

**UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE INGENIERÍA
CARRERA DE INGENIERÍA ELECTRÓNICA**



**SISTEMA DE CONTROL DE ACCESOS MEDIANTE SENSOR
BIOMÉTRICO DE HUELLAS DACTILARES**

Caso de uso: Centro de datos de la Agencia Para el Desarrollo de la
Sociedad de la Información en Bolivia

Proyecto de grado para obtener el Título de Ingeniero Electrónico

POR: DANIEL JIMENEZ JEREZ

TUTOR ACADÉMICO: ING. MARCELO RAMÍREZ

COTUTOR: ING. ARTURO HERNANDEZ

LA PAZ - BOLIVIA

Diciembre, 2017

Dedicatoria

Este trabajo está dedicado a mi esposa, a mis padres, a mi hermana y a todas las personas que me impulsaron a culminar mi querida carrera, la cual decidí estudiar cuando apenas comenzaba a aprender a leer y ahora gracias a todas las personas a mi alrededor puedo ver uno de mis sueños realizados.

Agradecimientos

Los más sinceros agradecimientos a mis tutores, Ingeniero Marcelo Ramírez e Ingeniero Arturo Hernandez, que pusieron a disposición todos sus conocimientos sin esperar nada a cambio y me apoyaron durante el transcurso del desarrollo de este proyecto.

A Nicolás y Sylvain que confiaron en mí al momento de seleccionarme para trabajar a su lado y de los cuales pude aprender un sin fin de cosas tanto en el ambiente laboral como en el personal.

A Ariel, Pedro, Carlos y Erick por brindarme su apoyo en todo momento y enseñarme el valor de la amistad.

Resumen

En el presente proyecto se desarrolla un sistema que cumple dos funciones, la primera es la de controlar la apertura de puertas mediante un subsistema que recoge los datos que envían los sensores de huellas dactilares, mismos que son procesados para verificar los permisos de un usuario para acceder por una de las puertas. La segunda función es la de hacer un puente interfaz entre el sensor de huellas dactilares y el servidor MQTT, este último será el que envíe las órdenes para realizar alguna acción en los sensores como por ejemplo la de grabar una huella en una posición definida de la base de datos.

En este proyecto también se desarrollan los programas necesarios para ambos usos del hardware obtenido, a su vez se desarrollan las bases de datos que se utilizan para las secuencias de acciones del sistema, así como también para almacenar los datos de los usuarios y los componentes del sistema.

Se analizan los conceptos fundamentales de seguridad física de ambientes e infraestructura que se contrastan con normas nacionales e internacionales. Por tal motivo también se realiza un estudio de las vulnerabilidades del sistema desarrollado y los pasos a seguir para evitar ataques o fallas en el sistema.

Por último también se realiza un estudio de costos y una comparación del sistema propuesto frente a un sistema de características similares que puede encontrarse en el mercado, para concluir con la realización de una instalación piloto en el centro de datos de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.

Palabras claves: Biométrico, Puertas, Accesos, Sensores, MQTT, Arduino, PostgreSQL, Node

Abstract

The present project performs the development of a system fulfills two functions, the first is to control the opening of doors by means of a subsystem that collects the data sent by the fingerprint sensors, which are processed to verify the permissions of a user to access by one of the doors. The second function is to make an interface bridge between the fingerprint sensor and the MQTT server, this latter will be the one that sends the commands to perform some action on the sensors such as for example recording a fingerprint in a defined position of the database.

This project also develops the necessary programs for both functions of the obtained hardware, in turn develop the databases that are used for the sequences of actions of the system, as well as for storing users data and system components.

It will be analyze the most important concepts of physical security of environments and infrastructure that are contrasted with national and international standards. For this reason also It will be performs a study of the vulnerabilities of the system developed and the steps to follow to avoid attacks or failures in this system.

Finally, will be performs a study of costs and a comparison of the proposed system against a system of similar characteristics that can be found in the market, in order to conclude with the realization of a pilot installation in the data center of the Agency for the Development of The Information Society in Bolivia.

Keywords: Biometric, Doors, Access, Sensors, MQTT, Arduino, PostgreSQL, Node

Índice general

| | |
|---|----------|
| Índice de figuras | X |
| Índice de cuadros | XIII |
| Índice de anexos | XV |
| 1 Presentación general del proyecto | 1 |
| 1.1 Introducción | 1 |
| 1.2 Antecedentes | 3 |
| 1.3 Planteamiento del problema | 4 |
| 1.4 Objetivos | 4 |
| 1.4.1 Objetivo general | 4 |
| 1.4.2 Objetivos específicos | 4 |
| 1.5 Justificación | 5 |
| 1.5.1 Justificación tecnológica | 5 |
| 1.5.2 Justificación institucional | 5 |
| 1.5.3 Justificación legal | 6 |
| 1.6 Alcances del proyecto | 6 |
| 2 Marco Teórico | 8 |
| 2.1 Estado del arte | 8 |
| 2.1.1 Técnicas de reconocimiento de identidad | 9 |
| 2.1.1.1 Reconocimiento mediante el iris | 9 |
| 2.1.1.2 Forma de las manos | 9 |
| 2.1.1.3 Contorno del rostro | 10 |
| 2.1.1.4 Huellas dactilares | 10 |
| 2.2 Sensores biométricos de huella dactilar | 10 |
| 2.2.1 Clasificación de sensores | 10 |

| | | |
|----------|---|-----------|
| 2.2.2 | Estándares técnicos | 12 |
| 2.3 | Fundamentos de seguridad | 12 |
| 2.4 | Biometría | 13 |
| 2.5 | Huella dactilar | 14 |
| 2.5.1 | Propiedades físicas de las huellas dactilares | 15 |
| 2.5.2 | Características de las huellas dactilares | 16 |
| 2.5.3 | Tipos de huellas dactilares | 18 |
| 2.5.4 | Aplicaciones | 19 |
| 2.6 | Sistemas de hardware embebido | 19 |
| 2.7 | Ethernet | 20 |
| 2.7.1 | POE (Power Over Ethernet) | 22 |
| 2.8 | Software | 23 |
| 2.8.1 | Internet de las cosas | 23 |
| 2.8.2 | Entorno de ejecución | 25 |
| 2.8.3 | Base de datos | 26 |
| 3 | Ingeniería del Proyecto | 27 |
| 3.1 | Estado previo a la instalación piloto del sistema en ADSIB | 27 |
| 3.1.1 | Especificación de requisitos a satisfacer con el desarrollo del sistema | 29 |
| 3.2 | Perspectiva global del sistema propuesto | 31 |
| 3.2.1 | Selección del sensor biométrico | 31 |
| 3.2.1.1 | Tasa de falso rechazo y tasa de falsa aceptación | 31 |
| 3.2.2 | Selección de los protocolos de comunicación | 36 |
| 3.2.3 | Selección del dispositivo de procesamiento de datos para el hardware de control y la interfaz sensorial | 41 |
| 3.2.3.1 | Selección del dispositivo controlador Ethernet para el hardware de control y la interfaz sensorial | 42 |

| | | |
|---------|---|----|
| 3.2.3.2 | Selección de la frecuencia de reloj para el microcontrolador ATmega328P | 43 |
| 3.2.4 | Selección del núcleo del dispositivo registrador de nuevas huellas | 48 |
| 3.2.5 | Selección del método de respaldo | 50 |
| 3.2.5.1 | Selección del módulo bluetooth | 50 |
| 3.2.5.2 | Selección del dispositivo de procesamiento de datos . . | 50 |
| 3.2.6 | Selección de la cerradura eléctrica | 51 |
| 3.2.7 | Selección de la base de datos | 51 |
| 3.2.8 | Diagrama de red del sistema de control de accesos | 51 |
| 3.2.9 | Diagrama de flujo para el ingreso posterior a la instalación del sistema desarrollado | 53 |
| 3.3 | Secuencia de acción para el registro de una nueva huella | 55 |
| 3.3.1 | Registro de usuarios en el servidor LDAP | 57 |
| 3.3.2 | Base de datos de huellas | 59 |
| 3.3.2.1 | Forma normal 1 para la base de datos de huellas | 60 |
| 3.3.3 | Hardware registrador de huellas | 62 |
| 3.4 | Secuencia de acción para el acceso mediante sensor biométrico de huellas dactilares | 65 |
| 3.4.1 | Hardware de control e interfaz sensorial | 67 |
| 3.4.1.1 | Separador POE, energía y datos | 67 |
| 3.4.1.2 | Conexión de red ENC28J60 | 69 |
| 3.4.2 | Base de datos del sistema de control de accesos | 76 |
| 3.4.2.1 | Forma normal 1 para la base de datos de accesos | 76 |
| 3.4.2.2 | Forma normal 2 para la base de datos de accesos | 77 |
| 3.4.2.3 | Forma normal 3 para la base de datos de accesos | 78 |
| 3.5 | Secuencia de acción para la apertura desde el interior | 82 |
| 3.6 | Secuencia de acción para el envío de una nueva huella a los sensores . . . | 84 |
| 3.7 | Secuencia de acción para la apertura mediante el respaldo bluetooth . . . | 87 |

| | | |
|--------------------|---|------------|
| 3.8 | Servicio web para la administración del sistema | 90 |
| 4 | Análisis y evaluación | 101 |
| 4.1 | Análisis de costos | 101 |
| 4.1.1 | Costo del dispositivo de control central | 102 |
| 4.1.2 | Costo del dispositivo de interfaz sensorial | 103 |
| 4.1.3 | Costo de la cerradura de cada puerta | 105 |
| 4.2 | Análisis de vulnerabilidades | 106 |
| 4.3 | Resultados de la prueba piloto | 109 |
| 5 | Conclusiones y recomendaciones | 115 |
| 5.1 | Conclusiones | 115 |
| 5.2 | Recomendaciones | 116 |
| Referencias | | 118 |
| Anexos | | 125 |

Índice de figuras

| | | |
|----|--|----|
| 1 | Biometría | 14 |
| 2 | SmartID, autenticación segura | 14 |
| 3 | Anexos cutáneos | 16 |
| 4 | Tipos de minucias | 17 |
| 5 | Corazón y Delta | 17 |
| 6 | Tipos de huellas dactilares | 18 |
| 7 | Power Over Ethernet | 23 |
| 8 | Internet de las cosas | 24 |
| 9 | Número de dispositivos conectados por persona | 25 |
| 10 | Diagrama de flujo para el ingreso antes de la instalación del sistema desarrollado | 28 |
| 11 | Diagrama de bloques del sistema de control de accesos | 31 |
| 12 | Punto de equilibrio EER | 32 |
| 13 | Tasa de error vs Sensibilidad | 33 |
| 14 | Arduino UNO SMD R3 | 42 |
| 15 | Ethercard | 43 |
| 16 | Captura de forma de onda de transmisión serial a 57600Hz | 45 |
| 17 | Captura de forma de onda de transmisión serial a 58824Hz | 46 |
| 18 | Diagrama de red del sistema | 52 |
| 19 | Diagrama de flujo posterior | 53 |
| 20 | Diagrama de flujo para el registro de una nueva huella | 56 |
| 21 | Diagrama de bloques del equipo registrador de huellas | 57 |
| 22 | Registro de usuario en el servidor de LDAP | 59 |
| 23 | Imagen de huella generada desde el sensor ZhianTec ZFM-20 | 60 |
| 24 | Diagrama entidad-relación para la base de datos de huellas | 61 |

| | | |
|----|---|----|
| 25 | Base de datos de huellas | 61 |
| 26 | Prototipo del hardware grabador de huellas | 62 |
| 27 | Diagrama de flujo para la apertura de puerta mediante biométrico | 66 |
| 28 | Diagrama de bloques de los dispositivos de control e interfaz sensorial | 67 |
| 29 | Diagrama de bloques del Splitter POE | 68 |
| 30 | Prototipo del circuito de interfaz sensorial | 71 |
| 31 | Prototipo del circuito de control de actuadores | 73 |
| 32 | Conexión de las cerraduras electromagnéticas | 74 |
| 33 | Diagrama entidad-relación para la base de datos de control de accesos | 79 |
| 34 | Base de datos de control de accesos | 80 |
| 35 | Diagrama para la apertura de una puerta desde el interior | 82 |
| 36 | Botón pulsador para la apertura desde el interior | 83 |
| 37 | Diagrama para envío de huellas a los sensores | 84 |
| 38 | Diagrama para apertura mediante respaldo bluetooth | 88 |
| 39 | Pantalla de vinculación de la aplicación Android | 88 |
| 40 | Pantalla de envío de contraseña de la aplicación Android | 89 |
| 41 | Conexión del módulo bluetooth HC-05 | 89 |
| 42 | Página de login del servicio web | 90 |
| 43 | Página de monitoreo del servicio web | 91 |
| 44 | Página de lista de usuarios del servicio web | 92 |
| 45 | Página de imagen de la huella del servicio web | 92 |
| 46 | Página de permisos indefinidos del servicio web | 93 |
| 47 | Página de permisos temporales del servicio web | 94 |
| 48 | Página de clientes MQTT del servicio web | 95 |
| 49 | Página de dispositivos de control del servicio web | 96 |
| 50 | Página de programa de control del servicio web | 96 |
| 51 | Página de dispositivos de interfaz sensorial del servicio web | 97 |
| 52 | Página de programa de interfaz sensorial del servicio web | 97 |

| | | |
|----|--|-----|
| 53 | Página de puertas del servicio web | 98 |
| 54 | Página de historial de accesos del servicio web | 99 |
| 55 | Página de historial de respuestas del servicio web | 99 |
| 56 | Página de usuario sin privilegios del servicio web | 100 |
| 57 | Programador USB-ISP | 110 |

Índice de cuadros

| | | |
|----|--|----|
| 1 | Formato de la trama IEEE 802.3 | 21 |
| 2 | Características de los sensores biométricos | 34 |
| 3 | Comparación de sensores de huella digital | 34 |
| 4 | Comparativa del medio cableado vs el medio inalámbrico | 37 |
| 5 | Comparación entre protocolos IoT | 38 |
| 6 | Comparación de envío de mensajes entre HTTPS y MQTT | 39 |
| 7 | Comparación de recepción de mensajes entre HTTPS y MQTT | 40 |
| 8 | Comparación de consumo de batería con señales de Keep Alive | 40 |
| 9 | Error de tasa de bits a 8MHz | 46 |
| 10 | Error de tasa de bits a 16MHz | 47 |
| 11 | Comparación Raspberry vs Cubieboard | 49 |
| 12 | Datos de prueba para la base de datos de huellas | 60 |
| 13 | Reducción a la Forma Normal 1 de la base de datos de huellas | 61 |
| 14 | Cálculo de potencia consumida por cada dispositivo capturador de huellas | 63 |
| 15 | Parámetros para el cálculo de potencia consumida del capturador de huellas | 64 |
| 16 | Potencia consumida por el dispositivo registrador de huellas al extremo receptor POE | 65 |
| 17 | Estándares 802.3af A y B, perspectiva desde el inyector | 68 |
| 18 | Cálculo de potencia consumida por cada dispositivo interfaz sensorial | 71 |
| 19 | Parámetros para el cálculo de potencia consumida por la interfaz sensorial | 72 |
| 20 | Potencia consumida por el dispositivo interfaz sensorial al extremo receptor POE | 72 |
| 21 | Cálculo de potencia consumida por cada dispositivo de control | 74 |
| 22 | Parámetros para el cálculo de potencia consumida por la placa de control | 75 |
| 23 | Potencia consumida por la placa de control al extremo receptor POE | 75 |

| | | |
|----|---|-----|
| 24 | Reducción a la Forma Normal 1 de la base de datos de accesos | 76 |
| 25 | Reducción a la Forma Normal 2 de la base de datos de accesos | 77 |
| 26 | Reducción a la Forma Normal 3 de la base de datos de accesos | 78 |
| 27 | Instrucción de handshake para el sensor de huellas | 85 |
| 28 | Respuesta de handshake desde el sensor de huellas | 85 |
| 29 | Instrucción modificada de handshake para el sensor de huellas | 86 |
| 30 | Comparación de costos para el dispositivo de control | 102 |
| 31 | Comparación de costos para el dispositivo interfaz sensorial | 104 |
| 32 | Comparación de costos para la cerradura magnética | 105 |
| 33 | Materiales y presupuesto utilizados en la instalación piloto | 112 |

Índice de Anexos

| | | |
|----|---|-----|
| 1 | Repositorios de los proyectos desarrollados para el sistema de control de accesos en Github | 125 |
| 2 | Documento de conclusión de instalación piloto en ADSIB | 126 |
| 3 | Esquemático de la placa de interfaz sensorial | 127 |
| 4 | Lado superior del PCB de la placa de interfaz sensorial | 128 |
| 5 | Lado inferior del PCB de la placa de interfaz sensorial | 129 |
| 6 | Circuitos del lado superior de la placa de interfaz sensorial | 130 |
| 7 | Circuitos del lado inferior de la placa de interfaz sensorial | 131 |
| 8 | Esquemático de la placa de respaldo bluetooth | 132 |
| 9 | Lado superior del PCB de la placa de respaldo bluetooth | 133 |
| 10 | Lado inferior del PCB de la placa de respaldo bluetooth | 134 |
| 11 | Circuitos del lado superior de la placa de respaldo bluetooth | 135 |
| 12 | Circuitos del lado inferior de la placa de respaldo bluetooth | 136 |
| 13 | Esquemático Raspberry Pi 3 B Modelo V1.2 | 137 |
| 14 | Hoja de datos de cables HSM Wire International Inc. según AWG | 138 |
| 15 | Esquemático Módulo Relé 5V Henry Bench | 139 |
| 16 | Esquemático Arduino Uno R3 | 140 |
| 17 | Esquemático Splitter POE LTC4267 | 141 |
| 18 | Esquemático Ethernet Controller ENC28J60 | 142 |

Capítulo 1

Presentación general del proyecto

En este capítulo se muestran los antecedentes del proyecto, el planteamiento del problema que se desea solucionar, los objetivos finales del desarrollo del sistema, la justificación institucional, tecnológica y legal para desarrollar el sistema y el alcance que tiene el sistema desarrollado.

1.1. Introducción

El presente proyecto tiene como finalidad desarrollar un sistema de control de accesos que identifique a las personas por medio de sus huellas dactilares para realizar la apertura de puertas de acuerdo a los permisos otorgados a cada individuo almacenados en una base de datos, de esta manera se cubrió la necesidad de un sistema de control de accesos que permite registrar, restringir y monitorear los ingresos a los diferentes ambientes del centro de datos de la institución estatal Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB).

Los ambientes que requieren ser protegidos necesitan métodos actuales para el reconocimiento de la identidad de las personas que permitan registrar y monitorear el ingreso de personas en tiempo real; debido a la naturaleza de estos ambientes que contienen tanto elementos tangibles, es decir de un valor económico representativo, como elementos intangibles por la sensibilidad de la información, es que se cubrieron todos los aspectos posibles mencionados en estándares para este tipo de sistemas.

Durante el desarrollo del proyecto se especifican las características, las secuencias de acciones y los criterios de selección para los dispositivos que conforman el sistema, así como la instalación del mismo.

Se muestran los servicios desarrollados para el servidor y el hardware embebido, así como el proceso de instalación de los mismos, como ser el servicio de bases de datos, el servicio de mensajería para intercambio de información con el hardware, la interfaz de aplicación del backend y la aplicación web para una administración cómoda del sistema.

Se utilizó la arquitectura REST¹ como proveedor de servicios, ya que conlleva muchas ventajas, entre ellas la descentralización de servicios y el enfoque actual de micro-servicios; también mejora la compatibilidad con otros sistemas, la escalabilidad y la seguridad durante el acceso a los datos.

Se utilizaron protocolos con estándares abiertos como MQTT², uno de los protocolos de comunicación más ligeros, muy útil en la comunicación Máquina-Máquina, que mejora a sus antecesores como AMQP³ o XMPP⁴. Este protocolo es utilizado desde proyectos básicos hasta proyectos de alto calibre como el de la comunicación humano-robot que utiliza la NASA⁵ para enviar órdenes desde la tierra a los robots que trabajan en el espacio.[23]

Se detallan también los recursos de hardware a utilizar y los diseños de los diagramas esquemáticos, de conexión, comunicación y secuencias de acciones del sistema. Se presentan los programas utilizados para configurar los diferentes dispositivos en función de las diferentes acciones del sistema.

Se muestran modelos de entidad-relación con los cuales se generan las bases de datos y también los estándares de los protocolos utilizados para la comunicación máquina-máquina.

El trabajo presentado contribuye al conocimiento colectivo ya que el código fuente y los

¹REpresentational State Transfer

²MQ Telemetry Transport o Message Queue Telemetry Transport

³Advanced Message Queuing Protocol

⁴eXtensible Messaging and Presence Protocol

⁵National Aeronautics and Space Administration

esquemáticos quedarán disponibles para su uso, estudio, modificación y redistribución, gracias a la licencia de software libre LPG-Bolivia⁶ que se encuentra reconocida legalmente en Bolivia desde el 13 de Mayo de 2014, fecha anterior a la presentación de este proyecto.

1.2. Antecedentes

Este trabajo es motivado por la necesidad de seguridad en los ambientes del centro de datos de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB). Debido al grado de importancia de la información que contienen los computadores de dichos ambientes es que surge este proyecto. A pesar de que en el mercado se pueden hallar sistemas similares, se ha decidido desarrollar este sistema debido a:

- El valor de un sistema en el mercado es bastante elevado con respecto al costo del desarrollo del sistema propuesto en este proyecto, como se puede observar en diferentes páginas web donde el valor de un sistema con características similares se encuentra por encima de los 3000Bs. por puerta, mientras que para el sistema propuesto se cuenta con un presupuesto promedio de 1600Bs. por puerta.⁷
- Los sistemas similares comerciales presentan restricciones en cuanto a la escalabilidad de los nodos ubicados en cada punto de acceso y al número de puertas que se puede llegar a controlar, además de la compatibilidad limitada con dispositivos de otras marcas.
- Debido a que la prueba piloto fué realizada en la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia que es una entidad pública, esta entidad se adhiere a la Ley de Telecomunicaciones, que en sus artículos 75 a 77 hace mención al uso prioritario de Software Libre y Estándares Abiertos, por lo cual se ahonda

⁶Licencia Pública General Bolivia para registro de software de código abierto

⁷ACT, Soluciones en Seguridad, Lista de precios 2017

en el esfuerzo de utilizar tecnologías de software libre y hardware libre durante el desarrollo de este proyecto.⁸

1.3. Planteamiento del problema

La Agencia para el Desarrollo de la Sociedad de la Información en Bolivia precisa de un método de control de accesos mediante el cual pueda registrar, restringir y monitorear los accesos de personas a los ambientes de su centro de datos, es por este motivo que busca un método accesible mediante tecnologías de hardware y software libre para prescindir de otros tipos de accesos con un mayor grado de inseguridad como ser llaves, tarjetas magnéticas o contraseñas numéricas.

1.4. Objetivos

1.4.1. Objetivo general

- Desarrollar un sistema de seguridad para el control de accesos mediante el uso de sensores biométricos de huellas dactilares demostrando su funcionamiento mediante la instalación del mismo en el centro de datos de la Agencia Para el Desarrollo de la Sociedad de la Información en Bolivia.

1.4.2. Objetivos específicos

- Evaluar el estado anterior y posterior a la instalación del sistema en el centro de datos de ADSIB.

⁸Ley N° 164, Ley de Telecomunicaciones, 8 de Agosto del 2011

- Desarrollar las bases de datos necesarias que almacenen la información útil para el sistema de control de accesos.
- Diseñar y programar el dispositivo de hardware para el control de puertas y el nodo sensor de huellas dactilares.
- Diseñar y programar el dispositivo de hardware para el respaldo bluetooth que se constituye como una manera adicional de apertura de emergencia en caso de producirse fallas en el sistema.
- Desarrollar las secuencias de acción que definan las diferentes maneras de apertura de las puertas en las instalaciones.
- Desarrollar una página web para la administración y el monitoreo del sistema.
- Efectuar la instalación del prototipo del sistema obtenido, en los ambientes del centro de datos de ADSIB.

1.5. Justificación

1.5.1. Justificación tecnológica

Este proyecto brinda un aporte de valor tecnológico por la originalidad del diseño y los medios utilizados en el desarrollo del hardware y del software para este sistema.

1.5.2. Justificación institucional

La ADSIB busca en primera instancia la opción de un sistema de control de accesos centralizado basado en hardware y software libre y al no encontrar un sistema con estas

características en el mercado o entre los desarrollos en Internet abre la oportunidad para que una persona o grupo de personas puedan desarrollar un sistema de este tipo.

1.5.3. Justificación legal

Dentro de los subproyectos para la implementación del centro de datos de ADSIB surge la necesidad de establecer un método de control de accesos a las instalaciones, para la cual la ADSIB firma un convenio de cooperación interinstitucional con AGETIC⁹, donde AGETIC tiene entre sus obligaciones, colaborar con las tareas necesarias para coadyuvar con la implementación del centro de datos de ADSIB como se menciona en el Artículo N° 7 del Decreto Supremo 2514¹⁰, AGETIC tiene la función de promover procesos de investigación, innovación y desarrollo en Gobierno Electrónico y Tecnologías de Información y Comunicación. De esta manera los materiales necesarios para el desarrollo de este proyecto que no se dispongan en ADSIB serán proporcionados por AGETIC gracias a este convenio interinstitucional.

1.6. Alcances del proyecto

En cuanto al hardware, el proyecto se limita al diseño de dos dispositivos de hardware, el primero funciona como un dispositivo de control central escalable para poder controlar un número muy grande de puertas y también como un dispositivo de interfaz sensorial que es instalado en cada una de las puertas, este dispositivo cuenta con alimentación de energía en el mismo cable de red mediante la tecnología de Power Over Ethernet. El segundo dispositivo es un respaldo bluetooth que sirve como método de apertura alternativa de hasta dos puertas para situaciones de emergencia o en caso de fallas del sistema.

⁹Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación

¹⁰Decreto Supremo 2514, 9 de Septiembre de 2015

En cuanto al software, el proyecto se limita al desarrollo de la base de datos, el desarrollo del backend en el servidor, el desarrollo del cliente web para la administración y monitoreo del sistema, la implementación de seguridad durante la etapa de conexión de los dispositivos de hardware mediante credenciales de usuario y contraseña y el diseño del software para los dispositivos de hardware desarrollados.

El alcance en cuanto a la prueba piloto del proyecto cubre cinco ambientes del centro de datos de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.

Los alcances fueron delimitados de acuerdo a los requisitos de la ADSIB en la etapa preliminar al desarrollo del sistema.

Capítulo 2

Marco Teórico

Este capítulo muestra los conceptos básicos y necesarios acerca de los sensores biométricos, fundamentos de seguridad, estándares de biometría, hardware embebido y el protocolo MQTT. También se muestra lo más sobresaliente de la historia de la identificación de personas y las características y propiedades de las huellas dactilares.

2.1. Estado del arte

La biometría (del griego *bios* vida y *metron* medida) es el estudio para el reconocimiento único de humanos basados en uno o más rasgos conductuales o rasgos físicos intrínsecos.[40]

La identificación y autenticación de personas por medio de la verificación de los rasgos físicos es una aplicación muy desarrollada dentro del ámbito de las tecnologías de la información. La biometría de identificación por medio de la comparación de huellas dactilares data desde hace alrededor de 100 años y se encuentra entre los medios más usados de identificación de personas en la actualidad, esto se debe al relativo bajo coste de los dispositivos necesarios para capturar la imagen de las huellas dactilares.

Cada persona tiene rasgos únicos que la diferencian de las demás. Entre estos rasgos podemos encontrar la voz, la forma del rostro, el iris de los ojos, termograma del rostro, mapa de venas de la mano, patrones de la retina y las huellas dactilares.

Durante la última década se ha observado el avance en la miniaturización y el uso de escáneres de huellas dactilares en dispositivos de uso diario como teléfonos móviles y computadoras portátiles.

La biometría electrónica, se acaba de incorporar a las transacciones bancarias por medio de

identificación de personas en cajeros automáticos, por tanto se puede usar como referencia para aspectos de seguridad dado su alto grado de fiabilidad.

2.1.1. Técnicas de reconocimiento de identidad

2.1.1.1. Reconocimiento mediante el iris

Estas técnicas son tan fiables que se pueden encontrar sensores de iris en aeropuertos internacionales como los de E.E.U.U., Canadá y los demás que forman parte del programa NEXUS y CANPASS Air¹.

Existen varias técnicas que se usan actualmente, entre las cuales se pueden mencionar: las de reconocimiento de cambios espaciales en la estructura de una imagen que destaca los patrones representativos, captura de imágenes basadas en la reflexión especular de la córnea, filtros artificiales de color que proveen el discriminante ortogonal para el discriminante espacial de patrones.[48]

2.1.1.2. Forma de las manos

Algunas de las técnicas utilizadas para reconocer la forma de las manos son por ejemplo: realizar transformaciones euclidianas para separar y reconocer dedos rígidos para introducir un modelo elíptico que representa los dedos y busca la alineación de los mismos, descomposición de imágenes en sub-bandas de frecuencias para su procesamiento.[13]

¹Canadian Passenger Accelerated Service System

2.1.1.3. Contorno del rostro

Las técnicas que se utilizan para detectar rostros se basan en el análisis y combinación de imágenes de luz visible e imágenes de luz infrarroja, de las cuales se puede realizar el procesamiento mediante técnicas de reconocimiento 2D y 3D, con los métodos holísticos donde cada pixel es una característica, métodos geométricos que comparan vectores característicos extraídos del perfil y métodos tridimensionales que comparan características mediante múltiples imágenes tomadas con un sistema multi-cámara.[50]

2.1.1.4. Huellas dactilares

Se obtienen todos los rasgos únicos de las huellas, para luego hacer un balance entre la maximización del número de correspondencias y minimización total de los rasgos entre todas las huellas almacenadas de referencia.[13]

2.2. Sensores biométricos de huella dactilar

Los sensores biométricos de huellas dactilares o sensores digitales son dispositivos sensibles al tacto que pueden leer, guardar e identificar un número limitado de huellas dactilares.

2.2.1. Clasificación de sensores

Ópticos reflexivos: Constan de un prisma iluminado por un LED². Cuando las crestas de las huellas del dedo tocan la superficie, la luz es absorbida, mientras que entre dichas

²Light-Emitting Diode

crestas se produce una reflexión total. La luz resultante y las zonas de oscuridad son registradas en un sensor de imagen.[49]

Ópticos transmisivos: Esta técnica funciona sin contacto directo entre el dedo y la superficie del sensor. La luz pasa a través del dedo desde la cara de la uña y al otro lado una cámara toma una imagen directa de la huella dactilar. El sensor ve a través de la superficie de la piel sobre una superficie más profunda y produce una imagen multi-espectral. El uso de diferentes longitudes de onda para generar imágenes nos proporciona información de diferentes estructuras subcutáneas, indicación de que el objeto en cuestión es un dedo genuino.[49]

Capacitivos: El sensor es un circuito integrado de silicio cuya superficie está cubierta por un gran número de elementos transductores (o pixeles), con una resolución típica de 500 dpi. Cada elemento contiene dos electrodos metálicos adyacentes. La capacidad entre los electrodos, que forma un camino de re-alimentación para un amplificador inversor, se reduce cuando el dedo se aplica sobre dicha superficie, se reduce más cuando detecta crestas y menos cuando detecta el espacio entre ellas.[49]

Mecánicos: Se trata de decenas de miles de diminutos transductores de presión que se montan sobre la superficie del sensor. Un diseño alternativo utiliza comutadores que están cerrados cuando son presionados por una cresta, pero permanecen abiertos cuando están bajo un valle. Esto sólo proporciona un bit de información por pixel, en lugar de trabajar con una escala de grises.[49]

Térmicos: En este caso se detecta el calor conducido por el dedo, el cual es mayor cuando hay una cresta que cuando hay un valle. Se ha desarrollado un componente de silicio con una matriz de pixeles denominado ‘FingerChip’, cada uno de los cuales está cubierto con una capa de material piro-eléctrico en el que un cambio de temperatura se traduce en un cambio en la distribución de carga de su superficie. La imagen está en la escala de grises que tiene la calidad adecuada incluso con el dedo desgastado, con suciedad, con grasa o con humedad.[49]

De salida dinámica: El dedo se desplaza lentamente a lo largo del mismo. El sensor sólo dispone de una estrecha zona sensible, y genera una secuencia completa de imágenes, las cuales pueden ser re-ensambladas, mediante un procesador, en una imagen completa. Las prestaciones se mejoran de modo apreciable y se garantiza la eliminación de cualquier grasa residual.[55]

2.2.2. Estándares técnicos

CJIS-RS-0010: Estándar creado en los Estados Unidos por el FBI³, que define las características técnicas que deben cumplir los escáneres de captura de huellas dactilares (escáneres de papel y los de captura en vivo) y las impresoras de huellas dactilares para asegurar que las imágenes obtenidas cumplan con criterios de calidad mínimos para ser usadas en procesos forenses manuales o automatizados de verificación o identificación dactilar. Actualmente, esta norma se encuentra en su versión 7, actualizada en 1999.[52]

IAFIS-IC-0110: Estándar creado por el FBI que define el formato para la compresión de imágenes de huellas dactilares conocido como WSQ⁴. Permite alcanzar niveles de compresión típicos de 15:1, manteniendo los detalles relevantes de la huella dactilar como las minucias y poros. Actualmente, esta norma se encuentra en la versión 3, actualizada en 1997.[16]

2.3. Fundamentos de seguridad

El término seguridad proviene del latín *securitas* y se usa para definir el concepto de algo donde no se registran peligros, daños ni riesgos. El término seguro define algo firme, cierto

³Federal Bureau of Investigation

⁴Wavelet Scalar Quantization

e indubitable.[54]

La seguridad, por lo tanto, puede considerarse como una certeza. Desde la prehistoria el hombre ha tratado de buscar seguridad en diferentes ámbitos de su diario vivir, desde tratar de encontrar un refugio donde se sienta a salvo de las inclemencias de la naturaleza, pasando por los candados con los que se impide el acceso a los diferentes ambientes, hasta las bóvedas que resguardan objetos e información confidencial.

En particular la seguridad informática permite que los recursos del sistema se utilicen de la manera en la que se espera y que quienes puedan acceder a la información sean las personas autorizadas para hacerlo.[38]

Existen dos tipos de instancias a proteger:

- Los objetos tangibles que se quieren proteger por su valor económico.
- Los objetos intangibles que se quieren proteger por la delicadez de los datos.

Entonces al trabajar con la seguridad de un recinto, se espera limitar el acceso solo a un cierto número de personas.

2.4. Biometría

La biometría (del griego *bios* vida y *metron* medida) es el estudio del reconocimiento único de humanos basado en uno o más rasgos conductuales o rasgos físicos intrínsecos.[40]

En un sistema de Biometría típico, la persona se registra con el sistema cuando una o más de sus características físicas y/o de conducta es obtenida, procesada por un algoritmo numérico, e introducida en una base de datos. Idealmente, cuando es identificada, casi todas sus características concuerdan; entonces cuando alguna otra persona intenta identificarse, no empareja completamente, por lo que el sistema no la identifica. Las

tecnologías actuales tienen tasas de acierto que varían desde valores bajos como el 60 %, hasta altos como el 99,9 %.

El rendimiento de una medida biométrica se define generalmente en términos de tasa de falso positivo (False Acceptance Rate o FAR), la tasa de falso negativo (False NonMatch Rate o FNMR, también False Rejection Rate o FRR), y la tasa de fallo de alistamiento (Failure-to-enroll Rate, FTE o FER).

Figura 1: Biometría



Fuente: Se avecina el fin del password, Noticias La Repubblica, Italia, 7 de Febrero de 2016

2.5. Huella dactilar

Se denomina dactilograma o lofograma papilar al conjunto de características provenientes de los dedos de la mano. Los dactilogramas se pueden clasificar de tres formas:

- Dactilograma natural: es el que está en la yema del dedo, formado por las crestas papilares de forma natural.
- Dactilograma artificial: es el dibujo que aparece como resultado al entintar un dactilograma natural e imprimirla en una zona idónea.

Figura 2: SmartID, autenticación segura



Fuente: Telefónica apuesta por un ecosistema digital seguro basado en la biometría, Revista Virtual Digital Security Magazine, España, 24 de Febrero de 2015

- Dactilograma latente: es la huella dejada por cualquier dactilograma natural al tocar un objeto o superficie. Este dactilograma queda marcado, pero es invisible. Para su revelación se requiere la aplicación de un reactivo adecuado.[16]

2.5.1. Propiedades físicas de las huellas dactilares

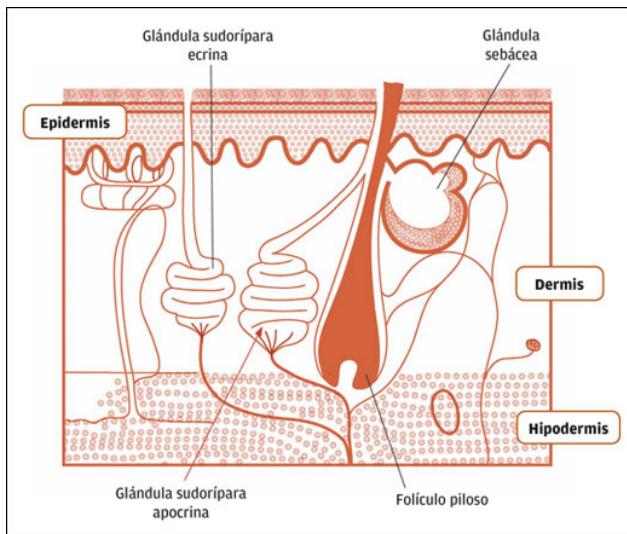
Está demostrado científicamente que los dibujos que aparecen visibles en la epidermis son:

- Perennes porque, desde que se forman en el sexto mes de la vida intrauterina, permanecen indefectiblemente invariables en número, situación, forma y dirección hasta que la putrefacción del cadáver destruye la piel.
- Inmutables, ya que las crestas papilares no pueden modificarse fisiológicamente; si hay un traumatismo poco profundo, se regeneran, y si es profundo, las crestas no reaparecen con forma distinta a la que tenían, sino que la parte afectada por el traumatismo resulta invadida por un dibujo cicatrizal.
- Diversiformes, pues no se ha hallado todavía dos impresiones idénticas producidas por dedos diferentes.
- Originales, ya que todo contacto directo de los lofogramas naturales producen impresiones originales con características microscópicas identificables del tejido epidérmico. Se puede establecer si fueron plasmadas de manera directa por la persona o si se trata de un lofograma artificial.

Las crestas papilares son glándulas de secreción de sudor, situadas en la dermis, llamadas glándulas sudoríparas. Constan de un tubo situado en el tejido celular subcutáneo, formado por un glomérulo glandular con un canal rectilíneo, que atraviesa la dermis, y termina en la capa córnea de la epidermis, concretamente en el poro, que es un orificio situado en los lomos de las crestas papilares.

Una vez que el sudor sale, se derrama por todas las crestas y se mezcla con la grasa natural de la piel; lo que da lugar a que, cuando se toque o manipule un objeto apto para la retención de huellas, las crestas dejen una impresión en el objeto.

Figura 3: Anexos cutáneos



Fuente: La Piel de la Web, Revista Virtual

Cosmetólogas, Buenos Aires, 14 de Febrero de 2017

por las crestas papilares reciben el nombre de dactilograma, palabra que deriva de los vocablos griegos; *daktylos* (dedos) y *grammas* (escrito). Se denominan dactilogramas papilares si provienen de los dedos de la mano, palmares cuando provienen de la palma de la mano y plantares si provienen de la planta del pie. [16]

2.5.2. Características de las huellas dactilares

Cresta: Son las líneas que sobresalen de la epidermis de forma natural, mismas que forman la impresión de la huella dactilar.

Valle: Son los surcos que se forman entre dos crestas, los espacios vacíos o blancos que quedan tras la impresión de la huella.

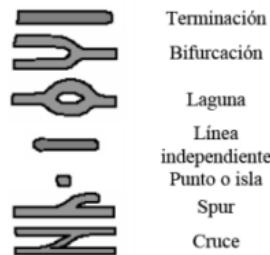
Los puntos característicos son las convergencias, desviaciones, empalmes, interrupciones, fragmentos, etcétera, de las crestas y de sus surcos.

Cuando se cotejan dos huellas dactilares, una dubitada y la otra indubitable; como ejemplo en España, se buscan como mínimo 12 puntos característicos, aunque la obtención de al menos 8 ya tiene validez jurídica.

Los dibujos o figuras formadas

Minucia: Son los puntos característicos que se hallan en la impresión de las huellas, la representación matemática es la siguiente: $M = \{x, y, \theta\}$, donde (x, y) es un punto o coordenada dentro de la impresión de la huella y θ es el ángulo medido en radianes que forma la minucia con el eje x .

Figura 4: Tipos de minucias



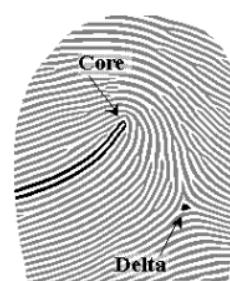
Fuente: Clasificación de huellas digitales mediante minucias, Instituto Nacional de Astrofísica, Óptica y Electrónica, México, Abril de 2009 [11]

Terminación: Se dá cuando una cresta llega a un punto final y no continua su recorrido.

Bifurcación: Se forma cuando una cresta se divide en dos y forma dos crestas que siguen un curso diferente la una de la otra.

Delta: Es un lugar específico dentro de la impresión donde dos o tres crestas forman la figura de un triángulo.

Figura 5: Corazón y Delta

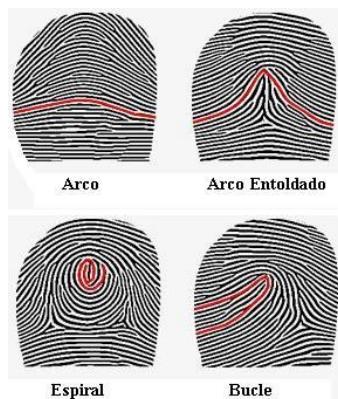


Fuente: Clasificación de huellas digitales mediante minucias, Instituto Nacional de Astrofísica, Óptica y Electrónica, México, Abril de 2009 [11]

Corazón: Es la convergencia donde se pueden hallar muchas terminaciones de crestas

2.5.3. Tipos de huellas dactilares

Figura 6: Tipos de huellas dactilares



Fuente: Patrones de Pukinje, Sistemas Biométricos, Juan Segura Martínez, Revista Virtual Seguridad Pasiva, 2012

Bucle: En este patrón las líneas en el reborde exterior que llegan al centro de la impresión dactilar se curvan y continúan en bucle hasta llegar nuevamente al mismo reborde; por esta razón solo se halla un delta en este tipo de patrones. 65% de la población mundial tiene este tipo de huellas.

Espiral: Este patrón contiene 2 o mas deltas, existe una curva ligera antes de comenzar cada delta. Existen cuatro tipos de espiral, la espiral simple, la espiral bolsillo central, el doble bucle y la espiral accidental. 30% de la población mundial tiene este tipo de huellas.

Arco: Es el patrón mas raro, en este tipo de patrones las líneas de cresta son divergentes y van desde un reborde del dedo al otro sin formar deltas. Existen dos tipos de arco, el arco simple que se asemeja a las olas del mar y el arco entoldado o tienda de

campaña donde las líneas se curvan de una manera más extrema hacia el centro de la impresión. 5 % de la población mundial tiene este tipo de huellas.

2.5.4. Aplicaciones

Actualmente los sensores biométricos se utilizan en gran número de aplicaciones, por ejemplo en computadoras portátiles y teléfonos inteligentes gracias a su alto grado de reducción de tamaño y su bajo costo económico.

También se pueden encontrar sensores digitales en discos duros, memorias USB y lectores de tarjetas. Últimamente se han desarrollado dispositivos que requieren de identificación biométrica para realizar transacciones bancarias.

Se pueden hallar dispositivos para la autenticación a diferentes cuentas en línea por medio de la huella dactilar.⁵

Estos sensores además son ampliamente utilizados para el control de personal en empresas o instituciones y para la identificación de personas para los sistemas de apertura de puertas o de marcado de llegadas y salidas para el control del horario laboral.

2.6. Sistemas de hardware embebido

Un sistema embebido es un hardware destinado a realizar algunas funciones dedicadas, generalmente orientadas a la computación en tiempo real. Los sistemas embebidos por lo general contienen un procesador de bajo costo y una memoria limitada para el almacenamiento de variables o partes del o los programas. Como parte central se pueden encontrar microprocesadores, procesadores digitales de señales y/o micro-controladores.

⁵Memoria Flash USB protegida por biometría, Patente de Google US 20050097338 A1, Kong Lee

Los sistemas embebidos se comunican con otras interfaces mediante puertos como ser: UART⁶, SPI⁷, I²C⁸, USB⁹, Ethernet, Wi-Fi¹⁰, GSM¹¹, GPRS¹², DSRC¹³, etc.

Las salidas de los sistemas embebidos pueden ser analógicas o digitales y se usan para controlar motores, activar diodos LED, polarizar transistores, activar relés, etc.

Las entradas pueden ser también analógicas o digitales procedentes de diferentes tipos de sensores. [24]

2.7. Ethernet

Ethernet es un sistema de transmisión de datos en banda base, diseñado por Xerox Corporation, a mediados de la década de 1970.

El subcomité de ANSI e IEEE 802.3 han definido la norma de transmisión Ethernet 10BASE-T que se basa en la topología de estrella. La “T” representa “UTP”, de unshielded twisted-pair wire, o cable de par de alambres trenzados. Se desarrolló el sistema 10BASE-T para permitir el uso de cableado telefónico existente, de grado de voz, para conducir señales de Ethernet.[44]

La estructura de la trama IEEE 802.3 es la siguiente:

Preámbulo: El preámbulo consiste en siete bytes, para establecer la sincronización de los relojes. El último byte del preámbulo se usa como delimitador de la trama de arranque.

⁶Universal Asynchronous Receiver-Transmitter

⁷Serial Peripheral Interface

⁸Inter-Integrated Circuit

⁹Universal Serial Bus

¹⁰Wireless Fidelity

¹¹Global System for Mobile

¹²General Packet Radio Service

¹³Dedicated Short Range Communications

Cuadro 1: Formato de la trama IEEE 802.3

| Preámbulo | Delimitador de trama de arranque | Dirección de destino | Dirección de fuente | Longitud | Payload | Secuencia de comprobación de trama | Delimitador de fin de trama | |
|-----------|----------------------------------|----------------------|---------------------|----------|---------|------------------------------------|-----------------------------|-------------|
| Bytes: | 7 | 1 | 2-6 | 2-6 | 2 | 46-1500 | 4 | 9.6 μ s |

Fuente: Sistemas de comunicaciones electrónicas, Wayne Tomasi, [44, p. 657]

Delimitador de la trama de arranque: No es más que una serie de dos unos lógicos agregada al final del preámbulo, cuyo objetivo es marcar el final del preámbulo y el principio de la trama de datos.

Dirección de destino: Las direcciones de la fuente y el destino forman el encabezado de la trama. La dirección del destino consiste en seis bytes (48 bits) y es la dirección del o los nodos que se han designado para recibir la trama. La dirección puede ser única, de grupo o global y se determina con las siguientes combinaciones:

- bit 0 = 0. Si el bit 0 es un 0, la dirección se interpreta como única, especial para una sola estación.
- bit 0 = 1. Si el bit 0 es un 1, la dirección se interpreta como de grupo. Todas las estaciones que tengan preasignada esta dirección de grupo aceptarán la trama.
- bit 0 = 47. Si todos los bits en el campo de destino son unos, quiere decir que la dirección es global, y que se identificó a todos los nodos como receptores de esta trama.

Dirección de fuente: Esta dirección consiste en seis bytes (48 bits), y corresponden a la dirección de la estación que manda la trama.

Campo de longitud: El campo de longitud de 2 bytes indica la longitud del campo de datos de control de enlace lógico (logical link control, LLC), también llamado Payload, que es de longitud variable y contiene incrustados todos los protocolos de capa superior.

Payload: El campo de Payload contiene la información, y puede tener de 46 a 1500 bytes de longitud.

Campo de secuencia de verificación de trama: El campo CRC (frame check sequence) contiene 32 bits para detección de errores, y se calcula a partir de los campos de encabezado y de datos.

Delimitador de fin de trama: El delimitador de fin de trama es un periodo de $9.6 \mu s$ en el que no se transmiten bits. En la codificación Manchester, cuando no hay transiciones de longitud mayor que el tiempo de 1 bit, se indica el final de la trama.

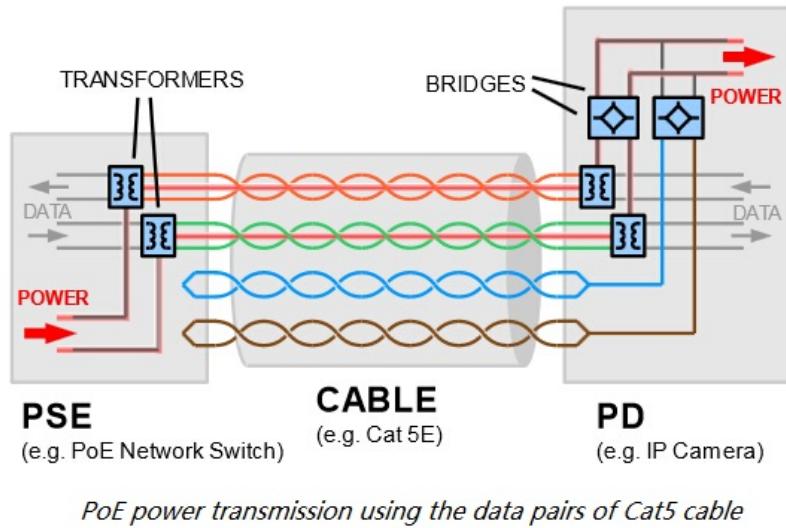
2.7.1. POE (Power Over Ethernet)

POE es un estándar IEEE desde el año 2003; éste sistema se compone de un inyector y un receptor conectados mediante un cable ethernet. Existen dos estándares, el primero 802.3af o POE activo, funciona con un inyector que realiza una prueba de carga mediante el consumo de corriente al lado del receptor, para verificar si el receptor es un dispositivo POE o no, en caso de no serlo envía los datos entre $+/-2.5V$; pero si detecta un dispositivo POE; es decir una carga, realiza una prueba, mediante niveles de voltaje, de cual es la potencia necesaria al lado del receptor para enviar los datos entre $+/-2.5V$ conjuntamente con un voltaje de $-48V$ en uno de los pares trenzados que puede ser el par verde o el azul del cable ethernet de categoría 5, 6 o 7; a su vez se cierra el circuito con una referencia en el otro par que puede ser el par naranja o café respectivamente.

Estos $48V$ son separados del voltaje de los datos en el lado del receptor y es con este que se alimenta al circuito que requiere energía, no sin antes realizar una conversión DC/DC adecuada a los requerimientos del circuito objetivo.

El segundo método es el 802.3at o POE pasivo, utiliza cuatro cables para datos y cuatro cables para energía, generalmente se puede encontrar que utiliza el par azul para enviar el

Figura 7: Power Over Ethernet



Fuente: Power Over Ethernet Analysis, Blog FS.com, 19 de Enero de 2016

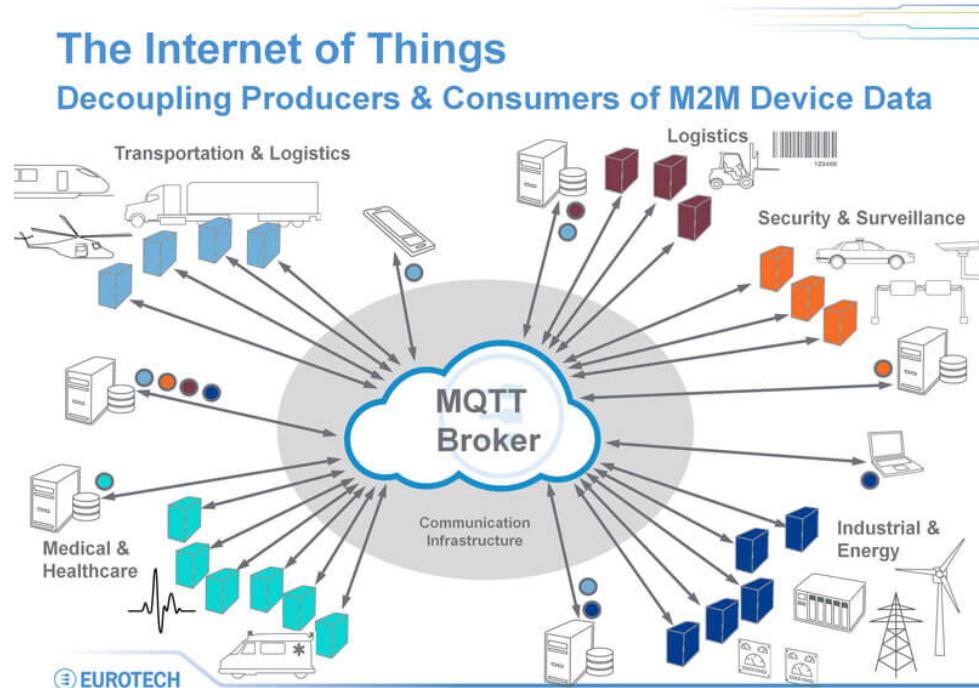
voltaje y el par café como referencia, la debilidad de este método es que la velocidad de transmisión/recepción disminuye debido a la eliminación de los dos pares usados para el voltaje, a cambio se puede prescindir del protocolo de reconocimiento de carga del circuito receptor. Cabe mencionar que un inyector 802.3at es compatible con un receptor 802.3af pero no al contrario.

2.8. Software

2.8.1. Internet de las cosas

El Internet de las Cosas es un concepto que se refiere a la interconexión de dispositivos de la vida cotidiana a una red local o al propio Internet. La mayoría de los dispositivos del Internet de las Cosas capturan información de sensores y envían estos datos a una o más bases de datos, un ejemplo de estos dispositivos son los refrigeradores inteligentes, que verifican la cantidad de alimentos de cada tipo e incluso pueden realizar pedidos de

Figura 8: Internet de las cosas

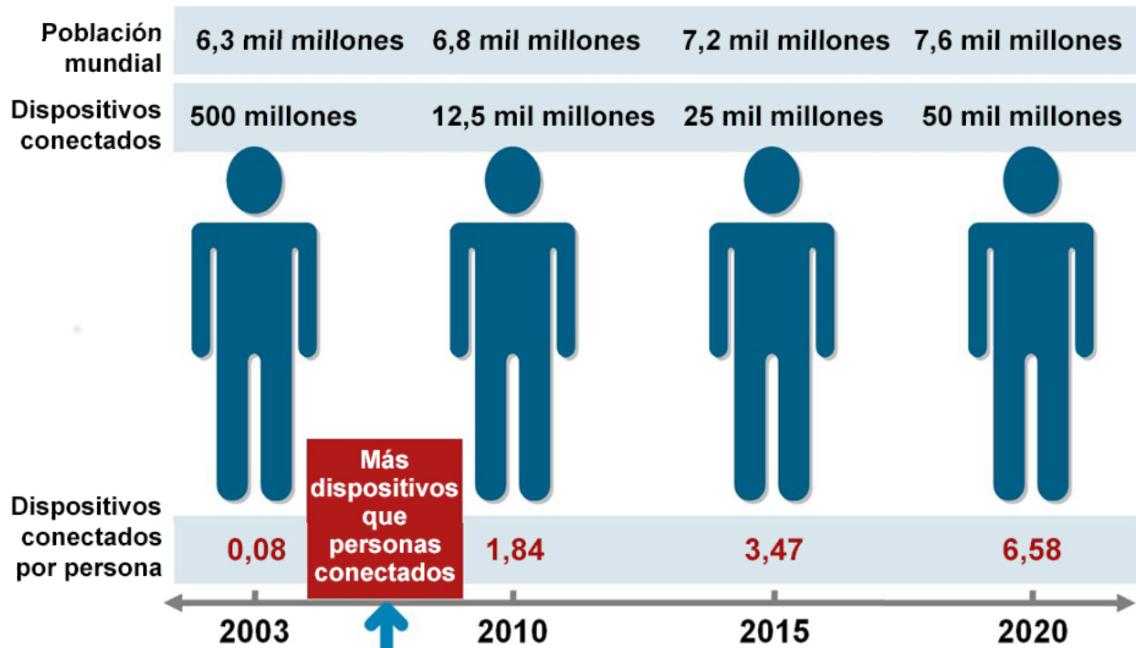


Fuente: Get to Know MQTT: The Messaging Protocol for the Internet of Things,
Industrias Janakiram & Associates, 2016

compra directamente a los supermercados cuando un alimento se encuentra por debajo de un límite definido por el usuario. Otro ejemplo son los sensores que se implantan a las vacas en Holanda, éstos recaban la información acerca de la salud, la posición y la edad de las vacas, generando hasta 200MB de datos al año por cada vaca, con estos datos se pueden generar gráficas para mejorar la crianza e incluso predecir y prevenir epidemias de enfermedades bovinas.[15]

Los dispositivos del Internet de las Cosas transmiten los datos mediante una gran gama de protocolos, entre los cuales el más conocido por su eficiencia en cuanto a energía consumida y pequeño tamaño en la trama de paquete de datos es MQTT. Este protocolo es usado en aplicaciones populares como Facebook Messenger, Amazon Web Services, OpenStack y Microsoft Azure entre otras.[53]

Figura 9: Número de dispositivos conectados por persona



Fuente: Internet de las cosas: Cómo la próxima evolución de Internet lo cambia todo,
Dave Evans, Cisco IBSG, 2011

2.8.2. Entorno de ejecución

Un entorno de ejecución es un estado de máquina virtual que suministra servicios para los procesos de un programa de computadora que se está ejecutando. Puede pertenecer al mismo sistema operativo, o ser creado por el software del programa en ejecución.

En la mayoría de los casos, el sistema operativo maneja la carga del programa con una parte del código llamada cargador, haciendo configuración básica de memoria y enlazando el programa con cualquier biblioteca de vínculos dinámicos a la cual haga referencia. En algunos casos un lenguaje o implementación hará esas tareas en lugar del runtime del lenguaje, a pesar de que es inusual en los lenguajes principales sobre los sistemas operativos de usuarios normales.

Cierta depuración de programas sólo puede realizarse (o ser más eficiente o precisa)

cuando se realiza en ejecución. La comprobación de errores lógicos y límites de arrays son algunos ejemplos. Por esta razón, algunos errores de programación no son descubiertos hasta que el programa es probado en un entorno “en vivo” con datos reales, a pesar de la comprobación en tiempo de compilación sofisticada y pruebas previas a la publicación. En este caso, el usuario final puede encontrar un mensaje de “error en tiempo de ejecución” (runtime error).[47]

2.8.3. Base de datos

Una base de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido; una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta. Actualmente, y debido al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos están en formato digital, siendo este un componente electrónico, por tanto se ha desarrollado y se ofrece un amplio rango de soluciones al problema del almacenamiento de datos.

Las bases de datos pueden ser estáticas, es decir de solo lectura, o dinámicas que cuentan con operaciones de actualización, borrado y edición.

Las bases de datos relacionales están formadas por “tuplas”, cada relación genera una tabla que está compuesta por registros (las filas de una tabla), que representan las tuplas, y campos (las columnas de una tabla).

La información puede ser recuperada o almacenada mediante consultas que ofrecen una amplia flexibilidad y poder para administrar la información. El lenguaje más habitual para construir las consultas a bases de datos relacionales es SQL¹⁴.[51]

¹⁴Structured Query Language

Capítulo 3

Ingeniería del Proyecto

En este capítulo se detallan las secuencias de acción del registro de una nueva huella en el sistema, del acceso de una persona mediante un sensor de huella dactilar y mediante un pulsador desde el interior de los ambientes, la secuencia de envío de nuevas huellas a los sensores y la secuencia para la apertura de emergencia mediante un respaldo bluetooth. Durante el desarrollo de estos procesos se muestra el diseño de los circuitos conjuntamente con los programas utilizados en cada uno de ellos, también se muestra el servicio web que sirve para ejecutar operaciones en los sensores y administrar los permisos de cada usuario sobre las puertas registradas; este software también muestra los accesos en tiempo real.

3.1. Estado previo a la instalación piloto del sistema en ADSIB

Antes de la instalación del sistema de control de accesos desarrollado en este proyecto, el centro de datos de ADSIB contaba con medidas de seguridad físicas cuyo flujo se muestra en la Figura 10, del cual los actores son:

Usuario: Persona que desea ingresar al centro de datos.

Policía: Guardia de seguridad que controla la puerta del edificio de la Vicepresidencia.

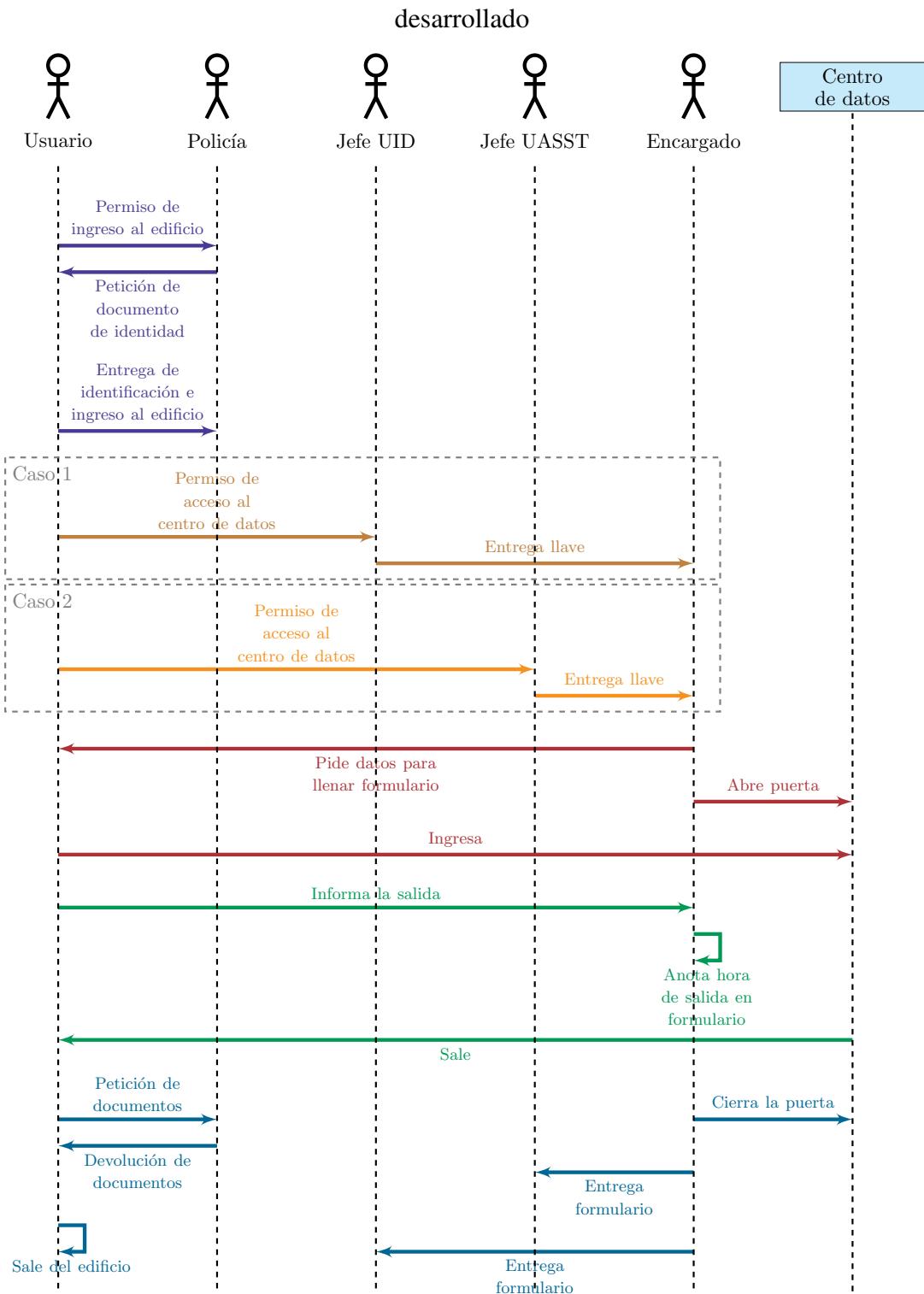
Jefe UID: Jefe de la Unidad de Innovación y Desarrollo de ADSIB.

Jefe UADSST: Jefe de la Unidad Administración de Sistemas y Soporte Técnico de ADSIB.

Encargado: Encargado de la apertura y cierre de la puerta de ingreso al centro de datos.

Centro de datos: Ambiente donde se encuentran los equipos informáticos de la entidad, cuenta con una puerta de madera y cerradura común al ingreso.

Figura 10: Diagrama de flujo para el ingreso antes de la instalación del sistema desarrollado



Fuente: Elaboración propia

El flujo promedio de personas que ingresa al centro de datos es de 4 personas/día, el tiempo promedio entre ingresos es de 1 vez cada 2 horas. Existen casos aislados, por ejemplo durante las auditorías donde el flujo incrementa hasta 12 personas/día y el tiempo entre ingresos promedio sube a 2 veces cada hora.

3.1.1. Especificación de requisitos a satisfacer con el desarrollo del sistema

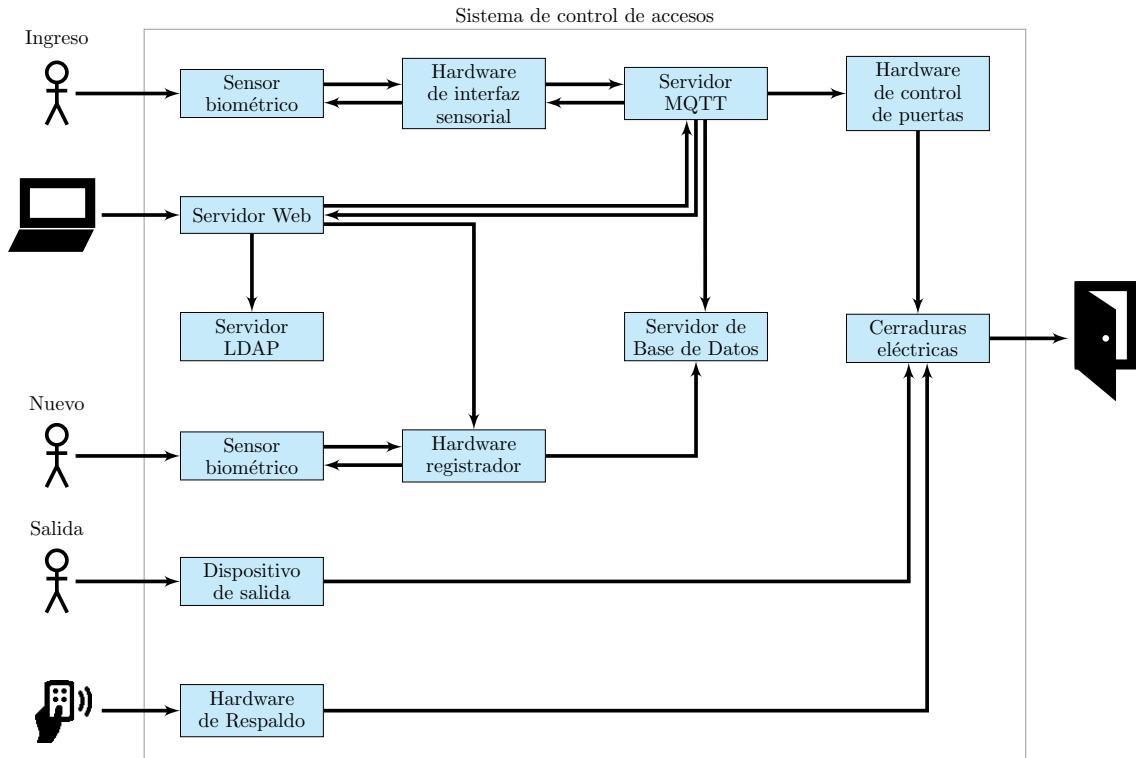
Los requerimientos funcionales del sistema especificados por el Jefe de la Unidad de Innovación y Desarrollo de ADSIB se enumeran por orden de prioridad:

1. Instalar el sistema en 5 ambientes del centro de datos
2. Utilizar un método de identificación biométrico para acceder a los ambientes
3. La salida de los ambientes no debe contar con ningún tipo de identificación y debe ser constituida con elementos pasivos para evitar que las personas queden atrapadas en los ambientes en caso de emergencia
4. Utilizar tecnologías de software y hardware libre en la mayor proporción posible
5. Compatibilizar el sistema con el respaldo de energía mediante UPS disponible en el centro de datos
6. El registro de nuevos usuarios debe realizarse en un dispositivo de hardware destinado específicamente para esa función
7. El hardware registrador estará ubicado en la oficina de ADSIB que se encuentra tres pisos más arriba del centro de datos pero contará con conexión de red mediante un conector RJ45
8. El sistema debe ser compatible con el servidor LDAP que almacena la lista de todo el personal de ADSIB

9. Proveer un sistema de apertura mediante otro medio diferente al principal para la apertura de emergencia de la puerta principal
10. El sistema de apertura alternativo deberá estar aislado del sistema central para evitar la falla simultanea de ambos sistemas
11. Proveer un sistema de administración web que permita registrar nuevos usuarios
12. Al momento del registro de un nuevo usuario el sistema web debe poder sincronizar los cambios producidos en el servidor LDAP
13. El sistema web debe tener una función que permita establecer permisos a cada usuario registrado para que pueda acceder por las diferentes puertas sin una fecha final para el permiso
14. El sistema web debe tener una función que permita establecer permisos a cada usuario registrado para que pueda acceder por una puerta de forma temporal estableciendo una fecha inicial y una fecha final
15. En caso de tener que registrar las nuevas identidades en los sensores, este registro se debe hacer mediante el sistema web
16. El sistema web debe mostrar la apertura de puertas en tiempo real identificando la persona que accedió y la puerta por la que accedió
17. El sistema web debe tener la capacidad de mostrar un historial de accesos con un filtro de fechas
18. El sistema web debe proveer otro nivel de acceso para usuarios sin permiso de administrador que permita abrir las puertas mediante botones en una página web
19. Los usuarios sin permiso de administrador no podrán abrir puertas en el sistema web por las cuales no puedan acceder mediante el sensor biométrico

3.2. Perspectiva global del sistema propuesto

Figura 11: Diagrama de bloques del sistema de control de accesos



Fuente: Elaboración propia

3.2.1. Selección del sensor biométrico

3.2.1.1. Tasa de falso rechazo y tasa de falsa aceptación

La tasa de falso rechazo (FRR¹) es la probabilidad de que el sensor no identifique a un usuario legítimo, mientras que la tasa de falsa aceptación (FAR²) es la probabilidad de que el sensor identifique a un usuario ilegítimo como legítimo. Un FRR elevado provoca

¹False Rejection Rate

²False Acceptance Rate

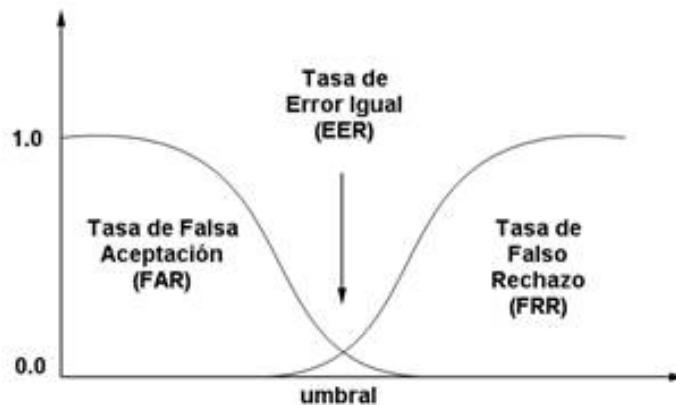
descontento en los usuarios ya que éstos tendrán que realizar más intentos para identificarse correctamente, pero un FAR elevado provoca graves problemas de seguridad ya que podría darse acceso a una persona no autorizada.

Para evaluar las prestaciones de un sistema biométrico se utiliza la tasa de éxito (SR³), la ecuación 3.1 demuestra como calcular el SR.

$$SR = 1 - (FAR + FRR) \quad (3.1)$$

FAR y FRR son inversamente proporcionales, para obtener un óptimo funcionamiento del sistema se debe fijar un umbral dependiendo del nivel de seguridad definido para el sistema, con este umbral se podrá identificar la tasa de error igual (EER⁴), este parámetro determina la capacidad de identificación del sistema.

Figura 12: Punto de equilibrio EER



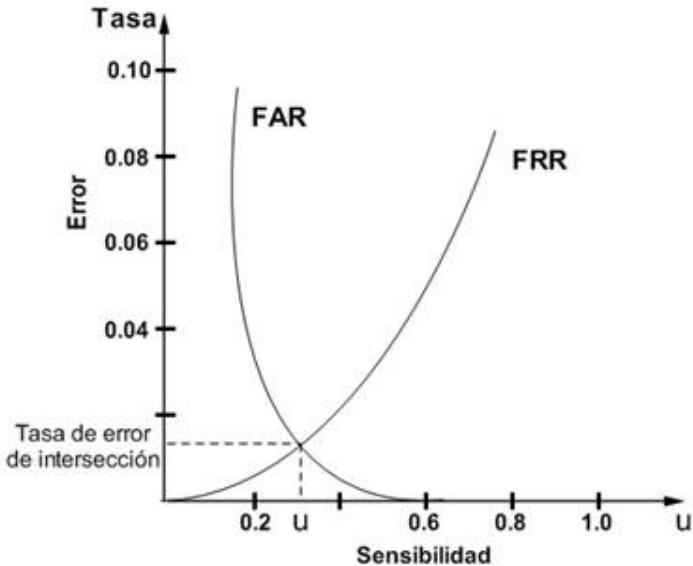
Fuente: Aplicación de Nuevas Tecnologías al Sistema Electoral, Sergio D. Werner[46]

El grado de seguridad deseado se define mediante el umbral de aceptación u , un número real perteneciente al intervalo $[0,1]$ que indica el mínimo grado de parentesco permitido para autorizar el acceso del individuo.[46]

³Success Rate

⁴Equal Error Rate

Figura 13: Tasa de error vs Sensibilidad



Fuente: Aplicación de Nuevas Tecnologías al Sistema Electoral, Sergio D. Werner[46]

En base a los datos mostrados en la sección de “Errores en sistemas biométricos” de la monografía “Aplicación de Nuevas Tecnologías al Sistema Electoral” de Sergio D. Werner[46], conjuntamente con la tabla mostrada en la “Diapositiva N°27” de la presentación del “Estudio de Dispositivos Biométricos” de Sebastián Ramos Bustos[6] que compara las ventajas y desventajas de las tecnologías biométricas, se realizó la comparación de las características de los diferentes sensores biométricos estimando cada característica con un valor numérico del 1 al 5, donde 1 es muy bajo y 5 es muy alto, como se muestra en la Tabla 2.

Del conjunto de características se calculó la estimación apreciada y con este resultado se seleccionó el método de identificación biométrica basada en la comparación de minucias de huellas dactilares.

Cuadro 2: Características de los sensores biométricos

| Característica | Ojo (iris) | Ojo (retina) | Huellas dactilares | Geometría de la mano | Voz | Rostro |
|------------------------------|---------------|-----------------|-----------------------|-------------------------|-----|--------|
| Fiabilidad | 5 | 5 | 4 | 4 | 4 | 4 |
| Facilidad de uso | 3 | 2 | 5 | 4 | 4 | 4 |
| Prevención contra ataques | 5 | 5 | 4 | 4 | 3 | 3 |
| Aceptación | 2 | 3 | 4 | 4 | 4 | 5 |
| Estabilidad | 4 | 4 | 4 | 3 | 3 | 3 |
| Estimación apreciada | 19 | 19 | 21 | 19 | 18 | 19 |

Fuente: Características de los rasgos biométricos, Aplicación de Nuevas Tecnologías al Sistema Electoral, Sergio D. Werner, Argentina, 9 de Marzo de 2011

Cuadro 3: Comparación de sensores de huella digital

| Característica | Sensor ZFM-20 | Sensor ARA-ME-01 |
|----------------------------|------------------------|------------------------|
| Interfaz serial | UART 9600 - 115200 bps | UART 9600 - 115200 bps |
| Nivel lógico | TTL | TTL |
| Alimentación | DC 3.6 - 6.0V | DC 5.0V |
| Corriente de operación | < 120mA | < 60mA |
| Resolución de la imagen | 256x288 pixeles | 256x288 pixeles |
| Memoria | 1000 huellas | 120 huellas |
| Precio | 50 \$us | 159.90 \$us |

Fuente: Elaboración propia

Definido el tipo de sensor a utilizar se selecciona el modelo, para esto se buscó sensores de huella dactilar disponibles en Bolivia, se encontró dos modelos comparados en la Tabla 3 de acuerdo a los datos descritos en la tienda virtual www.TecBolivia.com.

De la comparación de la Tabla 3 se pudo apreciar que la memoria para huellas dactilares en el sensor ARA-ME-01 se llenaría en un plazo de tiempo más corto que la memoria del sensor ZFM-20, además que el rango de alimentación del ZFM-20 es más amplio que el ARA-ME-01, por estas razones se seleccionó el sensor de huellas digitales ZFM-20.

El sensor ZFM-20 tiene 5 niveles de seguridad, se utilizó el nivel 3 ya que es el que tiene un umbral de aceptación más equilibrado, de acuerdo a su hoja de datos en el nivel 3 de seguridad $FAR=0.001\%$ y $FRR=0.1\%$ [56].

Para realizar el cálculo aproximado de intentos fallidos por cada cierto número de intentos, o también el número de ataques que fallarán por cada cierto número de ataques se utiliza la Ecuación 3.2.

$$SR = \frac{A_r}{A_i} \quad (3.2)$$

Para un número de 10000 intentos de ataque y los valores de FAR y FRR se reemplazan los valores en estos valores en la Ecuación 3.3 y se calcula el valor aproximado de intentos o ataques fallidos por cada 10000 intentos o ataques.

$$A_r = SR \cdot A_i = [1 - (FAR + FRR)] \cdot A_i \quad (3.3)$$

$$A_r = [1 - (0,001 + 0,1)] \cdot 10000 = 8990 \quad (3.4)$$

Por tanto se espera que por cada 10000 intentos, 8990 veces se reconozca correctamente la identidad de la persona que realiza el intento y 1010 veces el sensor cometerá un error de reconocimiento como falso positivo o falso negativo.

Con base en este valor se calculó el número aproximado de veces que el sensor reconocerá un falso positivo.

$$E_{lectura} = E_{cometidos} \cdot FAR = 1010 \cdot 0,001 = 1,01 \quad (3.5)$$

Se puede concluir con el resultado obtenido en la Ecuación 3.5 que se espera que de cada 10000 intentos, el sensor cometerá el error de identificar 1 huella en una posición incorrecta de su base de datos o una huella que no se encuentre registrada como válida, valor obtenido con un nivel de seguridad 3 de acuerdo al manual del sensor ZFM-20[56].

3.2.2. Selección de los protocolos de comunicación

El punto más importante para la decisión del protocolo a utilizar fué la seguridad en el medio de transmisión, los dos medios que se pueden utilizar son el cableado e inalámbrico, se puede ver la comparación de las ventajas y desventajas entre estos dos medios en la Tabla 4, de la cual se concluyó que el medio más conveniente para el desarrollo del proyecto es el medio cableado, porque en éste se tiene un mejor control contra ataques e infiltraciones mediante una infraestructura con una configuración óptima.

Ahora que se seleccionó el medio físico, se procedió a la selección del medio de comunicación, para la selección se tomó como principal criterio la distancia entre el control central y las interfaces sensoriales, de acuerdo a la disposición de los ambientes del centro de datos de ADSIB se pudo realizar la medición del tramo más largo hasta donde quedaría ubicado el control central obteniendo un valor de 40m, por lo cual se compararon dos medios de comunicación RS-485 y Ethernet, de entre los cuales se seleccionó mediante el criterio de escalabilidad y se optó por Ethernet ya que el número de nodos máximo es de 65535 a comparación del RS-485 que tan solo admite 32 nodos.

Cuadro 4: Comparativa del medio cableado vs el medio inalámbrico

| Cableado | | Inalámbrico | |
|---|------------------------------|--|---|
| Ventaja | Desventaja | Ventaja | Desventaja |
| No se pueden interceptar señales sin conexión física a la misma red | El cable puede ser destruido | No necesita infraestructura para cada punto cliente | Rango de señal limitada |
| Velocidades de transmisión muy elevadas | | Se puede expandir el área de servicio con repetidores de señal | La señal puede ser interceptada fácilmente |
| Los cables necesarios no son costosos | | | Las señales son afectadas por interferencia de otras señales |
| No precisa configuración en la conexión | | | La velocidad de transmisión es más baja que el medio cableado |

Fuente: Elaboración propia

Recientemente se produjo un cambio de paradigma en el campo de recolección de datos de sensores desde el desarrollo de IoT, en este enfoque sobresalen algunos protocolos que son comparados en la Tabla 5.

Cuadro 5: Comparación entre protocolos IoT

| Protocolo | Características |
|-----------|---|
| MQTT | <ul style="list-style-type: none"> Tamaño de paquete muy pequeño Comunicación doble vía Bajo consumo de energía NAT transversal es direccionado entre redes Hasta 10000 clientes |
| CoAP | <ul style="list-style-type: none"> Orientado a la arquitectura de servicios web Comunicación doble vía Fácil configuración de dispositivos para acceso a Internet El direccionamiento NAT transversal es muy problemático Hasta 10000 clientes |
| API REST | <ul style="list-style-type: none"> Comunicación de vía única El direccionamiento NAT transversal es muy sencillo Adaptado para buen funcionamiento en redes inalámbricas Tamaño de paquete muy grande en comparación a los demás No tiene límite de clientes |
| XMPP | <ul style="list-style-type: none"> Adaptado para soportar mucho tráfico en la red Tamaño de paquete muy grande en comparación a los demás Altamente seguro en la transmisión de datos Precisa de software o hardware para cifrado de datos Hasta 100000 clientes |

Fuente: Elaboración propia

La característica buscada es la mejor compatibilidad del protocolo con una red local ya que los dispositivos no gozan de conexión a Internet, otra característica importante fué el

direccionalamiento NAT, ya que se propuso el desarrollo de este sistema sobre una infraestructura de red previamente instalada de la cual no se conocía la topología. Con estas características se seleccionó MQTT como protocolo de comunicación para los dispositivos del sistema.

El protocolo MQTT mejor conocido como Mosquitto, es un protocolo desarrollado por IBM para la comunicación Máquina-Máquina (M2M). Desde 2013 es catalogado como el estándar ISO/IEC PRF 20922, es una alternativa más ligera que AMQP, XMPP o WAMP. Se ubica dentro de la capa de aplicación del modelo OSI en base al protocolo TCP/IP.

Este protocolo se basa en la topología de suscripción a tópicos y publicación de mensajes. Se puede implementar sobre una capa segura SSL, brindando la posibilidad de cifrado de los datos al momento de enviar o recibir mensajes, además implementa permisos de acceso al momento de la conexión mediante la combinación usuario/contraseña, y se pueden definir permisos para publicación o suscripción en diferentes tópicos para cada cliente.

Cuadro 6: Comparación de envío de mensajes entre HTTPS y MQTT

Enviando 1024 mensajes con carga útil de 1 byte

| | 3g | | Wi-Fi | |
|---------------------|---------|----------------|---------|----------------|
| | HTTPS | MQTT | HTTPS | MQTT |
| % Batería / Hora | 18,79 % | 17,80 % | 5,44 % | 3,66 % |
| Mensajes / Hora | 1926 | 21685 | 5229 | 23184 |
| % Batería / Mensaje | 0,00975 | 0,00082 | 0,00104 | 0,00016 |

Fuente: Power Profiling: HTTPS Long Polling vs. MQTT with SSL, on Android, Blog de Stephen Nicholas, 31 de Mayo de 2012

El dispositivo central llamado broker, puede gestionar y transmitir los mensajes de hasta 10.000 clientes. Por otro lado la ventaja más grande en comparación con el protocolo

HTTP es que MQTT no tiene un tamaño de paquete fijo, ya que el mismo se adapta de acuerdo al tipo de conexión y al tipo de mensaje enviado, solo necesita 69 bytes para un mensaje vacío mientras que HTTP necesita 302 bytes para un mensaje vacío. La cabecera de MQTT ocupa tan solo 2 bytes al contrario de HTTP cuya longitud mínima de cabecera es de 18 bytes. La carga útil de MQTT es de 0B a 256MB.

Cuadro 7: Comparación de recepción de mensajes entre HTTPS y MQTT

Recibiendo 1024 mensajes con carga útil de 1 byte

| | 3g | | Wi-Fi | |
|---------------------|------------|--------------------|---------------|--------------------|
| | HTTPS | MQTT | HTTPS | MQTT |
| % Batería / Hora | 18,43 % | 16,13 % | 3,45 % | 4,23 % |
| Mensajes / Hora | 1708 | 160278 | 3628 | 263314 |
| % Batería / Mensaje | 0,01709 | 0,0001 | 0,00095 | 0,00002 |
| Mensajes Recibidos | 240 / 1024 | 1024 / 1024 | 524 / 1024 | 1024 / 1024 |

Fuente: Power Profiling: HTTPS Long Polling vs. MQTT with SSL, on Android, Blog de Stephen Nicholas, 31 de Mayo de 2012

Cuadro 8: Comparación de consumo de batería con señales de Keep Alive

| Keep Alive (segundos) | % Bateria / Hora | | | |
|-----------------------|------------------|----------------|---------|----------------|
| | 3g | | Wi-Fi | |
| HTTPS | MQTT | HTTPS | MQTT | |
| 60 | 1.11553 | 0.72465 | 0.15839 | 0.01055 |
| 120 | 0.48697 | 0.32041 | 0.08774 | 0.00478 |
| 240 | 0.33277 | 0.16027 | 0.02897 | 0.00230 |
| 480 | 0.08263 | 0.07991 | 0.00824 | 0.00112 |

Fuente: Power Profiling: HTTPS Long Polling vs. MQTT with SSL, on Android, Blog de Stephen Nicholas, 31 de Mayo de 2012

Las datos observados en las Tablas 6, 7 y 8 fueron generados con un teléfono inteligente HTC Desire sobre el sistema operativo Android 2.2.2 - Compilación 2.33.161.6 CL345089.

La medida “% Batería / Hora” tiene referencia a una carga completa de la batería de Li-Ion de capacidad de 3.7V y 1400mAh.

La aplicación que se utilizó para obtener los datos es PowerTutor, que produce un margen de error entre 0.8 % y 2.5 %.

Por lo tanto el protocolo MQTT es el más conveniente para el desarrollo de este sistema.

En cuanto a los protocolos para el sistema de administración web se seleccionó REST en lugar de SOAP⁵ ya que los datos se intercambiarán mediante mensajes en formato JSON⁶ y no XML⁷ y para el servidor web se utilizó HTTP/2⁸ que entre sus ventajas principales sobre HTTP1.1 tiene el cifrado obligatorio de datos y el formato binario para el intercambio de datos que permite mostrar mensajes en tiempo real con un retardo menor al intercambio de mensajes en ASCII de HTTP1.1.

3.2.3. Selección del dispositivo de procesamiento de datos para el hardware de control y la interfaz sensorial

Se propuso un sistema escalable mediante el uso de un mismo hardware para el control de puertas y la interfaz sensorial que se ubicó en cada puerta, para este dispositivo se seleccionó entre un microprocesador y un microcontrolador, las operaciones a realizar por el hardware son el control de salidas digitales para la apertura de puertas y la transmisión serial con el sensor de huellas dactilares, las placas de desarrollo que se

⁵Simple Object Access Protocol

⁶JavaScript Object Notation

⁷eXtensible Markup Language

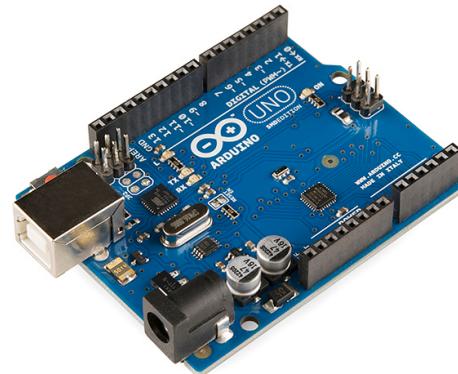
⁸HyperText Transfer Protocol

encontraron disponibles en el mercado para este fin fueron Arduino, Raspberry y CubieBoard.

De entre estas tres opciones se seleccionó Arduino porque éste cuenta con lo necesario para ejecutar las operaciones definidas para el sistema y tanto el diseño, la programación e instalación serían más fáciles, además Arduino garantizaría la estabilidad del sistema ya que el programa se encuentra encapsulado en la memoria Flash que no es accesible, a diferencia de la tarjeta SD que necesitan las tarjetas de desarrollo basadas en microprocesadores.

A continuación se debía seleccionar un modelo de Arduino, la tienda virtual de referencia www.TecBolivia.com disponía de microcontroladores: ATmega328P, ATmega32U2, ATmega32U4 y ATtiny85. Los dos microcontroladores que tienen compatibilidad con los módulos de red son ATmega328P y ATtiny85, la característica para la selección fué la capacidad de memoria Flash ya que el programa ocupa 23.336KB y la memoria del ATtiny85 tan solo cuenta con 8KB, por lo cual se seleccionó el microcontrolador ATmega328P, con la ventaja adicional de que en el desarrolló se pudo utilizar la placa Arduino UNO.

Figura 14: Arduino UNO SMD R3



Fuente: Wikipedia

3.2.3.1. Selección del dispositivo controlador Ethernet para el hardware de control y la interfaz sensorial

Arduino es compatible con dos dispositivos controladores de Ethernet, éstos son el circuito integrado W5100 y el integrado ENC28J60, en el mercado solo se pudo

encontrar el circuito integrado ENC28J60, por lo tanto la placa de desarrollo seleccionada fué Ethercard.

Figura 15: Ethercard



Fuente: Usando el Módulo Ethernet ENC28J60, Blog de Michael Brich, 24 de Marzo de 2015

Ethercard es una tarjeta de desarrollo para el circuito integrado ENC28J60, compatible con arduino, mediante el protocolo SPI (Serial Peripheral Interface) con una velocidad de hasta 10 Mb/s. Este chip es compatible con el estándar IEEE 802.3i y contiene toda la lógica anti-colisión y de rechazo de paquetes erróneos, listo para una conexión TCP/IP. También tiene opción para instalar 2 leds, uno para indicar el enlace y otro para indicar la transmisión de datos. Este circuito integrado necesita de un reloj externo que oscile a 25 MHz y una fuente de alimentación de 3.3V, pero las entradas de control trabajan en los niveles TTL de 5V. Se debe asignar una dirección MAC mediante software para identificar este hardware en la red.

3.2.3.2. Selección de la frecuencia de reloj para el microcontrolador ATmega328P

El principal criterio para la selección del reloj fué la conexión con el sensor de huellas. En base al esquema de Arduino UNO R3 [Anexo 16], de donde se conservó sólo la etapa de comunicación serial para la conexión con el sensor de huellas y cuatro pines digitales para las salidas hacia los relés para la apertura de puertas, se tuvo dos opciones, utilizar el reloj interno o uno externo.

Por defecto la placa Arduino UNO R3 trabaja a 16Mhz, que es una frecuencia totalmente compatible con la tasa de bits a la que trabaja el sensor de huellas, que por defecto es de 57600bps. Aunque también se podía utilizar el reloj interno de 8Mhz que incorpora el ATmega328P como se indica en su hoja de datos [4], se eligió utilizar un reloj externo de 16MHz de acuerdo a las reglas de diseño especificadas en el artículo *Determining Clock Accuracy Requirements for UART Communications* [17] y las ecuaciones obtenidas del Manual del ATmega328P [4], el primer paso es identificar un valor para el registro UxBRG (BaudRate Generator), mayormente conocido como variable BSEL para el cual se aplica la siguiente ecuación:

$$BSEL = \frac{f_{PER}}{2^{BSIZE} \cdot 16 f_{BAUD}} - 1 \quad (3.6)$$

Donde: f_{PER} es la frecuencia del periférico, BSCALE toma el valor de 0 para conexión UART asíncrona en modo normal y f_{BAUD} , es la velocidad de conexión a la que se desea llegar.

Insertando los valores numéricos se calcula BSEL:

$$BSEL = \frac{16000000}{2^0 \cdot 16 \cdot 57600} - 1 = 16,361 \simeq 16 \quad (3.7)$$

El valor de BSEL debe ser un número entero ya que es el valor que tomará un registro de control en el ATMEGA328P. Despejando de la ecuación N° 3.6

$$f_{BAUD*} = \frac{f_{PER}}{2^{BSIZE} \cdot 16 \cdot (BSEL + 1)} \quad (3.8)$$

Insertando los valores numéricos se calcula f_{BAUD} :

$$f_{BAUD*} = \frac{16000000}{2^0 \cdot 16 \cdot (16 + 1)} = 58824,53 \quad (3.9)$$

Ahora se calcula el error de tasa de bits, que según el estándar TIA RS-232C⁹ debe ser menor a 3%:

⁹Telecommunications Industry Association - Recommended Standard 232

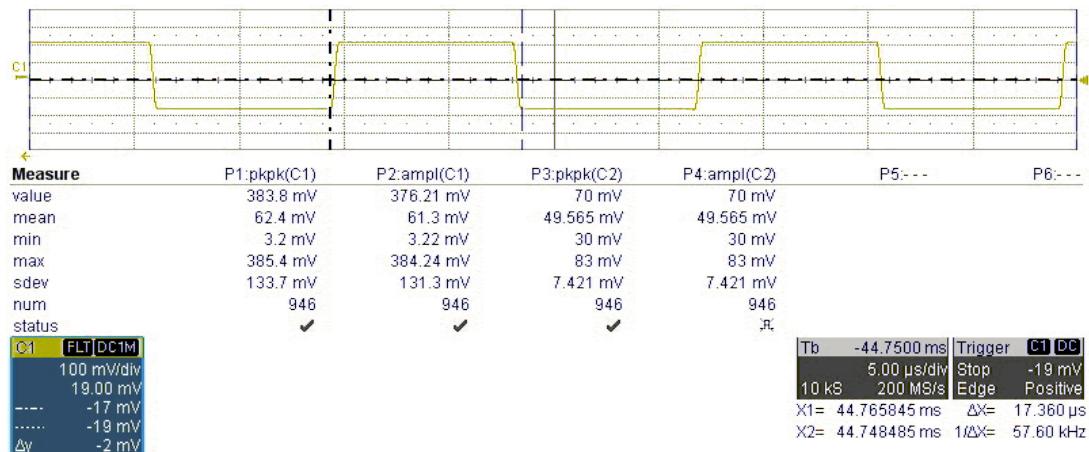
$$err_f = \frac{f_{BAUD} * -f_{BAUD}}{f_{BAUD}} * 100 \% \quad (3.10)$$

Insertando los valores numéricos se calcula err_f :

$$err_f = \frac{58824,53 - 57600}{57600} * 100 \% = 2,12 \% \quad (3.11)$$

Si se realizan los cálculos en base al reloj interno de 8MHz se obtiene un error de -3.54 % que se encuentra por encima del valor estándar, es por ello que se diseñó el circuito con un reloj externo de 16MHz para el microcontrolador ATmega328P.

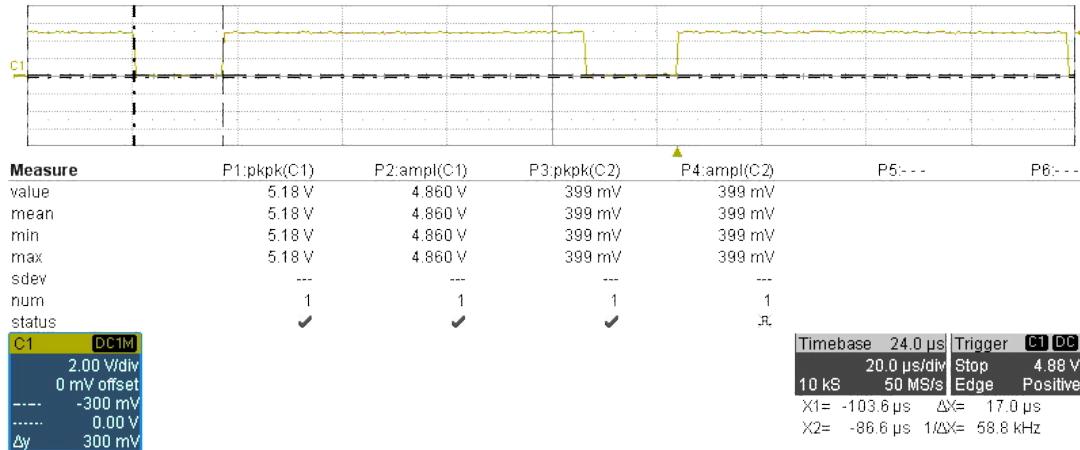
Figura 16: Captura de forma de onda de transmisión serial a 57600Hz



Fuente: Elaboración propia

En las tablas 9 y 10 se muestra un cálculo completo en base a las Ecuaciones 3.6, 3.8, 3.10 para los dos valores de reloj interno y externo respectivamente, de acuerdo a los valores de tasa de bits a los que se comunica el sensor de huellas dactilares, tomando en cuenta que la librería de comunicación serial de Arduino establece el registro U2Xn o BSCALE en 0.

Figura 17: Captura de forma de onda de transmisión serial a 58824Hz



Fuente: Elaboración propia

Cuadro 9: Error de tasa de bits a 8MHz

| $f_{PER} = 8.0000 \text{ MHz}$ | | | | |
|--------------------------------|------|-----------|--------------------------|--------|
| $f_{BAUD}(\text{bps})$ | BSEL | BSEL(hex) | $f_{BAUD}^*(\text{bps})$ | Error |
| 9.6K | 51 | 0x33 | 9.61K | 0.2 % |
| 19.2K | 25 | 0x19 | 19.23K | 0.2 % |
| 28.8K | 16 | 0x10 | 29.412K | 2.1 % |
| 38.4K | 12 | 0x0C | 38.462K | 0.2 % |
| 48K | 9 | 0x09 | 50K | 4.2 % |
| 57.6K | 8 | 0x08 | 55.556K | -3.5 % |
| 62.7K | 7 | 0x07 | 62.5K | -0.3 % |
| 76.8K | 6 | 0x06 | 71.429K | -7.0 % |
| 86.4K | 5 | 0x05 | 83.333K | -3.5 % |
| 96K | 4 | 0x04 | 100K | 4.2 % |
| 105.6K | 4 | 0x04 | 100K | -5.3 % |
| 115.2K | 3 | 0x03 | 125K | 8.5 % |

Fuente: Elaboración propia

Como se puede observar en la tabla 9 el error a una tasa de bits por arriba de los 62.7Kbps se eleva hasta los 8.5 %, valor que se desvía demasiado del estándar. Con una frecuencia de reloj de 16Mhz se obtienen mejores resultados en cuanto a la variación de tasa de bits.

Cuadro 10: Error de tasa de bits a 16MHz

| $f_{PER} = 16.0000 \text{ MHz}$ | | | | |
|---------------------------------|------|-----------|--------------------------|--------|
| $f_{BAUD}(\text{bps})$ | BSEL | BSEL(hex) | $f_{BAUD}^*(\text{bps})$ | Error |
| 9.6K | 103 | 0x67 | 9.61K | 0.2 % |
| 19.2K | 51 | 0x33 | 19.23K | 0.2 % |
| 28.8K | 34 | 0x22 | 28.571K | -0.8 % |
| 38.4K | 25 | 0x19 | 38.462K | 0.2 % |
| 48K | 20 | 0x14 | 47.619K | -0.8 % |
| 57.6K | 16 | 0x10 | 58.824K | 2.1 % |
| 62.7K | 15 | 0x0F | 62.5K | -0.3 % |
| 76.8K | 12 | 0x0C | 76.923K | 0.2 % |
| 86.4K | 11 | 0x0B | 83.333K | -3.5 % |
| 96K | 9 | 0x09 | 100K | 4.2 % |
| 105.6K | 8 | 0x08 | 111.111K | 5.2 % |
| 115.2K | 8 | 0x08 | 111.111K | -3.5 % |

Fuente: Elaboración propia

En la Figura 16 se muestra la captura de un osciloscopio que capturó la forma de onda otorgada por un generador de funciones a 57.6KHz, donde se observa que el tiempo de cada bit es de $17.36\mu\text{s}$. De la misma forma en la Figura 17 se muestra la captura de un osciloscopio que capturó la forma de onda durante la transmisión serial entre el Arduino UNO y el sensor serial a 57600bps, donde se observa que el tiempo de cada bit es de $17.0\mu\text{s}$, y además se observa que la frecuencia es de 58.8Khz.

Por lo tanto se demuestra que la transmisión serial asíncrona que existe entre el Arduino

UNO y el sensor biométrico ZFM-20 a 57600bps idealmente, en la práctica es de 58824bps produciendo un error del 2.1 % como se demostró en la Ecuación 3.11. Por lo tanto la frecuencia de reloj seleccionada para el ATmega328P fué de 16MHz.

3.2.4. Selección del núcleo del dispositivo registrador de nuevas huellas

Para la selección del núcleo del registrador de nuevas huellas se tomó en cuenta a los dispositivos con conexión serial, Ethernet y que además tengan acceso a realizar consultas y operaciones en la base de datos, para ello se buscaron opciones en la tienda virtual www.TecBolivia.com y entre las opciones de dispositivos con estas características se encontraron dos placas de desarrollo Cubieboard y Raspberry Pi.

En cuanto a Raspberry Pi, se descartó el modelo A ya que no tiene soporte para conexión Ethernet, se descartó también el modelo 2 en favor del modelo 3 ya que ambos tienen el mismo costo pero el modelo 2 tiene prestaciones menores al modelo 3.

Por lo tanto la comparación se realizó entre las placas de desarrollo Cubieboard ARM Cortex-A8 Mini PC, Cubieboard2 ARM Cortex-A7 Dual Core Mini PC y Raspberry Pi Modelo B Version 3 cuya comparación se muestra en la Tabla 11.

Gracias a esta comparación se seleccionó la placa de desarrollo Raspberry Pi Modelo B Versión 3 Mini PC porque tiene 2 núcleos más que la placa Cubieboard2 y 3 más que la placa Cubieboard, además la arquitectura es de 64 bits en comparación con los 32 bits de las placas Cubieboard y tiene incorporado un circuito para conexión Wi-Fi.

Por otro lado las placas Cubieboard tienen bondades como una entrada de señal de frecuencia modulada o el conversor analógico-digital que incrementan su precio y en este caso no tendrán ninguna funcionalidad.

Cuadro 11: Comparación Raspberry vs Cubieboard

| Característica | Cubieboard ARM Cortex-A8 | Cubieboard2 ARM Cortex-A7 | Raspberry Pi Modelo B Version 3 |
|------------------------|----------------------------|--------------------------------------|---|
| Procesador | SoC A10 ARM® Cortex™-A8 | SoC A20 ARM® Cortex™-A7 Dual-Core | SoC ARM® Cortex™-A53 Quad Core |
| Frecuencia de Clock | 1.0Ghz | 1.2GHz | 1.2GHz |
| Arquitectura | 32bits | 32bits | 64bits |
| Memoria RAM | 1GB DDR3 | 1GB DDR3 | 1GB DDR3 |
| Memoria de programa | 4GB Flash NAND | 4GB Flash NAND | - |
| Salida de video | HDMI 1080p | HDMI 1080p | HDMI 1080p, RAW LCD |
| Almacenamiento externo | Micro SD, SATA (+5v power) | Micro SD, SATA (+5v power) | Micro SD |
| Ethernet | 10/100M | 10/100M | 10/100M |
| WiFi | - | - | BCM43143 |
| Alimentacion | 5V @ 2A | 5V @ 2A | 5V @ 2.4 A via microUSB |
| GPIO | 96 pines | 96 pines | 40 pines |
| Sistemas operativos | Ubuntu, Android | Ubuntu 12.04, Android 4.2.2 | Raspbian, Windows 10 IoT Core, Pidora, Arch Linux |
| Precio | 98\$us | 118\$us | 70.30\$us |

Fuente: Elaboración propia

3.2.5. Selección del método de respaldo

Para la selección del método de respaldo se descartó el método de panel numérico por el estrecho espacio que existe en los ambientes del centro de datos para colocar un dispositivo al ingreso de cada puerta, por tanto se selecciono un método que también se basa en contraseñas numéricas pero que no precisa de un espacio visible en la instalación, el método seleccionado fué un circuito bluetooth.

3.2.5.1. Selección del módulo bluetooth

Se seleccionó el módulo bluetooth HC-06 porque solo se necesita que el módulo trabaje como esclavo y no como maestro, por eso se descartó el módulo bluetooth HC-05.

3.2.5.2. Selección del dispositivo de procesamiento de datos

Como ya se mencionó, para la selección de este dispositivo se tomó más en cuenta el espacio que ocuparía la placa desarrollada, por tanto se seleccionó el otro microcontrolador disponible en el mercado, el ATtiny85 que tiene las características suficientes para manejar dos relés para controlar la apertura de las puertas y conectarse con el módulo bluetooth HC-06.

Para la conexión con este dispositivo se desarrollo una aplicación en Android con la cual se envían las contraseñas almacenadas en la memoria del dispositivo con las cuales se abren las puertas controladas por este dispositivo en caso de que el sistema de control de accesos o el sensor de huellas presenten fallas.

3.2.6. Selección de la cerradura eléctrica

Para seleccionar la cerradura eléctrica se realizaron pruebas con 2 tipos de cerraduras, las de contacto magnético y las de tornillo tipo BOLT. Se seleccionó la cerradura de tornillo ya que la cerradura de contacto magnético cedía ante fuerzas aplicadas para forzar la apertura de la cerradura.

3.2.7. Selección de la base de datos

Ya que los datos tienen relación entre sí, se definió utilizar una base de datos SQL.

Para la selección del gestor de bases de datos se tomó como principal criterio la seguridad al momento de la conexión con la base de datos y las licencias de código abierto, por lo cual se descartó SQLite ya que no cuenta con un método de seguridad para filtrar IPs o hosts que intentan conectarse con la base de datos, por tanto las opciones que quedaron fueron MySQL y PostgreSQL. Ambas cuentan con las características que se buscan pero PostgreSQL cuenta con una adicional, la de reacción ante eventos o cambios en los datos, por lo tanto PostgreSQL se enfoca en la adquisición y monitoreo de datos en tiempo real, esta es la característica necesaria para realizar el monitoreo en el sistema web desarrollado, por lo tanto la base de datos que se utilizó en el proyecto fué PostgreSQL.

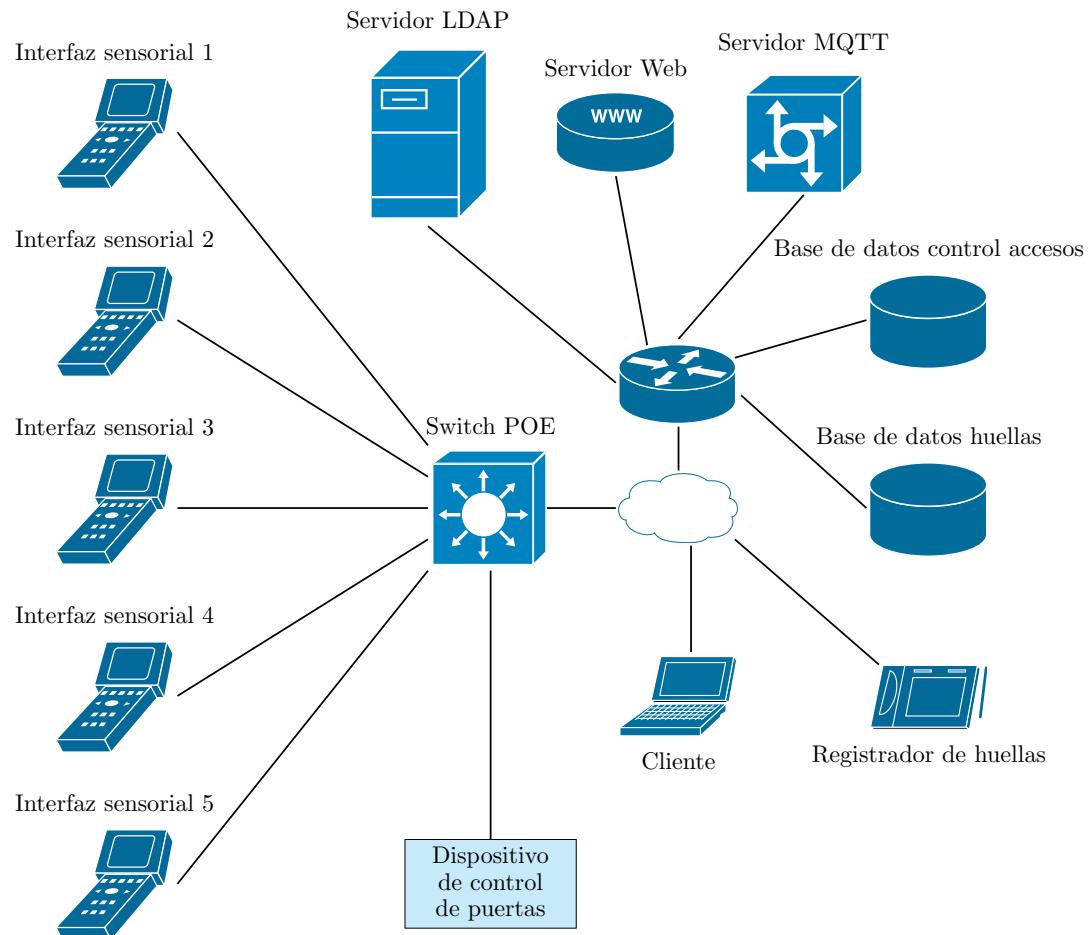
3.2.8. Diagrama de red del sistema de control de accesos

El diagrama de la Figura 18 muestra que la instalación se realizó en base a una topología desconocida entre el cliente y el sistema, pero para evitar ataques de spoofing o de suplantación de identidad se tiene un router que contiene reglas específicas para que solo las direcciones MAC de los dispositivos de interfaz sensorial, el controlador de puertas y el registrador de nuevas huellas puedan acceder a los servidores MQTT, LDAP y de bases

de datos. Por otra parte los clientes conectados a la red pueden acceder al servidor web sin ninguna restricción, esto no conlleva ningún riesgo ya que se cuenta con métodos de seguridad mediante login con credenciales de usuario y contraseña a los que el servidor devuelve un token en formato JSON para mantener la sesión activa por un tiempo determinado.

El Switch POE instalado es de 24 puertos previendo la escalabilidad del sistema a futuro, este Switch POE es compatible con el estándar 802.3af.

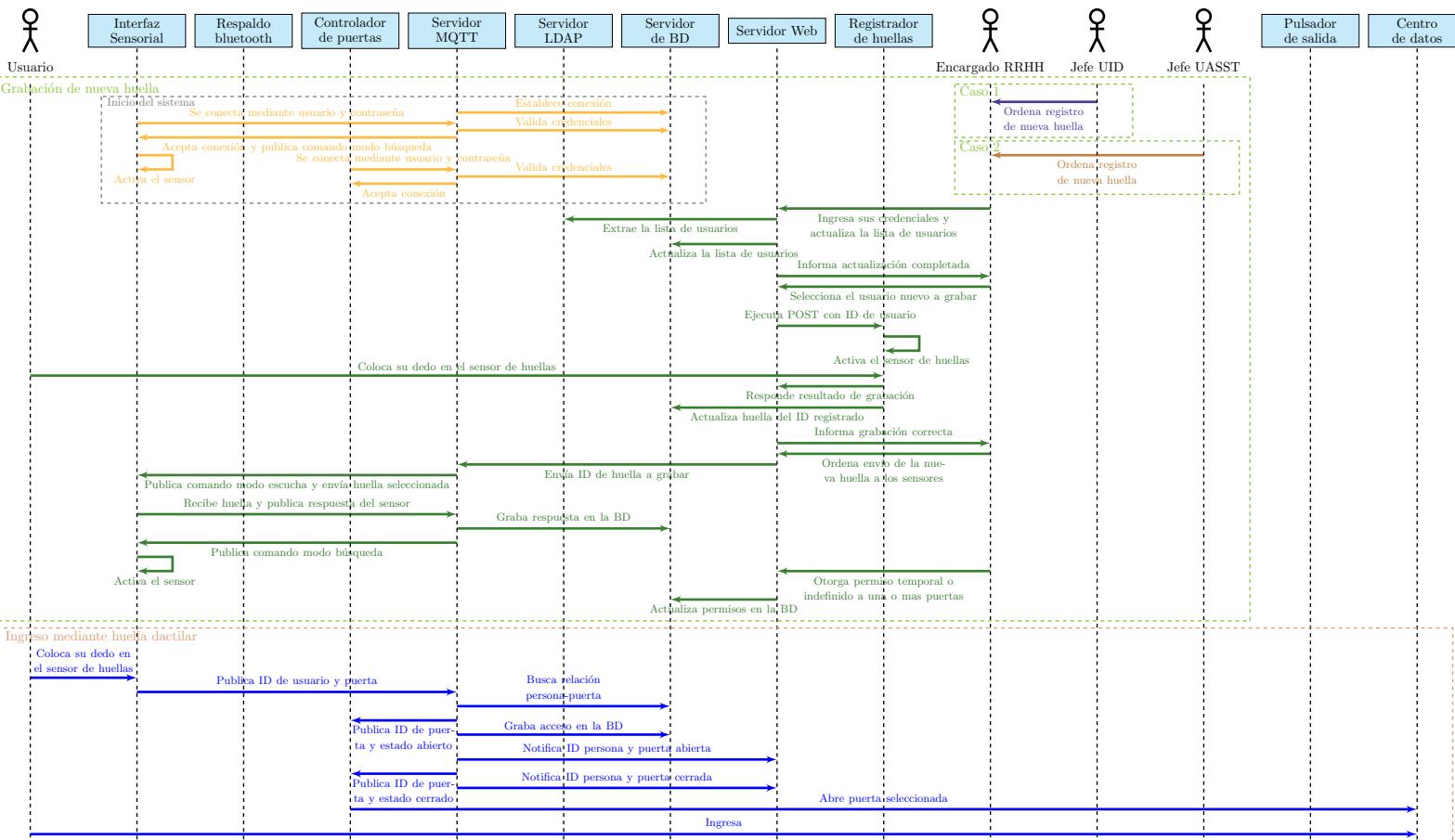
Figura 18: Diagrama de red del sistema



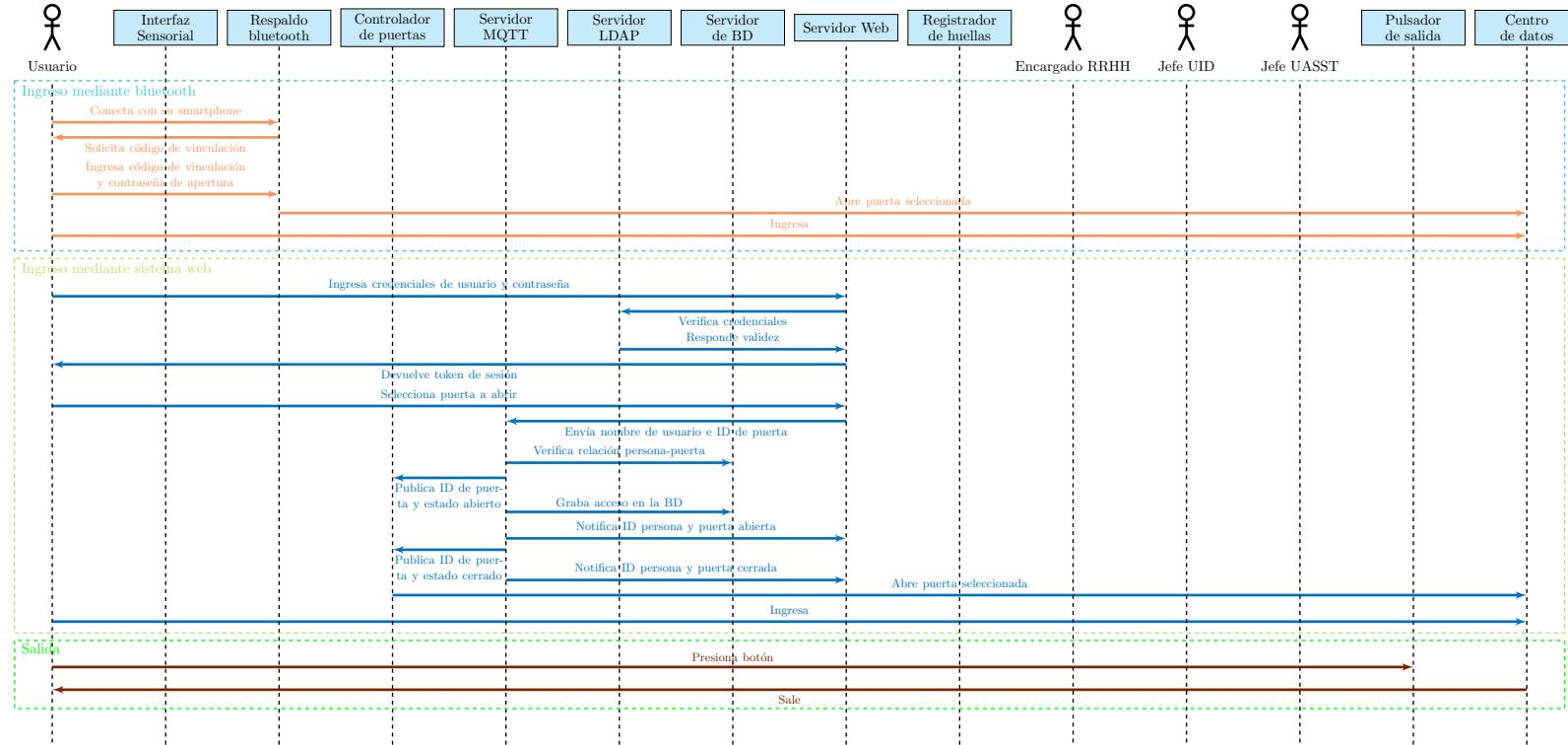
Fuente: Elaboración propia

3.2.9. Diagrama de flujo para el ingreso posterior a la instalación del sistema desarrollado

Figura 19: Diagrama de flujo posterior



Fuente: Elaboración propia. Continua en la siguiente página.



La Figura 19 muestra el flujo de las acciones que se producen al inicio del sistema, es decir una vez que el servidor MQTT se ha encendido y el switch POE alimenta a los dispositivos de interfaz sensorial y de control de puertas, para que inicie este proceso es requisito que el servidor de bases de datos se encuentre activo.

La grabación de huellas inicia mediante un email que recibe el encargado de recursos humanos de uno de los jefes designados por el Director Ejecutivo de ADSIB, el encargado se respalda en este correo y comienza el proceso de grabación siempre y cuando el dispositivo registrador se encuentre activo y tenga acceso a la red configurada para el sistema de control de accesos de acuerdo al diagrama de la Figura 18.

Para el ingreso al sistema web las credencias que utiliza el encargado son provistas por la persona que instaló el sistema ya que al momento de la instalación del sistema se crea un super-usuario con el que se pueden crear otros usuarios y proveerlos de permisos de administración.

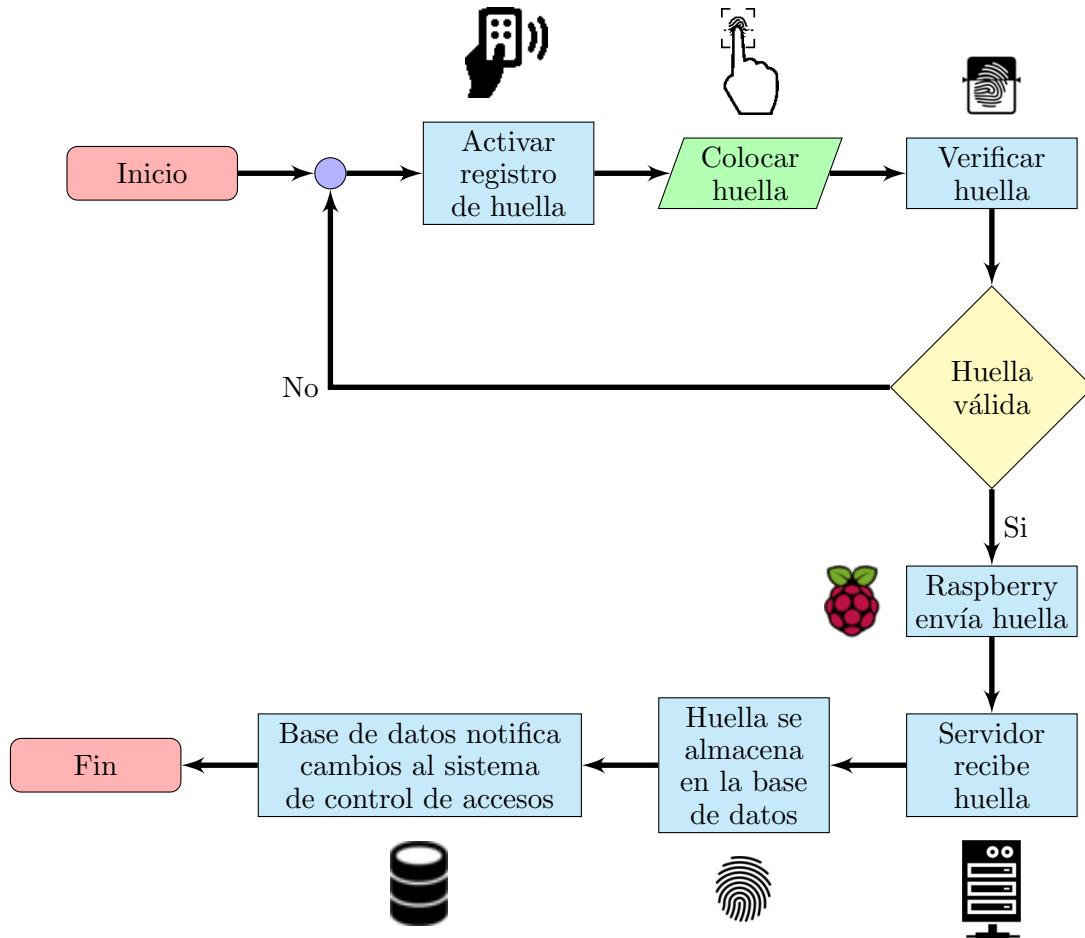
3.3. Secuencia de acción para el registro de una nueva huella

Para este proceso se desarrolló un sistema basado en Raspberry Pi 3 modelo B V1.2 (aunque también es compatible Raspberry Pi 2), un sensor de huellas dactilares ZFM-20 [56], un módulo receptor POE para la alimentación de energía y la conexión de red.

Este sistema se basa en la arquitectura de orquestación de micro-servicios, mediante la cual se levantan servicios particulares para cada sub-sistema; con este enfoque se observan dos micro-servicios en el lado del servidor, cuyo sistema operativo es Linux Debian 8.3, el primer micro-servicio proveé una base de datos PostgreSQL en su versión 9.4 (compatible con versiones superiores) y el segundo micro-servicio proveé una API REST en lenguaje Javascript con el manejador de rutas Express.

Por otra parte el hardware embebido levanta una imagen de Linux Raspbian contenida

Figura 20: Diagrama de flujo para el registro de una nueva huella

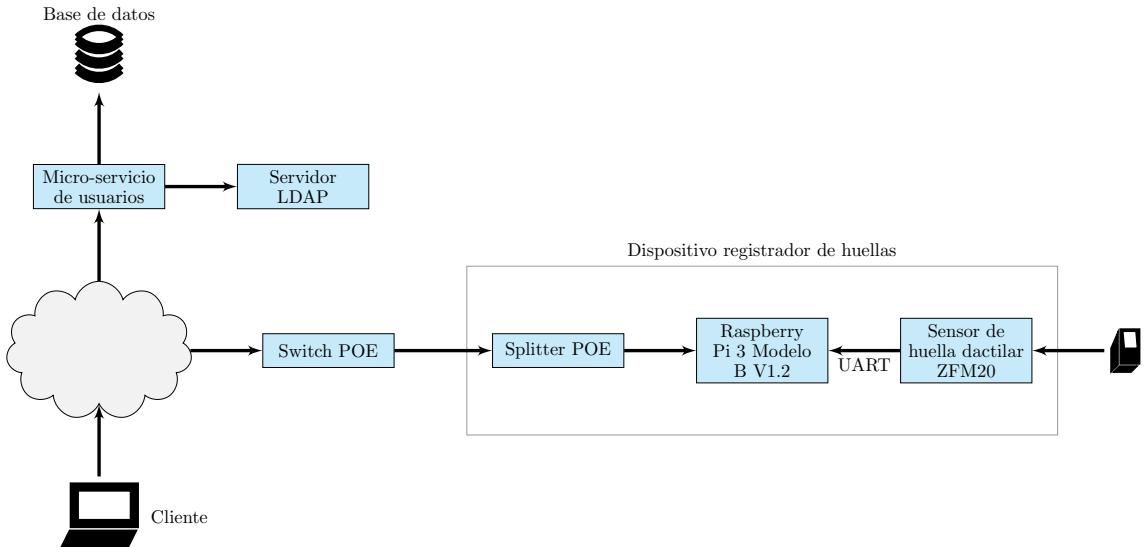


Fuente: Elaboración propia

en una tarjeta μ SD, sobre la cual se ejecutan dos micro-servicios, el primero es una API REST en Node.js con el manejador de rutas Restify que provee todos los comandos y se encarga de la comunicación con el sensor de huellas dactilares, el segundo se encarga de la sincronización de los datos de los usuarios almacenados en el servidor. Esta API es consultada por el servidor web, la comunicación se produce mediante intercambio de mensajes en formato JSON.

Todos los sub-procesos son orquestados por un proceso principal que se encarga del inicio de los procesos y la transferencia de mensajes entre sub-procesos. Este proceso principal

Figura 21: Diagrama de bloques del equipo registrador de huellas



Fuente: Elaboración propia

se ejecuta en el mismo servidor del broker MQTT. Todos los micro-servicios pueden ser instalados mediante la tecnología de virtualización Docker ya que el protocolo MQTT soporta la traducción de direcciones NAT¹⁰.

3.3.1. Registro de usuarios en el servidor LDAP

Para realizar este proceso se debe contar con un servidor OpenLDAP, el cual almacena todos los datos críticos de las personas que podrán hacer uso del sistema de puertas. El micro-servicio se conecta al servidor LDAP para obtener la lista de personas conjuntamente con sus datos adicionales como por ejemplo nombre de usuario, cargo, etc. Se pueden insertar usuarios con alguna herramienta como LDAP-utils, Apache Directory o phpLDAPadmin

El servidor LDAP debe estar organizado de la siguiente manera:

¹⁰Network Address Translation

Dominio de la entidad: dc=entidad,dc=com

Usuario administrador: cn=admin,dc=entidad,dc=com

Grupo de usuarios: ou=usuarios,dc=entidad,dc=com (organizational unit)

Identificador de usuario: uid=usuario1,ou=usuarios,dc=entidad,dc=com
(inetOrgPerson)

Todos los miembros (*member*) que se encuentren en el grupo *ou=usuarios* estarán disponibles para poder acceder por las puertas de acuerdo a la tabla de *permisos* que se mostrará mas adelante.

Los datos adicionales que se utilizarán para cada usuario son los siguientes:

Nombres: givenName=Jhon Juan

Apellidos: sn=Doe Pérez

Carnet de identidad: cn=5552368

Cargo: title=Encargado de recursos humanos

Tipo de cargo: employeeType=rrhh

Clave: userPassword=abc123

Correo: mail=jhon@doe.com

Teléfono: telephoneNumber=5550123

El tipo de cargo se puede utilizar para brindar permisos de administración del sistema solo a ciertos tipos de cargos.

Si el servidor LDAP se va a utilizar para la autenticación de usuarios en otros servicios como correos electrónicos, almacenamiento en la nube, etc, es muy recomendable cifrar la comunicación mediante SSL.

Figura 22: Registro de usuario en el servidor de LDAP

| DN: uid=usuario1,ou=usuarios,dc=entidad,dc=com | |
|--|--|
| Attribute Description | Value |
| objectClass | <i>inetOrgPerson (structural)</i> |
| objectClass | <i>organizationalPerson (structural)</i> |
| objectClass | <i>person (structural)</i> |
| objectClass | <i>top (abstract)</i> |
| cn | 5552368 |
| sn | Doe Pérez |
| employeeType | rrhh |
| givenName | Jhon Juan |
| mail | jhon@doe.com |
| telephoneNumber | 5550123 |
| title | Encargado de recursos humanos |
| uid | usuario1 |
| userPassword | SSHA hashed password |

Fuente: Elaboración propia

3.3.2. Base de datos de huellas

Esta base de datos se sincroniza con los datos del servidor LDAP mediante el micro-servicio de usuarios, dentro está contenida la lista de personas, sus huellas y la imagen de sus huellas.

Existe una relación 1-1 entre el campo id de la tabla *huella* que toma de referencia el ID de la tabla *personas*, la plantilla de cada huella es un número hexadecimal de 512 bytes en formato de cadena de caracteres, tal como se indica en la sección de *Character file buffer* del manual del sensor ZFM-20 [56].

Del mismo modo, la imagen de cada huella es un número hexadecimal de 36864 bytes en formato de cadena de caracteres, tal como se indica en la sección de *Image file buffer* del manual del sensor ZFM-20 [56]. Este número necesita un tratamiento antes de representarlo como una imagen ya que el sensor solo envía el nibble más alto de cada

pixel, por lo cual cada nibble debe desplazarse cuatro posiciones a la izquierda, con lo que se obtendría un número de 73728 bytes, los cuales se deben acomodar en una matriz de 288x256 para formar la imagen en formato de mapa de bits de escala de grises de cada huella.

Figura 23: Imagen de huella generada desde el sensor ZhianTec ZFM-20



Fuente: Elaboración propia

3.3.2.1. Forma normal 1 para la base de datos de huellas

La reducción de esta base de datos solo necesita de la Forma Normal 1 para eliminar los datos repetidos, eliminar errores lógicos y tener los datos ordenados. Los datos de prueba se observan el la Tabla 12.

Cuadro 12: Datos de prueba para la base de datos de huellas

| usuario | huella_imagen | huella_plantilla |
|---------|-----------------|------------------|
| jdoe | 8abddeeeefff... | 03014e138d00... |
| jperez | 21cff04631dc... | 8647a9cdf8a1... |

Fuente: Elaboración propia

Con la reducción de la Tabla 13 se obtiene el diagrama entidad-relación de la Figura 24.

Cuadro 13: Reducción a la Forma Normal 1 de la base de datos de huellas

(a) Tabla persona

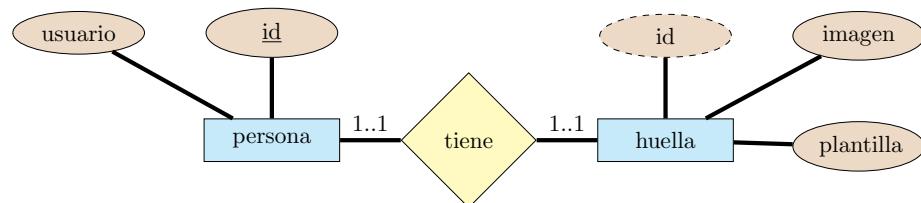
| id | usuario |
|----|---------|
| 1 | jdoe |
| 2 | jperez |

(b) Tabla huella

| id | imagen | plantilla |
|----|-----------------|-----------------|
| 1 | 8abddeeeefff... | 03014e138d00... |
| 2 | 21cff04631dc... | 8647a9cdf8a1... |

Fuente: Elaboración propia

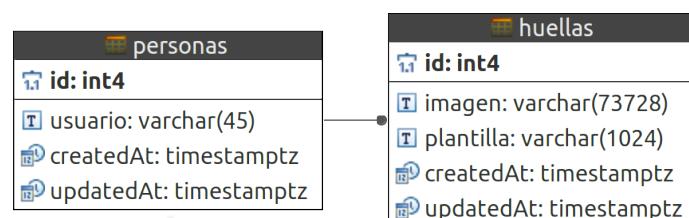
Figura 24: Diagrama entidad-relación para la base de datos de huellas



Fuente: Elaboración propia

Lo cual finalmente genera la base de datos mostrada en la Figura 25.

Figura 25: Base de datos de huellas



Fuente: Elaboración propia

3.3.3. Hardware registrador de huellas

Este hardware se compone de los siguientes componentes:

Splitter POE: Este equipo sirve para separar los datos de la energía que viajan juntos por la conexión Ethernet, se conecta la salida de datos a la entrada RJ-45 del Raspberry y se alimenta a todo el equipo con la energía recibida por el POE, dado que éste puede alcanzar hasta los 12.95W en el estándar 802.3af y el equipo completo consume como pico máximo 3.65W (Incluyendo el splitter mismo), se observa que este estándar es suficiente para alimentar el dispositivo.

Raspberry: Es el computador donde se realizan todos los procesos de captura de huellas y sincronización de la base de datos con el servidor LDAP.

Sensor dactilar ZFM-20: Es el módulo que se conecta mediante UART y se alimenta desde el GPIO del Raspberry.

Figura 26: Prototipo del hardware grabador de huellas



Fuente: Elaboración propia

Para realizar la validación de alimentación de energía mediante POE se debe calcular la potencia del equipo que se desea energizar, para ello se calcula la potencia consumida por cada dispositivo al extremo receptor de la línea de POE. En este caso tenemos 3 equipos a alimentar, los datos para este efecto fueron obtenidos de la hoja de datos del Splitter POE [45], la hoja de datos del Sensor de huella dactilar [56] y la tabla de consumo de energía de Raspberry Pi Dramble¹¹.

En corriente continua la potencia eléctrica desarrollada por un dispositivo entre dos terminales, es el producto de la diferencia de potencial entre las dos terminales y la intensidad de corriente que circula por el dispositivo:

$$P = \frac{dw}{dt} = \frac{dw}{dq} \cdot \frac{dq}{dt} = V \cdot I \quad (3.12)$$

Donde: V es el valor instantáneo del voltaje expresado en Voltios, I es el valor instantáneo de la intensidad de corriente expresado en Amperios y P es el valor instantáneo de la potencia expresado en Vatios.

Cuadro 14: Cálculo de potencia consumida por cada dispositivo capturador de huellas

| Dispositivo | Modelo | Voltaje de alimentación | Consumo de corriente | Potencia consumida |
|---------------------------|-----------|-------------------------|----------------------|--------------------|
| Splitter POE | TL-POE10R | 12V | 80mA | 0.96W |
| Raspberry Pi | 3 B V1.2 | 5V | 480mA | 2.40W |
| Sensor de huella dactilar | ZFM-20 | 5V | 150mA | 0.75W |
| Total | | | | 4.11W |

Fuente: Elaboración propia

Este resultado se adhiere a los parámetros de la instalación, como por ejemplo la longitud

¹¹<https://www.pidramble.com>

máxima del segmento de par trenzado UTP, el número de dispositivos a alimentar, el estándar a utilizar y el voltaje provisto desde el extremo inyector de la línea de POE.

Cuadro 15: Parámetros para el cálculo de potencia consumida del capturador de huellas

| Parámetro | Valor |
|---------------------------------------|---------|
| Estándar POE | 802.3af |
| Distancia | 100m |
| Voltaje de alimentación | 48V |
| Watts requeridos | 4.11W |
| Número de dispositivos para alimentar | 1 |

Fuente: Elaboración propia

Con todos estos datos se puede realizar el cálculo de la potencia real que debe suministrarse desde el inyector de la línea de POE, ya que a lo largo de la línea se producen pérdidas por la resistencia eléctrica del par trenzado. Muchas veces éste es un problema que no es considerado, por lo cual si no se contempló este cálculo al realizar la instalación, los equipos podrían funcionar incorrectamente o definitivamente podrían no funcionar.

El cable UTP previsto para los cálculos es de categoría 5e, de aleación cobre/aluminio al 10 %, de medida 28AWG cuya resistencia es de 101Ω para una longitud de 1000 pies.
[Anexo 14]

Mediante la herramienta de cálculos para diseños de red POE POE-Texas Calculator¹² y los parámetros mostrados anteriormente se obtiene la pérdida de energía en la línea de transmisión POE y la potencia real que debe ser suministrada en el extremo inyector de la línea.

¹²<http://poe-texas.com/Calculator/>

Cuadro 16: Potencia consumida por el dispositivo registrador de huellas al extremo receptor POE

| Parámetro | Valor |
|---|---------|
| Voltaje al extremo del tramo | 47.27V |
| Corriente al extremo del tramo | 90mA |
| Resistencia del cable | 8.3968Ω |
| Pérdida de potencia en la línea | 0.06W |
| Potencia suministrada desde el inyector | 4.17W |

Fuente: Elaboración propia

3.4. Secuencia de acción para el acceso mediante sensor biométrico de huellas dactilares

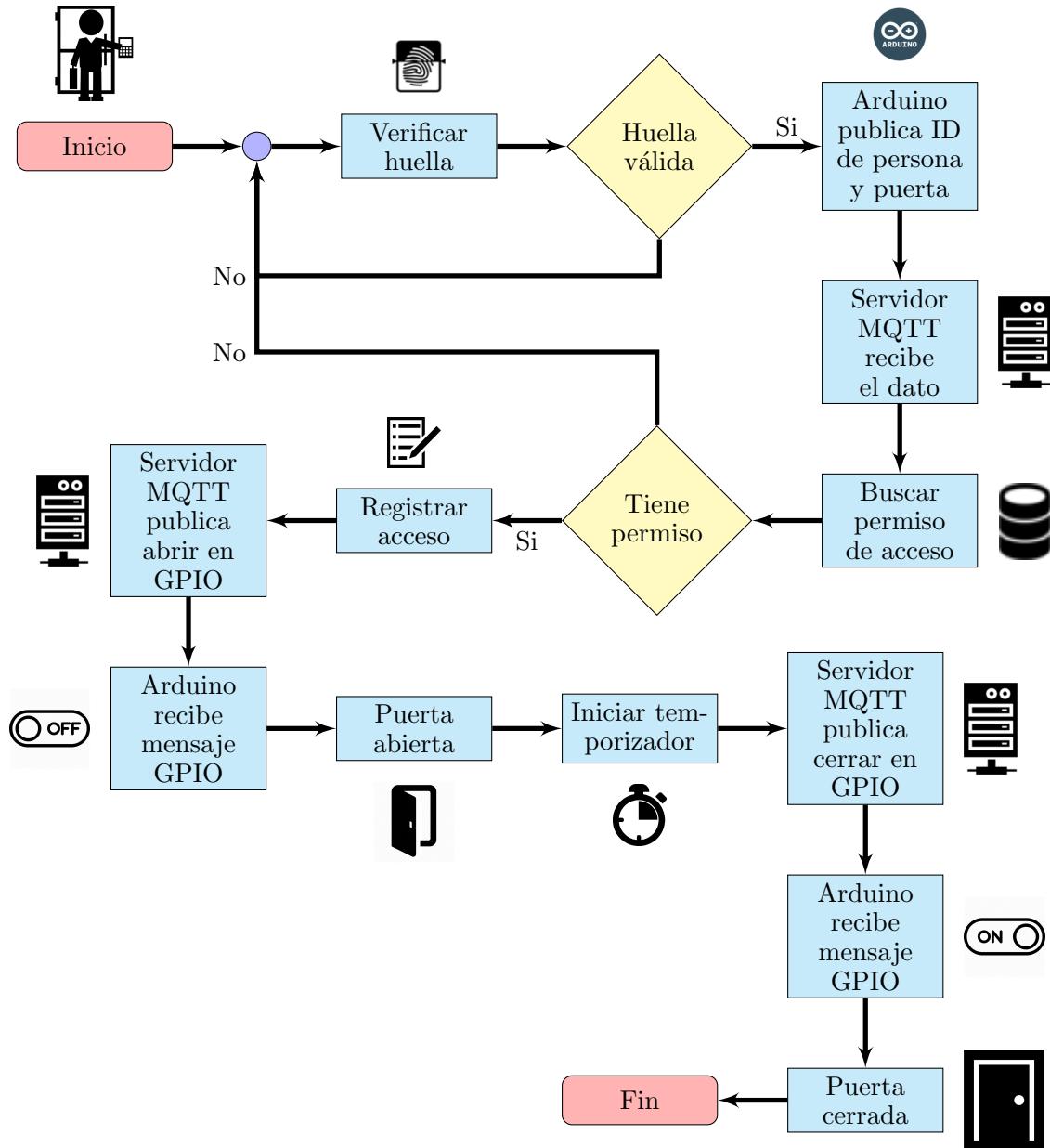
Antes de ejecutar este proceso se debe registrar la huella de las personas que ingresarán a los ambientes resguardados por el sistema tal como se menciona en la Sección 3.3, caso contrario el sistema no reconocerá una huella conocida y este proceso se truncará en el primer paso.

También se debe tener la certeza de que los dispositivos pueden acceder al servidor MQTT mediante una infraestructura de red como la que se muestra en la Figura 18, en caso de existir un router, éste debe contar con las reglas necesarias para permitir el envío y recepción de paquetes HTTP e ICMP¹³ desde y hacia el servidor MQTT.

Se debe verificar que los dispositivos se encuentren alimentados por el switch POE y no exista ningún tipo de alerta en el mismo.

¹³Internet Control Message Protocol

Figura 27: Diagrama de flujo para la apertura de puerta mediante biométrico



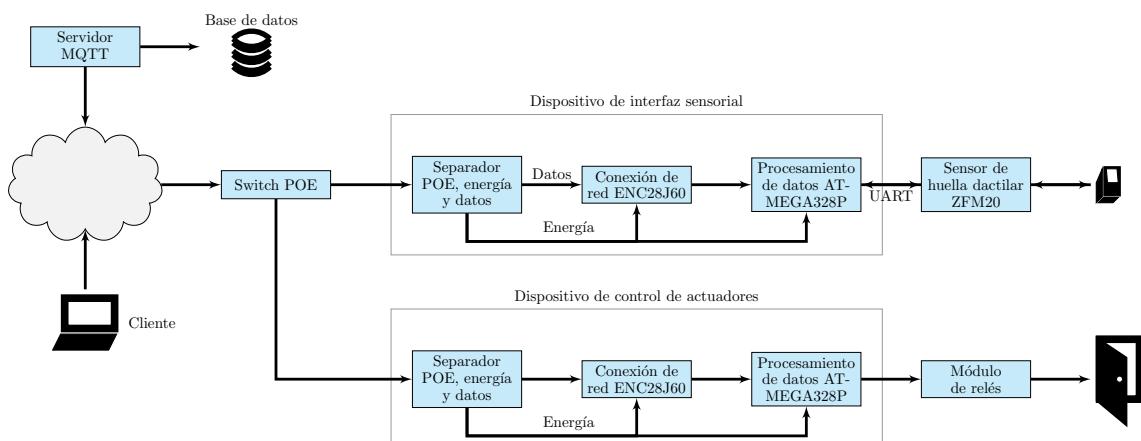
Fuente: Elaboración propia

3.4.1. Hardware de control e interfaz sensorial

El diseño de este hardware se realizó en base al esquema de Arduino UNO R3, al cual se habilita una conexión de red mediante el circuito integrado ENC28J60 y ambos bloques son alimentados mediante POE gracias al circuito integrado LTC4267-3, el esquema de la placa desarrollada se puede observar en el Anexo 3.

Este dispositivo se utiliza tanto para realizar la conexión con el sensor de huellas dactilares como para realizar el control de los actuadores que abren y cierran las puertas, ambos se conectan al sistema mediante el protocolo MQTT como se puede observar en el siguiente diagrama:

Figura 28: Diagrama de bloques de los dispositivos de control e interfaz sensorial

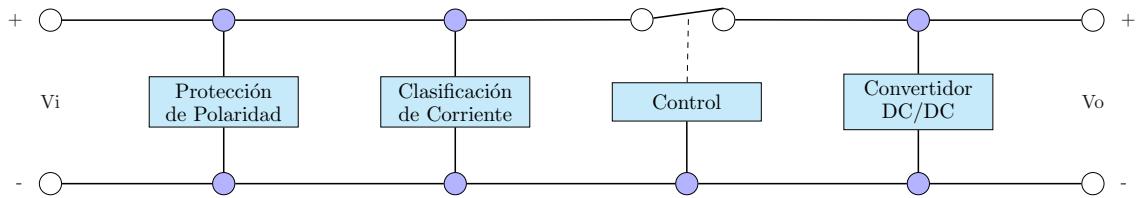


Fuente: Elaboración propia

3.4.1.1. Separador POE, energía y datos

Esta etapa se encarga de negociar la potencia requerida para alimentar el circuito de interfaz sensorial o de control de actuadores, se basa en el esquema de Splitter POE diseñado por Linear Technology [Anexo 17], cuyo componente central es el circuito integrado LTC4267-3, que se encarga de negociar la energía provista por el inyector.

Figura 29: Diagrama de bloques del Splitter POE



Fuente: Elaboración propia

El primer bloque del circuito POE es el de Protección de Polaridad, la tensión desde el inyector puede venir de dos formas, una es utilizar dos pares alternativos del cable ethernet para enviar el voltaje positivo en uno y el negativo en otro. La segunda forma es enviar la tensión conjuntamente con los datos, ésta forma tiene la ventaja de que los pares alternativos se pueden utilizar para llegar a la velocidad de 1Gigabit mientras que la primera forma solo alcanza los 10/100Megabits.

Cuadro 17: Estándares 802.3af A y B, perspectiva desde el inyector

| Pins at switch | T568A color | T568B color | 10/100 mode B, DC on spares | 10/100 mode A, mixed DC & data | 1000 (1 gigabit) mode B, DC & bi-data | 1000 (1 gigabit) mode A, DC & bi-data |
|----------------|---------------------|---------------------|--------------------------------|---|---|---|
| Pin 1 | White/green stripe | White/orange stripe | Rx + | Rx + DC + | TxRx A + | TxRx A + DC + |
| Pin 2 | Green solid | Orange solid | Rx - | Rx - DC + | TxRx A - | TxRx A - DC + |
| Pin 3 | White/orange stripe | White/green stripe | Tx + | Tx + DC - | TxRx B + | TxRx B + DC - |
| Pin 4 | Blue solid | Blue solid | DC + | Unused | TxRx C + | DC + TxRx C + |
| Pin 5 | White/blue stripe | White/blue stripe | DC + | Unused | TxRx C - | DC + TxRx C - |
| Pin 6 | Orange solid | Green solid | Tx - | Tx - DC - | TxRx B - | TxRx B - DC - |
| Pin 7 | White/brown stripe | White/brown stripe | DC - | Unused | TxRx D + | DC - TxRx D + |
| Pin 8 | Brown solid | Brown solid | DC - | Unused | TxRx D - | DC - TxRx D - |

Fuente: Power Over Ethernet, Pinouts, Wikipedia

El segundo bloque del circuito POE es el de Clasificación de Corriente, existen 4 fases durante la etapa de negociación, la primera es para verificar si el equipo al extremo receptor es o no POE, para ello el inyector aplicará una tensión de 2.7V a 10V buscando una resistencia de $25K\Omega$. Si ésta es demasiado baja o alta no continuará aplicando tensión.

En caso de que el dispositivo sí sea POE, la tensión se eleva de 14.5V a 20.5V y se mide la corriente que circula por el receptor, con este resultado el inyector determina cual es la tensión máxima permitida para el funcionamiento del dispositivo POE.

La tercera etapa es el comienzo de la alimentación del dispositivo y en la cuarta etapa se tiene una tensión constante para el funcionamiento continuo del dispositivo POE.

El tercer bloque del circuito POE es el de Control, en esta fase se tiene un convertidor DC/DC [37] que se mantendrá apagado hasta que se haya terminado la etapa de clasificación, es decir cuando el voltaje haya alcanzado los 35V.

El cuarto bloque es la activación del convertidor DC/DC, es el paso final para la alimentación del circuito POE, es aquí donde se reduce la tensión DC de 48V a la tensión necesaria para el funcionamiento del circuito.

3.4.1.2. Conexión de red ENC28J60

Esta etapa se basa en el esquema de la placa Olimex Ethercard [Anexo 18], cuyo componente central es el circuito integrado ENC28J60, este dispositivo tiene 6 registros en su mapa de registros de control que definen la dirección MAC al momento de realizar la conexión con el microcontrolador mediante el protocolo SPI. Precisa de un oscilador a 25MHz además de una alimentación de 3.3V, pero se debe tomar en cuenta que la comunicación SPI se realiza al nivel TTL de 5V.

Se le puede definir una IP estática pero también tiene soporte para la asignación de IP por DHCP, soporta las operaciones de Capa 3 o Capa de Red del Modelo OSI. Cabe mencionar

que este circuito brinda soporte para trabajar a 10/100MBits, pero para este proyecto no es necesaria una conexión más veloz, por lo cual el bajo costo del dispositivo justifica esta velocidad.

Es mediante este circuito integrado que todos los datos son enviados y recibidos desde el servidor MQTT hasta el microcontrolador para que puedan ser procesados de manera adecuada. Para comunicar el microcontrolador con este circuito se utilizó la librería UIP Ethernet¹⁴ compatible con Arduino. Mediante la cual se levanta un cliente MQTT con una dirección IP y MAC estáticas, mismas que son almacenadas en la base de datos para permitir o rechazar la conexión en el lado del servidor.

Circuito de interfaz sensorial

Cuando una persona coloca su dedo en un sensor de huellas, este sensor busca en su base de datos interna si la huella está registrada, si no está no realiza ningún proceso, pero si la huella se encuentra en su base de datos envía el id al circuito de interfaz sensorial; este lo reenvía hacia el servidor MQTT con el tópico *p* seguido del id de la puerta, y el contenido del mensaje es el id obtenido del sensor:

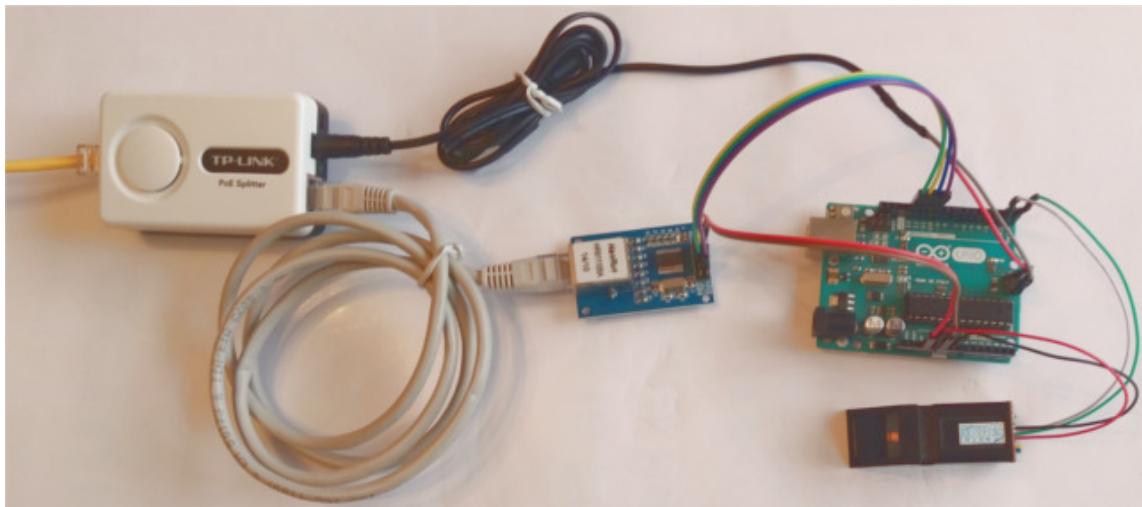
p/:idPuerta → *:idPersona*

El servidor MQTT recibe el mensaje y busca si el ID de la persona tiene permiso de acceso temporal o indefinido por el ID de la puerta; en caso de que la persona no tenga acceso el servidor no responde nada, pero si la persona tiene permiso de acceso el servidor envía un mensaje al circuito de control que se encarga de la apertura de dicha puerta.

En cuanto al consumo de energía del circuito de interfaz sensorial se realizan los cálculos en base a la ecuación 3.12.

¹⁴github.com/ntruchsess/arduino_uip

Figura 30: Prototipo del circuito de interfaz sensorial



Fuente: Elaboración propia

Cuadro 18: Cálculo de potencia consumida por cada dispositivo interfaz sensorial

| Dispositivo | Modelo | Voltaje de alimentación | Consumo de corriente | Potencia consumida |
|---------------------------|--------------------|-------------------------|----------------------|--------------------|
| Hardware diseñado | Interfaz Sensorial | 5V | 200mA | 1W |
| Sensor de huella dactilar | ZFM-20 | 5V | 150mA | 0.75W |
| Total | | | | 1.75W |

Fuente: Elaboración propia

Este valor se añade a los parámetros de instalación de cada puerta por donde se desea acceder mediante la huella dactilar.

Cuadro 19: Parámetros para el cálculo de potencia consumida por la interfaz sensorial

| Parámetro | Valor |
|---------------------------------------|---------|
| Estándar POE | 802.3af |
| Distancia | 100m |
| Voltaje de alimentación | 48V |
| Watts requeridos | 1.75W |
| Número de dispositivos para alimentar | 1 |

Fuente: Elaboración propia

Con un par trenzado UTP categoría 5e, mediante la herramienta de cálculos para diseños de red POE POE-Texas Calculator¹⁵ se obtiene la pérdida en la línea.

Cuadro 20: Potencia consumida por el dispositivo interfaz sensorial al extremo receptor

POE

| Parámetro | Valor |
|---|---------|
| Voltaje al extremo del tramo | 47.69V |
| Corriente al extremo del tramo | 40mA |
| Resistencia del cable | 8.3968Ω |
| Pérdida de potencia en la línea | 0.01W |
| Potencia suministrada desde el inyector | 1.76W |

Fuente: Elaboración propia

Círculo de control de actuadores

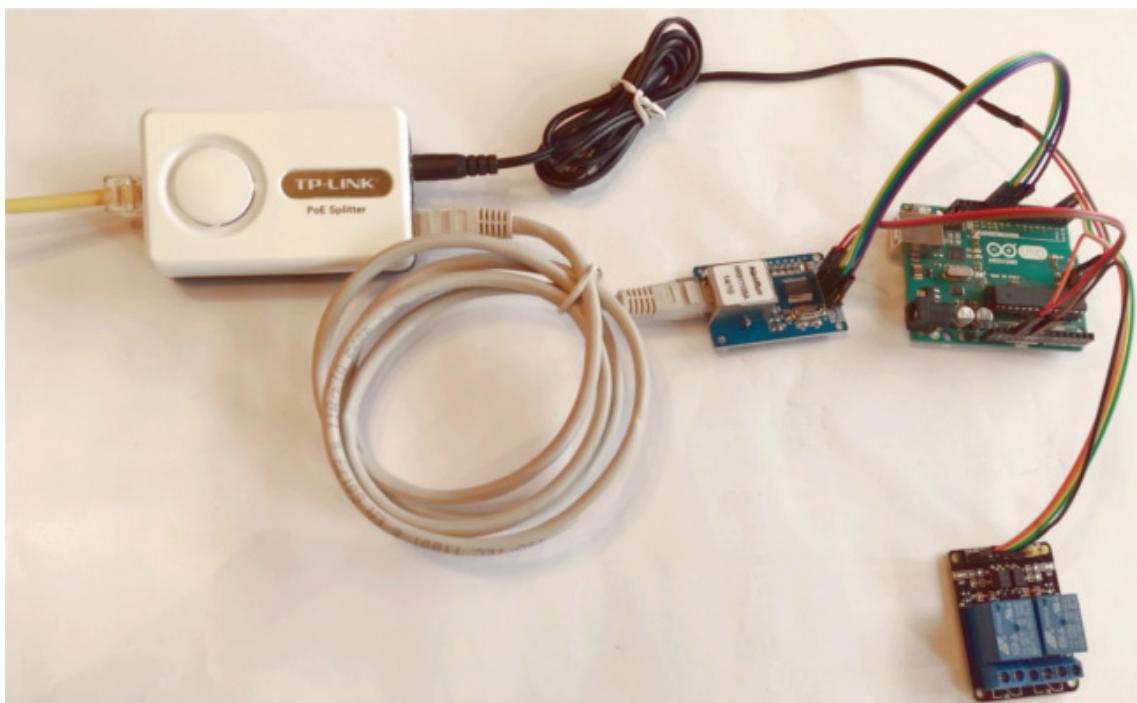
Una vez que el servidor MQTT determinó que una persona tiene acceso por una puerta, envía un mensaje en el siguiente formato:

¹⁵<http://poe-texas.com/Calculator/>

```
gpio/:idDispositivoControl/:pin → :estado
```

Donde el *idDispositivoControl* identifica el ID del dispositivo que controla la puerta que se desea abrir, el *pin* es la salida digital que está conectada al relé de la puerta y el *estado* puede ser 0 o 1, para abrir o cerrar la puerta.

Figura 31: Prototipo del circuito de control de actuadores

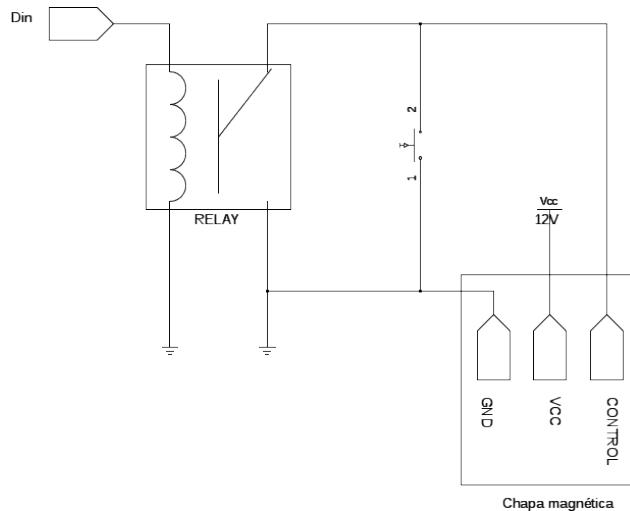


Fuente: Elaboración propia

Se ha determinado un tiempo de 6 segundos entre el envío de un mensaje de apertura de una puerta y el mensaje de cierre, dado que este tiempo es suficiente para que la persona pueda abrir la puerta e ingresar al recinto antes de que la puerta vuelva a cerrarse.

Como se mencionó antes, este dispositivo tiene conectado un módulo de relés que conectan el pin de control de cada cerradura magnética a tierra cuando reciben un impulso 0 lógico a la entrada, con lo que el pistón de la cerradura cambia de posición y deja la puerta abierta [43].

Figura 32: Conexión de las cerraduras electromagnéticas



Fuente: Elaboración propia

Para el dispositivo de control de puertas también se realizan los cálculos en base a la ecuación 3.12.

Cuadro 21: Cálculo de potencia consumida por cada dispositivo de control

| Dispositivo | Modelo | Voltaje de alimentación | Consumo de corriente | Potencia consumida |
|-------------------|------------------------|-------------------------|----------------------|--------------------|
| Hardware diseñado | Dispositivo de control | 5V | 200mA | 1W |
| Módulo relé | 4 canales | 5V | 470mA | 2.35W |
| Total | | | | 3.35W |

Fuente: Elaboración propia

Este valor se añade a los parámetros de instalación de cada puerta por donde se desea acceder mediante la huella dactilar.

Cuadro 22: Parámetros para el cálculo de potencia consumida por la placa de control

| Parámetro | Valor |
|---------------------------------------|---------|
| Estándar POE | 802.3af |
| Distancia | 100m |
| Voltaje de alimentación | 48V |
| Watts requeridos | 3.35W |
| Número de dispositivos para alimentar | 1 |

Fuente: Elaboración propia

Tomando como referencia el cable par trenzado UTP categoría 5e, mediante la herramienta de cálculos para diseños de red POE POE-Texas Calculator¹⁶ se obtiene la pérdida en la línea.

Cuadro 23: Potencia consumida por la placa de control al extremo receptor POE

| Parámetro | Valor |
|---|---------|
| Voltaje al extremo del tramo | 47.91V |
| Corriente al extremo del tramo | 70mA |
| Resistencia del cable | 8.3968Ω |
| Pérdida de potencia en la línea | 0.04W |
| Potencia suministrada desde el inyector | 3.39W |

Fuente: Elaboración propia

Como se puede observar en los resultados obtenidos, tanto el dispositivo de interfaz sensorial, como el de control de actuadores son totalmente compatibles con el estándar 802.3af, por lo cual todos los dispositivos se pueden alimentar mediante un switch POE, a excepción de las cerraduras, es conveniente que cada una de ellas tenga su propia fuente

¹⁶<http://poe-texas.com/Calculator/>

de energía de 12V @ 3A, ya que de acuerdo a su hoja de datos [43] precisan de 3A para el arranque y 250mA para mantener el pistón en posición de puerta cerrada.

3.4.2. Base de datos del sistema de control de accesos

3.4.2.1. Forma normal 1 para la base de datos de accesos

Cuadro 24: Reducción a la Forma Normal 1 de la base de datos de accesos

(a) Tabla persona

| persona | grabado | puerta nombre | puerta estado inicial | puerta estado actual | puerta arduino control | puerta arduino pin | acceso fecha | acceso hora | acceso puerta | permiso fecha inicio | permiso fecha fin |
|---------|---------|---------------|-----------------------|----------------------|------------------------|--------------------|--------------|-------------|---------------|----------------------|-------------------|
| jdoe | true | oficina 1 | true | false | control 1 | 19 | 01-03-2017 | 14:05:00 | oficina 1 | 01-02-2017 | - |
| jdoe | true | oficina 2 | true | true | control 1 | 20 | 02-03-2017 | 15:20:00 | oficina 2 | 01-03-2017 | 03-03-2017 |
| jperez | false | - | - | - | - | - | - | - | - | - | - |

(b) Tabla arduino

| arduino | MAC | IP | control | usuario MQTT | clave MQTT | pines | comando | respuesta | comando fecha | conectado | topico | topico permiso |
|-----------|-------------------|---------------|---------|--------------|------------|----------|---------------|-----------------|---------------|-----------|--------|----------------|
| control 1 | aa:bb:cc:dd:ee:00 | 192.168.1.100 | true | ard0 | AF8W... | 19,20,21 | - | - | - | true | c/1 | suscripcion |
| oficina 1 | aa:bb:cc:dd:ee:01 | 192.168.1.101 | false | ard1 | EC22... | - | grabar huella | proceso exitoso | 03-02-2017 | true | p/1 | publicacion |
| oficina 1 | aa:bb:cc:dd:ee:01 | 192.168.1.101 | false | ard1 | EC22... | - | grabar huella | proceso exitoso | 03-02-2017 | true | r/2 | publicacion |
| oficina 1 | aa:bb:cc:dd:ee:01 | 192.168.1.101 | false | ard1 | EC22... | - | grabar huella | proceso exitoso | 03-02-2017 | true | c/2 | suscripcion |
| oficina 1 | aa:bb:cc:dd:ee:01 | 192.168.1.101 | false | ard1 | EC22... | - | grabar huella | proceso exitoso | 03-02-2017 | true | c/0 | suscripcion |
| oficina 2 | aa:bb:cc:dd:ee:02 | 192.168.1.102 | false | ard2 | 43AD... | - | grabar huella | proceso exitoso | 03-02-2017 | true | p/2 | publicacion |
| oficina 2 | aa:bb:cc:dd:ee:02 | 192.168.1.102 | false | ard2 | 43AD... | - | grabar huella | proceso exitoso | 03-02-2017 | true | r/3 | publicacion |
| oficina 2 | aa:bb:cc:dd:ee:02 | 192.168.1.102 | false | ard2 | 43AD... | - | grabar huella | proceso exitoso | 03-02-2017 | true | c/3 | suscripcion |
| oficina 2 | aa:bb:cc:dd:ee:02 | 192.168.1.102 | false | ard2 | 43AD... | - | grabar huella | proceso exitoso | 03-02-2017 | true | c/0 | suscripcion |

Fuente: Elaboración propia

3.4.2.2. Forma normal 2 para la base de datos de accesos

Cuadro 25: Reducción a la Forma Normal 2 de la base de datos de accesos

(a) Tabla persona

| id | nombre | grabado | puerta | acceso fecha | acceso hora | acceso puerta | permiso fecha inicio | permiso fecha fin |
|----|--------|---------|-----------|--------------|-------------|---------------|----------------------|-------------------|
| 1 | jdoe | true | oficina 1 | 01-03-2017 | 14:05:00 | oficina 1 | 01-02-2017 | - |
| 2 | jdoe | true | oficina 2 | 02-03-2017 | 15:20:00 | oficina 2 | 01-03-2017 | 03-03-2017 |
| 3 | jperez | false | - | - | - | - | - | - |

(b) Tabla puerta

| puerta | estado inicial | estado actual | arduino control | arduino pin | acceso |
|------------------|----------------|---------------|-----------------|-------------|--------|
| puerta oficina 1 | true | false | 1 | 19 | 1 |
| puerta oficina 2 | true | true | 1 | 20 | 2 |

(c) Tabla arduino

| id | detalle | MAC | IP | control | pines salida | puerta |
|----|-----------|-------------------|---------------|---------|--------------|------------------|
| 1 | control 1 | aa:bb:cc:dd:ee:00 | 192.168.1.100 | true | 19,20,21 | - |
| 2 | oficina 1 | aa:bb:cc:dd:ee:01 | 192.168.1.101 | false | - | puerta oficina 1 |
| 3 | oficina 2 | aa:bb:cc:dd:ee:02 | 192.168.1.102 | false | - | puerta oficina 2 |

(d) Tabla respuesta

| id | arduino | comando | resultado | fecha |
|----|---------|---------------|-----------------|------------|
| 1 | 2 | grabar huella | proceso exitoso | 03-02-2017 |
| 2 | 3 | grabar huella | proceso exitoso | 03-02-2017 |

(e) Tabla cliente_mqtt

| arduino | usuario MQTT | clave MQTT | conectado | admin | topico | topico permiso |
|---------|--------------|------------|-----------|-------|----------|----------------|
| 1 | ard0 | AF8W... | true | false | gpio/1/+ | suscripcion |
| 2 | ard1 | EC22... | true | false | p/1 | publicacion |
| 2 | ard1 | EC22... | true | false | r/2 | publicacion |
| 2 | ard1 | EC22... | true | false | c/2 | suscripcion |
| 2 | ard1 | EC22... | true | false | c/0 | suscripcion |
| 3 | ard2 | 43AD... | true | false | p/2 | publicacion |
| 3 | ard2 | 43AD... | true | false | r/3 | publicacion |
| 3 | ard2 | 43AD... | true | false | c/3 | suscripcion |
| 3 | ard2 | 43AD... | true | false | c/0 | suscripcion |

Fuente: Elaboración propia

3.4.2.3. Forma normal 3 para la base de datos de accesos

Cuadro 26: Reducción a la Forma Normal 3 de la base de datos de accesos

| (a) Tabla persona | | | | | | |
|-------------------|--------|---------|--|--|--|--|
| id | nombre | grabado | | | | |
| 1 | jdoe | true | | | | |
| 2 | jperez | false | | | | |

| (b) Tabla puerta | | | | | | |
|------------------|--------|------------------|----------------|---------------|-----------------|-------------|
| id | nombre | detalle | estado inicial | estado actual | arduino control | arduino pin |
| 1 | puel | puerta oficina 1 | true | false | 1 | 19 |
| 2 | pue2 | puerta oficina 2 | true | true | 1 | 20 |

| (c) Tabla acceso | | | |
|------------------|------------------------|---------|--------|
| id | fecha hora | persona | puerta |
| 1 | 01-03-2017 14:05:00 | 1 | 1 |
| 2 | 02-03-2017 15:20:00 | 1 | 2 |

| (d) Tabla permiso_acceso | | | | |
|--------------------------|---------|--------|--------------|------------|
| id | persona | puerta | fecha inicio | fecha fin |
| 1 | 1 | 1 | 01-02-2017 | - |
| 2 | 1 | 2 | 01-03-2017 | 03-03-2017 |

| (e) Tabla arduino | | | | | | |
|-------------------|-----------|-----------------------|-------------------|---------|--------------|--------|
| id | detalle | MAC | IP | control | pines salida | puerta |
| 1 | control 1 | aa:bb:cc: dd:ee:00 | 192.168. 1.100 | true | 19,20,21 | - |
| 2 | oficina 1 | aa:bb:cc: dd:ee:01 | 192.168. 1.101 | false | - | 1 |
| 3 | oficina 2 | aa:bb:cc: dd:ee:02 | 192.168. 1.102 | false | - | 2 |

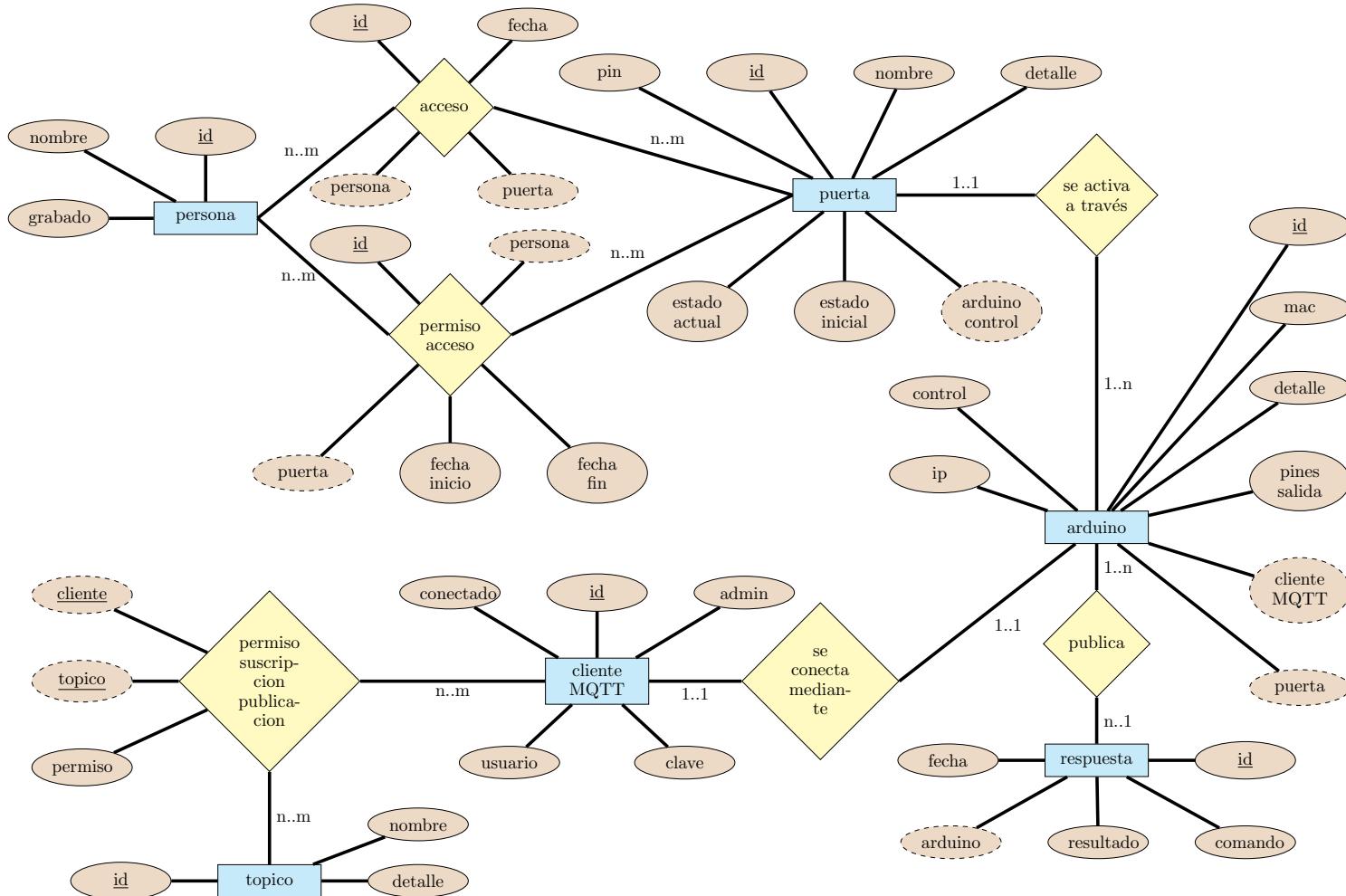
| (f) Tabla topico_permiso | | |
|--------------------------|--------|-------------|
| cliente MQTT | topico | permiso |
| 1 | 1 | suscripcion |
| 2 | 2 | publicacion |
| 2 | 3 | publicacion |
| 2 | 4 | suscripcion |
| 2 | 5 | suscripcion |
| 3 | 6 | publicacion |
| 3 | 7 | publicacion |
| 3 | 8 | suscripcion |
| 3 | 5 | suscripcion |

| (g) Tabla topico | | |
|------------------|----------|----------------------------|
| id | nombre | detalle |
| 1 | gpio/1/+ | Tópico de control 1 |
| 2 | p/1 | Tópico puerta 1 |
| 3 | r/2 | Tópico respuesta arduino 2 |
| 4 | c/2 | Tópico comandos arduino 2 |
| 5 | c/0 | Tópico comandos global |
| 6 | p/2 | Tópico puerta 2 |
| 7 | r/3 | Tópico respuesta arduino 3 |
| 8 | c/3 | Tópico comandos arduino 3 |

| (h) Tabla cliente_mqtt | | | | |
|------------------------|--------------|------------|-----------|-------|
| id | usuario MQTT | clave MQTT | conectado | admin |
| 1 | ard0 | AF8W... | true | false |
| 2 | ard1 | EC22... | true | false |
| 3 | ard2 | 43AD... | true | false |

Fuente: Elaboración propia

Figura 33: Diagrama entidad-relación para la base de datos de control de accesos

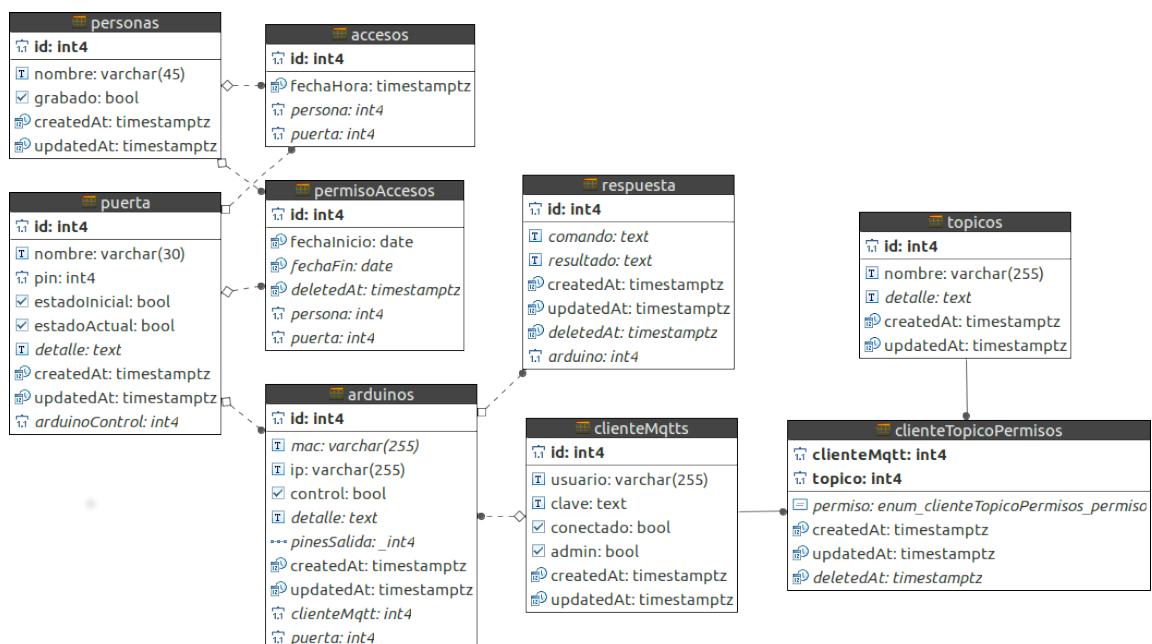


Fuente: Elaboración propia

Con la reducción de la Tabla 26 y la tabla de respuestas de la Tabla 25 se consiguió elaborar el diagrama entidad-relación mostrado en la Figura 33. Mediante el cual se desarollo la base de datos de la Figura 34.

Cabe resaltar que el micro-servicio de usuarios se encarga de sincronizar la tabla de *personas* con los datos del servidor LDAP, si se elimina algún usuario del servidor LDAP se eliminan en cascada los datos registrados con el ID del usuario eliminado. Este proceso de sincronización se ejecuta al inicio del sistema y periódicamente de acuerdo al tiempo establecido en las variables de entorno de ejecución, también se puede forzar este proceso mediante un botón en el sistema de administración web que ejecuta la sincronización manual.

Figura 34: Base de datos de control de accesos



Fuente: Elaboración propia

Esta base de datos está separada de la base de datos de huellas, ya que la base de datos de huellas se puede reutilizar para algún otro sistema que requiera de dichos datos, como por ejemplo un sistema de reloj marcador de hora de ingreso/salida.

La *lista de usuarios* es una copia exacta de la lista de usuarios de la base de datos de huellas, que a su vez se sincroniza con el servidor de LDAP.

La siguiente tabla es la de las *puertas*, ésta contiene los datos del nombre código de la puerta, el dispositivo de control y el pin donde se conecta la puerta, el estado lógico inicial y el estado actual que cambia cada vez que la puerta se abre o cierra.

La tabla de *accesos* es una relación entre el ID de una persona y el ID de una puerta conjuntamente con una fecha y hora en la que se produjo el acceso de una persona.

Los *permisos de acceso* son una relación entre el ID de una persona y el ID de una puerta donde se diferencian dos tipos de acceso, el indefinido que es un acceso permanente que solo contiene una fecha inicial desde la que la persona podrá acceder por una puerta o el acceso temporal que contiene también una fecha final que es la fecha límite en la cual dicha persona podrá acceder por una puerta.

La tabla *arduinoss* contiene tanto los dispositivos de control, como los dispositivos de interfaz sensorial, la diferencia la define el campo booleano control. Si es un dispositivo de control deberán definirse los pines de salida que estarán disponibles para la tabla *puertas*; mientras que si se trata de un dispositivo de interfaz sensorial debe relacionarse con una puerta ya que controlará el sensor de huellas mediante el cual se abrirá dicha puerta. Ambos tipos de dispositivos deberán relacionarse con un cliente MQTT para conectarse al servidor mediante un usuario y contraseña.

La tabla de *clientes MQTT* contiene el usuario y contraseña para los dispositivos del sistema, así como también contiene un usuario privilegiado que tendrá acceso al sistema servicio web de administración, que además podrá publicar o suscribirse en cualquier tópico del servidor MQTT.

La tabla *tópicos* contiene todos los tópicos a los cuales los clientes pueden suscribirse o publicar de acuerdo a los permisos definidos en la tabla que relaciona estos permisos.

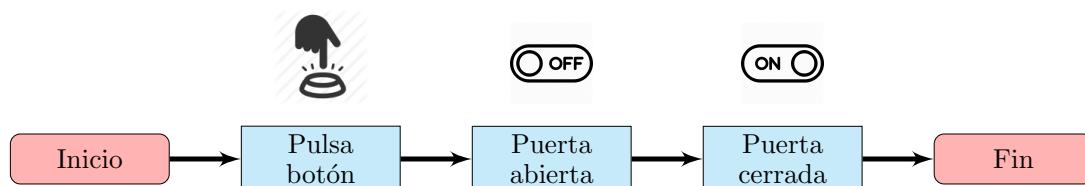
Por último la tabla de *respuestas* contiene un historial de todos los comandos del sistema, tanto los que se ejecutan en el servidor como las órdenes hacia los sensores, así como también las respuestas recibidas de cada sensor después de cada orden.

Cuando se registra un nuevo dispositivo de control se crea automáticamente, el tópico `gpio/:idArduino/+`, donde `idArduino` es reemplazado por el ID del arduino registrado.

Cuando se registra un dispositivo de interfaz sensorial se crean 3 tópicos automáticamente, `c/:idArduino` que sirve para enviar comandos únicamente a dicho arduino, `r/:idArduino` que sirve para que el arduino publique las respuestas que recibe del sensor de huellas, `p/:idPuerta` que sirve para que el arduino publique el ID de la persona que desea ingresar por dicha puerta. Un tópico adicional es creado cuando se registra el primer dispositivo de interfaz sensorial, `c/0` que sirve para enviar comandos a todos los arduinos conectados al sistema.

3.5. Secuencia de acción para la apertura desde el interior

Figura 35: Diagrama para la apertura de una puerta desde el interior



Fuente: Elaboración propia

De acuerdo al circuito de la figura 32 y la hoja de datos de la cerradura electromagnética [43], el pin de control de la cerradura va conectado a un pulsador normalmente abierto con el otro extremo se conecta a tierra; entonces cuando una persona presiona el botón pulsador el pin de control se conecta a tierra haciendo que el pistón de la cerradura se retrague y la puerta quede abierta por un tiempo, suficiente para que la persona pueda abrir

la puerta y salir. Este proceso se realiza enteramente en el lugar donde se halla instalada la cerradura, ya que el pulsador solo necesita conectarse a la misma tierra a la que se conecta la cerradura, por tanto ni el hardware, ni el software desarrollado intervienen en este proceso. Este sistema cuenta con dispositivos que garantizan una salida libre y sin demora, activada de forma manual¹⁷, estos dispositivos de salida requieren una operación de un solo movimiento ininterrumpido¹⁸, para que en casos de emergencia las personas que se encuentren dentro de uno de los ambientes que precisen de una salida, acudan a ésta sin ningún tipo de obstrucción, con la respectiva señalización¹⁹, ubicada a una altura adecuada²⁰ y sin ningún tipo de identificación a fin de poder salir con la mayor facilidad posible para llegar al punto de reunión más cercano.

Figura 36: Botón pulsador para la apertura desde el interior



Fuente: Pulsador de liberación de puerta, TodoElectrónica.com, España

Este dispositivo tiene la además posibilidad de conexión normalmente cerrada, por lo que podría adaptarse a las cerraduras magnéticas de contacto, mismas que no tienen el pin de control, por lo tanto en este caso se debe realizar un ajuste diferente para cortar la alimentación misma; es decir el pin de tierra haría de pin de control e iría conectado al pulsador y desde ahí hasta la placa de control central, logrando de ésta forma un funcionamiento similar al de las cerraduras de pistón.

¹⁷Portal de salida, Sección 6.1.6, Norma NFPA-731[30]

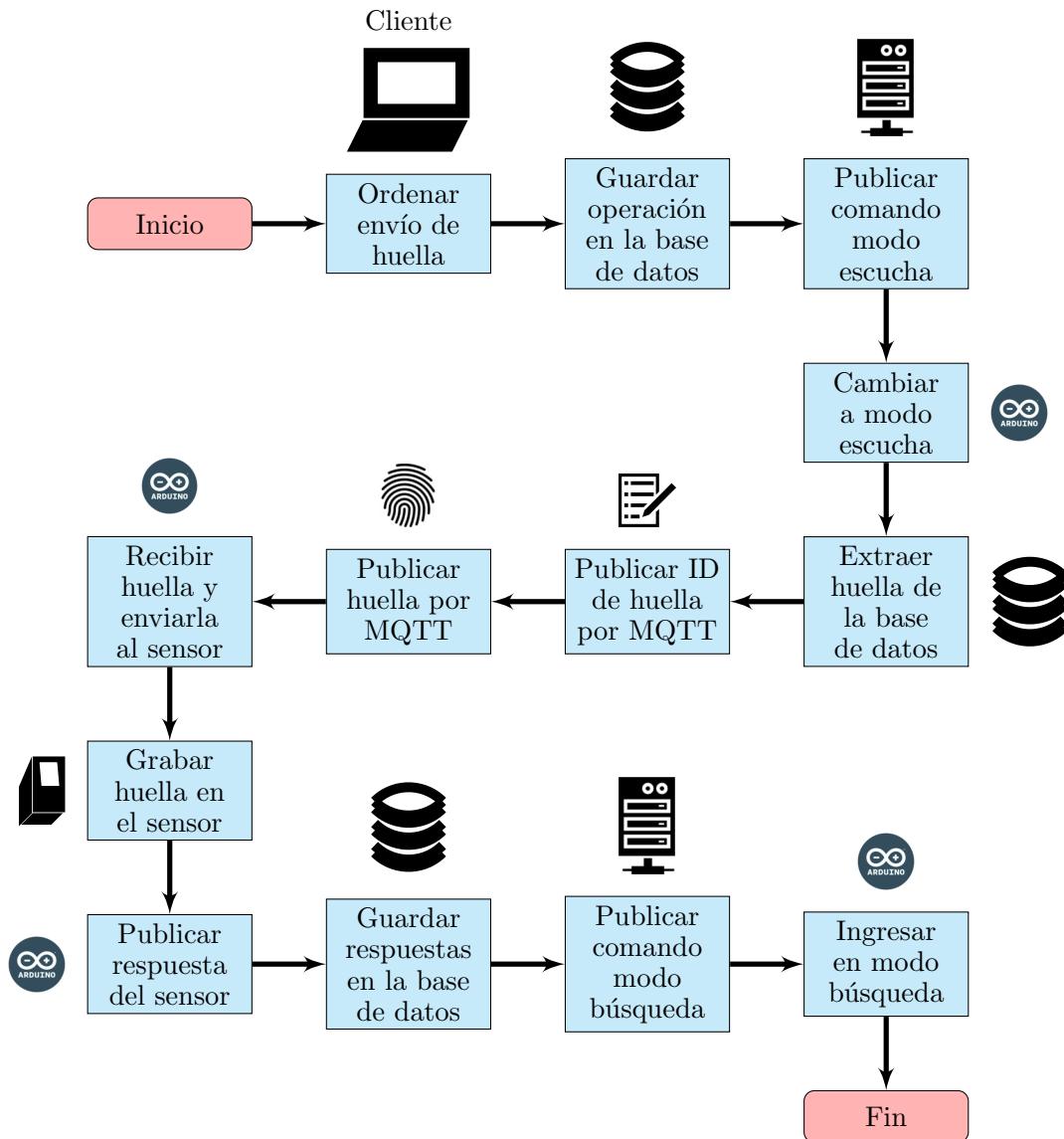
¹⁸Dispositivos de salida, Sección 7.2.9, Norma NFPA-730[29]

¹⁹Señales de salvamento y evacuación, Norma RM-849-14[27]

²⁰Ubicación, Sección 2.2, Norma NB-1220004[28]

3.6. Secuencia de acción para el envío de una nueva huella a los sensores

Figura 37: Diagrama para envío de huellas a los sensores



Fuente: Elaboración propia

Cuando el administrador del sistema inicia el proceso de envío de una huella hacia los sensores, el servidor MQTT publica un comando a los dispositivos de interfaz sensorial:

c/:idDispositivoSensor → :modo

El tópico *c* se utiliza para enviar comandos, el ID de dispositivo interfaz sensorial es el que identifica al dispositivo en la base de datos, o de otro modo 0 para enviar comandos a todos los dispositivos y el modo puede ser 0 para cambiar a *modo escucha*, con lo que los dispositivos de interfaz actuarán como un puente entre el servidor y los sensores, en este modo el servidor puede enviar directamente paquetes al lector de huellas, pero con la adición de dos bytes antes de la cabecera de cada paquete de acuerdo al manual del sensor [56]. Cuando se envía 1, el modo cambia a *modo búsqueda*, este es el modo predefinido para que los dispositivos busquen una huella en el sensor y envíen el ID de la persona al servidor.

Por ejemplo el paquete para realizar la operación de handshake en el sensor es el siguiente:

Cuadro 27: Instrucción de handshake para el sensor de huellas

| 2 bytes | 4 bytes | 1 byte | 2 bytes | 1 byte | 1 byte | 2 bytes |
|----------|---------------------|--------------------------|-------------------|-----------------------|-------------------|-------------------------|
| Cabecera | Dirección sensor | Identificador paquete | Tamaño paquete | Código instrucción | Código control | Suma de verificación |
| ef01H | ffffffffH | 01H | 0004H | 17H | 00H | 001cH |

Fuente: Manual Sensor ZFM-20, ZhianTec, V1.4, 2008 [56]

Para el cual la respuesta del sensor será:

Cuadro 28: Respuesta de handshake desde el sensor de huellas

| 2 bytes | 4 bytes | 1 byte | 2 bytes | 1 byte | 2 bytes |
|----------|---------------------|--------------------------|-------------------|-----------------------|-------------------------|
| Cabecera | Dirección sensor | Identificador paquete | Tamaño paquete | Código instrucción | Suma de verificación |
| ef01H | ffffffffH | 07H | 0003H | xxH | sumH |

Fuente: Manual Sensor ZFM-20, ZhianTec, V1.4, 2008 [56]

Mediante este comportamiento se puede observar que el tamaño total del paquete de respuesta del sensor es de 12 bytes (0cH) y que además el byte de respuesta se encuentra en la posición 9 (09H), con estos datos se desarrolló una librería para comunicarse con el sensor mediante el hardware de interfaz sensorial en *modo 0*.

Cuadro 29: Instrucción modificada de handshake para el sensor de huellas

| 1 byte | 1 byte | 2 bytes | 4 bytes | 1 byte | 2 bytes | 1 byte | 1 byte | 2 bytes |
|------------------|-------------------------|----------|------------------|-----------------------|----------------|--------------------|----------------|----------------------|
| Tamaño respuesta | Posición byte respuesta | Cabecera | Dirección sensor | Identificador paquete | Tamaño paquete | Código instrucción | Código control | Suma de verificación |
| 0cH | 09H | ef01H | ffffffffH | 01H | 0004H | 17H | 00H | 001cH |

Fuente: Elaboración propia

Donde el primer byte indica el tamaño de paquete de respuesta que debe esperar el dispositivo de interfaz sensorial y el siguiente byte indica la posición de donde se extraerá la respuesta para enviarla al servidor.

Entonces con este protocolo modificado el servidor publicará hacia el dispositivo cuya ID es igual a 1:

c/1 → 0c09ef01ffffffff0100041700001c

El dispositivo de interfaz sensorial 1 recibirá este paquete, extraerá los 2 primeros bytes para su uso y reenviará lo demás hacia el sensor de huellas. El sensor de huellas responderá de acuerdo a su estado y el dispositivo de interfaz sensorial publicará la respuesta recibida desde el sensor.

r/1 → 00

En caso de que el sensor se encuentre conectado y se halle funcionando este valor 00 indica que el “Proceso se realizó con éxito”. Esta respuesta literal será la que se envíe hasta el

servicio web para obtener en tiempo real todas las respuestas de los sensores conectados al sistema.

De este mismo modo es como se enviarán las huellas almacenadas en la base de datos hacia los sensores mediante la librería desarrollada para los sensores de huella dactilar ZFM-20.

Después de enviar todas las huellas a los sensores el servidor vuelve a poner los mismos en *modo búsqueda*. Cabe resaltar que durante el proceso de comunicación servidor-sensores, el sistema entrará en un estado de “Ocupado” en el cual no recibirá más órdenes hasta terminar todo el proceso.

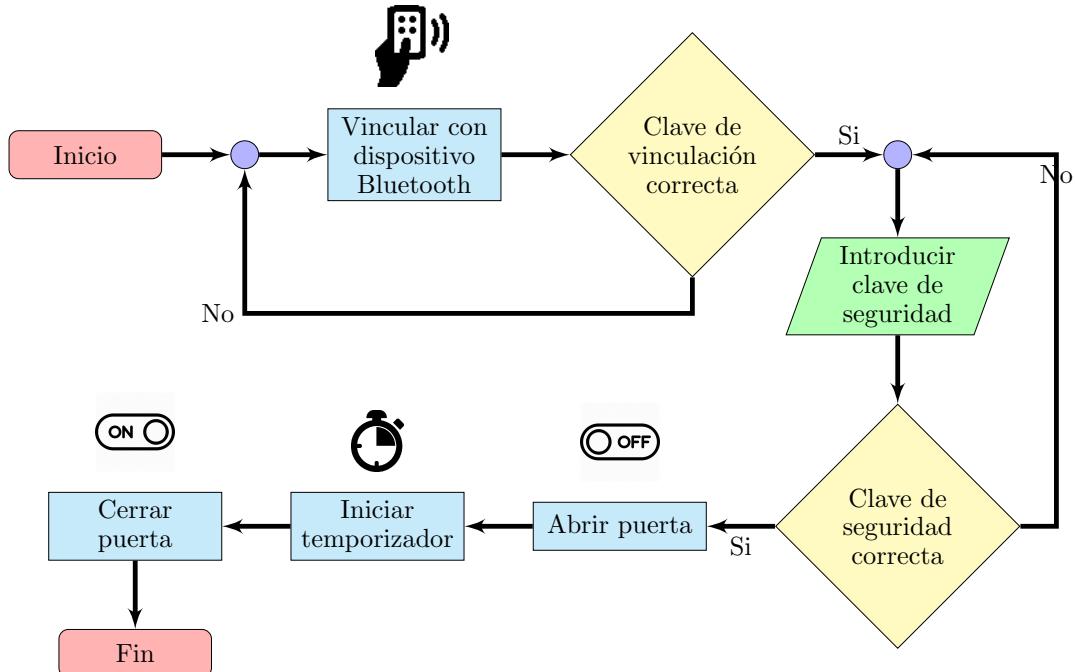
3.7. Secuencia de acción para la apertura mediante el respaldo bluetooth

Se ha desarrollado un circuito bluetooth con el microcontrolador ATtiny85 y el módulo bluetooth HC-06, en base al esquema de attiny85 arduino de www.arduino-projects4u.com. Se puede observar el esquema de este dispositivo en el Anexo 8.

En caso de que el servidor MQTT dejase de operar y fuera necesario el acceso físico hasta el servidor, este dispositivo se puede instalar en una de las puertas menos críticas para poder realizar los arreglos necesarios para volver a levantar el sistema. Este dispositivo deberá ser operado solo por una persona con un nivel mas alto que el administrador y deberá tener conocimientos del sistema para realizar el mantenimiento del mismo.

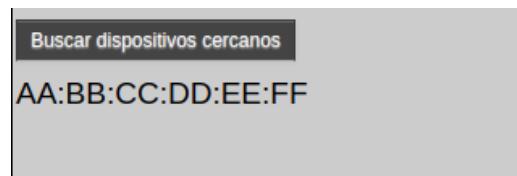
Este dispositivo tiene dos pasos de seguridad, el primero es una contraseña definida en el módulo HC-06 para la vinculación de un bluetooth en modo esclavo, el segundo paso es el envío de una contraseña mediante una aplicación Android para abrir una de las dos puertas que puede controlar el dispositivo.

Figura 38: Diagrama para apertura mediante respaldo bluetooth



Fuente: Elaboración propia

Figura 39: Pantalla de vinculación de la aplicación Android

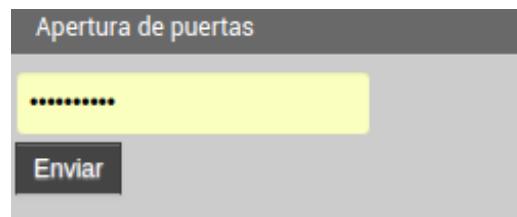


Fuente: Elaboración propia

Como medida de seguridad contra ataques de fuerza bruta, el dispositivo bluetooth tiene una restricción en el número de intentos que se puede realizar antes de entrar en un modo de reposo durante un tiempo definido. Por defecto se pedirá la contraseña tres veces, en caso de fallar todos los intentos el dispositivo no se encontrará disponible hasta dentro de 30 minutos. También hay un tiempo de espera entre cada intento que por defecto es de 3 segundos, antes de este tiempo no se podrá realizar otro intento de apertura. Estas

variables se pueden cambiar al momento de la programación del microcontrolador.

Figura 40: Pantalla de envío de contraseña de la aplicación Android

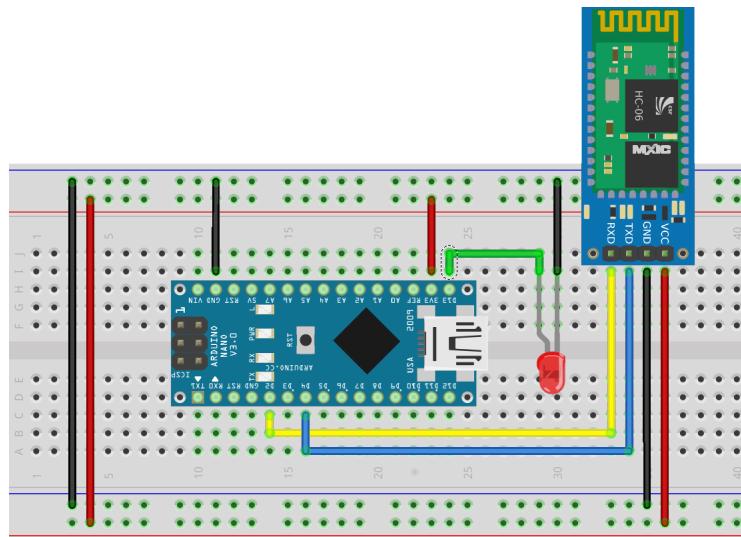


Fuente: Elaboración propia

Este dispositivo debe instalarse a menos de 10 metros de la puerta de ingreso para obtener una conexión fiable y evitar atenuación o interferencias en la comunicación al momento de enviar la contraseña de apertura.

La idea de este dispositivo fué adaptada del artículo “Encender un Led con Arduino y Arduino vía Bluetooth”, ElectronicaStore.Net, 15 de Marzo de 2016 [14].

Figura 41: Conexión del módulo bluetooth HC-05

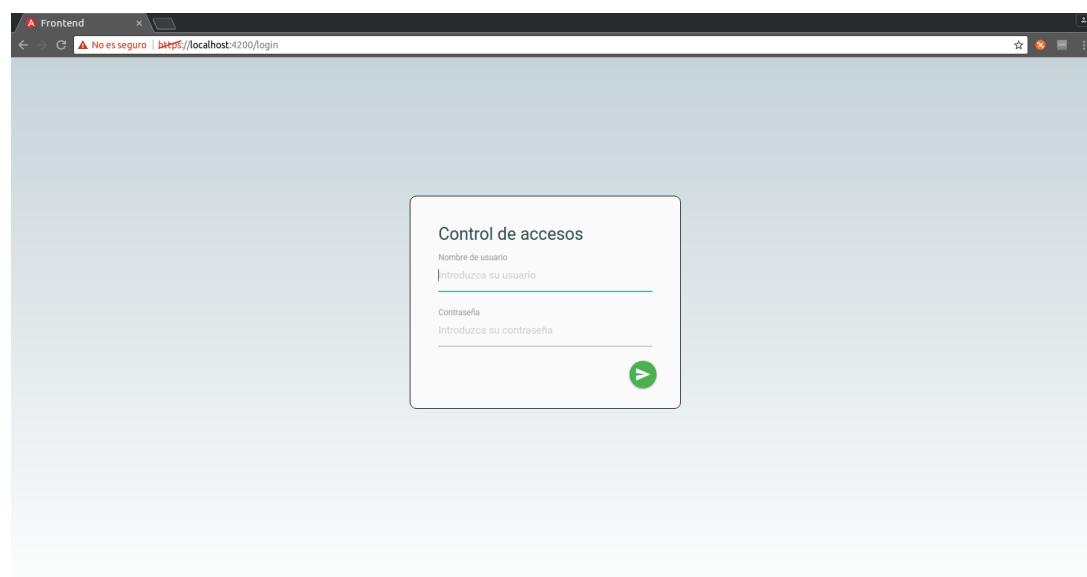


Fuente: Encender un Led con Arduino y Arduino vía Bluetooth, ElectronicaStore.Net, 15 de Marzo de 2016 [14].

3.8. Servicio web para la administración del sistema

Como se puede observar en la base de datos de la figura 34 existe un campo nombrado *admin*, los clientes que tengan habilitado este campo tendrán acceso al sistema web de administración.

Figura 42: Página de login del servicio web



Fuente: Elaboración propia

Una vez que se ingresa al sistema se observa una página con el estado de las puertas y un resumen de los últimos accesos ordenados por fecha de manera descendente, el estado de las puertas se identifica por un color rojo cuando se encuentran abiertas, además de un ícono con forma de candado abierto; cuando las puertas se cierran cambian a un color verde con el ícono de un candado cerrado. Tanto estos estados como la lista de últimos accesos cambia de forma dinámica en tiempo real para poder realizar el monitoreo por ejemplo desde una sala de seguridad o de control.

Figura 43: Página de monitoreo del servicio web

| User | Location | Date/Time |
|----------|-----------|-------------------|
| jdoe | Oficina 1 | Today at 10:50 AM |
| usuario1 | Oficina 1 | Today at 10:49 AM |
| jdoe | Oficina 1 | Today at 10:49 AM |
| jdoe | Sala 1 | Today at 10:45 AM |
| usuario4 | Sala 1 | Today at 10:45 AM |
| jdoe | Oficina 2 | Today at 10:44 AM |
| usuario3 | Oficina 2 | Today at 10:44 AM |
| jdoe | Oficina 1 | Today at 10:44 AM |

Fuente: Elaboración propia

Al extremo izquierdo se puede navegar por las diferentes páginas para administrar el sistema, la primera página es la lista de usuarios, en esta tenemos un botón en la parte superior **FORZAR SINCRONIZACIÓN** que actualiza la lista de usuarios sincronizando los valores con los almacenados en el servidor LDAP. Debajo está la tabla donde se halla el primer botón que sirve para grabar o actualizar las huellas de los usuarios, el segundo botón es el de enviar huella, este cambia de color naranja a verde cuando se ha realizado el envío de dicha huella a los sensores conectados al sistema, por último está el botón borrar huella que borra la huella elegida de los sensores. Cuando se pulsa **Grabar huella** y el proceso no se completa, o se presiona el botón **Borrar huella**, el color de **Enviar huella** cambia de verde a naranja.

Figura 44: Página de lista de usuarios del servicio web

| Persona | Grabar Huella | Enviar Huella | Borrar Huella |
|----------|---------------|---------------|---------------|
| jdoe | | | |
| usuario1 | | | |
| usuario2 | | | |
| usuario3 | | | |
| usuario4 | | | |
| usuario5 | | | |

Fuente: Elaboración propia

Si se hace clic sobre algún nombre de usuario de la tabla de la figura 44 se muestra la imagen de la huella del usuario seleccionado.

Figura 45: Página de imagen de la huella del servicio web



Fuente: Elaboración propia

La página de permisos de acceso contiene dos vistas, la de permisos indefinidos, es decir aquellos que no tienen una fecha final y que estarán habilitados hasta que se los deshabilite. En esta página se ve la lista de usuarios y las puertas por las cuales tiene acceso cada uno; en la primera fila de la tabla se pueden añadir nuevos accesos eligiendo un usuario que no se encuentre en la lista de abajo y haciendo clic en la puerta a la que se le desea dar acceso.

Figura 46: Página de permisos indefinidos del servicio web

| Usuario | Ingreso | Oficina 1 | Oficina 2 | Sala 1 |
|----------|--------------------------|--------------------------|-------------------------------------|-------------------------------------|
| jdoe | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| usuario1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| usuario2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| usuario3 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| usuario4 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Fuente: Elaboración propia

La otra vista es la de permisos temporales, son aquellos que tienen una fecha final en la cual el usuario podrá acceder por dicha puerta, en la primera fila se pueden crear nuevos permisos temporales eligiendo un usuario y una puerta, una fecha de inicio y una fecha final del permiso concedido, ambos son inclusivos, es decir que el usuario elegido podrá acceder desde las 00:00 horas de la fecha inicial hasta las 24:00 horas de la fecha final. En la tabla de abajo se tienen los permisos activos, estos se pueden modificar en ambas fechas y también se pueden eliminar con el botón X.

Figura 47: Página de permisos temporales del servicio web

The screenshot shows a web application window titled "Frontend". The address bar indicates a non-secure connection ("No es seguro"). The main content area has a header "Permisos Indefinidos" and "Permisos Temporales". On the left, a sidebar lists navigation options: Inicio, Lista de Usuarios, Permisos de Acceso, Clientes MQTT, Sensores, Puertas, Historial de accesos, and Salir. The "Permisos Temporales" section contains a table titled "Permisos de acceso temporal" with the following data:

| Usuario | Puerta | Desde | Hasta |
|----------|-----------|------------|------------|
| jdoe | Ingreso | 08/06/2017 | 10/06/2017 |
| usuario4 | Ingreso | 08/06/2017 | 10/06/2017 |
| usuario5 | Oficina 1 | 12/06/2017 | 13/06/2017 |

Each row includes a green "+" button to the right of the "Hasta" field and a red "X" button to the right of the "Hasta" field.

Fuente: Elaboración propia

La página de clientes MQTT alberga todos los clientes con los que los dispositivos de hardware se conectan al sistema, también tienen los clientes administradores que pueden suscribirse o publicar en cualquier tópico del servidor MQTT e ingresar al sistema web. Cabe resaltar que un usuario no puede conectarse múltiples veces al sistema, por lo cual si se desea tener un monitor del sistema por ejemplo en una televisión en un ambiente de seguridad como se realiza típicamente se deberá crear un usuario administrador diferente al usuario que se utiliza para realizar cambios, brindar permisos, etc.

Por otra parte cada usuario solo puede estar conectado en una instancia, lo cual brinda una capa más de seguridad al sistema ya que no se puede suplantar la identidad de un dispositivo si este ya se encuentra conectado.

Figura 48: Página de clientes MQTT del servicio web

The screenshot shows a web-based MQTT client management interface. On the left, there is a sidebar with the following navigation options: Inicio, Lista de Usuarios, Permisos de Acceso, Clientes MQTT (which is currently selected), Sensores, Puertas, Historial de accesos, and Salir. The main content area is titled "Clientes MQTT". It displays a table with five rows, each representing a registered client. The columns are "Usuario" (Username), "Contraseña" (Password), and "Administrador" (Administrator status). The data is as follows:

| Usuario | Contraseña | Administrador |
|---------|------------|---------------|
| admin | ✓ | ✗ |
| ard0 | ✗ | ✗ |
| ard1 | ✗ | ✗ |
| ard2 | ✗ | ✗ |
| ard3 | ✗ | ✗ |

A green circular button with a plus sign is located at the top right of the table, indicating the option to add new clients.

Fuente: Elaboración propia

La página de sensores tiene dos vistas, la primera es la de dispositivos de control, en esta se le asigna un nombre a cada dispositivo, la dirección IP, la dirección MAC, los pines de salida en caso de utilizar otro microcontrolador o utilizar más pines del mismo ATmega328P, por último se asigna un cliente MQTT a cada dispositivo para que pueda conectarse al sistema.

Una vez creado un dispositivo éste se mueve a la tabla inferior, donde se pueden actualizar sus datos, tomando en cuenta que la dirección IP y la dirección MAC deberán ser únicas; es decir, no se deben repetir, al igual que el cliente MQTT.

El sistema no permitirá la creación de un nuevo dispositivo si no se encuentra ningún cliente MQTT registrado.

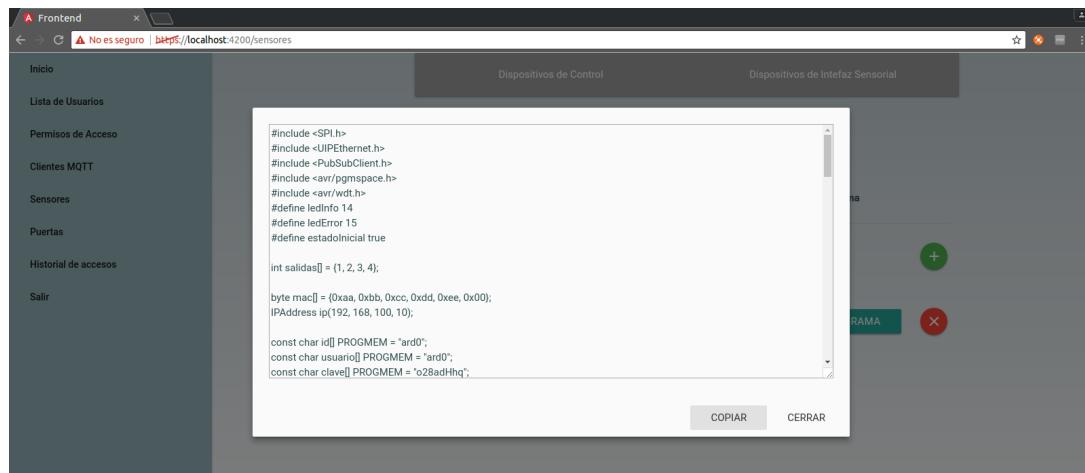
Figura 49: Página de dispositivos de control del servicio web



Fuente: Elaboración propia

En la vista que se muestra en la figura 49 se encuentra el botón **PROGRAMA** que al pulsarlo nos devuelve el código listo para grabar en el dispositivo de control mediante el software Arduino IDE, mismo que ya debe tener instaladas todas las librerías necesarias para grabar los dispositivos.

Figura 50: Página de programa de control del servicio web



Fuente: Elaboración propia

La vista de la página de dispositivos de interfaz sensorial tiene una lógica parecida, pero en lugar de los pines de salida el dispositivo se relaciona con una de las puertas registradas.

Figura 51: Página de dispositivos de interfaz sensorial del servicio web

The screenshot shows a web interface titled 'Dispositivos de interfaz sensorial'. On the left, there's a sidebar with links like 'Inicio', 'Lista de Usuarios', 'Permisos de Acceso', 'Clientes MQTT', 'Sensores', 'Puertas', 'Historial de accesos', and 'Salir'. The main area has tabs 'Dispositivos de Control' and 'Dispositivos de Interfaz Sensorial' (which is selected). Below these tabs, there's a table with columns: Dispositivo, IP, MAC, Puerta, Cliente MQTT, and Programa. Five rows of sensor data are listed:

- Sensor Ingreso: IP 192.168.100.11, MAC aa:bb:cc:dd:ee:ff, Puerta puein, Cliente MQTT ard0, with a green '+' button.
- Sensor Oficina: IP 192.168.100.12, MAC aa:bb:cc:dd:ee:ff, Puerta pueof1, Cliente MQTT ard1, with a blue 'PROGRAMA' button and a red 'X' button.
- Sensor Oficina: IP 192.168.100.13, MAC aa:bb:cc:dd:ee:ff, Puerta pueof2, Cliente MQTT ard2, with a blue 'PROGRAMA' button and a red 'X' button.
- Sensor Oficina: IP 192.168.100.14, MAC aa:bb:cc:dd:ee:ff, Puerta pueof3, Cliente MQTT ard3, with a blue 'PROGRAMA' button and a red 'X' button.
- Sensor Sala 1: IP 192.168.100.15, MAC aa:bb:cc:dd:ee:ff, Puerta puesal1, Cliente MQTT ard4, with a blue 'PROGRAMA' button and a red 'X' button.

Fuente: Elaboración propia

De igual forma al pulsar el botón **PROGRAMA** nos devuelve el código listo para grabar en el dispositivo de interfaz sensorial.

Figura 52: Página de programa de interfaz sensorial del servicio web

The screenshot shows a 'Programa' (Program) page. On the left, there's a sidebar with the same set of links as Figure 51. The main area has tabs 'Dispositivos de Control' and 'Dispositivos de Interfaz Sensorial'. A modal window is open, displaying C++ code for a sensor. The code includes #include directives for SPI.h, UIPEthernet.h, PubSubClient.h, pgmspace.h, and wdt.h, along with defines for ledInfo and ledError. It also defines a mac address and an IP address. Below the code, there are two buttons: 'COPIAR' (Copy) and 'CERRAR' (Close). At the bottom of the page, there's another row of sensor details: Sensor Sala 1, IP 192.168.100.14, MAC aa:bb:cc:dd:ee:ff, Puerta puesal1, Cliente MQTT ard4, with a blue 'PROGRAMA' button and a red 'X' button.

```

#include <SPI.h>
#include <UIPEthernet.h>
#include <PubSubClient.h>
#include <avr/pgmspace.h>
#include <avr/wdt.h>
#define ledInfo 14
#define ledError 15

byte mac[] = {0xaa, 0xbb, 0xcc, 0xdd, 0xee, 0x02};
IPAddress ip(192, 168, 100, 12);

const char [16] PROGMEM = "ard2";
const char usuario[16] PROGMEM = "ard2";
const char clave[16] PROGMEM = "4EX9HNB";
const char comandoParticular[16] PROGMEM = "c/3";
const char respuesta[16] PROGMEM = "r/3";
const char puerta[16] PROGMEM = "p/2";

```

Fuente: Elaboración propia

La página de puertas tiene los siguientes campos: un código único que identifica cada puerta, el detalle que es un nombre más legible para las personas, el estado inicial de la lógica de la puerta; es decir, si la puerta debe iniciar cerrada con un nivel alto en el pin de control este valor tendrá que ser establecido en nivel alto también.

El hardware de control es el dispositivo que controla la puerta, el sistema se ha dimensionado para que cada dispositivo de control pueda abrir o cerrar hasta seis puertas, esto debido a los pines disponibles en el microcontrolador.

Por último se define en cual de los pines del dispositivo de control irá conectado el pin de control de la puerta, este valor también es único ya que una sola puerta podrá ir conectada a cada pin definido en el hardware de control.

Figura 53: Página de puertas del servicio web

| Código | Detalle | Estado Inicial | Hardware de control | Pin de control |
|---------|-----------|----------------|---------------------|----------------|
| puein | Ingreso | Nivel Alto | Control central | 1 |
| pueofi1 | Oficina 1 | Nivel Alto | Control central | 2 |
| pueofi2 | Oficina 2 | Nivel Alto | Control central | 3 |
| puesal1 | Sala 1 | Nivel Alto | Control central | 4 |

Fuente: Elaboración propia

La página de historial de accesos contiene dos vistas, la primera muestra todos los accesos del día, pero tiene un campo de búsqueda donde se pueden revisar todos los accesos entre un rango de fechas.

Figura 54: Página de historial de accesos del servicio web

The screenshot shows a web browser window titled 'Frontend'. The address bar displays 'No es seguro | https://localhost:4200/historial'. The main content area has a header 'Historial de Accesos' and a sub-header 'Accesos'. Below this is a search bar with fields 'Desde' (08/06/2017) and 'Hasta' (08/06/2017), and a search button. A table lists access logs:

| Persona | Puerta | Fecha/Hora |
|----------|-----------|------------------------|
| jdoe | Sala 1 | June 8, 2017 - 10:45AM |
| usuario4 | Sala 1 | June 8, 2017 - 10:45AM |
| jdoe | Oficina 2 | June 8, 2017 - 10:44AM |
| usuario3 | Oficina 2 | June 8, 2017 - 10:44AM |
| jdoe | Oficina 1 | June 8, 2017 - 10:44AM |
| usuario1 | Oficina 1 | June 8, 2017 - 10:44AM |

Fuente: Elaboración propia

La vista de historial de respuestas alberga todos los comandos enviados hacia los sensores y las respuestas recibidas de los mismos de manera legible de acuerdo a los valores indicados en el manual del sensor ZFM-20 [56].

Figura 55: Página de historial de respuestas del servicio web

The screenshot shows a web browser window titled 'Frontend'. The address bar displays 'No es seguro | https://localhost:4200/historial'. The main content area has a header 'Historial de Resuestas' and a sub-header 'Respuestas'. Below this is a search bar with fields 'Desde' (08/06/2017) and 'Hasta' (08/06/2017), and a search button. A table lists response logs:

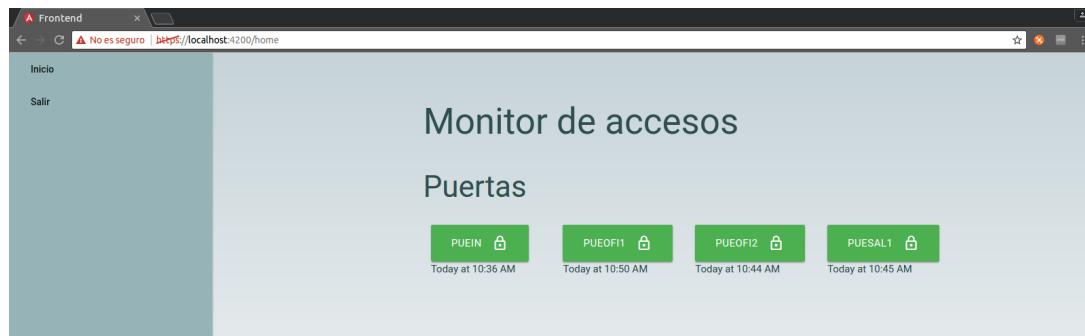
| Comando | Respuesta | Dispositivo | Fecha/Hora |
|-----------------------------|-----------|------------------|------------------------|
| Envio huella 1 | | | June 8, 2017 - 10:46AM |
| Proceso ejecutado con éxito | | Sensor Oficina 1 | June 8, 2017 - 10:48AM |
| Proceso ejecutado con éxito | | Sensor Oficina 2 | June 8, 2017 - 10:48AM |

Fuente: Elaboración propia

Cuando un usuario registrado en el servidor LDAP ingresa con su contraseña, puede acceder a una página donde solo se muestran las puertas por las que tiene acceso, para

que dicho usuario pueda abrir las puertas desde este mismo sistema web. Esto es muy útil en caso de que el sistema se instale por ejemplo en una oficina con una persona en recepción, para que esta persona desde su computadora pueda abrir las puertas a los visitantes o a las personas que no tengan registrada su huella y no tenga que colocar su dedo en sensor cada vez que deba abrir una puerta.

Figura 56: Página de usuario sin privilegios del servicio web



Fuente: Elaboración propia

Por último tanto para el usuario administrador como para el usuario sin privilegios, se tiene la opción **Salir**, que como indica cierra la sesión abierta del navegador y regresa a la pantalla de login. Por defecto las sesiones solo pueden durar abiertas 4 horas, después de ese tiempo la aplicación cerrará la sesión automáticamente y volverá a la pantalla de login, donde el usuario tendrá que introducir sus credenciales nuevamente. Esto es una medida de seguridad en caso de que la persona de recepción haya terminado su turno laboral y se retire dejando su computadora encendida y que otra persona intente abrir una puerta con la misma cuenta abierta de la persona que cometió el descuido.

Capítulo 4

Análisis y evaluación

En este capítulo se realiza una comparación de costos entre el sistema propuesto y uno de características similares que se puede encontrar en el mercado. Se realiza un análisis de vulnerabilidades observadas en el sistema desarrollado y los pasos a seguir para evitar ataques o fallas en el sistema. Por último se muestran los resultados de la instalación piloto ejecutada en la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.

4.1. Análisis de costos

Para poder justificar la reducción de costos, se realizó el análisis de costos de un sistema similar. Este análisis se estructuró en tres etapas: la instalación del controlador central, la instalación de los sensores en cada puerta y la instalación de las cerraduras de cada puerta.

Existe un sistema similar fabricado por la industria ZKSoftware, este tiene un controlador central que puede abastecer como máximo un número de 4 puertas, pero se le puede añadir módulos para incrementar el control de más puertas, módulos de Sensor de huellas, RFID o rostros. La ventaja de este sistema es que almacena hasta 3000 huellas, el sistema desarrollado solo puede almacenar hasta 1000 huellas, la desventaja es que solo tiene compatibilidad con los sensores, cerraduras, etc, de la misma marca. Cuenta con un servidor web que permite administrar fácilmente los permisos de acceso al igual que el sistema desarrollado. Otra desventaja de este sistema ZKSoftware es que todos los módulos de expansión de control de puertas deben estar conectados al controlador central, pero el sistema desarrollado solo necesita una conexión de red que comunique al servidor MQTT con los controladores sin importar la infraestructura que exista en medio.

4.1.1. Costo del dispositivo de control central

La tabla 30 muestra la comparación entre el sistema con más características similares que se puede encontrar en el mercado y el sistema propuesto en este proyecto.

Cuadro 30: Comparación de costos para el dispositivo de control

| Característica | Placa de control ZKSoftware | Placa de control desarrollada |
|---------------------------|---|--|
| Modelo | InBIO-460 | Placa de control POE |
| Cantidad de puertas | 6 | 6 |
| Cantidad de sensores | 6 | Puertos del switch POE Máximo 10000 |
| Accesorios necesarios | Expansión InBIO 260 | Módulo de relés Switch POE |
| Capacidad de huellas | 3000 | 1000 |
| CPU | 32bit @ 400Mhz | 8bit @ 16Mhz |
| Memoria RAM | 32MB | 2KB |
| Memoria Flash | 128MB | 32KB |
| Conexión con los sensores | RS485 | TCP/IP |
| Puertos de entrada | 4 Botón de salida 4 Sensor de puerta abierta 4 auxiliares +2 Botón de salida +2 Sensor de puerta abierta +2 auxiliares | 6 Pines de control de cerraduras |

Continua en la página siguiente

Cuadro 30 – Comparación de costos para el dispositivo de control (continuación)

| Característica | Placa de control ZKSoftware | Placa de control desarrollada |
|------------------------|--|--|
| Pines de salida | 4 Relés para cerraduras 4 Auxiliar +2 Relés para cerraduras +2 Auxiliar | 6 Relés para cerraduras |
| Indicador LED | LED de estado | LED de estado de energía LED de conexión con el servidor LED de conexión de red LED de transmisión de datos |
| Fuente de alimentación | DC 9.6V-14.4V | POE 802.3af - 48V |
| Dimensiones | 218mm x 106mm x 36mm | 94mm x 64mm x 17mm |
| Software | ZKAccess (Con licencia) | Código abierto |
| Costo del equipo | 527\$us | 40\$us |
| Costo de accesorios | 313\$us | 272\$us |
| Costo total | 840\$us | 312\$us |

Fuente: Elaboración propia

Los datos de los precios fueron adquiridos de las tiendas virtuales mercadolibre.com.co y www.tecbolivia.com.

4.1.2. Costo del dispositivo de interfaz sensorial

Se analizó el costo de instalación de un sensor en una sola puerta; para la comparación se tomó en cuenta un dispositivo que se pueda encontrar en el mercado y que sea compatible

con el controlador mostrado en la tabla 30.

Cuadro 31: Comparación de costos para el dispositivo interfaz sensorial

| Característica | Lector de huella ZKSoftware | Placa de interfaz desarrollada |
|-------------------------------|---|--|
| Modelo | FR-1500WP | Placa interfaz POE |
| Accesorios necesarios | Convertidor RS485 a RJ45 Cable ethernet cat. 5E de 100ft de longitud | Sensor de huellas Cable ethernet cat. 5E de 100ft de longitud |
| Protección | IP65 | Ninguna |
| Tipo de sensor | Óptico | Óptico |
| Fuente de alimentación | DC 12V | POE 802.3af - 48V |
| Dimensiones | 121.3mm x 77.3mm x 38mm | 94mm x 64mm x 17mm |
| Consumo en análisis de huella | 140mA | 100mA |
| CPU | 1GHz | 16MHz |
| Sensor | SilkID | ZFM-20 |
| LED | Indicador de tres colores | Indicador de lectura de huella |
| Compatibilidad | Paneles InBIO Paneles InBIO Pro | Código abierto |
| Costo del equipo | 310\$us | 40\$us |
| Costo de accesorios | 56\$us | 66\$us |
| Costo total | 366\$us | 106\$us |

Fuente: Elaboración propia

4.1.3. Costo de la cerradura de cada puerta

Este paso de la instalación fue analizado tomando en cuenta una sola cerradura, la comparación se realizó entre una cerradura compatible con el sistema hallado en el mercado y una compatible con el sistema propuesto en este proyecto.

Cuadro 32: Comparación de costos para la cerradura magnética

| Característica | Cerradura magnética ZKSoftware | Cerradura magnética Syscom |
|------------------------|--|--|
| Modelo | YB700B | YB300 |
| Accesorios necesarios | Botón pulsador ABK800A Cable ethernet categoría 5-E de 100ft de longitud | Botón pulsador Saxxon RB03 Cable ethernet categoría 5-E de 100ft de longitud |
| Tiempo de retardo | 0/3/6/9s | 0/3/6/9s |
| Fuente de alimentación | 12-24V | 12-24V |
| Consumo de corriente | 12V/900mA 12V/120mA 24V/730mA 24V/80mA | 12V/900mA 12V/130mA 24V/730mA 24V/90mA |
| Dimensiones | 205mm x 35mm x 41mm | 205mm x 35mm x 41mm |
| Diámetro pestillo | 16mm | 16mm |
| Peso | 0.7Kg | 0.7Kg |
| Fuerza de sujeción | 1000Kg | 1000Kg |
| Señal de salida | NC/COM | NC/COM |
| Nº operaciones | 500000 | 500000 |
| Costo del equipo | 87\$us | 54\$us |
| Costo de accesorios | 25\$us | 23\$us |
| Costo total | 112\$us | 77\$us |

Fuente: Elaboración propia

4.2. Análisis de vulnerabilidades

El sistema desarrollado cumple con los siguientes estándares de la Norma Boliviana NB-1220004[28]:

- Señales táctiles en los pulsadores de salida al interior de cada puerta, secciones 2.1.2.2(pp. 30) y 5.4(pp. 161)
- Ubicación de señales visuales, sección 2.2 (pp. 31)
- Características de las puertas corredizas y de vaivén, sección 3.4 (pp. 148)

La caja metálica donde se halla el control central del sistema cumple con los siguientes estándares de la Norma Boliviana RM-849-14[27]:

- Cuenta con señales de advertencia de peligro por electrocución, sección 2.1.4(pp. 16)
- El camino a las puertas está marcado con señales de evacuación, sección 2.1.5(pp. 20-21)

El sistema también cumple los estándares de la norma internacional NFPA-730[29]:

- Los ambientes cumplen con la definición de “Área Controlada”, secciones 3.3.5.1(pp. 9) y 8.2.1 (pp. 41)
- Las cerraduras son de tipo electrónicas, secciones 7.2.1 (pp. 29) y 7.2.3(pp. 30-31)

- Las puertas corredizas tienen protección antibandálica y no se pueden remover fácilmente para extraerlas de sus rieles, secciones 7.3.6.5 (pp. 34) y 7.3.6.6 (pp. 34)
- El sistema desarrollado cumple con la definición de “Sistema de Control de Acceso” de tipo Portal-Múltiple, secciones 8.13.1 (pp. 44-45) y 8.13.1.2 (pp. 45)
- La identificación se realiza mediante Verificación de Huellas Dactilares y se habilitan mediante sensores biométricos con la posibilidad de definir permisos con fechas definidas de inicio y fin, secciones 8.13.3 (pp. 47) y 8.13.3.1 (pp. 47)
- Cuenta con la posibilidad de instalar una o más Estaciones Monitoras, sección A3.3.35 (pp. 106)

El sistema es respaldado mediante un sistema de video-vigilancia que captura en video de manera ininterrumpida todos los ingresos y salidas de personas del centro de datos. La energía es suministrada al sistema mediante una UPS de respaldo en caso de fallas en la red eléctrica durante el tiempo necesario en el cual se activa un generador a diésel como se especifica en la Norma Internacional NFPA-731 en el capítulo 6 (pp. 21-23), pero se dejó de lado la encriptación de datos que requiere un hardware especializado cuya definición se encuentra en la sección 6.3 (pp. 23) de la misma norma. [30]

Por de ello este sistema no garantiza el nivel de seguridad en la capa SSL a través de TLS del estándar ISO/IEC PRF 20922¹ ya que los dispositivos desarrollados tan solo conllevan la seguridad de conexión mediante credenciales de usuario/contraseña, por lo cual el sistema es vulnerable ante ataques de interceptación con algún software como Wireshark mediante el cual se puede monitorear la red para observar cada paquete que se intercambia de un host a otro utilizando una tarjeta de red conectada físicamente a la misma red en modo promiscuo. Con este método se pueden ver en claro los usuarios y contraseñas de los dispositivos al momento de la conexión al servidor MQTT ya que éste

¹Message Queuing Telemetry Transport v3.1.1

levanta el servicio en el puerto 1883 y no en el puerto 8883. Para evitar este problema es recomendable aislar físicamente la red donde se encuentran conectados los dispositivos y de esta manera evitar la intrusión de atacantes.

Otra de las vulnerabilidades que se puede hallar en este y en cualquier sistema electrónico de seguridad se produce con una falla en la energía, este sistema no puede estar desprovisto de energía ya que las cerraduras magnéticas se liberan y las puertas se abren, quedando desprotegida el área donde se instaló el sistema. Para evitar este problema se recomienda aislar la energía eléctrica de este sistema, conectando todos los dispositivos a un respaldo de energía UPS; si las áreas que se van a resguardar son de alta criticidad además se tendrá que instalar un generador eléctrico alternativo o bien alimentar a la UPS con un banco de baterías.

Las bases de datos desarrolladas para este sistema tienen un grado de protección contra inyección SQL, pero aún así se recomienda configurar el servidor para que solo algunas direcciones IP tengan acceso a las dos bases de datos y cambiar el puerto de escucha por defecto al momento de la instalación.

Los sensores de huellas dactilares ZFM-20 vienen por defecto con una dirección hexadecimal de 4bytes *ffffffffH*, el manual de instalación del sistema tiene la posibilidad de cambiar esta dirección. Se recomienda cambiar la dirección de cada sensor antes de instalarlo en el sistema ya que una persona con el conocimiento del flujo y los protocolos de comunicación podría retirar un sensor y conectar un dispositivo que emule el funcionamiento del mismo, con lo cual podría realizar ataques de fuerza bruta para abrir alguna puerta del sistema. Para evitar este tipo de ataque se recomienda también instalar un respaldo en cuanto a la seguridad en los ambientes como cámaras que apunten o enfoquen a los lugares donde se hallan los sensores para tener una respuesta temprana en caso de actividad sospechosa. Cabe mencionar que el sistema desarrollado es compatible con otros sistemas de seguridad, ya que los esquemáticos son también hardware libre y están disponibles para realizar adaptaciones; por ejemplo con un sistema

de detección de gases o elementos nocivos en el aire, se puede lograr abrir las puertas en caso de emergencia con sólo un programa que publique el mensaje de apertura de cada puerta en los tópicos correspondientes del servidor MQTT.

En cuanto a los permisos de acceso temporal, éstos se brindan únicamente definiendo dos fechas, una inicial y la otra final, no se toma en cuenta una hora en ninguno de los dos datos, por lo cual las personas con permiso de acceso temporal podrán ingresar a los ambientes desde las 00:00 horas de la fecha inicial hasta las 24:00 horas de la fecha final. Aún así, dada la naturaleza del software libre, éste algoritmo es posible a cambios y adaptaciones para cada caso particular donde se necesite otro tipo de discriminación para los accesos temporales.

Para el sistema web se seleccionó el método de sesiones mediante tokens en formato JSON ya que este formato es compatible con dispositivos móviles como tablets o smartphones, pero se incluyó la encriptación de los tokens en el lado del servidor y se eliminó la información crítica como las contraseñas o los ID de usuario evitando de esta manera el ataque mediante la desencriptación por fuerza bruta de los tokens. Pero el problema que se genera en cualquier sistema web se debe también a motivos de descuido humano, ya que no se puede controlar el hecho de que algunas personas dejen sus cuentas abiertas o anoten sus credenciales de forma física en hojas de papel, entonces mediante este tipo de descuidos un atacante podría acceder al sistema con las credenciales de otra persona y abrir las puertas por las cuales tiene acceso la persona que descuidó sus credenciales. Las personas con acceso al sistema deberán capacitarse de manera periódica a fin de evitar este tipo de descuidos.

4.3. Resultados de la prueba piloto

Por razones de seguridad no se proporcionan detalles a profundidad de los ambientes o los datos utilizados en la prueba piloto, pero se pueden mencionar los aspectos generales de

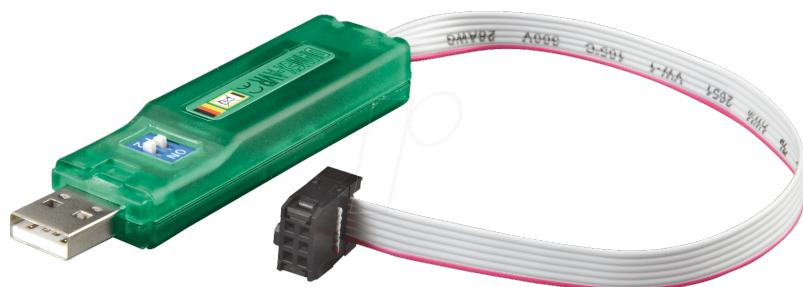
los resultados de dicha prueba para demostrar la reducción del costo en caso de instalar un sistema similar que se puede encontrar en el mercado.

El sistema fue implantado en todos los ambientes del centro de datos de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia, cada puerta cuenta con un dispositivo interfaz sensorial, un sensor de huellas ZFM-20, una cerradura magnética, un botón pulsador en el interior de cada ambiente, donde todas las conexiones se realizaron con cable UTP Categoría 5-E.

Cada dispositivo es alimentado mediante POE a través de un switch al cual también se conecta un dispositivo de control central que abastece para el número de puertas necesarias del sistema. Cada uno de los dispositivos fue grabado con el programa que genera el mismo sistema, por lo cual cada dispositivo tiene un usuario definido y una contraseña aleatoria. Cuando el administrador decide actualizar el sistema o cambiar uno de los dispositivos las contraseñas vuelven a generarse siempre de manera aleatoria de forma automática.

El método para grabar los programas en los dispositivos es mediante la conexión ISP disponible en la placa del circuito desarrollado. El administrador del sistema debe registrar un nuevo dispositivo para que el sistema habilite la opción de generar el programa a ser grabado. Para este proceso es necesario un dispositivo adaptador USB-ISP como el que se muestra en la figura 57.

Figura 57: Programador USB-ISP



Fuente: Tienda virtual Reichelt Electronik, Alemania, 2017

Las dos bases de datos, el servidor MQTT y la API de administración se hallan en un servidor aislado de la red al cual se accede solo desde equipos con una dirección MAC e IP específicas mediante reglas de un enrutador que comunica dos redes.

En la misma red del cliente que tiene acceso al servicio web de administración se conecta el dispositivo registrador de huellas para que éste pueda subir los datos de las huellas registradas a la base de datos sólo cuando el administrador conecta el equipo y prepara la grabación de una nueva huella.

Los materiales utilizados y el costo de instalación del sistema se muestran en la tabla 33. En esta tabla no se contemplan los trabajos de remodelación necesarios en la infraestructura como el de picar las paredes para insertar los ductos, los materiales de construcción para arreglar los desperfectos necesarios para la instalación como estuco o cemento, ni tampoco los materiales necesarios para recubrir y enmascarar la instalación como la pintura o el cemento adhesivo.

Cuadro 33: Materiales y presupuesto utilizados en la instalación piloto

| Tipo | Categoría | Recurso | Descripción | Cantidad | Monto \$us |
|----------------------|-----------------|-------------|---|-----------|------------|
| Recursos disponibles | Infraestructura | Equipo | Servidor broker MQTT | 1 equipo | |
| | | Equipo | Servidor de base de datos | 1 equipo | |
| | | Material | Alicates, desarmadores, estación de soldar, taladro, cierra mecánica, etc | 1 pieza | |
| Recursos necesarios | Materiales | Electrónico | Ethernet Cat. 5-E | 3 cajas | 423 |
| | | Material | Switch POE de 24 puertos | 1 equipo | 280 |
| | | Eléctrico | Cable 4 hilos para teléfono | 2 cajas | 58 |
| | | Eléctrico | Disyuntor | 1 pieza | 10 |
| | | Eléctrico | Borneras y fusibles | 15 piezas | 20 |
| | | Eléctrico | Chapas magnéticas 12V | 5 piezas | 270 |
| | | Eléctrico | Fuentes de 12V | 5 piezas | 100 |
| | | Eléctrico | Fuente de 5V | 1 piezas | 20 |
| | | Electrónico | Dispositivo interfaz sensorial | 5 piezas | 530 |
| | | Electrónico | Dispositivo control central | 1 piezas | 104 |
| | | Electrónico | Pulsador interno de pared | 5 piezas | 35 |

Continua en la página siguiente

Cuadro 33 – Materiales y presupuesto utilizados en la instalación piloto (continuación)

| Tipo | Categoría | Recurso | Descripción | Cantidad | Monto \$us |
|---------------------------|-----------|-------------|--|------------|-------------|
| | | Electrónico | Patch panel de 24 puertos | 1 pieza | 26 |
| | | Material | Tubos conduit, cable-ductos, tubos PVC | 90 metros | 100 |
| | | Material | Gabinete empotrable IP65 con cerradura | 1 pieza | 86 |
| | | Material | Termocontraibles, conectores, cables jumper hembra-hembra, cables jumper hembra-macho, cables jumper macho-macho, conectores RJ45 | 4 metros | 65 |
| | | Material | Tornillos y tuercas | 100 piezas | 20 |
| Costo total (\$us) | | | | | 2147 |

Fuente: Elaboración propia

Realizando una comparación de costos con las tablas 30, 31 y 32 se obtiene el resultado de que un sistema de la misma escala llegaría a tener un precio de aproximadamente 3230\$us, a diferencia del sistema propuesto que tuvo un costo de 2147\$us, con lo que se obtuvo una reducción del 33.5 % del costo en la instalación del sistema en los cinco ambientes para la prueba piloto.

Pero no debemos olvidar que no se tomaron en cuenta los recursos que la entidad ya tenía disponibles como por ejemplo los servidores o las herramientas para la instalación.

Este proceso fue realizado con la aprobación del Director Ejecutivo de ADSIB, Sylvain Damien Lesage, quien verificó el correcto funcionamiento del sistema al finalizar la instalación, realizó las pruebas correspondientes y calificó la instalación como favorable para la seguridad del centro de datos de dicha entidad.

La aprobación del Director Ejecutivo de ADSIB se remitió por escrito a mi persona como se puede observar en el Anexo 2.

Capítulo 5

Conclusiones y recomendaciones

En este capítulo se muestran las conclusiones obtenidas del desarrollo y la instalación del sistema propuesto y las recomendaciones para poder realizar un mejor uso del sistema y evitar fallas o ataques.

5.1. Conclusiones

- Mediante un estudio anterior a la instalación del sistema se seleccionó el medio de transmisión, el hardware y el software para el desarrollo del sistema, posteriormente se realizó el estudio del sistema instalado con lo que se pudo verificar que la instalación del prototipo añadió mejoras al control de accesos al centro de datos, como se puede observar en las Figuras 10 y 19.
- Para almacenar los datos de todas las personas y los recursos necesarios para el funcionamiento del sistema, además del registro histórico de la apertura de puertas, se han desarrollado dos bases de datos como se puede observar en la Figuras 34 y 25.
- Se ha desarrollado un prototipo de hardware que funciona como control central de puertas y como dispositivo de interfaz sensorial; la diferencia entre estos dispositivos es el software generado por el sistema web para cada uno de los dispositivos registrados en el sistema, como se muestra en el Anexo 3.
- Como respaldo de apertura de puertas, se ha desarrollado un dispositivo que funciona mediante conexión Bluetooth con una aplicación para Android, este dispositivo puede controlar la apertura de hasta dos puertas y es independiente del sistema principal para evitar la falla simultánea de ambos sistemas, como se muestra en el Anexo 8.

- Se han elaborado las secuencias o flujos que muestran cada acción que realiza el sistema de control de accesos para la apertura mediante sensor biométrico, pulsador al interior de cada puerta, respaldo bluetooth y también mediante el sistema web, como se muestra en las figuras 20, 27, 35, 37y 38.
- Se ha desarrollado un sistema web que cuenta con las funciones especificadas por ADSIB previas al desarrollo, entre ellas, registrar o actualizar huellas, registrar nuevos dispositivos y obtener la programas para los mismos, monitorear los accesos y obtener los registros históricos, abrir las puertas mediante botones en una pagina web, como se muestra en las Figuras 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56.
- Se ha instalado el prototipo del sistema en el centro de datos de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia. Los resultados de la instalación fueron satisfactorios y aprobados por el Director Ejecutivo de ADSIB de acuerdo al Anexo 2.

Por tanto habiendo cumplido los objetivos establecidos en este proyecto se ha concluido el desarrollo de un Sistema de Control de Accesos Mediante Sensor Biométrico de Huellas Dactilares y se ha demostrado su funcionamiento mediante la instalación del mismo en el Centro de datos de la Agencia Para el Desarrollo de la Sociedad de la Información en Bolivia.

5.2. Recomendaciones

- Realizar una actualización constante de todos los componentes del sistema a fin de evitar la obsolescencia por la actualización de las librerías externas de las cuales depende cada módulo del sistema que se puede hallar en el Anexo 1.

- Se recomienda desarrollar un circuito intermedio entre el servidor MQTT y cada dispositivo cliente para poder cifrar/descifrar los datos y realizar la transmisión de datos con el servidor MQTT a través de una capa segura SSL con el uso de TLS.
- Es recomendado que después de cada actualización en el desarrollo de este proyecto, aquellas entidades o personas que utilizan este sistema de control de accesos, migren sus datos a las nuevas versiones y mantengan actualizados sus sistemas en producción.
- Se recomienda tomar en cuenta el análisis de vulnerabilidades realizado en la sección 4.2 para evitar accesos no autorizados o corrupción del sistema o las bases de datos.

Referencias

- [1] Alvez, Carlos Eduardo; Benedetto, M. G. E. G. R. L. L. J. L. C. R. F. M. A. B. G. L. L. S. R. (2014). Identificación de personas mediante sistemas biométricos. estudio de factibilidad y su implementación en organismos estatales. *Suplemento Ciencia, Docencia y Tecnología*, 4(4):71. Recuperado el 10 de Enero de 2017 desde <http://www.pcient.uner.edu.ar/index.php/Scdyt/article/download/7/18>.
- [2] Atmel (2010). *Manual Atmel XMEGA USART*. Atmel.
- [3] Atmel (2013). *Datasheet Atmel ATtiny85*. Atmel. Recuperado el 28 de Mayo de 2017 desde http://www.atmel.com/images/atmel-2586-avr-8-bit-microcontroller-attiny25-attiny45-attiny85_datasheet.pdf.
- [4] Atmel (2015). *Datasheet Atmel ATmega328P*. Atmel. Recuperado el 27 de Mayo de 2017 desde <http://www.mouser.com/ds/2/268/atmel-8271-8-bit-avr-microcontroller-atmega48a-48p-1065900.pdf>.
- [5] Banzi, M. and Shiloh, M. (2014). *Getting Started with Arduino*. Maker Media, Inc.
- [6] Bustos, S. R. (2016). Introducción a umanick y sus soluciones. Recuperado el 10 de Julio de 2017 desde <http://slideplayer.es/slide/10260150/>.
- [7] Butrón, J. P. (2012). Autenticación biométrica por huella dactilar en estadios. Tesis de licenciatura, Universidad del Aconcagua.
- [8] Carlos, S. (2008). Principio de identidad criminalística libre 3.5. Recuperado el 4 de Mayo de 2017 desde <http://principiodeidentidad.blogspot.com/2008/01/biografia-de-juan-vucetich.html>.
- [9] Carrasco, M. J. Z. (2012). Sistema de alarma para mejorar la seguridad de la empresa auplatec ubicada en el canton pelileo. Tesis de licenciatura, Universidad Técnica de Ambato.

- [10] Craig I. Watson, Michael D. Garris, E. T. C. L. W. R. M. M. S. J. K. K. (2004). *User's Guide to NIST Biometric Image Software*. National Institute of Standard and Technology, 100 Bureau Dr, Gaithersburg, MD 20899, Estados Unidos.
- [11] Cruz, A. R. (2009). Clasificación de huellas digitales mediante minucias. resreport, Instituto Nacional de Astrofísica, Óptica y Electrónica. Recuperado el 12 de Marzo de 2017 desde http://ccc.inaoep.mx/~esucar/Clases-mgp/Proyectos/reporte_modelos_huellas.pdf.
- [12] de Carvajal Hedrich, E. M. (2016). *100 Proyectos de Robótica con Bitbloq y Arduino (Spanish Edition)*. Ernesto Martínez de Carvajal Hedrich.
- [13] Eduardo, B. C. L. (2006). Verificación de identidad de personas mediante sistemas biométricos para el control de acceso a una universidad. Tesis de maestría, Pontificia Universidad Católica del Perú.
- [14] ElectronicaStore.Net (2016). Encender un led con android y arduino vía bluetooth. Recuperado el 12 de Julio de 2017 desde <https://electronicastore.net/encender-un-led-con-android-y-arduino-via-bluetooth/>.
- [15] Evans, D. (2011). Internet de las cosas. Informe técnico, Cisco. Recuperado el 9 de Julio de 2017 desde http://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf.
- [16] Fierer Noah, Lauber Christian L., Z. N. M. D. C. E. K. K. R. (2010). Forensic identification using skin bacterial communities. *PNAS*, 107(14). Recuperado el 1 de Febrero de 2017 desde <http://www.pnas.org/content/107/14/6477.full?tab=author-info>.
- [17] Integrated, M. (2003). Determining clock accuracy requirements for uart communications. resreport 2141, Maxim Integrated. Recuperado el 15 de Mayo de 2017 desde <http://pdfserv.maximintegrated.com/en/an/AN2141.pdf>.

- [18] Janet Johanna Cirineo Huamani, M. A. V. Y. (2012). Diseño de un sistema de identificación biométrico según el lector de iris para cajeros automáticos del banco bbva. Tesis de licenciatura, Universidad Tecnológica del Perú.
- [19] Jorge Eduardo Velasquez Valencia, A. A. L. J. (2013). Soluciones inteligentes para el control de acceso físico mediante el uso de tecnología biométrica. Tesis de licenciatura, Universidad Tecnológica de Pereira.
- [20] la Rocha Diaz Jorge, D. (2000). Portal de seguridad para control de acceso a recintos y/o areas de alta seguridad. Tesis de licenciatura, Universidad Mayor de San Andrés.
- [21] LITE-ON. *Datasheet Optoacoplador Lite-On LTV-817*. LITE-ON. Recuperado el 20 de Mayo de 2017 desde <http://henrysbench.capnfatz.com/wp-content/uploads/2015/05/817C-Optocoupler-Datasheet.pdf>.
- [22] Luzmila Pró, Juan Carlos Gonzáles, W. C. C. Y. (2009). Tecnologías biométricas aplicadas a la seguridad en las organizaciones. *Revista de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos*, 6(2):66. Recuperado el 11 de Enero de 2017 desde http://sisbib.unmsm.edu.pe/BibVirtual/Publicaciones/risi/2009_n2/v6n2/a07v6n2.pdf.
- [23] Mandell, D. (2014). Connecting the internet of things: Interoperability depends on protocols. Recuperado el 6 de Marzo de 2017 desde <http://www.vdcresearch.com/News-events/iot-blog/2014/connecting-the-internet-of-things-interoperability-depends-on-protocols.html>.
- [24] Marwedel, P. (2010). *Embedded System Design*. Springer-Verlag GmbH.
- [25] Microbot (2015). *Datasheet Microbot Relay Module 2-Channel*. Microbot. Recuperado el 29 de Mayo de 2017 desde http://www.microbot.it/documents/mr009-004_datasheet.pdf.

- [26] MICROCHIP (2004). *Datasheet ENC28J60 Stand-Alone Ethernet Controller with SPI Interface*. MICROCHIP. Recuperado el 25 de Mayo de 2017 desde <http://ww1.microchip.com/downloads/en/DeviceDoc/39662c.pdf>.
- [27] Ministerio de Trabajo, E. y. P. S. (2014). *Norma de Señalización de Seguridad, Salud en el Trabajo y Emergencias de Defensa Civil*. Ministerio de Trabajo, Empleo y Previsión Social.
- [28] MOPSV, V. (2015). *Accesibilidad de las Personas con Discapacidad al Medio Físico*. Ministerio de Obras Públicas, Servicios y Vivienda, Viceministerio de Vivienda y Urbanismo.
- [29] NFPA (2006a). *NFPA 730 Guide for Premises Security*. National Fire Protection Association.
- [30] NFPA (2006b). *NFPA 731 Standard for the Installation of Electronic Premises*. National Fire Protection Association.
- [31] Noble, J. (2009). *Programming Interactivity: A Designer's Guide to Processing, Arduino, and Openframeworks*. O'Reilly Media.
- [32] of Investigation, F. B. (1997). *WSQ Gray-Scale Fingerprint Image Compression Specification*. Criminal Justice Information Services, 935 Pennsylvania Avenue, N.W., Washington, D.C, 3 edition.
- [33] of Investigation, F. B. (1999). *Electronic Fingerprint Transmission Specification*. Criminal Justice Information Services, 935 Pennsylvania Avenue, N.W., Washington, D.C, 7 edition.
- [34] Olimex (2010). *Datasheet Olimex HC-06*. Olimex, 2.0 edition. Recuperado el 30 de Mayo de 2017 desde <https://www.olimex.com/Products/Components/RF/BLUETOOTH-SERIAL-HC-06/resources/hc06.pdf>.

- [35] Olimex (2015). *Datasheet Olimex Ethercard ENC28J60*. Olimex. Recuperado el 20 de Mayo de 2017 desde <https://www.olimex.com/Products/Modules/Ethernet/MOD-ENC28J60/resources/MOD-ENC28J60.pdf>.
- [36] Oxer, J. and Blemings, H. (2011). *Practical Arduino*. Apress.
- [37] Pulse (2007). *Datasheet Pulse POE Trasformer EP10*. Pulse. Recuperado el 24 de Mayo de 2017 desde <http://html.alldatasheet.com/html-pdf/536082/PULSE/PA1260NL/151/1/PA1260NL.html>.
- [38] Pérez Porto Julián, G. A. (2008). Definición del concepto de seguridad. Recuperado el 18 de Marzo de 2017 desde <http://definicion.de/seguridad/>.
- [39] Ricardo, J. E. G. (2007). Estudio de factibilidad para el control de acceso biométrico en una empresa empleando lectores de huella digital. Tesis de maestría, Universidad de la Salle, Bogotá D.C.
- [40] Sigüenza, J. A. and Mateos, M. T. (2004). *Tecnologías biométricas aplicadas a la Seguridad*. Ra-Ma Editorial, S.A.
- [41] SONGLE. *Datasheet Songle Relay 5V*. SONGLE. Recuperado el 29 de Mayo de 2017 desde <http://henrysbench.capnfatz.com/wp-content/uploads/2015/05/Songle-SRD-Relay-Datasheet.pdf>.
- [42] Technology, L. (2015). *Datasheet Linear Technology LTC4267-3*. Linear Technology, 7 edition. Recuperado el 22 de Mayo de 2017 desde <http://cds.linear.com/docs/en/datasheet/42673fb.pdf>.
- [43] TESA (2008). *Catálogo TESA Cerraduras Electromecánicas*. TESA. Recuperado el 3 de Junio de 2017 desde <http://www.tesa.es/Other/Tesa/PDF/Mec%C3%A1nica%20Nacional/TESA%20dispositivos%20electromecanicos.pdf>.
- [44] Tomasi, W. (2003). *Sistemas de Comunicaciones Electrónicas*. Prentice Hall, 4 edition.

- [45] TP-LINK (2012). *Datasheet PoE Splitter TL-POE10R*. TP-LINK. Recuperado el 3 de Mayo de 2017 desde http://static.tp-link.com/resources/document/TL-POE10R_V4_Datasheet_ES.pdf.
- [46] Werner, S. (2011). Aplicación de nuevas tecnologías al sistema electoral – biometría y voto electrónico. Recuperado el 10 de Julio de 2017 desde <http://www.monografias.com/trabajos82/biometria-y-voto-electronico/biometria-y-voto-electronico.shtml>.
- [47] Wikipedia (2007). Tiempo de ejecución. Recuperado el 9 de Julio de 2017 desde https://es.wikipedia.org/wiki/Tiempo_de_ejecucion.
- [48] Wikipedia (2010a). Reconocimiento de iris. Recuperado el 17 de Marzo de 2017 desde https://es.wikipedia.org/wiki/Reconocimiento_de_iris.
- [49] Wikipedia (2010b). Sensor de huella digital. Recuperado el 17 de Marzo de 2017 desde https://es.wikipedia.org/wiki/Sensor_de_huella_digital.
- [50] Wikipedia (2012). Sistema de reconocimiento facial. Recuperado el 17 de Marzo de 2017 desde https://es.wikipedia.org/wiki/Sistema_de_reconocimiento_facial.
- [51] Wikipedia (2015a). Base de datos. Recuperado el 10 de Julio de 2017 desde https://es.wikipedia.org/wiki/Base_de_datos.
- [52] Wikipedia (2015b). Huella dactilar. Recuperado el 19 de Marzo de 2017 desde https://es.wikipedia.org/wiki/Huella_dactilar.
- [53] Wikipedia (2016a). Mqtt. Recuperado el 10 de Julio de 2017 desde <https://en.wikipedia.org/wiki/MQTT>.
- [54] Wikipedia (2016b). Seguridad. Recuperado el 18 de Marzo de 2017 desde <https://es.wikipedia.org/wiki/Seguridad>.

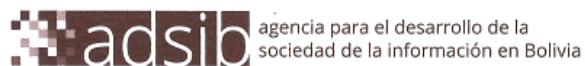
- [55] Zen, C. (2013). Biometría - huella digital. Recuperado el 7 de Mayo de 2017 desde <http://www.codigodebarras.pe/biometria-huella-digital-tecnologias/>.
- [56] ZhianTec (2008). *ZFM-20 Series Fingerprint Identification Module User Manual*. ZhianTec, 1.4 edition.
- [57] ZKSoftware. *Datasheet ZKSoftware placa controladora de accesos de 4 puertas*. ZKSoftware, 2017 edition. Recuperado el 1 de Junio de 2017 desde <http://www.zksoftware.com.ar/brochures/inbio-460.pdf>.
- [58] ZKSoftware (2017a). *Datasheet ZKSoftware botón pulsador para solicitud de salida ZK-ABK800A*. ZKSoftware. Recuperado el 4 de Junio de 2017 desde http://www.zksoftware.com.ar/brochures/zk_abk800a.pdf.
- [59] ZKSoftware (2017b). *Datasheet ZKSoftware cerradura eléctrica ZK-YB300*. ZKSoftware. Recuperado el 5 de Junio de 2017 desde <http://www.zksoftware.com.ar/brochures/zk-yb300.pdf>.
- [60] ZKSoftware (2017c). *Datasheet ZKSoftware lector de huella esclavo con sensor de huella SilkID*. ZKSoftware. Recuperado el 5 de Junio de 2017 desde <http://www.zksoftware.com.ar/brochures/zk-fr1500.pdf>.
- [61] ZKSoftware (2017d). *Datasheet ZKSoftware placa controladora para el control de accesos de 2 puertas*. ZKSoftware. Recuperado el 1 de Junio de 2017 desde <http://www.zksoftware.com.ar/brochures/inbio-260.pdf>.

Anexos

Anexo 1. Repositorios de los proyectos desarrollados para el sistema de control de accesos en Github

- Backend de administración del sistema:
github.com/djimenezjerez/control_accesos_backend
- Frontend de administración del sistema:
github.com/djimenezjerez/control_accesos_frontend
- Hardware registrador:
github.com/djimenezjerez/control_accesos_registrador
- Hardware de interfaz sensorial y control de puertas:
github.com/djimenezjerez/control_accesos_hardware

Anexo 2. Documento de conclusión de instalación piloto en ADSIB



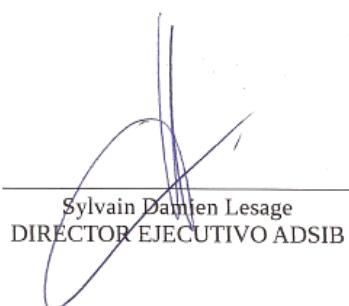
La Paz, 13 de Junio de 2017

A quien corresponda

REF.: CONCLUSIÓN DE LA INSTALACIÓN DEL SISTEMA DE SEGURIDAD DE CONTROL DE ACCESOS EN EL CENTRO DE DATOS DE ADSIB

Por medio de la presente hago saber que la instalación del Sistema de Seguridad de Control de Accesos Mediante Sensor Biométrico de Huellas Dactilares en el Centro de Datos de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia desarrollado por el proyectista Daniel Jimenez Jerez para la carrera de Ingeniería Electrónica de la Universidad Mayor de San Andrés, ha concluido satisfactoriamente y cumple con las expectativas deseadas.

Sin más que informar, me despido atentamente:

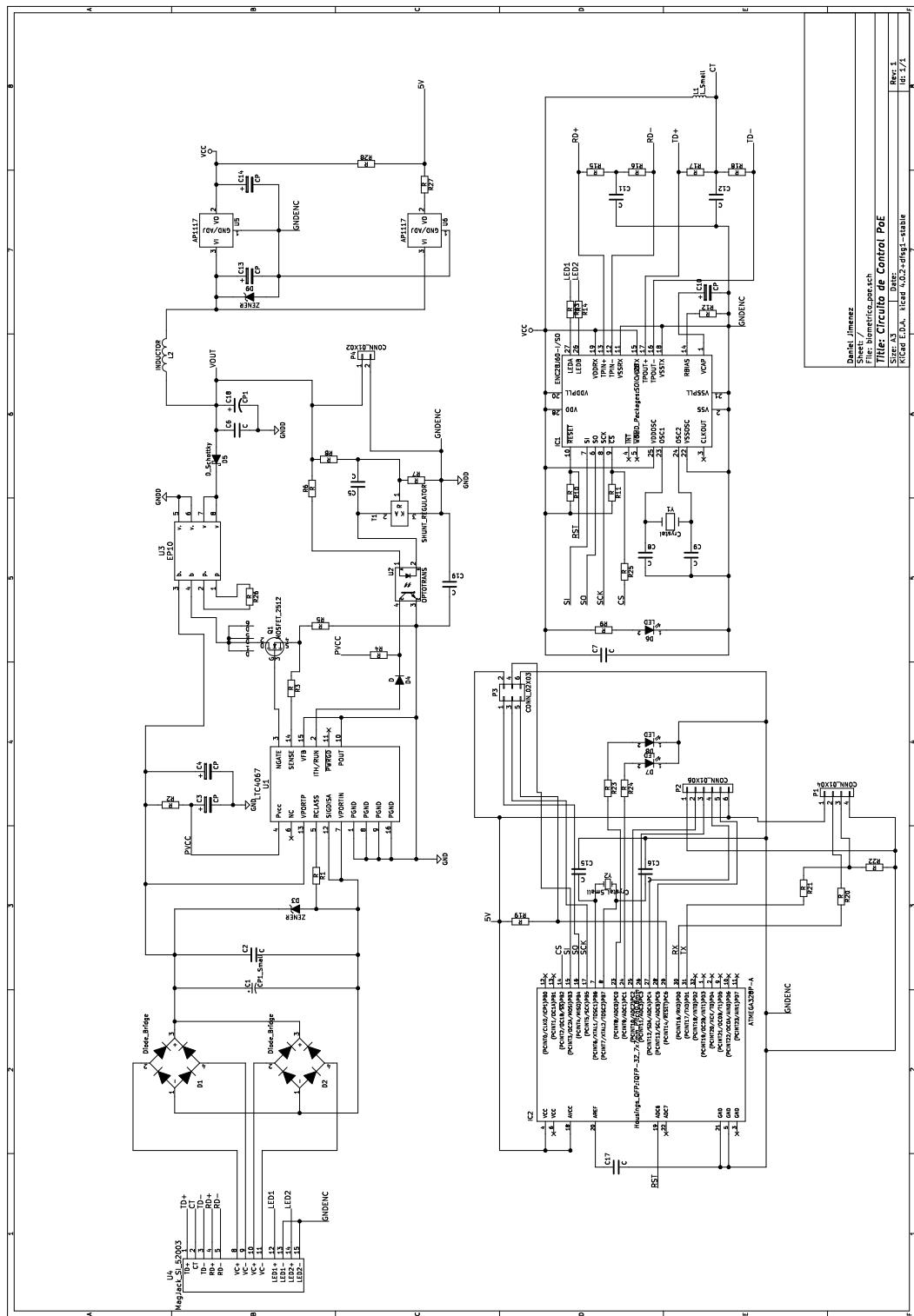


The image shows a handwritten signature in blue ink. Below the signature, there is a typed name and title.

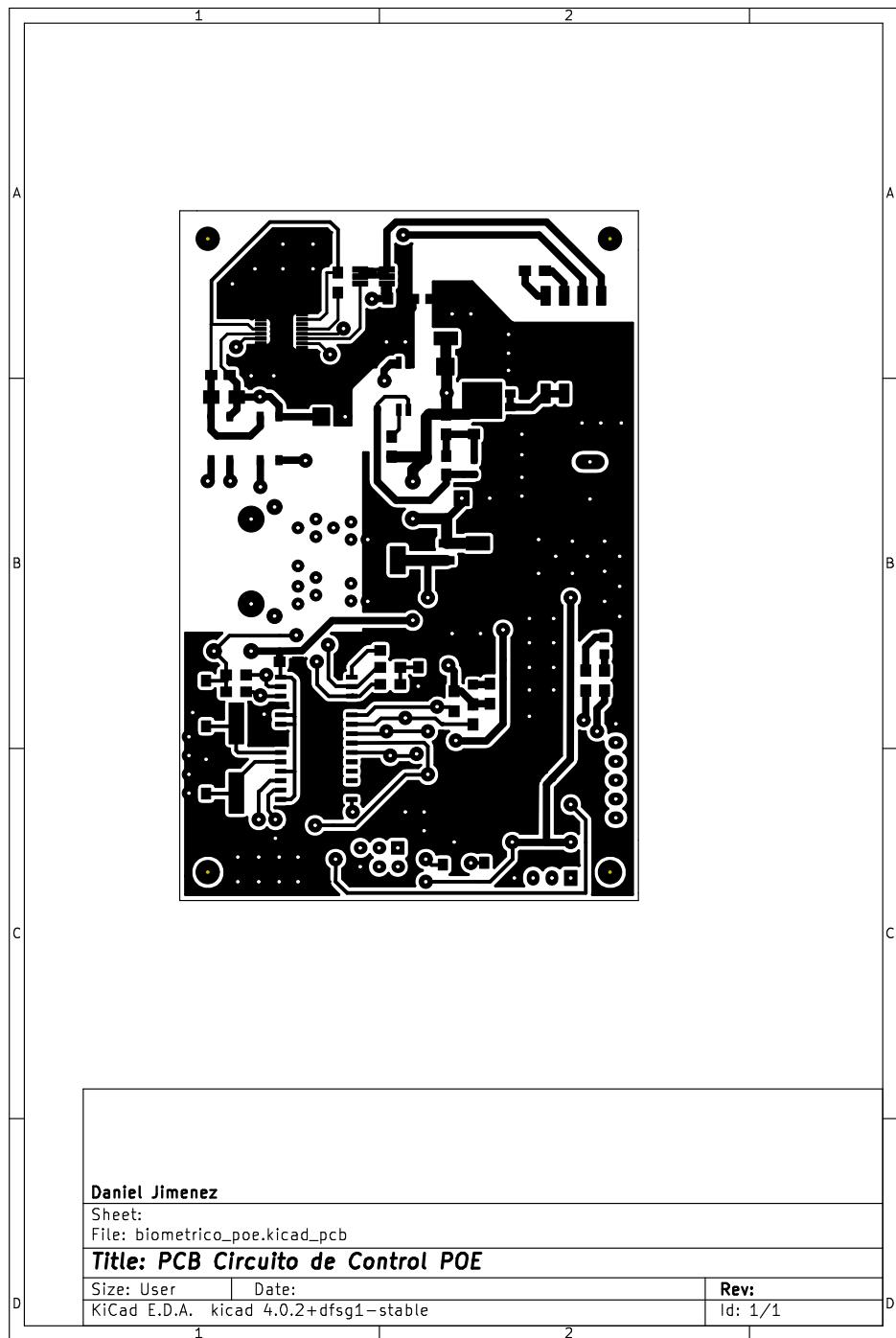
Sylvain Damien Lesage
DIRECTOR EJECUTIVO ADSIB



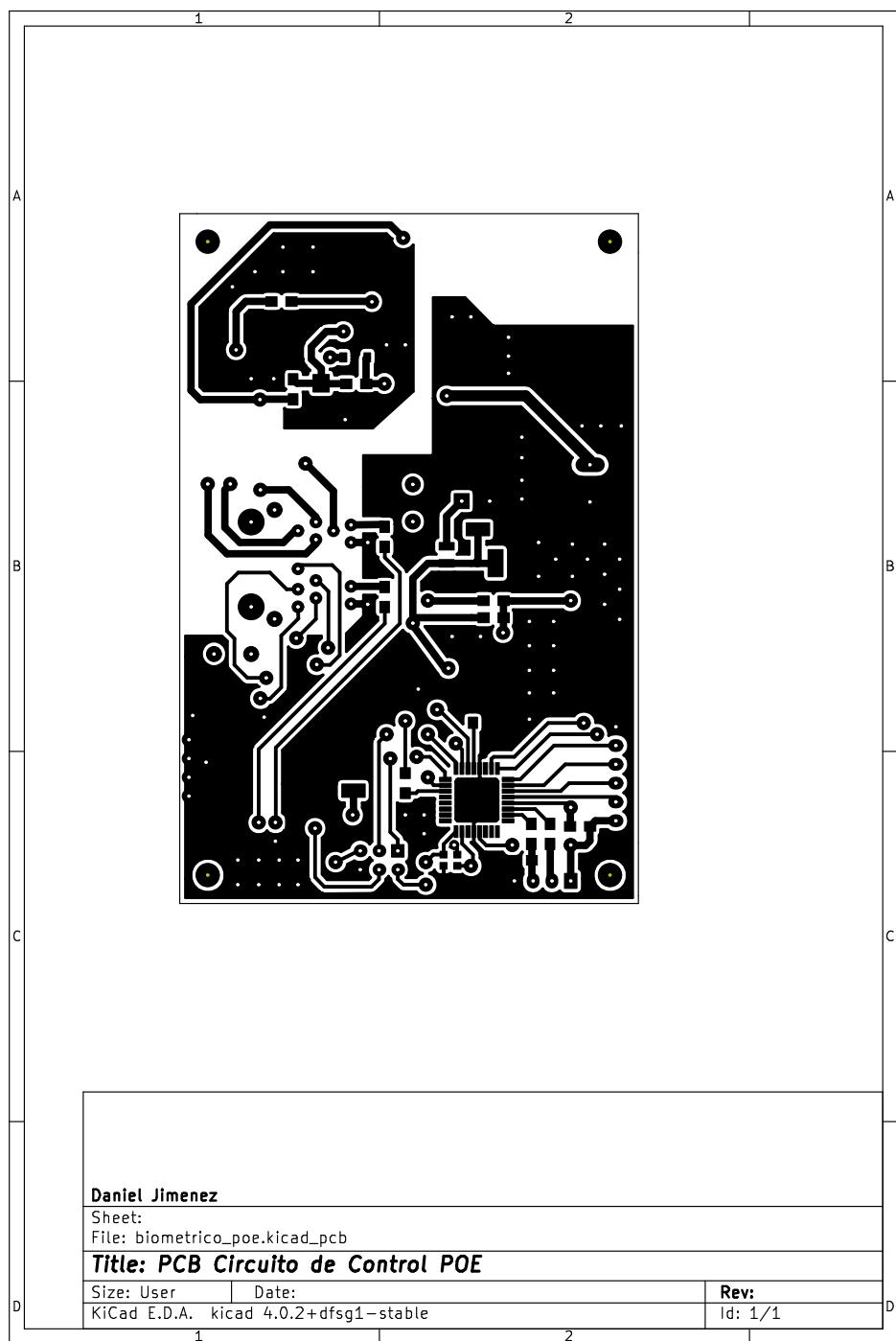
Anexo 3. Esquemático de la placa de interfaz sensorial



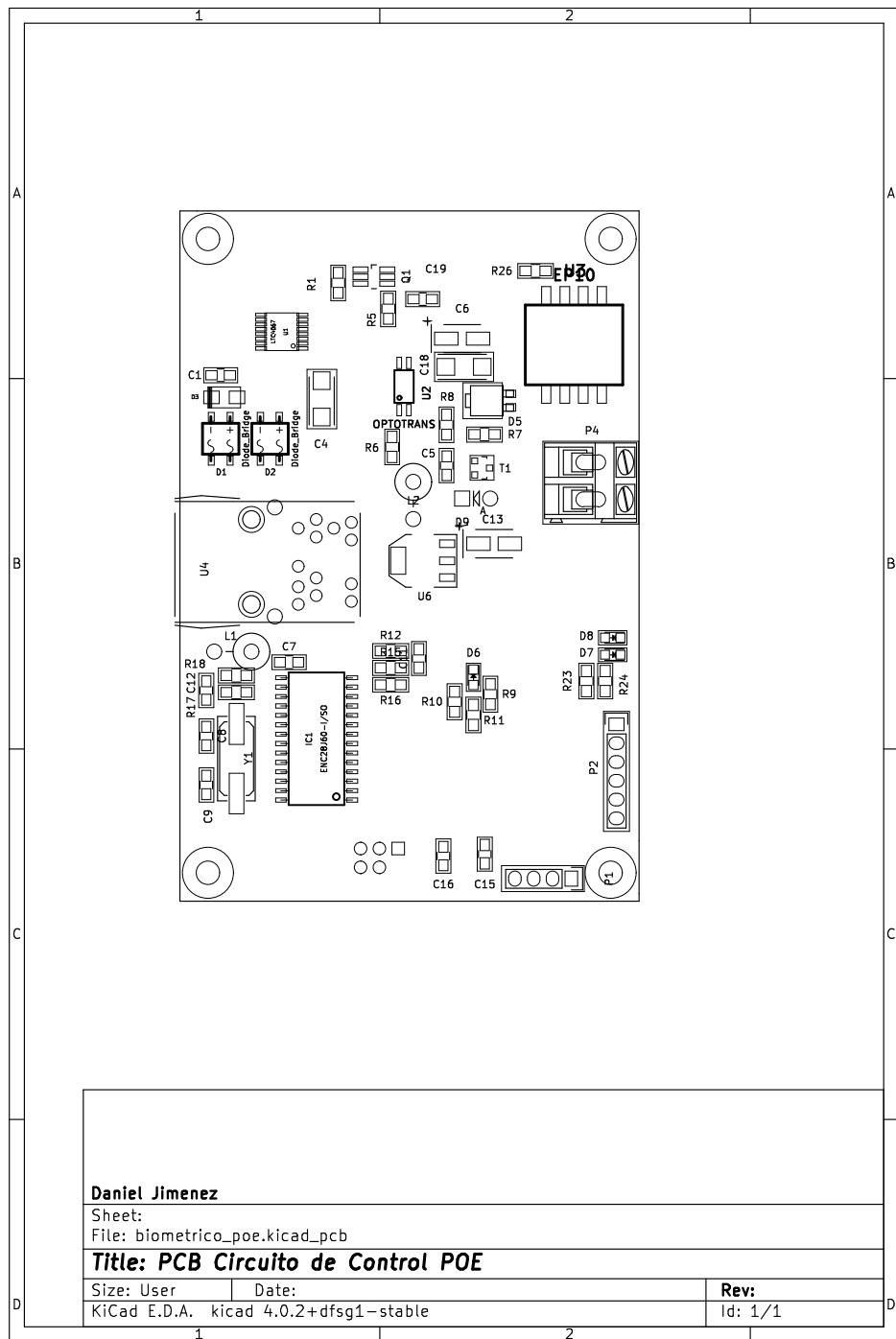
Anexo 4. Lado superior del PCB de la placa de interfaz sensorial



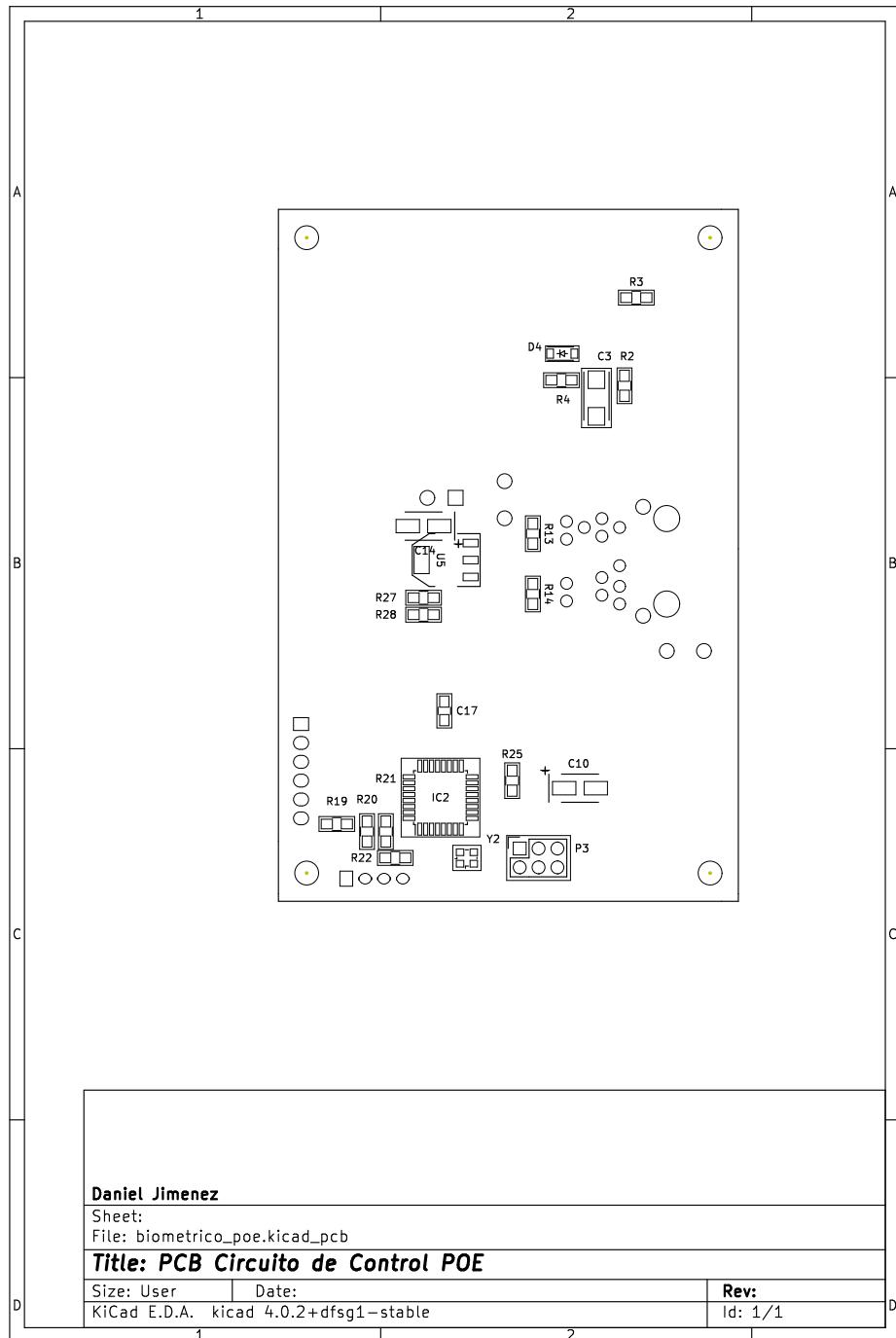
Anexo 5. Lado inferior del PCB de la placa de interfaz sensorial



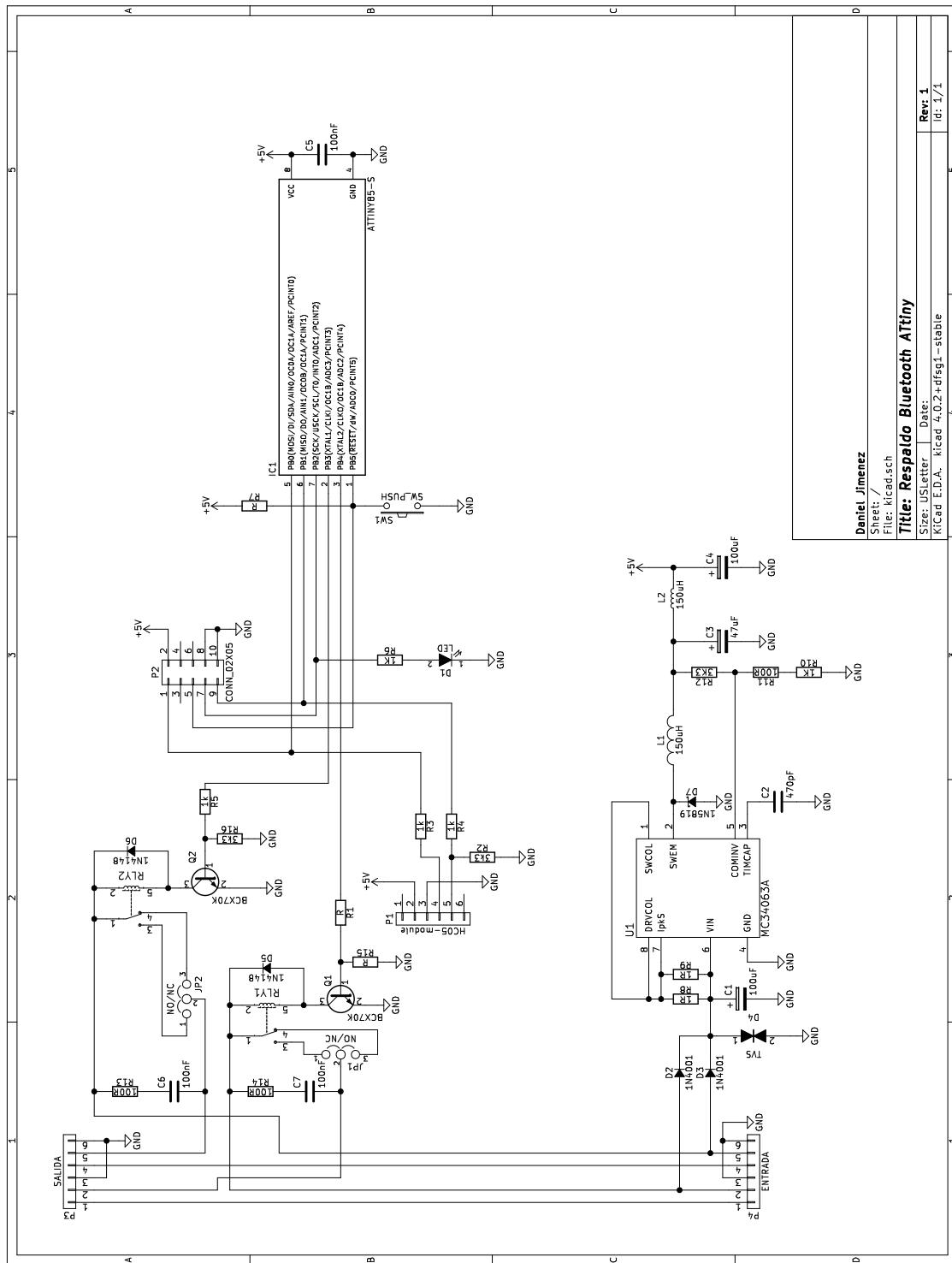
Anexo 6. Circuitos del lado superior de la placa de interfaz sensorial



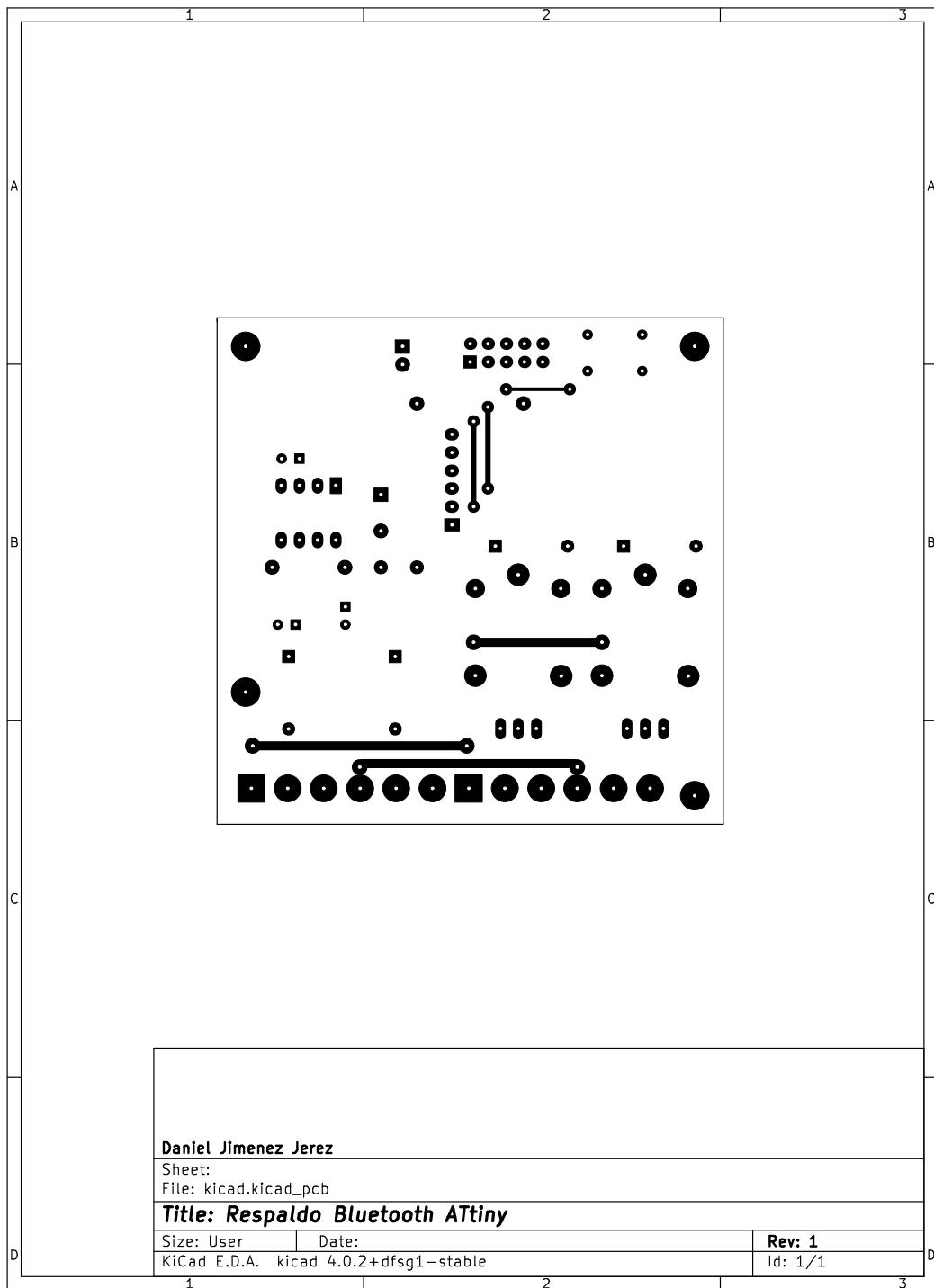
Anexo 7. Circuitos del lado inferior de la placa de interfaz sensorial



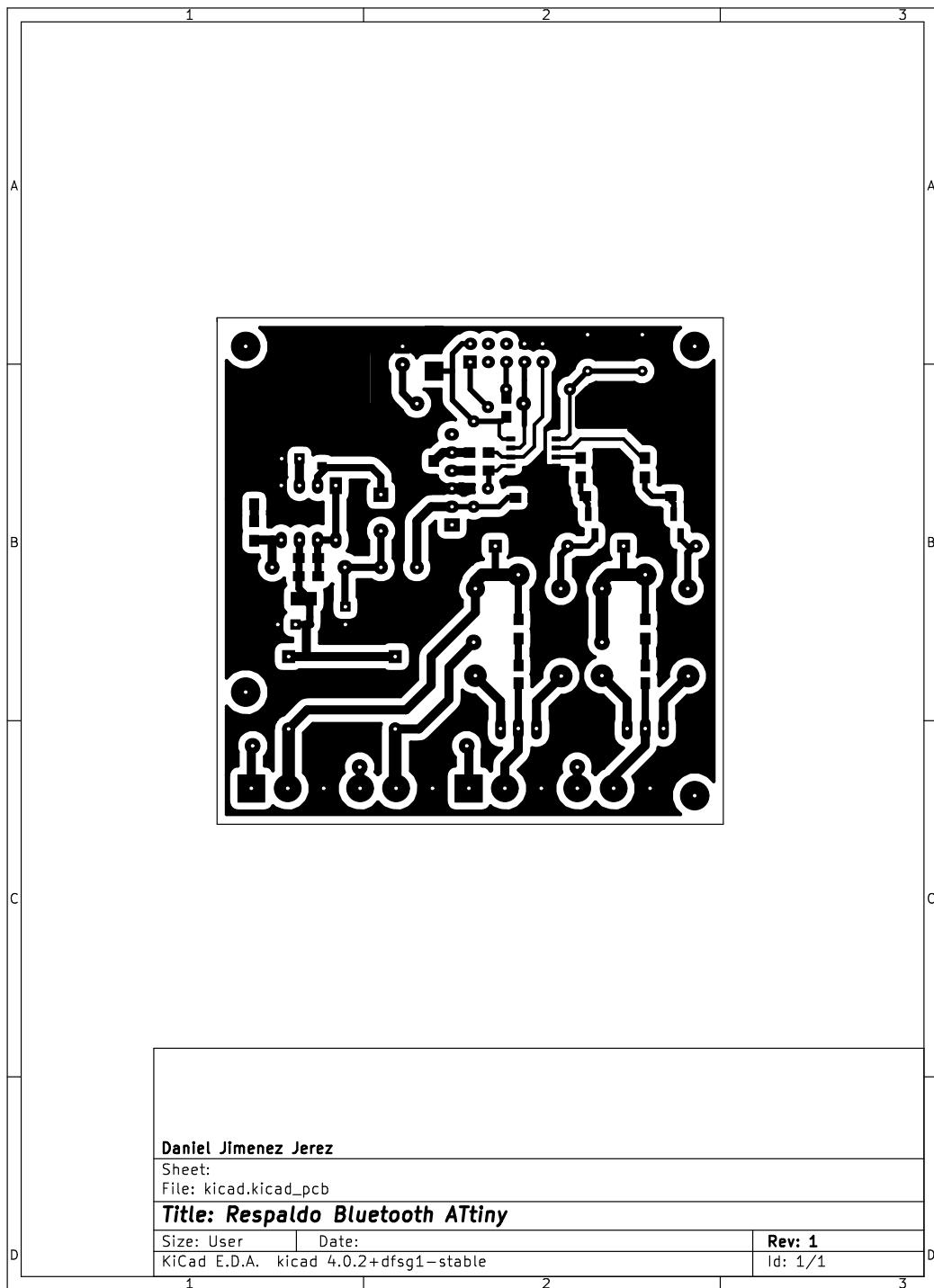
Anexo 8. Esquemático de la placa de respaldo bluetooth



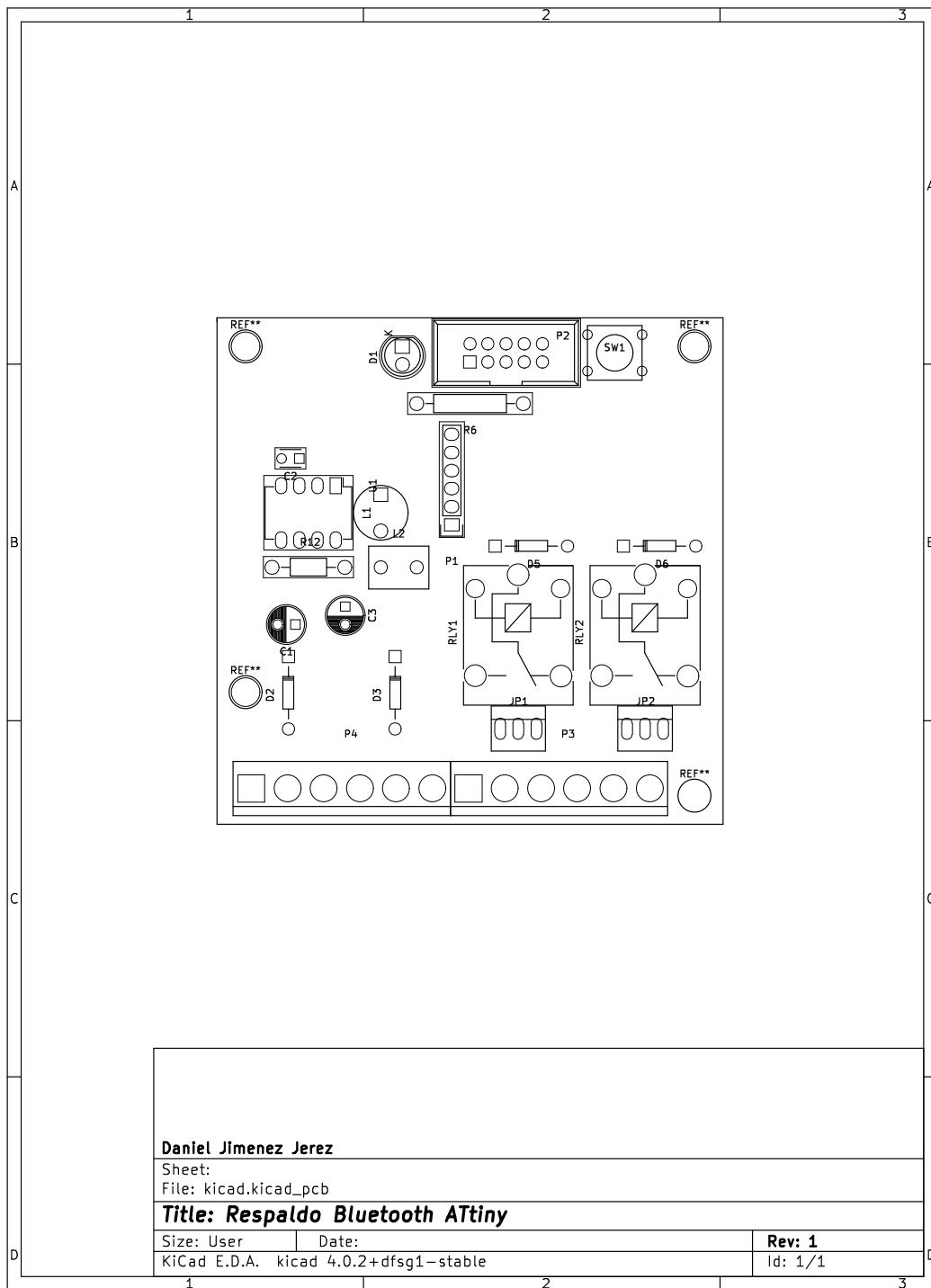
Anexo 9. Lado superior del PCB de la placa de respaldo bluetooth



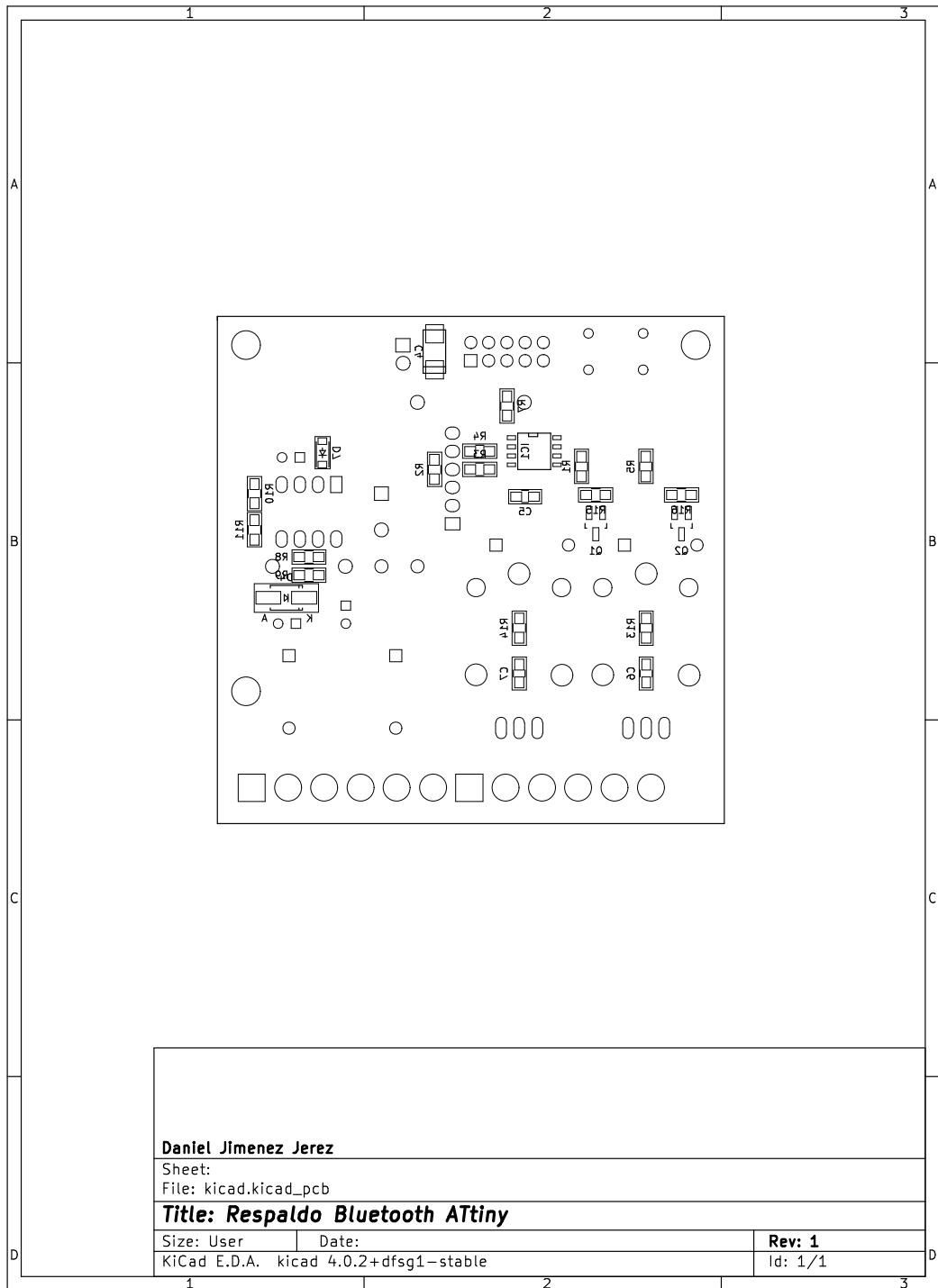
Anexo 10. Lado inferior del PCB de la placa de respaldo bluetooth



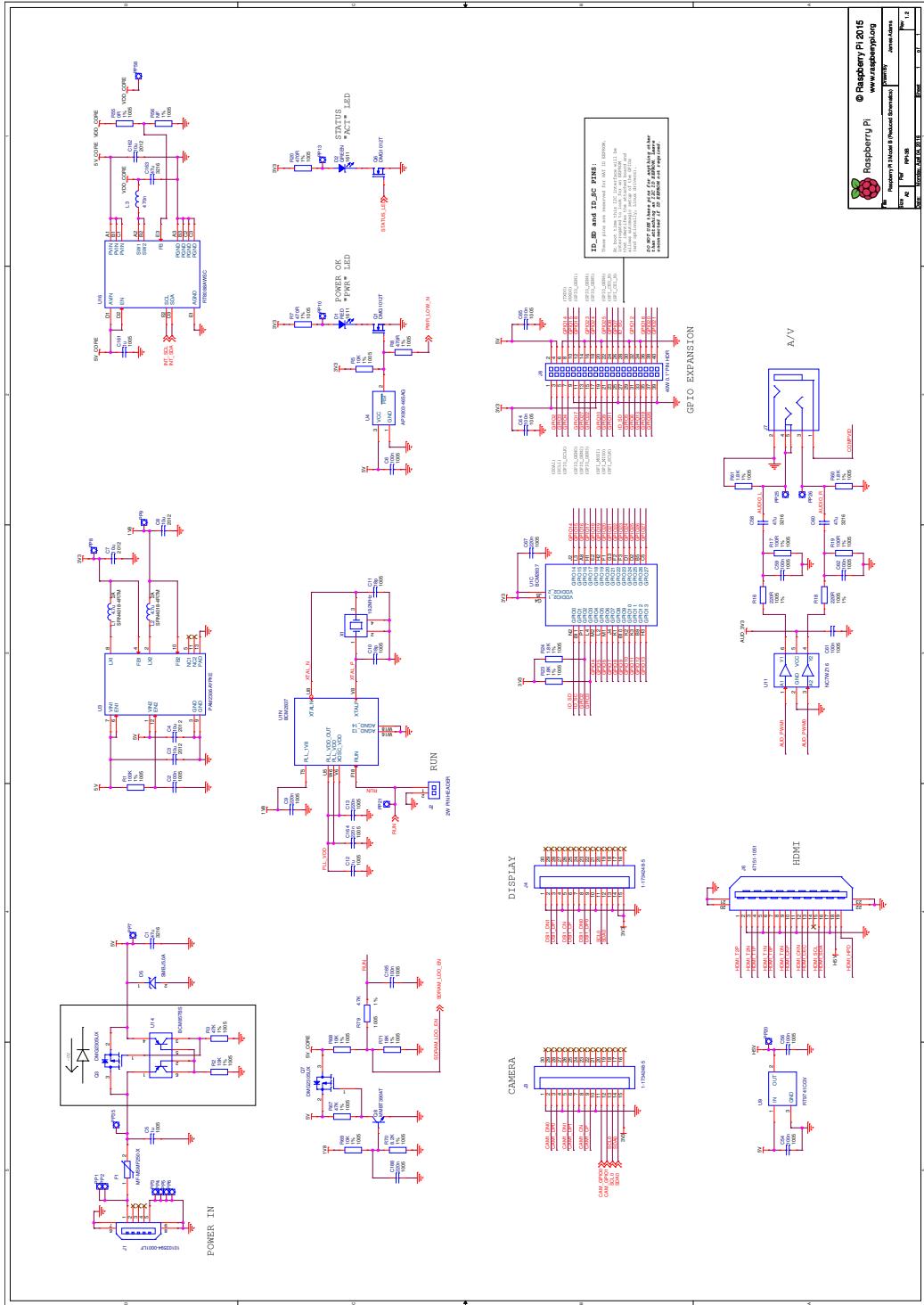
Anexo 11. Circuitos del lado superior de la placa de respaldo bluetooth



Anexo 12. Circuitos del lado inferior de la placa de respaldo bluetooth



Anexo 13. Esquemático Raspberry Pi 3 B Modelo V1.2



Anexo 14. Hoja de datos de cables HSM Wire International Inc. según AWG

HSM Wire International, Inc
Ph: 330-244-8501 Fax: 330-244-8561
www.hsmwire.com

**REQUEST
A
QUOTATION**

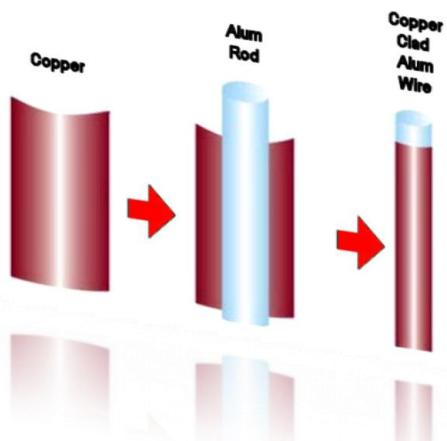
| Size AWG | Diameter (inches) Nominal | Area (sq inches) Nominal | Feet per Pound | | Pounds per 1000 ft | | Resistance (ohms per 1000 feet @ 20°C) | |
|-------------|---------------------------------|--------------------------------|----------------|-----------|--------------------|-----------|---|-----------|
| | | | Copper | 10% Cu/AL | Copper | 10% Cu/AL | Copper | 10% Cu/AL |
| 14 | 0.0641 | 0.00323 | 80.4 | 215 | 12.4 | 4.64 | 2.52 | 3.91 |
| 15 | 0.0571 | 0.00256 | 101 | 270 | 9.87 | 3.69 | 3.18 | 4.93 |
| 16 | 0.0508 | 0.00203 | 128 | 342 | 7.81 | 2.92 | 4.02 | 6.23 |
| 17 | 0.0453 | 0.00161 | 161 | 430 | 6.21 | 2.32 | 5.05 | 7.83 |
| 18 | 0.0403 | 0.00128 | 203 | 542 | 4.92 | 1.84 | 6.39 | 9.9 |
| 19 | 0.0359 | 0.00100 | 256 | 684 | 3.90 | 1.46 | 8.05 | 12.5 |
| 20 | 0.0320 | 0.000804 | 323 | 862 | 3.10 | 1.16 | 10.1 | 15.7 |
| 21 | 0.0285 | 0.000636 | 407 | 1087 | 2.46 | 0.920 | 12.3 | 19.8 |
| 22 | 0.0253 | 0.000503 | 516 | 1378 | 1.94 | 0.726 | 16.2 | 25.1 |
| 23 | 0.0226 | 0.000401 | 647 | 1728 | 1.55 | 0.580 | 20.3 | 31.5 |
| 24 | 0.0201 | 0.000317 | 818 | 2184 | 1.22 | 0.456 | 25.7 | 39.8 |
| 25 | 0.0179 | 0.000252 | 1030 | 2750 | 0.970 | 0.363 | 32.4 | 50.2 |
| 26 | 0.0159 | 0.000199 | 1310 | 3498 | 0.765 | 0.286 | 41.0 | 63.6 |
| 27 | 0.0142 | 0.000158 | 1640 | 4378 | 0.610 | 0.228 | 51.4 | 79.7 |
| 28 | 0.0126 | 0.000125 | 2080 | 5554 | 0.481 | 0.180 | 65.3 | 101 |
| 29 | 0.0113 | 0.000100 | 2590 | 6915 | 0.387 | 0.145 | 81.2 | 126 |
| 30 | 0.0100 | 0.0000785 | 3300 | 8811 | 0.303 | 0.113 | 104 | 161 |

To be used as a guide only. ©HSM Wire International Inc. Rev 1.06.01.13

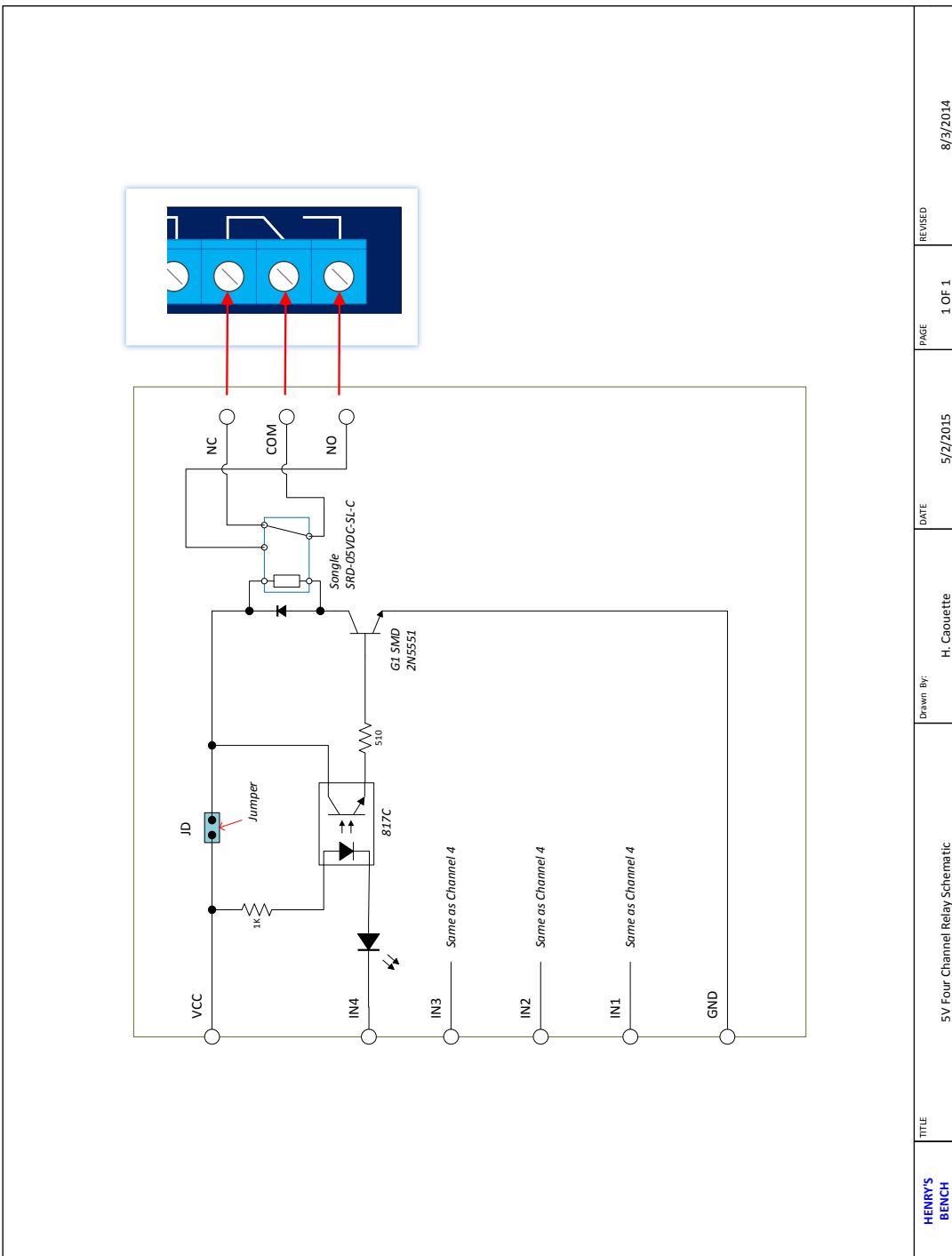
Copper Clad Aluminum is a composite wire consisting of an aluminum core clad with ETP Copper.

Typical Physical Properties

A.C. conductivity ≥ 5 MHz --- Equal to Solid Copper
 D.C. conductivity = 65% IACS
 Density = 1199 lbs / cubic inch
 % Copper by volume = 10% ± 2%
 % Copper by weight = 26.8% ± 2%
 Coefficient of thermal expansion = 22.9 ppm / C°
 Tensile Strength - Annealed = 16,500 psi
 Tensile Strength - Hard = 23,5000 psi
 Yield Strength - Annealed = 12,000 psi
 Yield Strength - Hard = 21,6000 psi
 % Elongation - Annealed = 15%
 % Elongation - Hard = 2.5%



Anexo 15. Esquemático Módulo Relé 5V Henry Bench



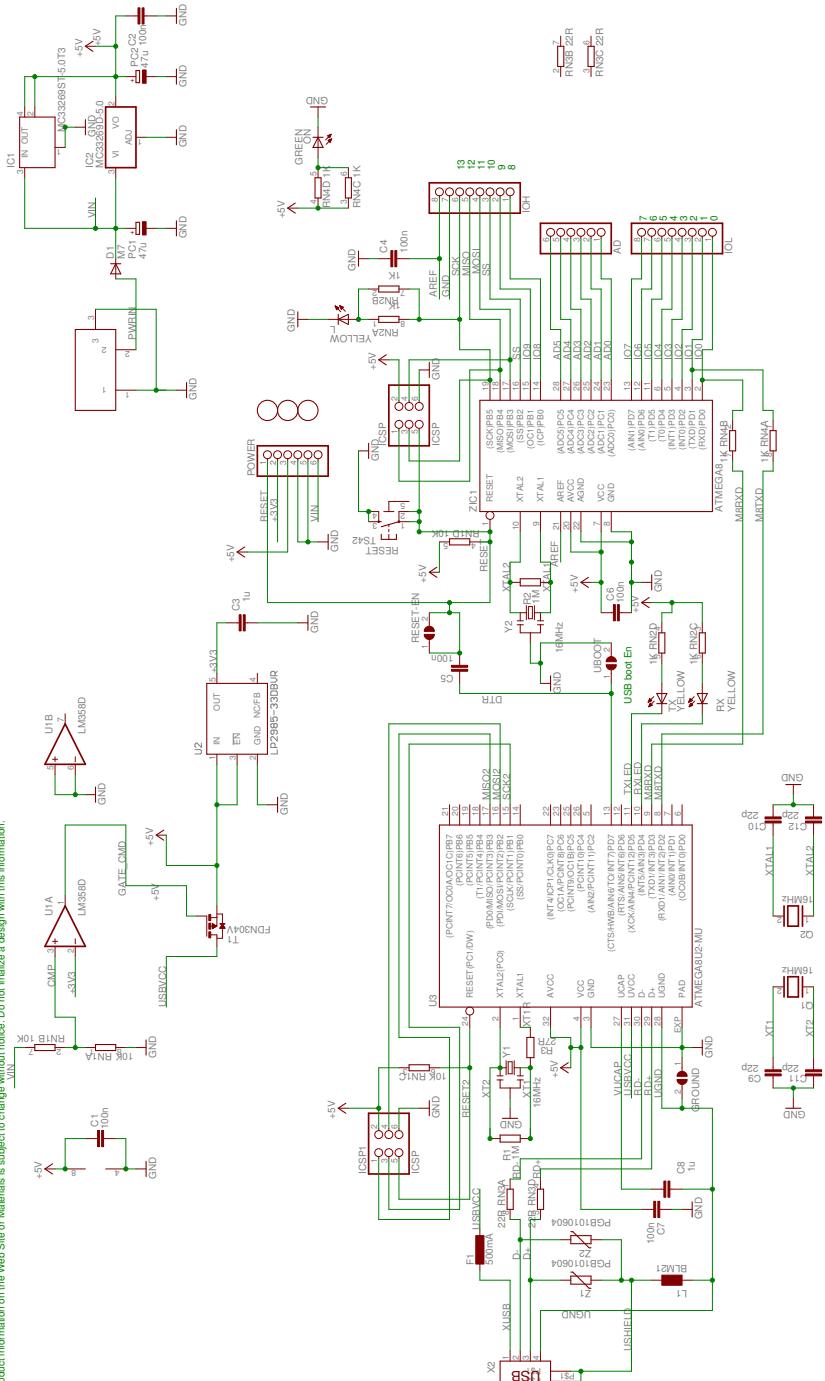
Anexo 16. Esquemático Arduino Uno R3

Arduino™ UNO Reference Design

Reference designs are provided "AS IS" and "WITH ALL FAULTS". Arduino disclaims all other warranties, express or implied, regarding products, including but not limited to, any implied warranties of merchantability or fitness for a particular purpose.

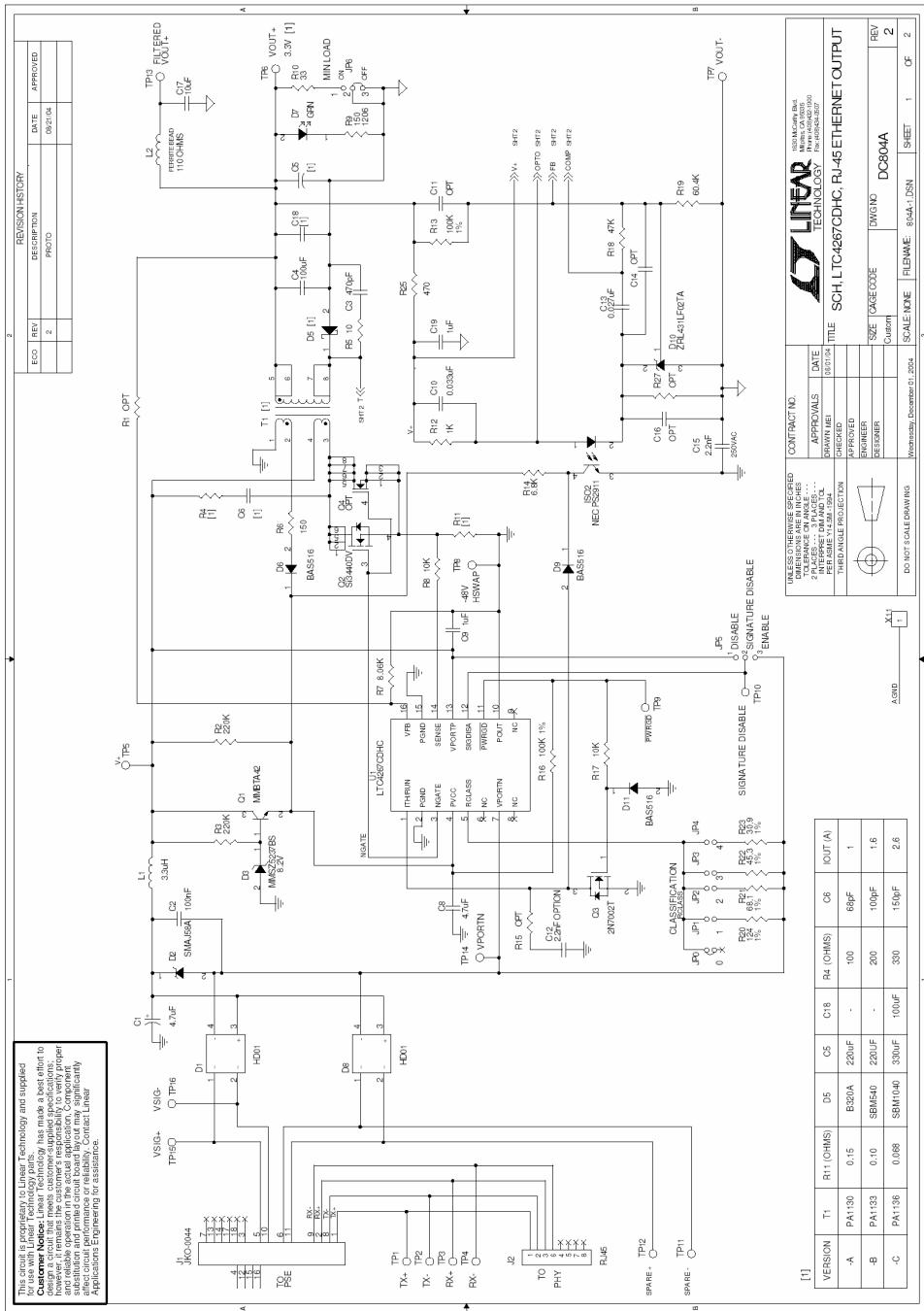
Arduino may make value changes to specifications at any time without notice. The customer must not rely on this information to define their future definition and design. It is the responsibility of the customer to evaluate and determine whether these components are suitable for the intended application and to take all appropriate safety and other measures to protect life, property and the environment.

The product information on the Web Site or Materials is subject to change without notice. Do not finalize a design with this information.



Anexo 17. Esquemático Splitter POE LTC4267

QUICK START GUIDE FOR DEMONSTRATION CIRCUIT 804 POWER OVER ETHERNET PD INTERFACE WITH INTEGRATED SWITCHING REGULATOR



Anexo 18. Esquemático Ethernet Controller ENC28J60

