Diseño y evaluación de la eficacia de un sistema de control de acceso mediante RFID para implementación en entradas a la institución, al servicio de urgencias y cirugía de la IPS Universitaria

Informe Final de Prácticas Académicas

Estudiante
Felipe Castillo Patiño

Asesor Interno
Jonathan Gallego Londoño
Profesor Programa de Bioingeniería
Universidad de Antioquia

Asesor Externo
German Cumplido Mendoza
Coordinador de Ingeniería Biomédica
IPS Universitaria

Universidad de Antioquia
2019

Diseño y evaluación de la eficacia de un sistema de control de acceso mediante RFID para implementación en entradas a la institución, al servicio de urgencias y cirugía de la IPS Universitaria

1 Resumen

En la IPS Universitaria surgió la idea de implementar un sistema de control de acceso para obtener información precisa acerca del flujo de personal, con el objetivo de mejorar procesos, controlar horarios y restringir el acceso a las áreas de urgencias críticas y cirugía. Después de evaluar las posibilidades de implementación con unas licencias previamente adquiridas, se decidió desarrollar un software de control de acceso que supliera los requerimientos de la institución. El programa desarrollado permite conexión con bases de datos tipo SQL e interacción con lectoras de RFID de conexión USB, su función es de registrar los ingresos y mantener una base de datos de usuarios con sus respectivos permisos de ingreso. Se realizó una prueba piloto que arrojó como resultado la eficacia del sistema para cumplir los requerimientos establecidos, el programa respondió sin errores durante la prueba y mediante el análisis de las rutas habituales de la institución se proyectó un costo aproximado de la implementación del proyecto.

2 Introducción

Existen recintos en los que, por seguridad, el acceso debe estar restringido a personas no autorizadas. Los hospitales son un claro ejemplo de esto, el alto flujo de personas, entre visitantes, proveedores, pacientes y trabajadores, da pie a muchas brechas de seguridad en donde pueden presentarse hurtos, contaminaciones de áreas estériles y traspaso de zonas restringidas. Por lo anterior, la vigilancia física de los accesos del personal ha ido migrando, gracias al desarrollo de las nuevas tecnologías, a los sistemas de control de accesos mediante aparatos electrónicos; los dispositivos más comúnmente usados para este fin son aquellos que usan biometría (lectores de huella digital) y la tecnología de tarjetas RFID (Radio Frecuency Identification) [1].
Las tecnologías previamente mencionadas no solo apoyan la seguridad de una institución sino también la gestión logística y del talento humano. Mediante el uso del software de control de acceso es posible determinar a qué hora una persona ingresó al edificio, cuánto tiempo permaneció dentro y qué puertas usó en todo el proceso, con esta información se puede llevar una trazabilidad de cumplimiento de horarios y control de personal. Adicional a lo mencionado anteriormente, se puede usar el mismo sistema para acceder a servicios personalizados, como casilleros, servicios de alimentación y préstamo de salas de reuniones[2], [3], [4].

El uso de la tecnología RFID para resolver problemas o facilitar procesos en el ámbito de la salud ha sido ampliamente estudiado. Por ejemplo en [5], el hospital San Raffaele en Milán, Intel, Auténtica y Cisco, realizaron un programa piloto usando tecnología inalámbrica y RFID para realizar la verificación en el proceso de transfusión y manejo de sangre. Fue diseñado para minimizar los errores humanos que se puedan llegar a producir y que den como resultado la administración de sangre equivocada a un paciente, entre los beneficios de este proyecto se encuentran: mejor movilidad y eficiencia del personal, mayor uso de la base de datos, acceso

a los datos de la sangre desde cualquier lugar con internet y reducción dramática del potencial de error.

La tecnología RFID también se ha utilizado para proveer identificación, posicionamiento, seguridad y otras funciones, tanto a personas como objetos dentro de un hospital. En el uso de posicionamiento de un objeto o persona se requiere de una etiqueta con una batería interna, esta con el paso del tiempo se desgasta y eventualmente la batería se descarga, con lo cual se hace necesario adquirir una nueva etiqueta cada vez que esta falle, esto eleva enormemente el costo del sistema. Sin embargo, esta tecnología ha probado ser útil para mantener un registro de la localización de los equipos, encontrar equipos perdidos, y evitar que pacientes psiquiátricos evadan la seguridad del hospital [6], [7].

En la IPS Universitaria surge la idea de realizar un control de acceso al personal, esto con el fin de obtener información del flujo del personal en la clínica e implementar medidas para mejorar el rendimiento del personal y la seguridad en general de la institución; a futuro puede ser implementado en el servicio de alimentación y posiblemente sea extendido a más servicios propios de la institución. Lo anterior está enmarcado en el plan de desarrollo 2017-2026 de la IPS Universitaria, este establece que para el 2026 será reconocida internacionalmente como el hospital universitario de la Universidad de Antioquia, siendo un referente nacional e internacional por sus resultados en gestión del conocimiento, producto de la docencia, la investigación y la innovación. Para esto, entre muchos otros, se tiene el programa "Gerencia de la información" en donde existe un proyecto que apunta a integrar todas las herramientas que provean información e indicadores para la efectiva toma de decisiones en todos los niveles de la institución [8].

En la actualidad existen dos sistemas implementados pero en desuso en la institución; el primero es el *Andover Continuum* un sistema de control de edificios empresariales diseñado como un sistema HVAC (por sus siglas en inglés Heating, Ventilating and Air Conditioning), el cual permite gestionar de manera centralizada sistemas como: control de acceso en red, seguridad mediante circuito cerrado de televisión, sistemas anti incendios y control de intrusos, además de realizar una optimización del uso de la energía eléctrica por medio del análisis de datos y el uso de controladores que permitan gestionar el consumo y uso de sistemas de iluminación, ventilación y aire acondicionado. Este sistema está implementado como un control de acceso en solo un piso de la institución y no tiene ningún otro uso dentro de esta [9].

El segundo sistema es, al igual que el primero, un sistema de control de edificios llamado *EBI* de la empresa *Honeywell*, este entre otras cosas permite el control de las alarmas contra incendios, control HVAC, de cámaras de seguridad y de control de acceso; este sistema está implementado como control de acceso en la sede ambulatoria de la IPS Universitaria para unas pocas puertas en unas áreas específicas [10], [11]. Ambos sistemas son bastante robustos y presentan la facilidad de poder acceder a toda esta información desde un solo software, no obstante, estos sistemas para su implementación requieren una alta inversión debido al alto costo de lo que se conoce como controladoras, que es el dispositivo que enlaza los actuadores con el servidor y posteriormente con el software.

Por lo anterior, la metodología que se lleva a cabo en este proyecto se centra en el desarrollo de un software de control de acceso por medio de tecnología RFID y que sea capaz de acceder a bases de datos con el fin de recopilar la información de la hora de salida e ingreso de cada persona; este software debe cumplir con requerimientos específicos de la institución y de los

servicios en donde serán instalados, además de ser escalable para su posible implementación en la IPS Universitaria. El alcance de este proyecto es el desarrollo de un prototipo funcional del sistema anteriormente descrito y a la caracterización de todas las necesidades extras que requiera este sistema para que tenga un funcionamiento adecuado, como las rutas de desplazamiento mas comunes del personal, los tipos de personal y su nivel de acceso dentro de la institución.

3 Objetivos

3.1 General:

Diseñar un sistema de control de acceso que pueda implementarse a futuro en las salas de urgencias y cirugía de la IPS Universitaria usando tarjetas RFID de identificación y evaluar su eficacia mediante la implementación de una prueba piloto.

3.2 Específicos:

- Evaluar el estado actual de herramientas y recursos informáticos disponibles en la IPS Universitaria para la elección del software a usar en la ejecución del proyecto.
- Diseñar el sistema de control de acceso que pueda implementarse en las salas de urgencias y cirugía usando tarjetas RFID de identificación.
- Evaluar la eficacia del sistema de control de acceso realizando una prueba piloto con el fin de poder implementarse a futuro en urgencias y cirugía.
- Determinar los requerimientos para la implementación del control de acceso a escala macro en la IPS Universitaria.

4 Marco Teórico

4.1 Control de Acceso

El mundo cambia rápidamente y las compañías privadas y agencias de gobierno están reconociendo la necesidad vital de asegurar personas, propiedad e información, para cumplir esto existen los sistemas de control de acceso, el cual se puede definir como una restricción selectiva de acceso a algún lugar o recurso, la acción de *acceder* puede significar entrar al lugar o bien, usar o consumir el recurso [12]. El control de acceso físico puede ser realizado por personal de seguridad o por un dispositivo como un torniquete de acceso, mientras que el control de acceso digital o virtual se realiza por medio de protocolos de *autenticación* y *autorización*, que no son más que la función que poseen los sistemas informáticos de identificar el usuario y determinar si este tiene el permiso requerido para acceder o modificar la información que ellos contienen.

En general, un control de acceso de cualquier tipo consta principalmente de un punto de acceso, un actuador, una lectora, credenciales y un control autónomo o en red. Dichos componentes se describen a continuación:

4.1.1 Punto de acceso

Es el lugar u objeto a través del cual se realizará el acceso, este puede ser una puerta, un torniquete, un ascensor, un datáfono, una pantalla de ingreso o cualquier otro tipo

de restricción, sea física o digital. Su función es evitar que sea atravesado por cualquiera que intente acceder sin la autorización o permiso requerido.

4.1.2 Actuador

Es el objeto u software que permite el acceso de la persona al habilitar el paso a través del punto de acceso, en el caso de ser un acceso físico son generalmente electroimanes o servo motores que controlan los mecanismos de seguridad del punto de acceso; si es un acceso virtual o digital el actuador está embebido en el programa como una condición lógica que permite el acceso al sistema.

4.1.3 Lectora

Es aquello que permite identificar la persona que trata de atravesar el punto de acceso, por ejemplo, una cerradura, un teclado, un sensor de variables biométricas, un lector de bandas magnéticas o un dispositivo de reconocimiento de RFID.
Existen diferentes tipos de lectoras:

- **Básicas:** su única funcionalidad es identificar la credencial y enviar estos datos a una controladora principal, desde donde se maneja el resto del sistema.
- **Semi-Inteligentes:** tienen embebidos todas las entradas y salidas necesarias para controlar una puerta o acceso, sin embargo, estas no toman decisiones, cuando se realiza la identificación esta se envía a una controladora principal en donde se realiza la validación de la credencial.
- **Inteligentes:** estas lectoras tienen las mismas capacidades de las lectoras semi inteligentes adicionando la capacidad de una memoria interna en la cual se almacenan los registros de permisos; con lo cual esta lectora es autónoma y puede tomar decisiones de acceso.

4.1.4 Credencial

Existen tres tipos de credenciales dependiendo de la información de autenticación:

1. Algo que el usuario sabe, un usuario y contraseña, frase o pin.
2. Algo que el usuario posee, una llave, tarjeta o carnet de identificación.
3. Algo que el usuario es, se refiere a huellas digitales, iris o reconocimiento facial.

El objetivo de una credencial es el de servir como identificador para la persona que está tratando de acceder al sistema, dado que el sistema en si no posee la habilidad para reconocer personas, la credencial es la manera en la que el sistema puede reconocer el usuario, verificar sus permisos y autorizar o no el acceso que se solicitó.

El proceso para pasar a través de un control de acceso se cumple independiente del sistema que sea (físico o digital), al igual que las definiciones de *Punto de acceso*, *Actuador*, *Lectora* y *Credencial*. El proceso es el siguiente:

1. Se desea cruzar el *punto de acceso* para acceder al lugar o servicio que este custodia.
2. Para ello hace interactuar la *credencial* de cada persona con la *lectora*.
3. Se identifica correctamente la credencial, es decir, el sistema reconoce la identidad de la persona que está tratando de cruzar.
4. Si la persona identificada tiene autorización para seguir, el *actuador* habilita el paso.

El control de acceso físico se puede reducir al conocimiento de tres ítems *quién*, *cuándo* y *dónde*, con esto se puede averiguar la identidad de la persona, el tiempo y el lugar en dónde se realizó el acceso; todos estos datos pueden ser agrupados en una base de datos y mediante un

análisis se pueden llegar a determinar patrones de conducta como tiempo promedio de estancia en un lugar, tiempo de movilización de un lugar a otro, afluencia de personas a través de un acceso, hora del día de más movilidad, entre otras. En general el control de acceso se puede clasificar en dos grandes grupos, el control de acceso *autónomo* y *en red*.

4.1.5 Control de acceso autónomo

El primero hace referencia a aquellos cuya única funcionalidad es el control de un solo punto de acceso, es decir, es un sistema aislado; funciona configurando la lectora con una base de datos de identificaciones, internamente se ejecuta la lectura de la credencial y se permite o no el paso, este tipo de sistema no cuenta con ningún tipo de trazabilidad o interacción con otros sistemas por lo que es idóneo para empresas que requieran un nivel de seguridad medio.

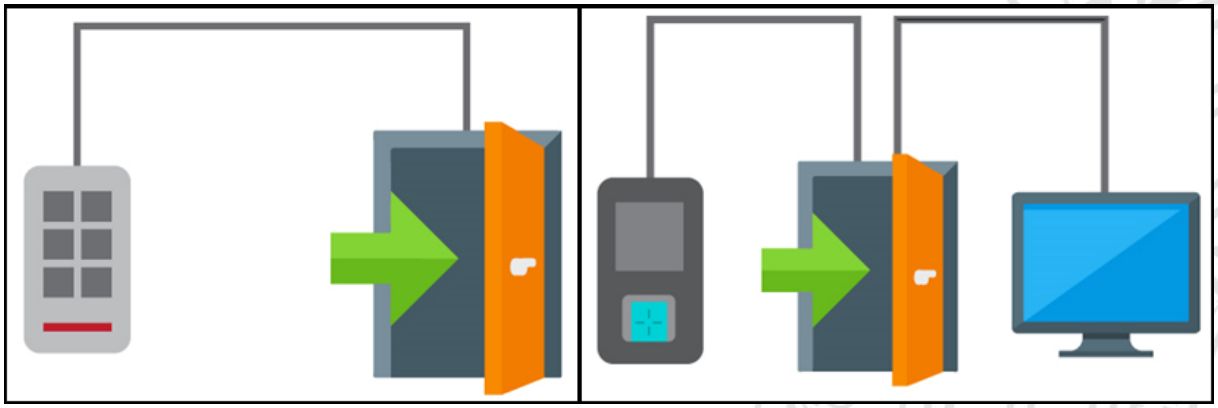

Figura 1. Sistema de control de acceso autónomo (a) y en red (b)

4.1.6 Control de acceso en red

El sistema de control de acceso en red consiste en una o más lectoras conectadas a una red (LAN o WAN) con un servidor o computador como controladora central, mediante este se puede tener un registro y trazabilidad de la fecha y hora de entrada y de cuál punto de acceso se utilizó, también está la posibilidad de dar y revocar permisos de acceso de forma inmediata mediante un software de control, esto es muy importante debido a que en el caso de pérdida de una credencial esta se puede desactivar de manera remota; este tipo de sistema se considera de alta seguridad dado a la cantidad de datos que se pueden obtener del uso y funcionamiento del sistema.

Los sistemas de control de acceso en red son usados comúnmente en donde se debe revisar el acceso de muchas personas por unas pocas entradas, este es el caso, por ejemplo, de las entradas principales de edificios de oficinas y de grandes factorías [13].

4.2 Radio Frecuencia

La idea y concepción de la radio viene de la realización de experimentos para crear una "telegrafía inalámbrica", en 1895 el italiano Guglielmo Marconi envió y recibió la primera señal de radio, materializando así la primera comunicación inalámbrica del mundo. Dentro del espectro de radio frecuencia se encuentran todas las comunicaciones inalámbricas existentes, incluyendo Bluetooth, WiFi, telefonía móvil, emisoras de radio, señales satelitales, televisión, identificación por radio frecuencia, entre otros.

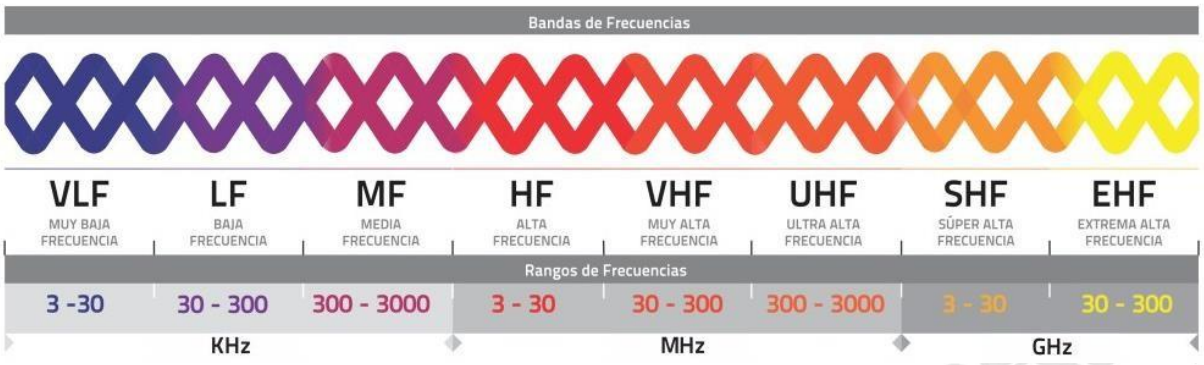

Figura 2. Espectro electromagnético para radio frecuencia [14]**.**

La radio frecuencia se refiere a las ondas electromagnéticas en un rango de frecuencias entre aproximadamente 3kHz hasta los 300GHz, estas están categorizadas por rangos de frecuencia más cortos como se puede apreciar en la Figura 2. Cada una de estas bandas de frecuencia está categorizada y subdividida en diferentes tipos de uso dependiendo de cada país, sin embargo, se mantienen algunos lineamientos generales gracias a la normalización por ISO para los dispositivos de comunicación inalámbrica. El envío de información en una señal de radio se puede realizar de diversas maneras, entre ellas están:

- Frecuencia modulada (FM)
- Amplitud modulada (AM)
- Transmisión por modulación de la fase de la onda portadora (PM)
- Transmisión por modulación de pulsos
- Transmisión por codificación

Mediante estos formatos se puede enviar información tanto analógica como digital y establecer así comunicaciones inalámbricas; gracias a los diversos desarrollos en este campo es que se tiene una tan amplia variedad y aplicaciones del espectro electromagnético, entre los cuales resaltan la comunicación inalámbrica por supuesto, radioastronomía, radar, resonancia magnética nuclear, medicina y tratamientos estéticos.

4.3 Identificación por Radio Frecuencia (RFID)

RFID es una sigla que proviene del inglés *Radio Frequency Identification*, esta tecnología se refiere al uso de dispositivos electrónicos con el fin de identificar un objeto específico. RFID es un sistema de manejo de datos inalámbrico que consta de dos componentes, el "transpondedor" y la "lectora"; el protocolo de comunicación con el cual se realiza el intercambio de datos entre estos componentes está especificado en la norma ISO 7816. Los transpondedores (que viene del inglés Transponder, **Trans**mitter-Res**ponder**) tienen la capacidad de realizar una comunicación inalámbrica con otro dispositivo por medio de ondas electromagnéticas de alta frecuencia, este componente funciona como el "esclavo" de la comunicación, responde a las instrucciones que son enviadas por la lectora con los datos correspondientes que están almacenados en la memoria interna.

La lectora genera un campo electromagnético esperando que un transpondedor entre en rango de comunicación, una vez este se encuentre a la distancia adecuada responde a la petición inicial de la lectora comenzando así la comunicación; independientemente que sea llamada lectora esta puede tener la capacidad de solo lectura o de lectura-escritura [3], [4].

4.3.1 Formatos de construcción de transpondedores

- **Discos o "monedas":** son de los formatos mas comunes, estos están hechos por inyección de plástico ABS y poseen usualmente un hoyo en su centro para permitir el uso de tornillos y así anclarlo a los diversos objetos

- **Capsula de vidrio:** usado principalmente para la identificación de animales, son unos tubos de 12 a 32mm que en su interior llevan embebido todo el sistema de identificación.

- **Empaques plásticos:** están diseñados para aquellas aplicaciones que requieren unas condiciones de alta resistencia mecánica, este tipo de empaque puede ser fácilmente integrado a, por ejemplo, llaves electrónicas de automóviles.

- **Llaves:** se usan para sistemas con requerimientos de seguridad especiales, se acopla un identificador de plástico a la llave, de modo que cuando esta sea usada el transpondedor esté a la distancia ideal de la lectora.

- **Tarjetas:** un formato muy popular hoy en día, se pueden ver como sistemas de control de acceso o como aplicaciones de monederos para sistemas de transporte masivo alrededor del mundo. Son ideales también para aplicaciones de carnetización en una empresa gracias a la posibilidad de imprimir sobre el plástico de la tarjeta, con lo que se puede crear una identificación visible y funcional para sistemas RFID.

- **Etiquetas inteligentes:** son transpondedores que tienen el grosor de una hoja de papel, generalmente se fabrican sobre materiales auto adhesivos, esto con el fin de usarlo, por ejemplo, en aeropuertos para la identificación de maletas durante su carga en el avión o en fábricas, dado que se pueden colocar en los objetos que estén siendo producidos o almacenados con el fin de mantener un inventario inteligente.

4.3.2 Frecuencia, rango y acople

El criterio mas importante para la diferenciación de sistemas RFID son las frecuencias de operación de la lectora, el método de acople físico y el rango del sistema. Se usan frecuencias ampliamente diferentes desde los 135kHz hasta los 5,8GHz, para realizar el acople se usan campos eléctricos, magnéticos y electromagnéticos. Finalmente, el rango que puede llegar a alcanzar el sistema va desde unos pocos milímetros hasta más de los 15m.

Los sistemas RFID con un rango muy corto, 1cm aproximadamente, se conocen como *sistemas de acople estrecho*, para la operación el transpondedor debe estar ubicado sobre la superficie de la lectora destinada para este propósito, estos sistemas utilizan campos electromagnéticos y la corta distancia hace que el acople tenga la potencia necesaria para que sea posible el uso de un procesador que no tenga un alto consumo de energía debido a que a distancias tan pequeñas se puede hacer una muy buena transferencia de energía y por lo tanto la transmisión es estable dentro de este rango.

Existen sistemas con rangos de lectura-escritura de hasta un metro, estos usan el método de acople inductivo (magnético), el cual abarca más del 90% del mercado de la tecnología RFID hoy en día. Dentro de esta definición están las tarjetas inteligentes,

las cuales están reguladas por la ISO 14443. Estas tarjetas utilizan frecuencias desde los 125kHz hasta los 13,65MHz.

4.3.3 Transpondedor Activo y Pasivo

Un criterio de distinción importante entre los sistemas RFID es como funciona la fuente de energía para que el transpondedor pueda funcionar.
Los *Transpondedores Pasivos* son aquellos que no tienen ninguna fuente de poder, a través de la antena por medio de campos eléctricos o magnéticos se provee de la energía requerida para operar. Esto quiere decir que se usa la misma energía que envía la lectora para suplir el requerimiento del transpondedor y a su vez responder la información a la lectora [15], [16].
Por otro lado, los *Transpondedores Activos* tienen su propia fuente de alimentación, esto permite que los sistemas que utilizan esta metodología puedan alcanzar rangos de lectura muchísimo mas altos que los transpondedores pasivos.

Cada una de las anteriores características tiene como finalidad responder a una necesidad específica que el mercado ha ido desarrollando, como lo son:

- Sistemas de control de acceso
- Gestión y seguimiento de documentos
- Sistemas de pago electrónico
- Sistema de control y cobro de peajes
- Seguimiento de contenedores
- Control de activos
- Trazabilidad de medicamentos

4.4 Dispositivos USB

4.4.1 USB

Un *Bus Serial Universal (USB)* es una interfaz común que permite la comunicación entre dispositivos periféricos y un controlador, como un ordenador personal; este es un estándar internacional de fabricación de cables, conectores y protocolos de conexión, la idea original fue simplificar y mejorar la interfaz entre ordenadores personales y dispositivos periféricos. Los conectores USB se diseñaron de manera de que los dispositivos fueran auto programables, es decir, el usuario final únicamente tenía que conectar el periférico a su ordenador e inmediatamente este se configuraría solo y estaría listo para su uso, sin la necesidad de mayor configuración ni de reiniciar el equipo [17]–[19].

4.4.2 SparkFun RFID Starter Kit

Sparkfun ha desarrollado un kit para uso básico de las tarjetas RFID de 125KHz, este kit posee una lectora que envía por medio de protocolo serial el identificador único de cada tarjeta, este envío se puede realizar por medio de la interfaz USB que se incluye en el kit, o directamente con un microcontrolador o con un dispositivo que tenga la capacidad de realizar comunicación serial; en la Figura 3 se puede observar una imagen de referencia del dispositivo.
Mediante el uso de la interfaz USB se puede recibir en un ordenador la cadena de caracteres enviada por el sensor y mediante código de programación manipular esta información para ejecutar diversas tareas [20].

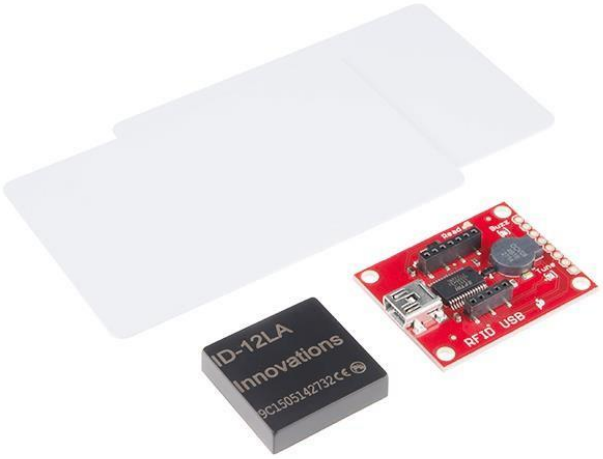

Figura 3. SparkFun RFID Starter Kit

4.5 Sistemas de Control de Acceso

4.5.1 Andover Continuum

Es un sistema de control de edificios empresariales concebido desde un principio como un sistema de supervisión y control para la climatización y la seguridad; Integrando lo anteriormente mencionado se tienen los sistemas de control de temperatura conocidos como *HVAC* (por sus siglas en inglés *Heating, Ventilating and Air Conditioning*), control de acceso en red, seguridad mediante circuito cerrado de televisión, sistemas anti incendios y control de intrusos, además de realizar una optimización del uso de la energía eléctrica por medio del análisis de datos y el uso de controladores que permitan gestionar el consumo y uso de sistemas de iluminación, ventilación y aire acondicionado. En la Figura 4 se puede ver un diagrama del modelo de funcionamiento del software y la interconexión entre los dispositivos periféricos y controladoras.

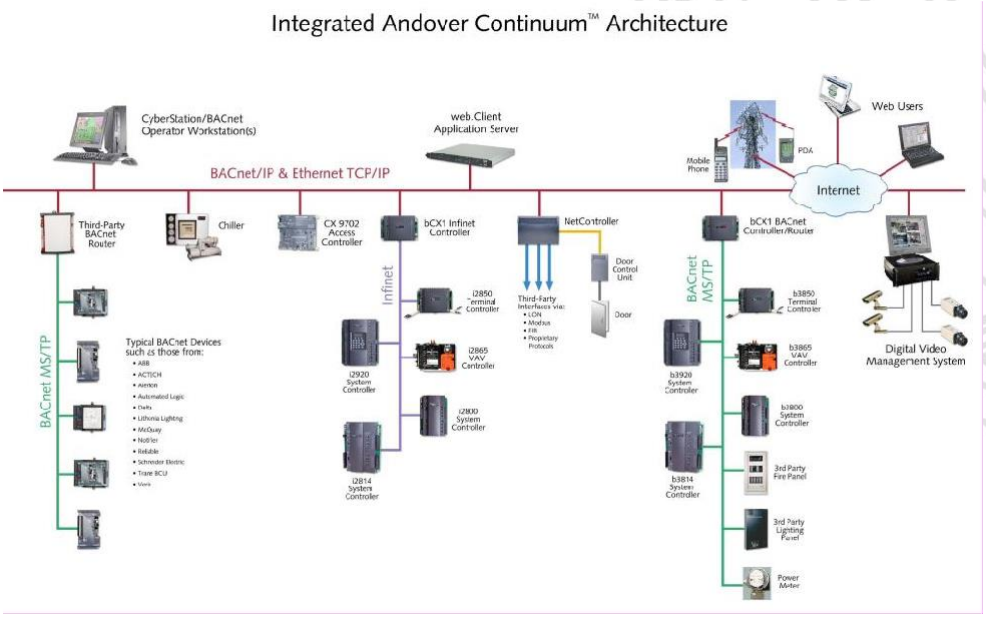

Figura 4. Arquitectura de Andover Continuum

4.5.2 Honeywell EBI

EBI es la sigla que significa *Enterprise Buildings Integrator*, es el software diseñado por la empresa de equipos y control industrial Honeywell que tiene como objetivo transformar grandes edificios y estructuras en edificios inteligentes mediante la integración de todos los sistemas relacionados en un solo software y una sola plataforma para realizar un control eficiente que permita optimizar procesos y tener información en tiempo real acerca de las condiciones de todos los sistemas.

El software permite integrar una amplia variedad de equipos de diferentes fabricantes, esto a través de protocolos abiertos programados; es decir, se pueden tener equipos y controladores físicos de otras empresas o fabricantes, pero aun así se pueden integrar al sistema por medio de los protocolos de comunicación establecidos en normas internacionales destinadas a regular estos dispositivos [10].

4.5.3 Anviz W2

Es un control de acceso autónomo, este cuenta con una pantalla a color, teclado numérico, lector de huellas digitales y lector de tarjetas RFID de 13.56MHz; el sistema trae también una controladora para accionar un electroimán para el control de una puerta y controlar un botón de salida, tiene capacidad de hasta 3.000 usuarios y 100.000 registros; también posee un servidor web interno en donde se puede interactuar con el equipo [21]–[23].

4.6 Bases de Datos

Este término se refiere a una colección de datos que está creada de tal manera que sea fácilmente comprensible, gestionable y actualizable; la idea detrás de una base de datos es tener un consolidado general de una cantidad de información que se maneje en un ambiente en particular, por ejemplo, la ubicación y contenido de un libro dentro de una biblioteca; siguiendo con el ejemplo la base de datos necesita unas características propias de los objetos llamados libros, como lo son título, autor, año de publicación e identificador de la biblioteca; esta información debe ser visible para todo el público de modo que se les facilite encontrar el libro que buscan, sin embargo esta no debería ser modificable por cualquier persona, solo por la persona encargada de la organización de la biblioteca [24], [25].

Con el ejemplo planteado se evidencian las necesidades básicas que presenta una base de datos:

- Debe ser accesible desde diversos puntos, pero la información solo puede ser vista o modificada por ciertas personas.
- Debe permitir almacenar las características referentes a un objeto, persona, lugar o evento.
- Debe tener la capacidad de manejar una gran cantidad de información.
- Debe permitir almacenar diferentes tipos de datos (números, letras, caracteres especiales, imágenes) y realizar operaciones básicas con estos.
- Debe poder actualizar, crear y eliminar datos.

Estos procesos se realizan a través de un tipo de software conocido como *Sistema de Manejo de Bases de Datos* o *DBSM* por sus siglas en inglés. Desde mediados de la década de 1980 los *DBSM* han evolucionado creando nuevos lenguajes, algoritmos y técnicas de software que permiten al usuario final una mejor interacción con la base de datos y mayor eficiencia computacional de los procesos que se realizan. Dentro de estos desarrollos está lo que se conoce como *Structured Query Language* o por sus siglas *SQL*, esto traduce *Lenguaje de Consulta Estructurado*, es un lenguaje de alto nivel que utiliza palabras clave del idioma

inglés para generar líneas de comando que tienen como objetivo afectar de diversas maneras a una base de datos.

Un *DBSM* muy conocido y utilizado es *Microsoft SQL Server*, desarrollado por la empresa *Microsoft*, este utiliza el lenguaje T-SQL (Transact-SQL, una adición al SQL estándar) y generalmente se usa en conjunto con el programa *Microsoft SQL Server Management Studio* el cual da una interfaz gráfica para crear, diseñar, visualizar y modificar las bases de datos, su contenido y propiedades [26].

5 Metodología

En esta sección se describen detalladamente las actividades que se llevaron a cabo para cumplir a cabalidad los objetivos propuestos anteriormente, con esto en mente se enuncia y describe la actividad realizada. Se incluyen aquí los objetivos específicos para dar claridad acerca de que actividades les dan cumplimiento.

- Actividades relacionadas con la escritura de la propuesta:
  - **Actividad 1** ***Estudio y formulación del proyecto:*** Se estudiaron las necesidades de la IPS Universitaria propuestas por el área de docencia de la institución y se realizó la formulación según la necesidad elegida.
  - **Actividad 2** ***Revisión bibliográfica:*** Se realizó una revisión bibliográfica acerca del proyecto formulado.
  - **Actividad 3** ***Presentación formal de la propuesta del proyecto***: se presentó la propuesta al comité de carrera para su aprobación.

- Actividades para el objetivo específico: "Evaluar del estado actual de herramientas y recursos informáticos disponibles en la IPS Universitaria para la elección del software a usar en la ejecución del proyecto".

  - **Actividad 4** ***Búsqueda las alternativas existentes en la institución, así como recursos y sistemas implementados:*** se buscaron que tipos de licencias o equipos están implementados en la institución.
  - **Actividad 5** ***Elección de sistema a usar, teniendo en cuenta las licencias disponibles para el proyecto***: se validó cual es la opción más apropiada para usar, teniendo en cuenta los requerimientos de la solución propuesta.

- Actividades para el objetivo específico: "Diseñar el sistema de control de acceso que pueda implementarse en las salas de urgencias y cirugía usando el software disponible y las tarjetas RFID de identificación".
  - **Actividad 6** ***Diseño una prueba piloto basada en el sistema elegido:*** Se diseñó una prueba piloto, cuantificando el hardware y software necesario para su realización.
  - **Actividad 7** ***Adquisición de controladoras, sensores o similares necesarios para el desarrollo la prueba piloto.***
  - **Actividad 8** ***Mediante manual de uso, guías, o instrucción personal se aprendió el manejo del software elegido teniendo en cuenta el alcance del proyecto:*** Se adquirió la información necesaria para programar el software utilizado para la realización prueba.

- **Actividad 9** ***Realización del montaje de hardware y software necesario para la prueba.***

- Actividades para el objetivo específico: "Evaluar la eficacia del sistema de control de acceso realizando una prueba piloto con el fin de poder implementarse a futuro en urgencias y cirugía".
  - **Actividad 10** ***Ejecución la prueba piloto en un área controlada emulando las condiciones de control de acceso*****:** Se ejecutó la prueba piloto en un ambiente controlado.
  - **Actividad 11** ***Modificación del alcance del proyecto dependiendo de los resultados de la prueba piloto.***

- Actividades para el objetivo específico: "Proyectar las necesidades para la implementación del control de acceso a escala macro en la IPS Universitaria".
  - **Actividad 12** ***Cuantificación del costo del proyecto a gran escala y su implementación en la institución:*** Con toda la información recolectada se proyectó la implementación en todas las entradas y su posibilidad en áreas críticas.
  - **Actividad 13** ***Redacción del informe final del proyecto***

En la Figura 5 se puede apreciar una representación gráfica de la metodología empleada para llevar a cabo este proyecto.

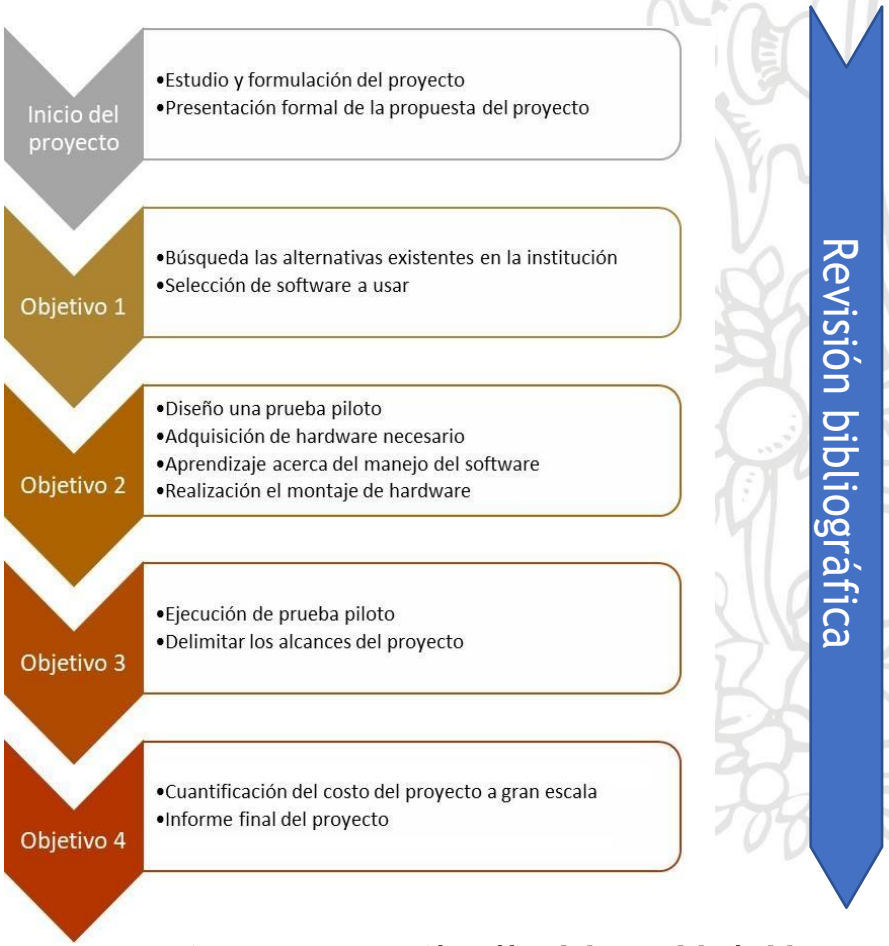

Figura 5. Representación gráfica de la metodología del proyecto

5.1 Estudio y formulación del proyecto

En un principio se realizó el contrato de prácticas académicas con la IPS Universitaria con la idea de realizar un desarrollo tecnológico que supliera alguna de las necesidades que se presentaban en la institución en aquel entonces; en una reunión con los coordinadores de docencia e ingeniería biomédica de la IPS se listaron una serie de necesidades de las cuales se tenía conocimiento o la idea de desarrollarla, entre estas: "Desarrollo de un aplicativo para el control de alimentación de pacientes", "Desarrollo de una aplicación móvil que permita modificar los permisos de visitas de estudiantes universitarios" y "Implementación de un sistema de control de acceso para servicios dentro de la institución".

En conversación con los asesores de práctica se decidió optar por el sistema de control de acceso, pero modificando el alcance del mismo, dado que este no era apto para ser realizado durante el tiempo proyectado para la práctica académica; la idea original que se había planteado por parte de docencia era ampliar el cubrimiento de un sistema de control de acceso que está instalado en el área administrativa de la sede León XIII de modo que fuera usado en todas las entradas principales y así poder tener un registro del tiempo que los empleados están dentro de la institución y cuales puertas son las más concurridas para el ingreso, también se pensó usar en el acceso a servicios que podría llegar a prestar la IPS como lo es la alimentación o refrigerios, préstamo de salas de reunión y acceso a áreas críticas dentro de la institución. A pesar de tener un planteamiento muy interesante, este es un proyecto demasiado grande como para ser diseñado e implementado durante una práctica académica, por esta razón se modificó el alcance del proyecto y se plantea entonces únicamente el diseño del control de acceso a la IPS y a áreas críticas.

5.2 Búsqueda las alternativas existentes en la institución

Dentro de la institución se consultó con el área de TICS (Tecnologías de Información y Comunicación) acerca del conocimiento de softwares implementados en la IPS que pudieran llegar a cumplir la función que se requiere suplir, de esta consulta se obtuvieron los datos de 2 softwares de control de edificios, los cuales poseían una licencia parcial de uso a través de proveedores externos, y un sistema de control de acceso autónomo con identificación biométrica por huella digital.
La primera de estas opciones evaluada fue el control de acceso autónomo, este dispositivo es el Anviz W2 el cual permite controlar una puerta con una gran variedad de formas de acceso, sin embargo, tiene una capacidad de usuarios limitada (3000) y su unidad controladora solo puede accionar una puerta, propiamente el dispositivo está diseñado para ser un control de acceso autónomo, con lo cual se complicaría el proceso de integrarlo a una red de control.
La siguiente opción es el software de control de edificios Honeywell EBI, este está instalado en dos puertas internas en la sede Prado de la IPS, sin embargo, en conversación con el personal de esta sede, el control en estas puertas está en desuso debido a que no todo el personal posee las tarjetas de acceso. Al tratar de obtener el contacto del proveedor del servicio se descubre que no hay un proveedor encargado de este, y ninguna de las áreas de la IPS tiene asignado la responsabilidad de este sistema, por lo que se descarta para el uso en este proyecto debido a la falta de soporte técnico.

La última opción de los softwares que posee la IPS es el Andover Continuum, al igual que el EBI es un software de control de edificios, este está implementado y se usa activamente en el piso administrativo, tiene una plataforma web con la cual se puede tener registro de las entradas y salidas, además de una interfaz gráfica que permite abrir y cerrar puertas

interactuando con un plano del piso en donde se encuentran. El primer acercamiento con el proveedor fue exitoso, se obtuvo una cotización para una asesoría técnica acerca del manejo del software y del valor de los dispositivos que se requieren por puerta, sin embargo, el proceso no avanzó. Posteriormente se tuvo conocimiento de un problema financiero con este proveedor, por lo que se cerró la plataforma web que se utilizaba comúnmente, aunque el sistema siguió funcionado con las tarjetas RFID no es posible ingresar nuevas tarjetas al sistema ni abrir las puertas por medio del software. Por lo tanto, este también fue descartado de los posibles sistemas a usar.
Con todo lo anterior se decidió con los asesores programar un código de control de acceso, que cumpliera con las necesidades para realizar la prueba piloto y así cumplir satisfactoriamente los objetivos del proyecto. Esta decisión da cumplimiento a la actividad 5: *Elección de sistema a usar, teniendo en cuenta las licencias disponibles para el proyecto*

5.3 Diseño de una prueba piloto

El objetivo de un sistema de control de acceso es, en su forma más básica, identificar correctamente a una persona que esté intentando cruzar el punto de acceso y otorgar o no acceso dependiendo de las autorizaciones que el usuario tenga asignadas. Con esto en mente se requiere un software que pueda:

- Identificar personas mediante el uso de tarjetas RFID
- Crear, actualizar y borrar usuarios.
- Tener una manera de mostrar claramente si el acceso fue permitido
- Conectarse a una base de datos
- Crear registro de la fecha y la hora de cada persona que cruce un punto de acceso.

Se utilizó un sistema de prototipado hecho por SparkFun, que funciona con tarjetas RFID, este se comunica de manera serial, por medio de puertos TX/RX o mediante el uso de USB, envía una cadena de caracteres con el número de identificación único de cada tarjeta. Con los requerimientos del software y teniendo disponible el dispositivo de SparkFun se decidió realizar un programa en lenguaje C# por su flexibilidad a la hora de trabajar con clases y la posibilidad de conectarse con bases de datos.

Para desarrollar el programa se usaron los programas de Microsoft Visual Studio 2017 para realizar el código en C# y el SQL Server Management Studio 2017 para crear las bases de datos; se usaron estos dos programas dado a que Microsoft provee licencias gratuitas a estudiantes universitarios y que estos programas son ampliamente utilizados por lo que ambos tienen un amplio soporte técnico, tanto por parte de Microsoft como desarrollador de estos como de la comunidad en foros públicos.

Para la ejecución de la prueba se usaron 3 tarjetas de identificación, cada una portada por una persona, la prueba se realizó en la puerta de la entrada de ingeniería biomédica de la IPS Universitaria, usando un computador portátil y el dispositivo de SparkFun. Cada una de las tres personas realizaría sus funciones diarias con la única modificación de registrar cada entrada y salida al área de ingeniería colocando su tarjeta de identificación en la lectora y también registrándose de forma manual en una tabla, esto con el fin de realizar un comparativo y verificar que todos los registros estuvieran completos.

6 Resultados y análisis

En esta sección se presentan los resultados obtenidos durante todo el proyecto acorde a como se plantearon las actividades en pos del cumplimiento de los objetivos específicos; por lo tanto, se hace menciona primero la actividad y luego las acciones que se tomaron para completar la misma, con sus respectivos resultados y análisis.

6.1.1 Desarrollo del programa

En la Figura 6 podemos ver la interfaz de programación de Visual Studio 2017 con un fragmento del código desarrollado, en las Figura 7,Figura 8 y Figura 9 podemos ver la interfaz de usuario del programa desarrollado, este está diseñado de modo que cumpla los requerimientos previamente mencionados, en la pestaña "Conexión" se configura y conecta de manera manual la conexión serial con el dispositivo SparkFun, en la pestaña "Usuarios" se puede administrar la base de datos de personas, agregar, eliminar y modificar todos los campos que allí se tienen. En la pestaña "Ingreso" se puede ver la base de datos de registro y control, así como un claro indicador del acceso.

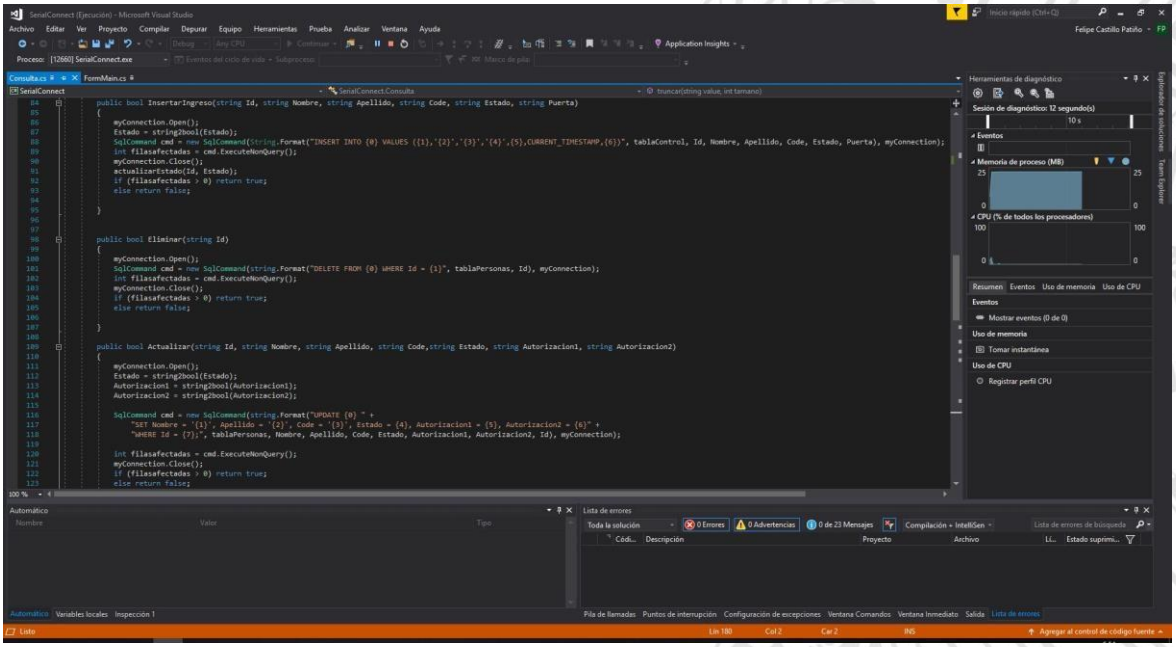

Figura 6. Interfaz de usuario de Visual Studio 2017

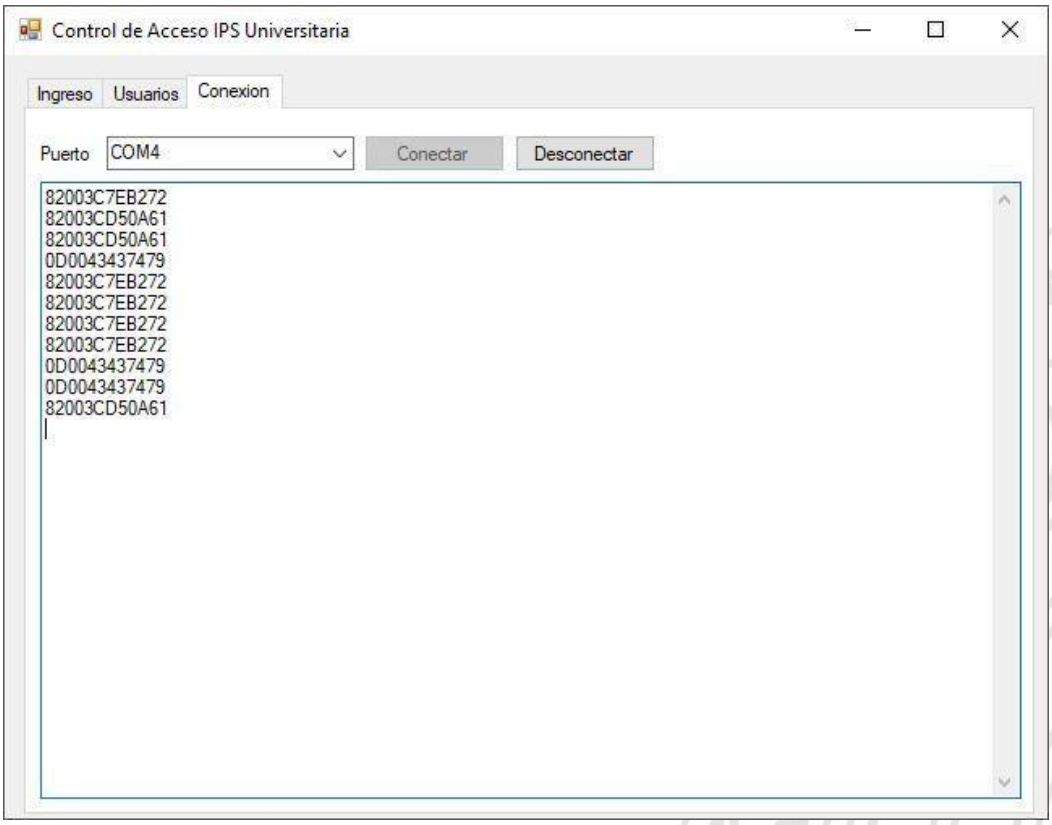

Figura 7. Pestaña "Conexión" del programa

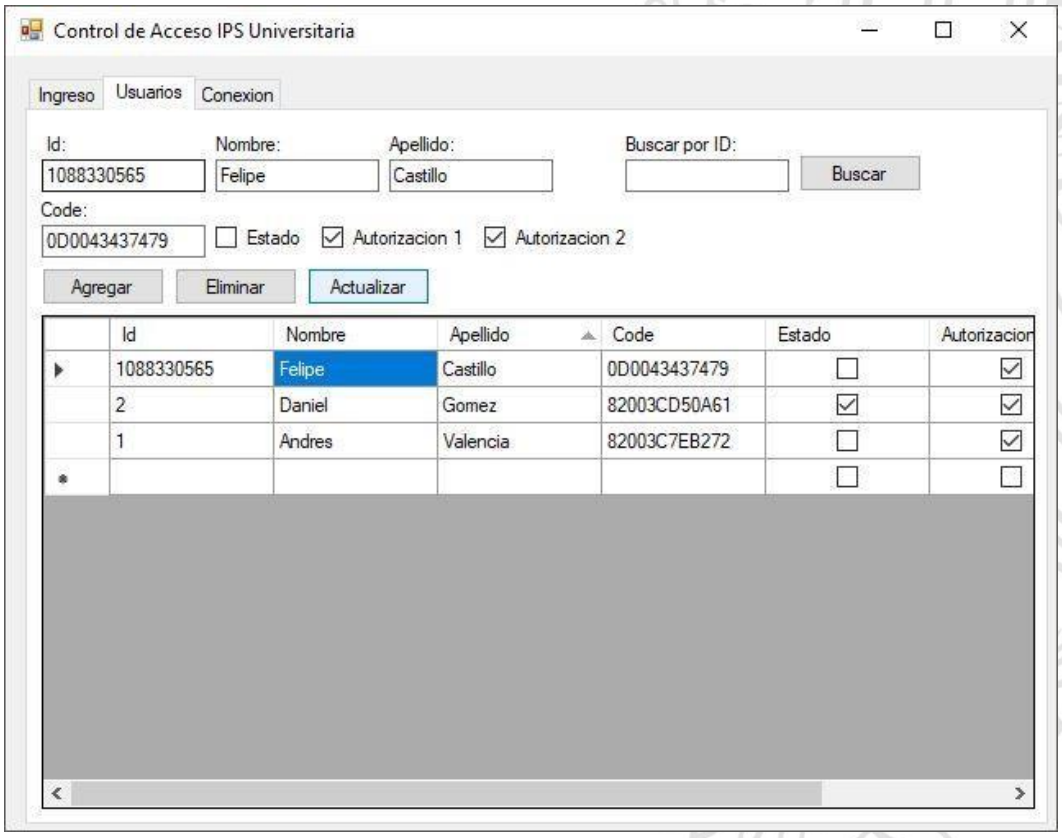

Figura 8. Pestaña de "Usuarios" del programa

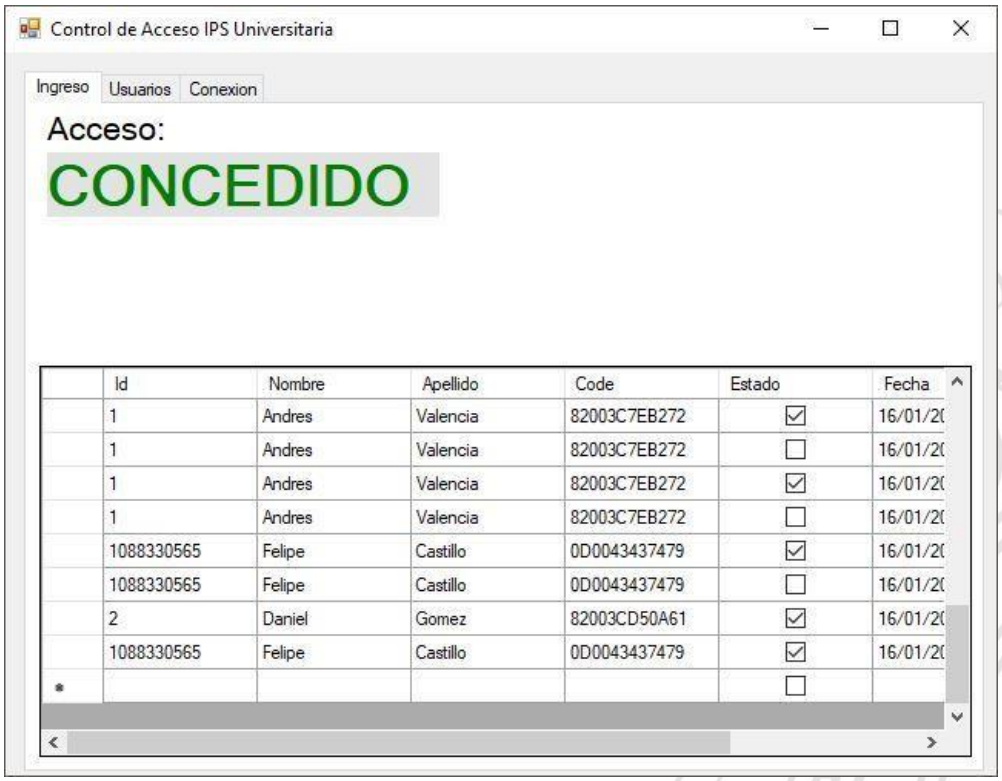

Figura 9. Pestaña de "Ingreso" del programa

El programa anteriormente mostrado se enlaza a unas bases de datos soportadas en Microsoft SQL Server y administradas a través del software SQL Server Management Studio 2017, su interfaz se puede ver en la Figura 10.

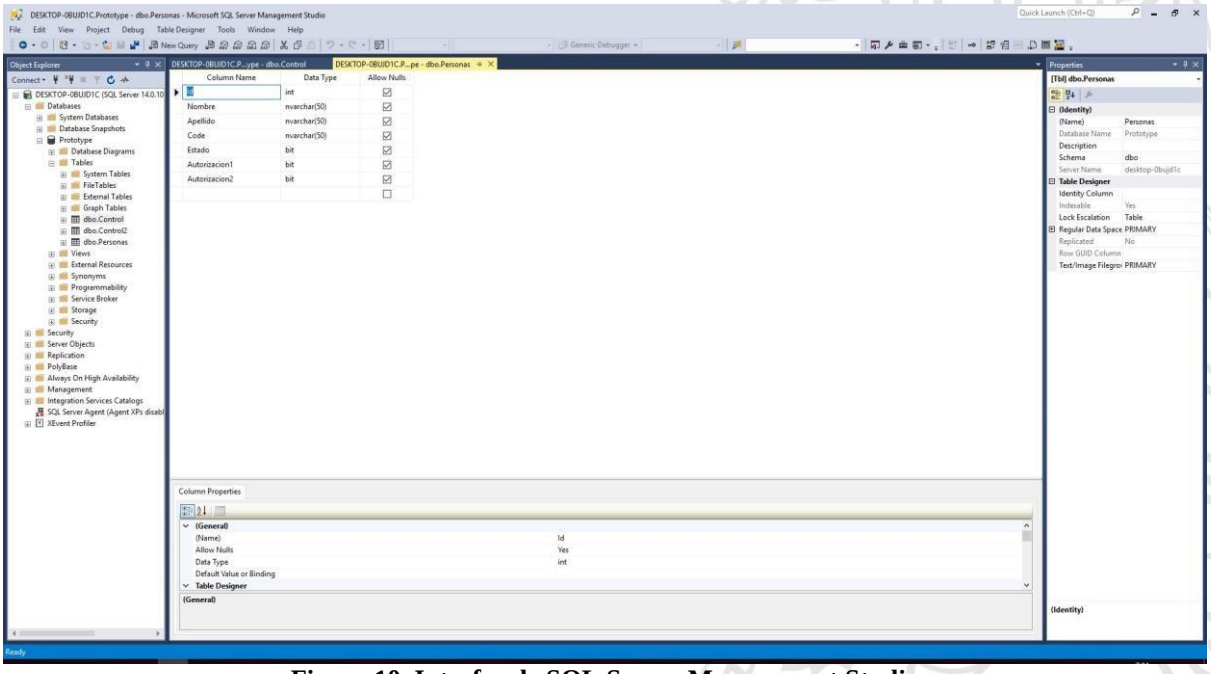

Figura 10. Interfaz de SQL Server Management Studio

Para de alguna manera ilustrar el procedimiento lógico que usa el programa desarrollado se presenta la Figura 11, se inicia el programa, en un primer momento se debe conectar con el dispositivo de SparkFun, para esto se elige el puerto en el cual se encuentra y se da click al

botón conectar; una vez hecho esto las pestañas de “Ingreso” y “Usuario” quedan completamente habilitadas para su uso, en la Figura 11 se muestra el proceso dentro de la pestaña de “Ingreso”, cuando se acerca una tarjeta a la lectora, esta capta la cadena de caracteres propia de la tarjeta y busca en la base de datos la persona que tenga asignado este código, en caso de no encontrar nada el programa deniega el acceso inmediatamente, si se encuentra la persona se verifica que tenga la autorización pertinente, si la posee se cambia el acceso a “Concedido” y se ingresa una nueva entrada en la base de datos, con toda la información de la persona que ingresó y se incluye la hora a la que ingresó y que puerta utilizó. En la pestaña de “Usuario” no hay un flujo lógico, simplemente son acciones que puede implementar el usuario al llenar los campos y oprimir un botón de aquellos que están disponibles

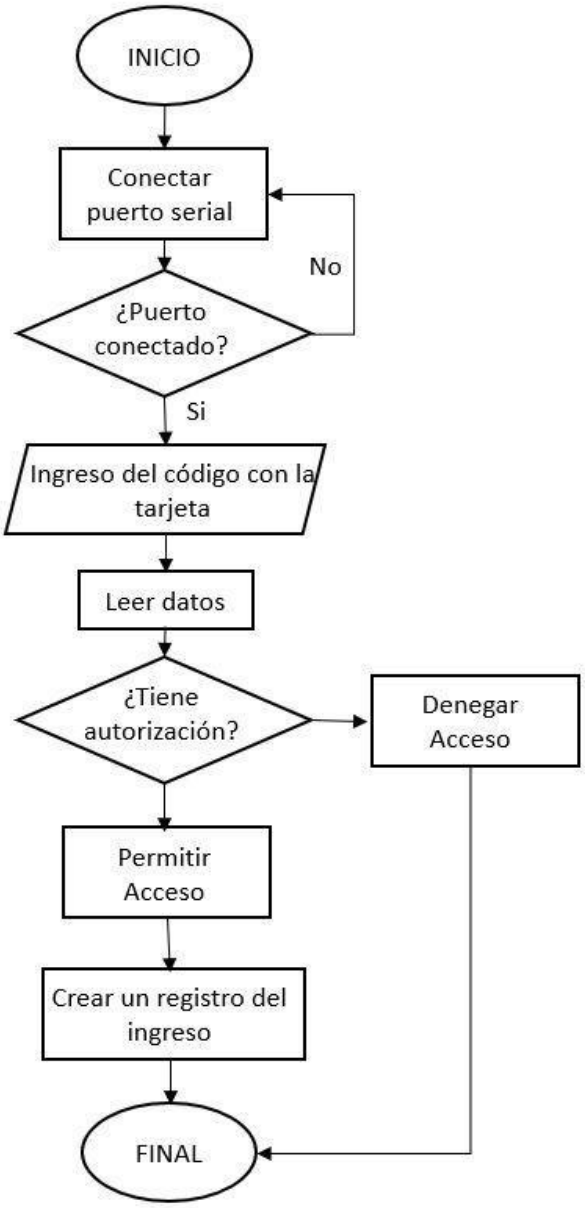

Figura 11. Diagrama de flujo del programa

6.1.2 Ejecución de la prueba

Pasada una jornada de diez horas (7am a 5pm) se cierra el programa y se guarda la tabla de registros manual. Una revisión posterior da cuenta de 25 registros, contando entradas y salidas de las 3 personas, todas estas estuvieron correctamente registradas en el programa. Con la realización de esta prueba se puede inferir que con las indicaciones adecuadas del uso del programa no debería de haber ningún problema en el uso de este en cualquier tipo de punto de acceso. Adicional a esto, las bases de datos en servidores tienen capacidades de almacenamiento del orden de los petabytes, por lo cual la capacidad de almacenamiento de registros y de usuarios es prácticamente ilimitada con lo cual la cantidad de datos no es un problema. En la se observa de manera resumida la información que se obtuvo durante la prueba piloto.

Tabla 1. Resumen de la prueba piloto

Ítem	Cantidad
Número de Personas	3
Tiempo de ejecución de la prueba	10 horas
Puntos de acceso	1
Número de accesos realizados	25
Número de accesos registrados	25
Efectividad	100%

Como parte del ejercicio de la prueba, se planteó realizar pruebas in situ, es decir, ir a los servicios en cuestión, dar las tarjetas al personal y vigilar que las personas que entren o salgan realicen correctamente el registro, no obstante, esto no se pudo realizar debido a problemas logísticos; sin embargo, para los servicios que se definieron de forma particular se tiene un bosquejo del plano arquitectónico y las rutas que sigue el personal asistencial para acceder a estas áreas, en la Figura 12 se aprecia el área de urgencias, las flechas de color rojo representan la movilidad de los pacientes, desde que ingresan (1), esperan su turno en la sala de espera (2), pasan al triage (3) y dependiendo de su condición son llevados a la sala de críticos (4); las flechas de color azul representan la ruta de acceso del personal asistencial, el ingreso a la clínica de estos es por el piso uno del bloque tres desde donde se deben desplazar por corredores hasta llegar a las escaleras que conducen al semisótano, en donde se encuentra urgencias y posteriormente deben caminar al área de críticos siguiendo la ruta.

Es muy importante conocer las rutas por las cuales se desplaza el personal, esto para tener en cuenta el flujo de personas que puede pasar por determinado punto de acceso y así tomar decisiones acerca de que tan restringida debe ser la seguridad en algún punto en particular. En la Figura 13 se puede ver la ruta que se debe tomar para entrar al área de cirugía, se toman las escaleras (1) desde el cuarto piso hasta el quinto una vez allí se llega a un corredor (2) donde en algún momento funcionó el sistema de control Anviz W2, se pasa por el vestier y una vez vestido con la indumentaria adecuada se ingresa al área de cirugía (4). Es importante resaltar que dentro de esta última área no debe haber sistemas de control de acceso por temas de sanidad.

Figura 12. Rutas de acceso en el área de urgencias

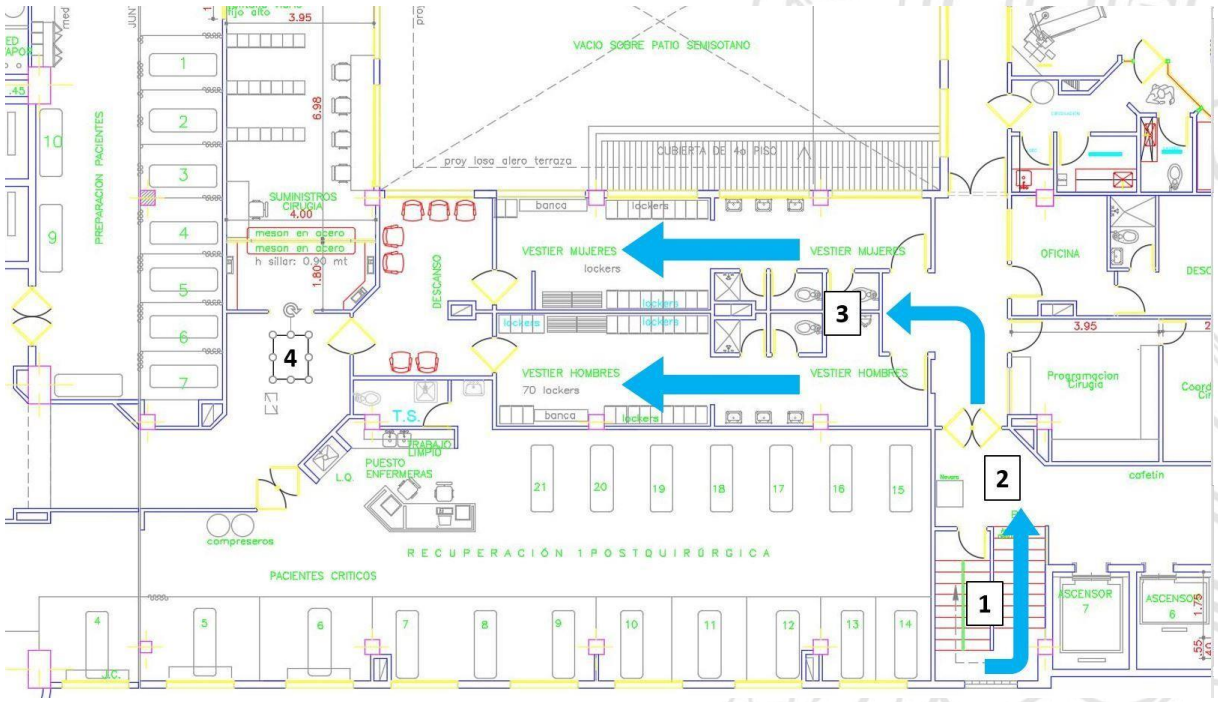

Figura 13. Rutas de acceso en el área de cirugía

6.1.3 Análisis de la prueba

Teniendo en cuenta que los registros se realizan de una manera exitosa y sin contratiempos en la base de datos, que la cantidad de usuarios es prácticamente ilimitada, al igual que la cantidad de registros que se pueden hacer; se puede decir que el sistema es eficaz para registrar la entrada a un área restringida, sin embargo, se debe tener en cuenta que la colaboración de los usuarios es de vital importancia, dado que en este proyecto no se tuvo la posibilidad de interactuar con un sistema de bloqueo de puertas tipo cerradura electrónica o electroimán, por lo que el control de acceso debe ser realizado por un integrante de la seguridad del hospital o se debe adaptar el sistema para interactuar con un dispositivo que permita manejar el acceso de una puerta.

6.2 Proyección de las necesidades de implementación

Como se mencionaba anteriormente la implementación de este proyecto tiene una cantidad considerable de requerimientos para poder funcionar de forma fluida y ordenada, sin errores en la ejecución y con el menor impacto para la cotidianidad del personal, primero se mencionarán los requerimientos técnicos y un estimado de precios de lo que costarían los dispositivos para ser implementados, luego los requerimientos locativos.

6.2.1 Requerimientos técnicos

Se parte de la premisa de que el sistema se implementará tal cual se desarrolla en este proyecto, es decir no se añadirá ningún dispositivo como cerradura o electroimán, esto con el fin de omitir los costos y la proyección de lo que sería el desarrollo del acople entre este nuevo dispositivo y el sistema. Para que el sistema funcione se debe tener un dispositivo que tenga la capacidad de ejecutar archivos ".exe", que posea puertos USB o posibilidad de conexión serial para interactuar con la lectora de SparkFun, con lo anterior en mente surge la idea de las RaspberryPi, estos dispositivos poseen microprocesadores y tienen funcionamiento basado en linux, pines de conexión serial y puertos USB; como un añadido permite usar una versión de máquina virtual de Windows, lo que permitiría ejecutar sin ningún problema el programa desarrollado. Después vendría el dispositivo de SparkFun, el cual ya esta testeado y no necesita de mayor adaptación para que funcione en conjunto con la Raspberry Pi; se necesita también una pantalla para mostrar el programa y que se pueda dar la realimentación visual del sistema, por lo que se proyecta una pantalla touchscreen, de modo que el método de entrada del dispositivo sea la misma pantalla.

La IPS Universitaria en su sede León XIII tiene cinco accesos peatonales habilitados para la entrada del personal, dos accesos en el bloque 1, un acceso en el bloque 2 y 2 accesos en el bloque 3; a los accesos mencionados se suman los puntos de acceso de la sala de críticos en urgencias y la entrada al área de cirugía son siete puntos de acceso. En la Tabla 2 se muestran los precios de los dispositivos previamente mencionados, con una cantidad inicial de 100 usuarios y 7 puntos de acceso. Basado en las Figura 12 y Figura 13, se evidencian distintos requerimientos para estas áreas; primero la restricción especial del personal que ingresa, los pacientes que están en las áreas en mención tienen una condición de salud crítica y requieren cuidados específicos, por lo que el acceso debe ser solo concedido al personal asistencial asignado a esa área, es decir, aunque una persona tenga autorización para ingresar a la institución puede no tener permiso para entrar a las áreas en mención si no está asignada a ellas, por lo que se requieren campos de autorización para críticos en urgencias, y el ingreso al

área de cirugía. Pensando también en los acompañantes de los pacientes, se puede crear un enlace entre la base de datos de los pacientes ingresados y una cantidad limitada de acompañantes que puedan entrar, esto para el área de urgencias, con el fin de mantener un registro de quién cruza por el punto de acceso y de las personas que están dentro del área de críticos en un determinado momento del día.

Tabla 2. Precios de dispositivos

Ítem	Precio (USD)	Cantidad	Precio total
Raspberry Pi 3	35	7	245
SmartiPi Touch case	28	7	196
Sparkfun RFID Kit	51,95	7	363,65
Tarjeta RFID	1,95	100	195
		Total (USD)	999,65

6.2.2 Requerimientos locativos

Para la implementación de este proyecto se necesitan como mínimo 7 nuevos puntos de acceso de cable de red con conexión a la intranet de la IPS Universitaria, no se puede dar un precio exacto de este proceso, dado que cada punto requiere su estudio, distancia de cables a enrutadores y modificaciones estructurales; por otro lado, el aprovisionamiento del servidor, es decir, la creación de las bases de datos y las credenciales de usuario para cada uno de los puntos de acceso.

7 Conclusiones

Se realizó una evaluación e investigación juiciosa acerca de los softwares y dispositivos presentes en la IPS universitaria y se concluyó que en todos los casos no se tenía la disponibilidad de para utilizar los recursos propios de la IPS, por lo tanto, se opta por la realización de un programa que cumpliera con las necesidades de la institución, con esto en mente se desarrolló un sistema de control de acceso que cumple con todas las necesidades planteadas para las áreas de urgencias y cirugías, así como para los ingresos normales de la institución., posterior a esto se diseña y ejecuta una prueba piloto, esta fue llevada a cabo en el área de ingeniería, en donde se comprueba la eficacia del software para crear registros de llegada y salida de una persona a un área correctamente delimitada.

Como un resultado obtenido durante la ejecución de la prueba se observa que la colaboración del personal en el momento de ser implementada esta solución es de vital importancia, dado que la veracidad de la información que se pueda obtener del software depende directamente de que tan estricto se sea a la hora de registrar las entradas o salidas que se realicen. La implementación de este software tiene un costo relativamente bajo con respecto a los otros sistemas, sin embargo, este sistema no es tan robusto como sus competidores, dado que no tiene tarjetas de 13,56MHz, que pueden almacenar una gran cantidad de información, como lo son los datos personales de cada una de las personas que posee una tarjeta.

Para un trabajo a futuro se propone realizar una prueba inicial con personal asistencial de la institución, se pueden adquirir tarjetas y dos puntos de acceso, con lo cual sería suficiente para probar en su totalidad la capacidad del software, la implementación debe ser durante al menos una semana, para obtener datos suficientes y cubrir todas las posibilidades dentro del sistema. Una vez realizado esto se puede obtener retroalimentación de los usuarios y mejorar el software para una implementación completa en la institución.

8 Referencias Bibliográficas

[1] E. Valero, A. Adán, and C. Cerrada, "Evolution of RFID Applications in Construction: A Literature Review.," *Sensors (Basel).*, vol. 15, no. 7, pp. 15988–6008, Jul. 2015.

[2] S. Rijal, "RFID Technology in Logistical Activities."

[3] J. Israelslaan, "RADIO RADIO FREQUENCY FREQUENCY IDENTIFICATION (RFID) IN HEALTHCARE BENEFITS, LIMITATIONS, AND RECOMMENDATIONS."

[4] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, Third Edition*, 3rd ed. West Sussex: Wiley, 2010.

[5] J. Dalton, C. Ippolito Autentica, and S. Rossini, "Using RFID Technologies to Reduce Blood Transfusion Errors," 2005.

[6] "Radio-frequency identification: its potential in healthcare.," *Health Devices*, vol. 34, no. 5, pp. 149–60, May 2005.

[7] M. M. Pérez, G. V. González, and C. Dafonte, "The Development of an RFID Solution to Facilitate the Traceability of Patient and Pharmaceutical Data," *Sensors*, vol. 17, no. 10, p. 2247, Sep. 2017.

[8] H. F. Giraldo, "Plan Estratégico IPS Universitaria 2017-2026." [Online]. Available: http://www.ipsuniversitaria.com.co/es/quienes-somos/plataforma-estrategica/plan-estrategico-2017-2026.

[9] "Seguridad - Andover Continuum | Schneider Electric." [Online]. Available: https://www.schneider-electric.com.co/es/product-range/6823-andover-continuum/?subNodeId=210029152es_CO.

[10] C. Buildings, "Enterprise Buildings Integrator R500 Table of Content."

[11] "EBI R500." [Online]. Available: https://www.ebi.honeywell.com/en-US/Pages/EBI-R500.aspx.

[12] "Access Control Systems - Secure Physical Access Cards." [Online]. Available: https://www.hidglobal.com/access-control.

[13] K. Finkenzeller, *RFID HANDBOOK FUNDAMENTALS AND APPLICATIONS IN CONTACTLESS SMART CARDS, RADIO FREQUENCY IDENTIFICATION AND NEAR-FIELD COMMUNICATION, THIRD EDITION*. 2010.

[14] "Espectro Radioeléctrico | CONATEL." [Online]. Available: http://www.conatel.gob.ve/espectro-radioelectrico/. [Accessed: 20-Jan-2019].

[15] "¿Como funciona un Sistema RFID UHF?" [Online]. Available: http://www.dipolerfid.es/es/blog/Como-Funciona-Sistema-RFID-UHF.

[16] J. L. Pañar, "Qué es RFID y cómo funciona | TAKTIC." [Online]. Available: https://taktic.es/que-es-rfid-y-como-funciona/.

[17] N. Sclater, "COMPUTER TECHNOLOGY," in *Electronic Technology Handbook*, McGraw-Hill Professional, 1999.

[18] "USB (Universal Serial Bus) Definition." [Online]. Available: https://techterms.com/definition/usb.

[19] "What is a Universal Serial Bus (USB)? - Definition from Techopedia." [Online]. Available: https://www.techopedia.com/definition/2320/universal-serial-bus-usb.

[20] "SparkFun RFID Starter Kit - KIT-13198 - SparkFun Electronics." [Online]. Available: https://www.sparkfun.com/products/13198.

[21] C. S. Fingerprint, "Color Screen Fingerprint & RFID Access Control," pp. 2–3.

[22] "Anviz W2 | Lector Biométrico Autónomo." [Online]. Available: https://www.visiotechsecurity.com/es/productos/control-de-accesos/anviz/control-de-acceso/w2-detail#tab=prod_0. [Accessed: 20-Jan-2019].

[23] "Anviz Global - Intelligent.Security." [Online]. Available:

https://www.anviz.com/product/77.html.
[24] R. Elmasri and S. Navathe, "The worlds of database systems," in *Fundamentals of database systems*, Pearson, 2011, p. 1172.
[25] D. Systems, "Introduction to Database Concepts," p. 64, 2007.
[26] "SQL Server 2017 on Windows and Linux | Microsoft." [Online]. Available: https://www.microsoft.com/en-us/sql-server/sql-server-2017. [Accessed: 20-Jan-2019].