurados a la Raspberry.

2. Validación

a. Servidor

i. Registro

El servidor permite la captura de datos mediante la interfaz desplegada en el sitio web, en donde se capturarán los datos del usuario como RUN, serial, correo electrónico, foto de perfil y MAC del dispositivo con el cual desea interactuar con el servidor. Luego, estos son almacenadas en la base de datos.

ii. Comunicación

Permite entablar un enlace por medio de Bluetooth entre servidor y dispositivo inteligente. A su vez permite la navegación por el sitio web e internet.

iii. Búsqueda

Se puede buscar usuarios registrados dentro de la base de datos, interactuando a través del sitio web, de esta manera el usuario no tiene que tener grandes conocimientos técnicos para utilizarlo. Para proteger los intereses de los usuarios, no se puede desplegar todos los datos, solo si se conoce el RUN.

iv. Registro

Por medio de un formulario en el sitio web, es posible la captura de datos para luego procesarla y enviarlas hacia la respectiva tabla en la base de datos.

v. Auto Explicativo

Este requerimiento no está absolutamente cubierto, ya que no toda persona está familiarizada con la navegación en nuevos sitios web. Es por esto que se crea un enlace a un tutorial el cual explica paso a paso cómo hacer uso de las herramientas disponibles. Cabe destacar que el acceso al menú de instrucciones esta también visible en el encabezado del registro de usuarios.

b. Cliente

i. Instalación

El Smartphone permite la instalación de aplicaciones de terceros, y en este caso la aplicación de seguridad creada. Se realiza mediante el traspaso del archivo ".apk" hacia el Smartphone.

ii. Emparejamiento

El Dispositivo debe tener una versión 3.0 o superior de Bluetooth y debe permitir el emparejamiento hacia otros dispositivos. Además, debe permitir ser configurado como un punto de acceso de red.

iii. Inicialización

Se instala la Aplicación en el Smartphone al traspasar hacia él archivo de la aplicación de seguridad Luego con un gestor de archivos se abre e instala. La primera vez que se abra solicitará el emparejamiento – si es que no se ha hecho – y se conectará al servidor.

iv. Comunicación

Los comandos enviados a través de los botones desplegados en la aplicación del Smartphone deben permitir el control de los *GPIO* de la Raspberry, pudiendo así controlar los dispositivos comandados por el servidor como los accesos al edificio, portón o ascensor.

3. Plan de Testing

a. Servidor

Ordenado de Pruebas Iniciales a Finales	Test
1	Determinar el comportamiento del servidor ante más de una solicitud de manera simultánea (múltiples formularios de registro o búsqueda).
2	Probar el sitio web en todas las plataformas de los diversos dispositivos móviles, para probar compatibilidad
3	Solicitar registro a individuos de poco conocimiento en navegación, para determinar que el sistema sea auto explicativo.
4	Determinar comportamiento del servidor ante corte inminente de suministro eléctrico y cambio al *bypass*.

b. Cliente

Pruebas	Test
Compilación	Compilación de códigos en Android Studio y Raspberry con la finalidad de solucionar errores de programación.
Distintos dispositivos	Probar la aplicación en diversos dispositivos móviles, como Tablet y Smartphone de distintas marcas.
Distintos usuarios	Solicitar a usuarios inexpertos que interactúen con el sistema, con el fin de recopilar la mayor cantidad de consejos.

4. Análisis Crítico y Evaluación de Riesgos

a. Servidor

La ventaja de operar en un sistema basado en UNIX:

- Carencia de virus informáticos (scripts autoejecutables).
- Todos los archivos se cifran de acuerdo a la contraseña del usuario.
- Las bases de datos en mySQL son cifradas por autentificaciones independientes a las cuentas de usuarios. Además, cada una de las credenciales generadas posee distintos privilegios (unos más amplio y otros más reducidos).
- Debido a que el sistema se encuentra aislado de Internet (Bluetooth PAND), para poder acceder a este se debe estar asociado al sistema.
- Para lograr vulnerar la red, se debe emparejar el dispositivo atacante al sistema por Bluetooth.

A su vez, las desventajas ocurren en las vulnerabilidades del sistema. Esto se debe a que los OS basados en UNIX son ampliamente programables y modificables. No cualquier usuario puede acceder y modificar estos archivos (permiso de *superusuario*); además que las contraseñas son almacenadas a través de un código *hash*. Pero en el caso de que una persona ajena al sistema consiga la contraseña de un *superusuario*, se genera el alto riesgo de la obtención de datos en el sistema.

Evento	**Nivel de Riesgo (1 al 5)**	**Forma de Prevención**
Hurto de contraseña de *superusuario*	1	–Toda persona con acceso al sistema debe proteger siempre sus contraseñas y no revelarlas a nadie. –Cambio periódico en las contraseñas
Ataque Informático	1	–Mantener los procedimientos y rutinas de forma confidencial. –Siempre solicitar al momento de registro la cédula de identidad, tanto a los residentes como visitas.
Falla de Componentes	3	– •Realizar copias periódicas de la tarjeta de memoria. •Monitorear la temperatura del sistema para prevenir sobrecalentamiento.

b. Cliente – Aplicación

- La máxima distancia soportada es de 10 metros, al sobrepasar este umbral la aplicación deja de funcionar sin informar al usuario. Además, se puede apreciar que a mayor distancia mayor lentitud al transmitir datos.
- La aplicación una vez abierta establece la comunicación con el servidor Bluetooth, sin necesidad de accionar algún botón, lo cual disminuye el tiempo de manipulación con el sistema.
- En caso de tener el Bluetooth apagado, la aplicación emite la solicitud de permiso para encender éste, lo cual disminuye el tiempo de manipulación con el sistema y previene el error de funcionamiento por parte del usuario.

Evento	Nivel de Riesgo (1 al 5)	Forma de Prevención
Hurto de dispositivo móvil	1	La MAC Bluetooth del dispositivo debe ser eliminada inmediatamente de la base de datos, a través del conserje. Así en caso de presentar requerimientos, éstos sean denegados por no contar con los permisos correspondientes.
Dispositivo móvil sin batería	1	El conserje puede optar de intermediario para realizar las solicitudes pertinentes al sistema.
Replicación de aplicación entre dispositivos móviles de manera no oficial	1	El sistema se debe encargar de no permitir el acceso, ya que éste posee un control de identificación MAC Bluetooth asociado a cada usuario.
Distancia conexión	2	Crear un sistema de alerta en el cual el usuario pueda reconocer si se encuentra dentro del umbral permitido.

Conclusión

La generación de una red Bluetooth PAN le otorga al sistema una robustez muy alta, la cual no podría ser alcanzada por redes LAN, pero trae consigo una desventaja: disminución en la cantidad de colas del servidor. Los servidores tipo LAMP históricamente se utilizan sobre redes LAN debido al buen manejo de colas debido al diseño de capas OSI (23). Al utilizar una red Bluetooth PAN como LAN, se fuerza al sistema a utilizar las capas perdiendo así gran capacidad de ancho de banda. Debido a lo anterior, se probó de forma experimental, que las redes Bluetooth PAN no son capaces de manejar más de 10 usuarios de forma simultánea.

De acuerdo al diseño del sistema, se cumple con todos los requisitos expuestos por el cliente, tales como no invasividad, filtrar peticiones – denegar o permitir acceso de forma selectiva – hechas al servidor, no interferir con la circuitería del ascensor y la generación de perfiles de usuarios, en el cual cada tipo de usuario cuenta con diversos privilegios a la hora de utilizar la aplicación. El problema en el diseño, es que utiliza de premisa que todos los usuarios andarían de forma permanente con su *Smartphone*, desbloqueado, cargado y listo para utilizar, ya que de lo contrario no se estaría respetando la no invasividad planteada por el cliente. En base a esto, el sistema muestra una fuerte dependencia al uso del *Smartphone*, impidiendo ingresar al recinto a aquellos usuarios: que tengan descargados sus dispositivos, han borrado accidentalmente la aplicación, se les ha acabado la energía, entre otros.

La utilización de una aplicación por *Smartphone* y de enlazarla vía Bluetooth al servidor, genera un sistema de vanguardia y que atrae a un mercado muy particular de clientes. El problema es que, al mismo tiempo, segmenta el mercado para usuarios que no están dispuestos a la utilización permanente del *Smartphone*, como lo pueden ser usuarios de edad avanzada que no estén familiarizados con el uso de estos, usuarios que no posean dispositivos inteligentes o inclusive aquellos que simplemente no están dispuestos a hacer uso de este sistema.

Finalmente, como se ha mencionado anteriormente, la utilización de Bluetooth como red PAN le otorga al sistema una robustez altísima, impidiendo ataques cibernéticos y vulneraciones a la base de datos, pero de acuerdo a conversaciones sostenidas vía correo electrónico con Bluetooth Inc, el costo de licencia, derechos de autor y usos de logo corresponden a US $8.000 anuales más un porcentaje sobre el costo de la aplicación. Este gasto tendrá que formar parte del cliente, y no cualquiera será capaz de solventarlo.

Trabajo Futuro

De la forma en que fue diseñado el sistema, deja la posibilidad de innumerables potenciales aplicaciones y usos que puede dársele al sistema. Entre ellos los que más destacan y que se encuentran muy cerca de desarrollo:

- Hacer uso de los correos electrónicos alojados en la base de datos, para enviar por medio de ellos los gastos comunes a cada departamento, como también notificaciones masivas de mantenciones programadas, reuniones, entre otros.

- Interconectar todos los edificios de la inmobiliaria y generar una base de datos general – además de las locales – de tal forma que actúe como respaldo en caso de daños al servidor local. Además, con la información a la cual se tendrá acceso, es viable desarrollar estadísticas, evaluar que segmento de clientes son los que están buscando este tipo de inmueble y prevenir robos al interior de los inmuebles debido a el nuevo perfil de ladrón el cual arrienda un departamento para solo tener acceso libre al edificio.

- Disponer un Tablet al interior de cada departamento con acceso directo a un sitio web personalizado, dándoles control del ascensor, portón y puerta de acceso, pudiendo así reducir el conflicto de la no invasividad y dando un paso hacia el internet de las cosas.

- Nuevas versiones de la aplicación permitirían la intercomunicación entre habitantes del inmueble, generando así sociabilización entre los habitantes, avisar en caso de problema, informar si uno de los habitantes sale de viaje y se escuchan ruidos al interior y de esta manera fomentar el civilismo en la comunidad del edificio.

- Como parte de unas de las solicitudes del cliente, se considera para versiones posteriores la localización de los usuarios dentro del recinto utilizando múltiples receptores Bluetooth posicionados en todos los pisos, otorgándole al conserje la capacidad de saber en tiempo real si el usuario que acaba de hacer ingreso al recinto se dirige al departamento que le corresponde o si está yendo a otro piso, en el segundo caso consultar a los habitantes del piso si están esperando visitas. De esta manera es viable saber de antemano si es que uno de los *Smartphones* de los clientes ha sido robado y un ladrón está tratando de obtener acceso al recinto.

Referencias

1. **Techtarget. [En línea] http://searchmobilecomputing.techtarget.com/definition/personal-area-network..**

2. Sensornet. [En línea] http://www.sensornet.cl/index.php/productos/item/252-rfid.

3. Juels, Ari. RFID Journal. [En línea] 28 de Febrero de 2005. http://www.rfidjournal.com/articles/view?1415.

4. NearFieldCommunication.org. NFC Comunnication. [En línea] http://nearfieldcommunication.org/technology.html.

5. Bioelectronix. [En línea] http://www.bioelectronix.com/what_is_biometrics.html.

6. The Verge. [En línea] Russell Brandom, 2016 de Mayo de 2016. http://www.theverge.com/2016/5/2/11540962/iphone-samsung-fingerprint-duplicate-hack-security.

7. IBM. [En línea] http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/magnetic/.

8. HowStuffWorks. [En línea] http://money.howstuffworks.com/personal-finance/debt-management/magnetic-stripe-credit-card.htm.

9. Jennifer Acosta Scott. CreditCards. [En línea] http://www.creditcards.com/credit-card-news/demagnetization-ruin-credit-card-magnetic-stripe-1273.php.

10. BCData. [En línea] http://bcdata.com/encoding.html.

11. NEC. [En línea] http://www.nec.com/en/global/solutions/biometrics/technologies/face_recognition.html.

12. KGuard Security. [En línea] http://www.kguardsecurity.com/global/p/el431-4wa713a/.

13. Swift. [En línea] https://swift.org/about/.

14. Bluetooth Org. [En línea] https://www.bluetooth.com/specifications/bluetooth-core-specification.

15. Brown, Matt. CRN. [En línea] 30 de Julio de 2015. http://www.crn.com/slide-shows/storage/300077615/top-8-best-selling-server-brands-of-2015-q2.htm?itc=ticker.

16. Interoute. [En línea] http://www.interoute.com/what-are-cloud-servers.

17. Top Ten Reviews. [En línea] http://www.toptenreviews.com/services/web-hosting/best-cloud-hosting/.

18. Ingenieria Electrónica y Proyectos PICmicro. [En línea] http://www.electronicaestudio.com/microcontrolador.htm.

19. Micro Controller Manufacturer. [En línea] https://microcontrollermanufacturer.wordpress.com/2013/09/25/top-ten-microcontroller-manufacturing-companies-across-the-globe-use-the-companies-listed-below/.

20. Censo INE (Instituto Nacional de Estadística). [En línea] 2012. www.ine.cl .

21. Raspberry Org. [En línea] https://www.raspberrypi.org/help/what-is-a-raspberry-pi/.

22. How to Forge. [En línea] https://www.howtoforge.com/bluetooth_pand_debian_etch.

23. Microsoft. [En línea] https://support.microsoft.com/es-cl/help/103884/the-osi-model-s-seven-layers-defined-and-functions-explained.

24. PAND. [En línea] http://searchmobilecomputing.techtarget.com/definition/personal-area-network.

25. Bluetooth PAND. [En línea] https://www.howtoforge.com/bluetooth_pand_debian_etch.

Anexo

Código PHP de lectura y procesamiento de códigos QR

En index.php

```
<?php
include_once('./lib/QrReader.php');
if(isset($_FILES['UploadFileField']))        //Si el formulario sube una
                                             //captura de pantalla, se
                                             //ejecuta el código
{
/*Toma el nombre del archivo, el tipo y el tamaño*/
        $UploadName = $_FILES['UploadFileField']['name'];
        $UploadName = "tmp.png";
        $UploadTmp = $_FILES['UploadFileField']['tmp_name'];
        $UploadSize = $_FILES['UploadFileField']['size'];


        if($UploadSize<512000)                   //Si el tamaño supera los 500 KB
                                                 //no será subido
        {
                if($UploadTmp)
                {
                //Se mueve el archivo a la carpeta temporal, se le asigna el
                //nombre tmp.png, se decodifica y se obtiene la cadena de
                //carácteres asociada

                        move_uploaded_file($UploadTmp, "Upload/$UploadName");
                        $file = $UploadName;
                        $qrcode = new QrReader('Upload/'.$file);
                        $text = $qrcode->text();

                        if(!empty($text))
                        {
                                $query = parse_url($text, PHP_URL_QUERY);
                                //Se extrae la dirección url asociada a la cédula de
                                //identidad

                                $count=0;
                                foreach (explode('&', $query) as $chunk)
                                {
```

```
 //El formato de la URL extraída es
//https://portal.sidiv.registrocivil.cl/docstatus?RUN=12345678-9&type=CEDULA
//&serial=1000000000 &mrz=123456789123456789102345 6
//Donde PHP_URL_QUERY extrae todos los datos después de slash, vale decir
// docstatus?RUN=12345678-9& type=CEDULA &serial=1000000000 &mrz
//=123456789123456789102345 6

//Por ende, por cada &, se extraerá el argumento que le sigue después del signo igual,
//el primero será el tipo de cedula (carnet o pasaporte), el segundo el serial y el tercero
//el RUN

                    $param = explode("=", $chunk);
                    if ($param)
                    {
                        switch($count)
                        {
                        case 0:
                            $run = $param[1];
                            $count++;
                            break;

                        case 1:
                            $count++;
                            break;
                        case 2:
                            $serial = $param[1];
                            $count++;
                            break;
                            }
                      }
                        }
                        $dia = date("D m Y");
                        $qr_link = $text;
                    }
                    else
                    {
                        $qrErr = "Codigo Ilegible, favor intente con otra captura";
                    }
                   }
                  }
                  else
                  {
                     $qrErr = "El tamaño de la imagen es superior al admitido (500 KB)";
                  }
            }
```

```
if(isset($_FILES['UploadPhotoField']))
{
//Similar al caso del QR, se sube la foto de perfil y luego es almacenada en el
//servidor bajo el nombre numeroderut.png

        $UploadPhotoName = $_FILES['UploadPhotoField']['name'];
        $UploadPhotoName = $_POST['run'].".jpg";
        $UploadPhotoTmp = $_FILES['UploadPhotoField']['tmp_name'];
        $UploadPhotoType = $_FILES['UploadPhotoField']['size'];


        if(empty($UploadPhotoTmp))
        {
                $photoErr = "Debe ingrear una Captura Facial";
        }
        else if($UploadPhotoTmp)
        {
                move_uploaded_file($UploadPhotoTmp,
                                "Upload/$UploadPhotoName");
                $photo = $UploadPhotoName;
        }
}
?>
```

./lib/QrReader.php

Código libre en github por Zxing

```
<?php

include_once ('Reader.php');
require_once ('BinaryBitmap.php');
require_once ('common/detector/MathUtils.php');
require_once ('common/BitMatrix.php');
require_once ('common/BitSource.php');
require_once ('common/BitArray.php');
require_once ('common/CharacterSetEci.php');//
require_once ('common/AbstractEnum.php');//
require_once ('BinaryBitmap.php');
include_once ('LuminanceSource.php');
include_once ('GDLuminanceSource.php');
include_once ('IMagickLuminanceSource.php');
include_once ('common/customFunctions.php');
include_once ('common/PerspectiveTransform.php');
include_once ('common/GridSampler.php');
include_once ('common/DefaultGridSampler.php');
include_once ('common/DetectorResult.php');
require_once ('common/reedsolomon/GenericGFPoly.php');
require_once ('common/reedsolomon/GenericGF.php');
include_once ('common/reedsolomon/ReedSolomonDecoder.php');
include_once ('common/reedsolomon/ReedSolomonException.php');
include_once ('qrcode/decoder/Decoder.php');
include_once ('ReaderException.php');
include_once ('NotFoundException.php');
include_once ('FormatException.php');
include_once ('ChecksumException.php');
include_once ('qrcode/detector/FinderPatternInfo.php');
include_once ('qrcode/detector/FinderPatternFinder.php');
include_once ('ResultPoint.php');
include_once ('qrcode/detector/FinderPattern.php');
include_once ('qrcode/detector/AlignmentPatternFinder.php');
include_once ('qrcode/detector/AlignmentPattern.php');
include_once ('qrcode/decoder/Version.php');
include_once ('qrcode/decoder/BitMatrixParser.php');
include_once ('qrcode/decoder/FormatInformation.php');
```

```
include_once ('qrcode/decoder/ErrorCorrectionLevel.php');
include_once ('qrcode/decoder/DataMask.php');
include_once ('qrcode/decoder/DataBlock.php');
include_once ('qrcode/decoder/DecodedBitStreamParser.php');
include_once ('qrcode/decoder/Mode.php');
include_once ('common/DecoderResult.php');
include_once ('Result.php');
include_once ('Binarizer.php');
include_once ('common/GlobalHistogramBinarizer.php');
include_once ('common/HybridBinarizer.php');

final class QrReader
{
   const SOURCE_TYPE_FILE = 'file';
   const SOURCE_TYPE_BLOB = 'blob';
   const SOURCE_TYPE_RESOURCE = 'resource';
   public $result;

   function __construct($imgsource, $sourcetype = QrReader::SOURCE_
                           TYPE_FILE,   $isUseImagickIfAvailable = true)
   {
         try {
         switch($sourcetype) {
            case QrReader::SOURCE_TYPE_FILE:
               if($isUseImagickIfAvailable && extension_loaded('imagick')) {
                  $im = new Imagick();
                  $im->readImage($imgsource);
               }else {
                  $image = file_get_contents($imgsource);
                  $im = imagecreatefromstring($image);
               }
               break;

            case QrReader::SOURCE_TYPE_BLOB:
               if($isUseImagickIfAvailable && extension_loaded('imagick')) {
                  $im = new Imagick();
                  $im->readimageblob($imgsource);
               }else {
                  $im = imagecreatefromstring($imgsource);
               }
               break;

            case QrReader::SOURCE_TYPE_RESOURCE:
```

```
                $im = $imgsource;
                if($isUseImagickIfAvailable && extension_loaded('imagick')) {
                    $isUseImagickIfAvailable = true;
                }else {
                    $isUseImagickIfAvailable = false;
                }
                break;
            }
            if($isUseImagickIfAvailable && extension_loaded('imagick')) {
                $width = $im->getImageWidth();
                $height = $im->getImageHeight();
                $source = new \Zxing\IMagickLuminanceSource($im, $width, $height);
            }else {
                $width = imagesx($im);
                $height = imagesy($im);
                $source = new \Zxing\GDLuminanceSource($im, $width, $height);
            }
            $histo = new \Zxing\Common\HybridBinarizer($source);
            $bitmap = new \Zxing\BinaryBitmap($histo);
            $reader = new \Zxing\Qrcode\QRCodeReader();
            $this->result = $reader->decode($bitmap);
        }catch (\Zxing\NotFoundException $er){
            $this->result = false;
        }catch( \Zxing\FormatException $er){
            $this->result = false;
        }catch( \Zxing\ChecksumException $er){
            $this->result = false;
        }
    }
    public function text()
    {
        if(method_exists($this->result,'toString')) {
            return  ($this->result->toString());
        }else{
            return $this->result;
        }
    }
    public function decode()
    {
        return $this->text();
    }
}
```

Características Tablet Lenovo Essential

Información extraída del sitio web del fabricante:
http://shop.lenovo.com/cl/es/tablets/lenovo/serie-a/tab3-7-essential/

Puerto Micro USB y ranura micro SD
Trabaja, juega, mirá o simplemente toca la hermosa pantalla de la TAB 3 7 Essential de 7", con alta resolución (1024 x 600) y tecnología IPS. La tecnología IPS facilita compartir lo que estás viendo con tus amigos, y con una pantalla táctil de alta transparencia, ultradelgada, cada imagen aparece más cercana, más clara y más nítida.

Dos excelentes cámaras
Con la Tab3 7 Essential tienes la opción de dos cámaras para capturar todos tus recuerdos. Utiliza la cámara frontal Visio de 0,3 megapíxeles para tomar selfies perfectas para compartir y chatear por web con tus amigos, y la cámara posterior de 2 MP, para capturar imágenes y videos brillantes.

Siempre lista para ti
Propulsada con una batería de 3450 mAh, esta tablet de bolsillo ofrece hasta 10 horas de batería con una sola carga. Ahora puedes disfrutar sin interrupciones de mirar películas, jugar a tus juegos preferidos o disfrutar las redes sociales sin necesidad de recargarla.

GPS satelital y 3G opcional
Nunca te desorientarás con el satélite GPS que funciona sin conexión. Los modelos con 3G también están disponibles para una verdadera experiencia móvil.

Audio Dolby®
La optimización de sonido Dolby® permite un sonido más alto y natural, sin distorsión, ya sea que estés escuchando con los auriculares o a través de los parlantes integrados de la tablet.

Procesador Quad-Core
Con el procesador MediaTek® 1.3 GHz quad-core, la Tab3 7 Essential es ideal para realizar multiples tareas, ofreciendo una experiencia más fluida con Android y eliminando las interferencias cuando juegas o miras video HD.

Hasta Android™ 5.1, Lollipop
Con la última versión de Android, prepárate para un rendimiento más rápido, más potente y con menos interrupciones. Encontrarás que es más fácil estar conectado, interactuar con otros y hasta administrar la energía de la batería. También puedes resguardar mejor tu Tab3 7 Essential y acceder a tus aplicaciones y juegos favoritos en Google Play Store, lo que te hará la vida mucho más placentera.

Aplicación de comunicación entre Raspberry y Aplicación en Smartphone

```
# -*- coding: utf-8 -*-

import os
import glob
import time
from bluetooth import *
import MySQLdb
import RPi.GPIO as GPIO

os.system('modprobe w1-gpio')

GPIO.setmode(GPIO.BCM)
GPIO.setup(17, GPIO.OUT)
GPIO.setup(22, GPIO.OUT)
GPIO.setup(23, GPIO.OUT)

DB_HOST = 'localhost'
DB_USER = 'mm-fundamenta'
DB_PASS = 'mm2016_fund'
DB_NAME = 'edificio_1'


def run_query(query=''):
     datos = [DB_HOST, DB_USER, DB_PASS, DB_NAME]

     conn = MySQLdb.connect(*datos)
     cursor = conn.cursor()
     cursor.execute(query)

     if cursor.fetchone()[0]:  # mac registrada
           data = 1

     else: # mac no registrada
           data = 0


     cursor.close()
     conn.close()

     return data

def run_query2(query=''):
        datos = [DB_HOST, DB_USER, DB_PASS, DB_NAME]

     conn = MySQLdb.connect(*datos)
     cursor = conn.cursor()
     cursor.execute(query)

     if query.upper().startswith('SELECT'):
                data = cursor.fetchall()

     else:
                conn.commit()
```

```
    data = None


    cursor.close()
    conn.close()

    return data


server_sock=BluetoothSocket( RFCOMM )
server_sock.bind(("",PORT_ANY))
server_sock.listen(1)

port = server_sock.getsockname()[1]

uuid = "94f39d29-7d6d-437d-973b-fba39e49d4ee"

advertise_service( server_sock, "MMFundamenta",
                   service_id = uuid,
                   service_classes = [ uuid, SERIAL_PORT_CLASS ],
                   profiles = [ SERIAL_PORT_PROFILE ],
                   protocols = [ OBEX_UUID ]
                    )
while True:
    print "Esperando conexion en RFCOMM canal %d" % port

    client_sock, client_info = server_sock.accept()
    print "Se acepta conexiòn desde ", client_info

    criterio = client_info[0]
    query = "SELECT COUNT(btmac) FROM usuarios WHERE btmac='%s'" %
criterio
    result = run_query(query)
    print result


    try:

          if result == 1:

                data = client_sock.recv(1024)
                     if len(data) == 0: break
                  print "received [%s]" % data

                if data == 'puerta':
                     GPIO.output(17, GPIO.HIGH)
                     data = 'Puerta abierta !'
                     time.sleep(1)
                     GPIO.output(17,GPIO.LOW)
                     time.sleep(1)
```

```
    elif data == 'porton':
          GPIO.output(22,GPIO.HIGH)
          data = 'Porton abierto!'
          time.sleep(1)
          GPIO.output(22,GPIO.LOW)
          time.sleep(1)

    elif data == 'piso1':
          GPIO.output(23,GPIO.HIGH)
          data = 'Ascensor en camino al piso 1!'
          time.sleep(1)
          GPIO.output(23,GPIO.LOW)
          time.sleep(1)

    elif data == 'mipiso':
     query = "SELECT floor FROM usuarios WHERE btmac='%s'" %criterio
     result = run_query2(query)
     print result[0][0] #piso cambiar pines de salida

     if result[0][0] == 1:
          GPIO.output(23,GPIO.HIGH)
          data = 'Ascensor en camino al primer piso!'
          time.sleep(1)
          GPIO.output(23,GPIO.LOW)
          time.sleep(1)
     elif result[0][0] == 2:
          GPIO.output(23,GPIO.HIGH)
          data = 'Ascensor en camino al piso 2!'
          time.sleep(1)
          GPIO.output(23,GPIO.LOW)
          time.sleep(1)
     elif result[0][0] == 3:
          GPIO.output(23,GPIO.HIGH)
          data = 'Ascensor en camino al piso 3!'
          time.sleep(1)
          GPIO.output(23,GPIO.LOW)
          time.sleep(1)
        else:
     print "Solo para personas que vivan en los tres primeros pisos"

     else:
          data = 'Error!'
          data = 'piso no valido!'

     else:
          print "Usuario no válido"
          data = 'No cuenta con permiso para ingresar!'

          client_sock.send(data)
          print "Enviando[%s]" %data
```

```
    except IOError:
          pass

    except KeyboardInterrupt:

          print "Desconectado"

          client_sock.close()
          server_sock.close()
          print "Todo listo"

          break
```

Ilustración 33: Ascensor a escala utilizado en la demostración de Prototipo Funcional