Diseño, fabricación e implementación de un control de acceso para ascensores en la clínica Medilink

Argemiro Eliecer Amézquita Jiménez

Director

Adriana Del Pilar Noguera Torres.

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas, Tecnología e Ingenierías ECBTI

Ingeniería Electrónica

2024

Resumen

El presente documento aborda el diseño, la fabricación y la implementación de un sistema de control de acceso para los ascensores en la clínica Medilink, en Yopal, Casanare. Este proyecto fue creado con el objetivo de seguir manteniendo el control sobre el ascensor camillero, al mismo tiempo que aumentar la eficiencia y priorizar el transporte del personal médico y los pacientes en situaciones críticas.

Los dispositivos fueron diseñados para gestionar el acceso de hasta 100 usuarios, disminuir el acceso no autorizado y garantizar la disponibilidad del ascensor para las situaciones más críticas. Se utilizó tecnología RFID y microcontroladores programables en un diseño robusto y adaptable al entorno hospitalario. Durante la fase de fabricación, se fabricaron tarjetas electrónicas optimizadas, y los componentes fueron configurados para asegurar la confiabilidad y la durabilidad del sistema. Posteriormente, se llevó a cabo la implementación, en la que se hicieron ajustes en las botoneras del ascensor y pruebas para verificar la operación e integración clínica.

Como resultado, se puede afirmar que el sistema cumple los objetivos propuestos. Propone la importancia de aplicar tecnología avanzada en situaciones críticas, y promueve la autenticación multifactorial y un análisis en tiempo real como futuras áreas de mejora para asegurar la sostenibilidad a largo plazo.

Palabras clave: RF, Microcontrolador, Control de Acceso

Abstract

This document addresses the design, manufacture and implementation of an access control system for the elevators at the Medilink clinic in Yopal, Casanare. This project was created with the objective of continuing to maintain control over the stretcher elevator, while increasing efficiency and prioritizing the transportation of medical personnel and patients in critical situations.

The devices were designed to manage access for up to 100 users, decrease unauthorized access and ensure the availability of the elevator for the most critical situations. RFID technology and programmable microcontrollers were used in a robust and adaptable design for the hospital environment. During the manufacturing phase, optimized electronic cards were manufactured, and the components were configured to ensure the reliability and durability of the system. Subsequently, the implementation was carried out, in which adjustments were made to the elevator button panels and tests were performed to verify the operation and clinical integration.

As a result, it can be affirmed that the system meets the proposed objectives. It proposes the importance of applying advanced technology in critical situations and promotes multifactor authentication and real-time analysis as future areas of improvement to ensure long-term sustainability.

Keywords: RFID, Microcontroller, Access Control

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

Los sistemas de control son herramientas utilizadas para garantizar el control y la seguridad de instalaciones cruciales, tales como hospitales, instituciones educativas y oficinas corporativas. Favorecen la regulación del flujo de entrada y salida de personas a áreas determinadas gracias a sus tres principios fundamentales. Estos pilares son la autenticación, la autorización y la auditoría. La autenticación comprueba la identidad de los usuarios a través de credenciales, como tarjetas RFID, códigos PIN, registros biométricos o aplicaciones móviles, para evitar que el acceso a usuarios no esté registrado en los sistemas. La autorización determina los permisos otorgados según su puesto de trabajo o situación. La auditoría registra y rastrea todas las actividades de la persona, creando trazabilidad y seguridad general. (Cristaldo, 2023)

Tecnologías de autenticación se han multiplicado con el tiempo a medida que la tecnología se ha vuelto más avanzada para responder a los desafíos de los entornos cada vez más complejos. En particular, la biometría y la autenticación de usuario basada en aplicaciones móviles son especialmente precisas y fáciles de usar. De acuerdo con (Xie, 2014) y (Sánchez Gómez, 2020), en ambas imprescindibilidades, los sistemas de aseguramiento evitan un fraude potencial mediante la verificación de características biológicas o conductuales específicas de los individuos, como huellas dactilares o características faciales exclusivas. Los enfoques clásicos en la autenticación, irónicamente, sin embargo, los métodos antiguos como las etiquetas RFID continúan siendo utilizados ya que son prácticos y eficaces. Sin embargo, para evitar su uso indebido en caso de robo o extravío, deben implementarse salvaguardias adicionales.

En cuanto a los entornos hospitalarios, donde la seguridad y la velocidad de los servicios prestados son críticos, los sistemas de control de acceso deben realizarse sin alterar las operaciones diarias de un entorno tan crítico. No solo esta tecnología protege áreas sensibles,

sino que también ayuda a mejorar la eficiencia garantizando que el personal solo tenga acceso a las áreas necesarias para llevar a cabo sus tareas. Esa prestación, que en efecto mejora dentro de la gestión de cualquier institución, también garantiza la seguridad del paciente y del personal, lo que se suma a la adhesión a las leyes y regulaciones de privacidad y seguridad.

El elevador de camillas de la Clínica Medilink en Yopal, Casanare, fue elegido como prototipo para implementar un sistema de control de acceso con tecnología RFID. El objetivo de este proyecto fue diseñar, fabricar e instalar un sistema que garantice el libre acceso del caudal múltiple de emergencias, minimice el uso sin autorización y refuerce la seguridad en un ambiente crítico hospitalario. Dentro del alcance del proyecto se llevó a cabo desde el diseño de las tarjetas electrónicas hasta la formación al personal y su integración suave en la clínica.

El presente documento consta de diversas secciones en las cuales se desarrolla el proyecto y se describen los resultados obtenidos. En primer lugar, en el marco teórico, se definen las bases de los sistemas de control de acceso a espacios y los lineamientos de diseño de dispositivos de seguridad. Luego, se describe la metodología empleada y los resultados, su análisis y una discusión de los resultados que los enmarcan en base a los objetivos planteados. Por último, se presentan las conclusiones, propuestas de recomendaciones para futuros trabajos y propuestas de mejoras en el sistema implementado.

Tabla 1

Tipos de Sistemas de Control de Acceso y Sus Características

Tipo de Sistema de Control de Acceso	Descripción	Ventajas	Desventajas
Tarjetas de Proximidad (RFID) (Zhang, 2021)	Los usuarios presentan una tarjeta RFID válida ante un lector para desbloquear el acceso.	Rápidas, económicas y fáciles de usar.	Pueden perderse o ser copiadas.
Teclados y Códigos PIN (hen, 2020)	Los usuarios ingresan un código PIN para acceder a áreas restringidas o pisos específicos.	Sencillos y sin necesidad de dispositivos.	Vulnerables si el código no se cambia frecuentemente.
Biometría (Bolle, 2020)	Identificación mediante características físicas únicas (huella, rostro, iris) de los usuarios.	Alta seguridad y personalización.	Costosos y requieren mantenimiento regular.
Aplicaciones Móviles y Bluetooth (Kim, 2022)	Acceso mediante una app en el celular que se conecta al sistema por Bluetooth.	Convenientes y modernas.	Requieren dispositivos compatibles.

Nota. Se describe los diferentes sistemas de acceso.

Justificación

La Clínica Medilink ha estado en constante evolución en su camino para mejorar la calidad de la atención brindada a sus usuarios y mejorar el entorno de trabajo para su médico personal. La seguridad y el control en áreas de uso común, como los ascensores, han sido pilares fundamentales en la prestación de este tipo de atención, ya que su uso ha sido crítico para la movilización de pacientes hospitalizados, pacientes en sillas de ruedas y un rápido. acceso en situaciones de emergencia por parte del personal de salud.

Entre los problemas a los que se enfrentaba la clínica se incluía la falta de un sistema de control de acceso específico para los ascensores. El uso no autorizado de estos recursos, así como el mal uso, ha disminuido la eficiencia del propio servicio y ha hecho perder el tiempo a las personas por la necesidad de hacer cola para ser "atendidas". En situaciones críticas, algunas personas no tenían acceso rápido a los ascensores cuando realmente se necesita; por lo tanto, dichos dispositivos deben permitir a los empleados y a las personas con emergencias de salud que ascendieran rápidamente.

Además, estos dispositivos no solo han beneficiado a la Clínica Medilink, sino que también se perfilan como un modelo adaptable a otras instituciones de salud que han enfrentado problemas similares de seguridad y flujo de personas. El diseño y fabricación de estos dispositivos, enfocado en las necesidades de un entorno hospitalario, ha permitido una gestión más efectiva del acceso y, en consecuencia, ha contribuido a la creación de un ambiente más seguro y organizado para todos.

Objetivos

Objetivo General

Implementar una tarjeta RF para el control de acceso en el ascensor camillero en la clínica Medilink para 100 usuarios.

Objetivos Específicos

Documentar la información de primera y de segunda mano para el diseño de la tarjeta.

Diseñar las condiciones físicas, electrónicas y funcionales de la tarjeta RF para control de acceso de ascensores.

Implementar la tarjeta RF para control de acceso en el elevador camillero en la clínica Medilink.

Marco Teórico

El control de acceso es esencial para garantizar la seguridad en una amplia variedad de ubicaciones, especialmente en aquellas consideradas críticas, como hospitales, universidades y colegios, instalaciones gubernamentales y oficinas corporativas. En general, el propósito de un sistema de control de acceso es controlar quién puede o no puede ingresar a través de las puertas, y lo hace basándose en tres pilares fundamentales: autenticación, autorización y auditoría. La autenticación, o principio de identificación, afirma que solo los usuarios registrados pueden hacer un intento de acceso para un área restringida. La autorización, o principio del derecho, significa que los usuarios autorizados pueden acceder a una puerta a través de ciertas condiciones fijas y situaciones dinámicas. La auditoría significa que un sistema de control de acceso debería tener la capacidad de monitorear y registrar todas las acciones. La auditoría proporciona trazabilidad y protección más estricta.

El desarrollo de tecnologías dictó la creación de métodos avanzados de autenticación basados en la prueba de biometría y la implementación de aplicaciones móviles, que se caracterizan por alta precisión, seguridad y practicidad. (Xie, 2014) y (Sánchez Gómez, 2020) enfatizan que estas herramientas son particularmente necesarias en lugares donde el acceso está restringido, tal como hospitales, donde la biometría permite la autenticación única de la identidad de usuario y reduce la posibilidad de su suplantación. Por otro lado, la tarjeta de identificación de radiofrecuencia ha demostrado ser una solución accesible y utilizada para el acceso a los edificios públicos y privados. Sin embargo, requiere la adopción de medidas exacerbadas en caso de su pérdida. Es común que los sistemas de control de accesos también se utilicen en varios entornos para proteger las áreas críticas de la actividad y facilitar el trabajo mediante la adopción de medidas especiales.

Fundamentos de los Sistemas de Control de Acceso

Los sistemas de control de acceso son esenciales en la seguridad de diversas instalaciones, ya que determinan quién puede ingresar o salir de un área específica. Estos sistemas cumplen con tres funciones principales: autenticación, autorización y auditoría, las cuales trabajan en conjunto para fortalecer la seguridad.

Autenticación

La primera etapa dentro de los sistemas de control de acceso es la autenticación, cuyo objetivo es comprobar si la persona que intenta ingresar al área restringida es realmente quien dice ser. Puede expresarse de manera simple con la siguiente pregunta: ¿esta persona es quien dice ser? para responder a la interrogante, se utilizan credenciales de un u otro tipo. Las credenciales son características singulares que hacen únicos a los elementos y a las personas.

Por el contrario, la autenticación biométrica se ha convertido en la mejor opción debido a su alta precisión y seguridad, que reduce en gran medida el riesgo del análisis de la persona. (Xie, 2014) destacan que las características biométricas, como el reconocimiento facial y las huellas dactilares, son difíciles de predecir, lo que otorga a esta opción una ventaja significativa sobre los métodos generales. Además, (Sánchez Gómez, 2020) señala que esta autenticación no solo asegura la exclusividad de la identificación, sino que también habilita el acceso controlado a los espacios críticos, como los hospitales, lo que implica el permiso de ingreso solo para personal autorizado.

Entre las formas de autenticación más comunes se encuentran las tarjetas de proximidad (RFID), los códigos PIN, los datos biométricos (huellas dactilares, reconocimiento facial) y las aplicaciones móviles. Cada una de las opciones anteriores, tienen sus propias ventajas y desafíos en términos de seguridad y facilidad de uso.

Tarjetas de Proximidad (RFID)

Una de las formas más comunes de autenticación son las tarjetas RFID que contienen un chip que se comunica con un lector cercano. De acuerdo con (Hussain, 2023) los sistemas de autenticación por tarjetas RFID son comunes debido a que se puede emparejar cada tarjeta con un usuario. Debido a no siempre se cuentan con recursos para hacer un registro individual de cada tarjero permanente, pero, por ejemplo, en espacios compartidos o frecuentemente visitados como oficinas, edificios públicos, etc., esta opción puede ser muy útil. Las tarjetas RFID para los usuarios son prácticas porque simplemente tienen que acercar la tarjeta al lector para ser autenticadas, y el sistema puede rastrear su tiempo de llegada además de su identidad. Sin embargo, estas tarjetas se deben proteger, porque otra persona puede tomarla y pedirla usado como acceso.

Códigos PIN. Otra opción común es el uso de códigos PIN, que el usuario debe ingresar en un teclado para desbloquear el acceso. Esta es una solución sencilla, que no requiere un dispositivo adicional, y que puede ser práctica en áreas donde el acceso es menos crítico. Sin embargo, este método puede volverse inseguro si los códigos no se cambian con frecuencia o si se comparten entre varias personas. A diferencia de las tarjetas RFID, que son "físicas," los códigos PIN solo requieren que el usuario recuerde una secuencia de números, lo que es útil, pero presenta riesgos de seguridad.

Biometría. En los últimos años, la autenticación biométrica ha ganado popularidad debido a su alto nivel de seguridad. Este tipo de autenticación se basa en características físicas únicas de cada persona, como sus huellas dactilares, el rostro, o el iris. (Xie, 2014) destacan que las características biométricas son difíciles de replicar o falsificar, lo cual hace que este método sea muy seguro. Además, a diferencia de las tarjetas o los códigos PIN, la biometría no puede ser

olvidada o perdida, lo cual la convierte en una opción ideal en entornos donde se necesita un control muy estricto. (Sánchez Gómez, 2020) agrega que en hospitales y otros lugares críticos, el uso de biometría facilita que solo los usuarios autorizados ingresen a áreas sensibles, ayudando a evitar riesgos asociados con el acceso no autorizado.

Aplicaciones Móviles. Una forma más reciente de autenticación es mediante aplicaciones móviles, que se conectan al sistema de acceso a través de tecnología Bluetooth. Este método permite que el usuario utilice su teléfono como una "llave virtual," lo que resulta práctico para personas que ya están acostumbradas a llevar el móvil consigo todo el tiempo. Además, estas aplicaciones pueden ofrecer autenticación de múltiples factores, como combinar la verificación mediante PIN y biometría, aumentando la seguridad. Sin embargo, este sistema depende de que los usuarios tengan dispositivos móviles compatibles y de que la conexión funcione correctamente.

Autorización

La autorización es el paso que sigue a la autenticación en un sistema de control de acceso. Una vez que un usuario ha sido identificado, la autorización determina a qué áreas o recursos puede acceder esa persona y en qué condiciones. En otras palabras, si la autenticación responde a la pregunta "¿Quién eres?", la autorización responde a "¿Qué estás autorizado a hacer?"

Este proceso es fundamental para la seguridad, ya que no todos los usuarios necesitan el mismo nivel de acceso. En un hospital, por ejemplo, el personal médico podría tener autorización para acceder a áreas restringidas, mientras que el personal administrativo solo podría ingresar a ciertos sectores. Al gestionar los permisos de acceso en función del rol de cada persona, el

sistema de control de acceso garantiza a solo aquellos que realmente necesitan ingresar a ciertas áreas puedan hacerlo.

Existen diferentes maneras de configurar la autorización en un sistema de control de acceso:

Autorización Basada en Roles. Uno de los métodos más comunes es la autorización basada en roles, donde los permisos se asignan en función del cargo o rol dentro de la organización para cada usuario. Por ejemplo, un médico tendría acceso a áreas de tratamiento y quirófanos, mientras que el personal de limpieza podría ingresar solo en horarios específicos a áreas comunes. Este tipo de autorización permite a cada usuario tener acceso únicamente a las áreas que le competen, lo que reduce el riesgo de que personas no autorizadas accedan a áreas críticas. (Mehdipour, 2013) destacan que los sistemas de autorización basados en roles son eficaces porque permiten configurar permisos específicos de forma centralizada, facilitando su gestión en instalaciones grandes como hospitales.

Autorización dinámica. En algunos sistemas avanzados, la autorización puede adaptarse a situaciones específicas. Por ejemplo, un hospital podría configurar permisos temporales para permitir que ciertos usuarios accedan a áreas restringidas en caso de emergencia. Este tipo de autorización dinámica permite que el sistema reaccione a circunstancias inusuales o de emergencia, proporcionando un control más flexible y seguro. La implementación de esta autorización en tiempo real requiere sistemas más sofisticados, que puedan identificar la necesidad de acceso en el momento y ajustar los permisos de forma instantánea.

Autorización Mediante Autenticación de Múltiples Factores.

En situaciones de seguridad, los sistemas pueden exigir una segunda capa de autenticación antes de dar el acceso a áreas muy sensibles. Por ejemplo, realizar aplicaciones más robustas al incluir

una tarjeta RFID combinada con datos biométricos, como, huella dactilar. Este método, conocido como autenticación de múltiples factores, refuerza la seguridad, ya que exige que el usuario cumpla con más de un requisito para poder acceder a áreas específicas. Esta técnica se usa comúnmente en lugares donde el acceso debe ser extremadamente restringido y controlado, como laboratorios o salas de datos.

En entornos hospitalarios, la autorización ayuda a asegurar que cada persona registrada tenga acceso solo a las áreas necesarias para cumplir con sus funciones. Esto no solo optimiza el flujo de trabajo, sino que también contribuye a un ambiente seguro para los pacientes, al restringir el acceso a áreas sensibles o de atención especializada. De esta forma, el sistema de control de acceso cumple su propósito de proteger tanto a las personas como los recursos de la institución.

Auditoría

La auditoría es el último componente en un sistema de control de acceso y se encarga de registrar las entradas y salidas de los usuarios. Este registro permite que las actividades de acceso queden documentadas, proporcionando una "huella digital" de quién ha ingresado a cada área, en qué momento y durante cuánto tiempo. La auditoría es clave para la seguridad, ya que facilita el monitoreo permanente y Adicionalmente, permite identificar patrones o eventos inusuales que puedan representar un riesgo.

En entornos hospitalarios, la auditoría no solo cumple con el propósito de realizar un registro detallado, sino que también contribuye al cumplimiento de normativas de seguridad y privacidad, especialmente en áreas sensibles, como quirófanos, salas de pacientes y laboratorios. A continuación, se explican los beneficios principales de la auditoría en los sistemas de control de acceso:

Registro de Actividades. La función básica de la auditoría es registrar cada acceso, detallando quién ingresó, a qué área y en qué momento. Este registro continuo ayuda a mantener un control sobre las personas que utilizan áreas sensibles y es útil para revisar los eventos en caso de incidentes de seguridad. (Woo-Garcia, 2016) mencionan que estos registros permiten realizar análisis de seguridad y facilitan la trazabilidad en caso de necesitar información sobre accesos pasados.

Alertas y Reportes. Algunos sistemas de registros avanzados pueden integrarsen con plataformas de software que generan reportes y alertas automáticas cuando detectan actividades inusuales. Por ejemplo, si una persona intenta ingresar a un área restringida varias veces sin éxito, el sistema podría enviar una alerta para advertir de un posible acceso no autorizado. Este tipo de alertas en tiempo actual es especialmente útil en instalaciones donde se requiere una respuesta rápida ante eventos sospechosos, como hospitales y centros de datos.

Análisis de Patrones de Acceso. La información recopilada en los registros manuales o digitales también permite analizar patrones de entradas y salidas, para ajustar los protocolos de seguridad según las necesidades. Por ejemplo, al identificar los periodos pico y valle en que ciertos accesos son más frecuentes, se puede tomar medidas de seguridad y asignar recursos operativos durante esos momentos. (Xie, 2014) destacan que el análisis de patrones ayuda a detectar accesos inusuales o anómalos, lo cual es clave para anticiparse a posibles riesgos y mejorar la seguridad de manera preventiva.

La auditoría no solo ayuda a mantener un registro detallado de todas las actividades de acceso, sino que también, permite responder rápidamente a posibles incidentes y ajustar los protocolos de seguridad en función de la información recopilada. En el contexto de la Clínica Medilink, el registro de entrada y salida manual o digital es esencial para garantizar que cada

acceso esté documentado y que se mantenga un entorno seguro y controlado, especialmente en áreas críticas para la atención de los pacientes.

Principios de Diseño y Fabricación de Dispositivos de Seguridad

Seguridad

La seguridad es el aspecto más importante en el diseño de dispositivos de control de acceso. Estos dispositivos deben estar preparados para resistir tanto manipulaciones físicas como accesos no autorizados a nivel digital. En otras palabras, un sistema de control de acceso debe ser lo suficientemente seguro para proteger las áreas restringidas de cualquier intento de interferencia externa.

Un ejemplo práctico de esta seguridad es el uso de microcontroladores como el ATmega328P (Atmel Corporation, 2015), que incluye un "código de bloqueo programable". Este bloqueo impide que el software del dispositivo sea modificado o manipulado sin autorización, asegurando que el dispositivo funcione siempre según lo planeado y sin vulnerabilidades.

Además, las tecnologías con el uso de inteligencia artificial (IA) y redes neuronales, están comenzando a mejorar la seguridad de sistemas de control de acceso más complejos, como aplicaciones basados en reconocimiento facial. Según (Aldana Porras, 2018), estas técnicas permiten que el sistema de reconocimiento facial sea más preciso y difícil de engañar. Los algoritmos de redes neuronales profundas pueden analizar detalles específicos de cada persona y reducir significativamente el riesgo de suplantación de identidad o acceso no autorizado, algo especialmente útil en ambientes donde la seguridad es prioritaria, como los hospitales.

En sistemas que requieren comunicación entre varios dispositivos, como las redes CAN utilizadas en los elevadores, también se implementan medidas de seguridad fuertes. Estas redes asignan diferentes niveles de prioridad a los mensajes que intercambian los dispositivos, de

manera que las funciones críticas están protegidas. Así, se evita que un intento de manipulación en la red afecte la operación del sistema. (Huseinbegovic, 2009) destacan que este enfoque de seguridad en las redes de control es esencial para que los sistemas operen de manera confiable y segura en entornos donde hay múltiples dispositivos en funcionamiento.

El principio de seguridad en el diseño de dispositivos de control de acceso asegura que estos sean robustos y puedan enfrentar tanto intentos de manipulación física como digital, garantizando que el sistema proteja adecuadamente las áreas sensibles.

Fiabilidad

La fiabilidad es fundamental en el diseño de dispositivos de control de acceso, ya que garantiza que estos sistemas funcionen en diferentes condiciones y no presenten fallos inesperados. En entornos críticos, como los hospitales, una falla en el sistema de control de acceso podría comprometer la seguridad de las personas y el flujo adecuado de trabajo. Por eso, es esencial que estos dispositivos sean confiables y estables en su funcionamiento diario.

Para garantizar la fiabilidad de los sistemas de control de acceso, es esencial seguir las directrices establecidas en normativas técnicas como la NTC 5926-1 (Instituto Colombiano de Normas Técnicas y Certificación, 2021) , la cual detalla las condiciones de seguridad e inspección técnica para ascensores eléctricos e hidráulicos en Colombia. Estas normas establecen que el uso de componentes resistentes y las inspecciones periódicas realizadas por personal competente son esenciales para prevenir fallos operativos y garantizar la seguridad de los usuarios. Además, la normativa destaca que un mantenimiento adecuado y la implementación de sistemas de control basados en seguridad técnica y normativa son clave para instalaciones de uso intensivo, como hospitales y edificios de oficinas.

Los dispositivos de tecnología RFID, que se emplean con frecuencia en control de acceso, pueden enfrentar desafíos como interferencias y pérdida de comunicación, especialmente en áreas donde hay muchos dispositivos en uso. Para dar solución a estas condiciones, se aplican algoritmos de anti-colisión, que permiten que cada dispositivo funcione correctamente sin interferir con otros, incluso en lugares con alta densidad de dispositivos (Xie, 2014)Esto asegura que el sistema de control de acceso mantenga su fiabilidad y funcione sin interrupciones.

Otro ejemplo de fiabilidad en los dispositivos de control de acceso es el uso de módulos de comunicación y sensores diseñados para condiciones de uso continuo, como los módulos VVVF (Zhong Wu, 2015) y CompactRIO (Ye, 2016). Estos módulos están diseñados para soportar un uso prolongado y variar sus funciones según las necesidades del entorno. En instalaciones hospitalarias, esta capacidad permite que el sistema de control de acceso funcione sin interrupciones, brindando la seguridad necesaria en todo momento.

La fiabilidad en los dispositivos de control de acceso asegura que el sistema mantenga su funcionamiento constante, sin errores, y en condiciones variables. Esto es decisivo en lugares como hospitales, donde la seguridad y el acceso controlado deben estar garantizados en todo momento.

Usabilidad

La usabilidad es otro aspecto clave en el diseño de dispositivos de control de acceso, ya que asegura que estos sistemas sean fáciles de usar para todos los usuarios o para quien utilice el dispositivo. En un entorno como un hospital, donde el personal médico y de apoyo necesita acceder rápidamente a diferentes áreas, los sistemas de control de acceso deben ser intuitivos y no dificultar el flujo de trabajo. La usabilidad, entonces, se enfoca en hacer que los dispositivos sean eficientes y simples para quienes los usan diariamente.

Los sistemas de autenticación biométrica, como el reconocimiento facial, representan un avance significativo en términos de usabilidad y seguridad en el control de acceso. Estos sistemas no solo eliminan la necesidad de contacto físico, algo esencial en entornos hospitalarios para mantener altos estándares de higiene, sino que también mejoran la eficiencia al integrar tecnologías modernas. (Bagga, 2022) destacan que, en el ámbito del Internet de las Cosas (IoT), las soluciones de acceso basadas en blockchain y biometría fortalecen la autenticidad de los usuarios y facilitan una experiencia más segura al eliminar dependencias de dispositivos físicos o contraseñas que pueden perderse o ser comprometidas. Por otro lado, (Kushwaha, 2019)enfatizan que los sistemas biométricos tienen una gran capacidad de discriminación y persisten en el tiempo, características que los hacen ideales para aplicaciones en seguridad y control de acceso.

Otro aspecto importante de la usabilidad es el diseño de interfaces de usuario que sean intuitivas y minimicen la posibilidad de errores. Por ejemplo, los sistemas RFID son populares no solo por su seguridad, sino también porque son muy fáciles de utilizar: el usuario simplemente debe acercar su tarjeta al lector y el acceso se otorga en segundos. Estos sistemas, además, pueden utilizarse en conjunto con plataformas de software como LabVIEW, que permite desarrollar interfaces interactivas con monitoreo el sistema y hacer ajustes cuando sea necesario (Mezzanotte, 2021).

la usabilidad garantiza que los sistemas de control de acceso no solo sean seguros, sino también fáciles de usar. En lugares como los hospitales, donde la rapidez y la comodidad son esenciales, un sistema que sea intuitivo y eficiente facilita el trabajo del personal y mejora el acceso seguro a las áreas clave. Además, la facilidad de uso también contribuye a que los usuarios se sientan cómodos y confiados al emplear el sistema, lo cual reduce errores y ayuda a que el sistema sea aceptado y adoptado rápidamente por todos.

Escalabilidad

La escalabilidad es otro principio fundamental en el diseño de dispositivos de control de acceso, ya que permite que estos sistemas crezcan y se adapten a necesidades futuras, sin el requisito de una reestructuración completa. En instalaciones grandes, como hospitales, donde el número de áreas restringidas y de personal puede aumentar con el tiempo, es esencial contar con un sistema de control de acceso que pueda expandirse fácilmente para cubrir nuevas zonas o integrar nuevos usuarios.

Un sistema escalable permite añadir dispositivos o actualizar la configuración del sistema sin grandes complicaciones. Por ejemplo, los sistemas de control basados en redes CAN, que permiten que varios dispositivos se estén comunicando entre sí, son una opción popular en sistemas distribuidos, como el control de ascensores. Estos sistemas pueden adaptarse a múltiples configuraciones y extenderse según las necesidades de la infraestructura, manteniendo siempre su funcionalidad central. (Liu, 2013) destacan que esta flexibilidad es importante en instalaciones de gran envergadura, donde las necesidades de seguridad cambian constantemente.

Además, los sistemas IoT (Internet de las Cosas) también ofrecen una gran ventaja en términos de escalabilidad. Con la capacidad de conectar y gestionar múltiples dispositivos, los sistemas IoT permiten controlar y monitorear una gran cantidad de puntos de acceso en tiempo actual, lo cual es ideal en ambientes hospitalarios. (Mezzanotte, 2021) subrayan que esta flexibilidad de integración y la posibilidad de manejar datos en tiempo real hacen que los sistemas basados en IoT sean una solución adaptable y eficiente para las instituciones que necesitan una escalabilidad dinámica y rápida.

La escalabilidad permite que los sistemas de control de acceso evolucionen junto con las necesidades de la institución. Esto garantiza que el sistema de seguridad pueda expandirse y

adaptarse a medida que el hospital crece, sin afectar la operatividad ni la seguridad, y manteniendo siempre el control sobre cada nueva área o usuario que se integre.

Aspectos Técnicos del Diseño e Implementación

Hardware

El diseño de hardware en los sistemas de control de acceso requiere la implementación de componentes electrónicos y mecánicos que puedan soportar el uso intensivo y el desgaste físico, así como condiciones ambientales adversas. Entre estos componentes se encuentran los microcontroladores, sensores de precisión, y lectores biométricos o de RFID. Según (Mezzanotte, 2021) los dispositivos de RFID deben ser especialmente duraderos y de bajo consumo energético para prolongar su funcionalidad en condiciones diversas. Estas condiciones tienen un valor significativo en el diseño y la selección de materiales, para asegurar que el hardware mantenga un desempeño óptimo y se adapte a las necesidades de control de acceso en estado actual.

Los avances en microelectrónica y el desarrollo de sensores precisos también juegan un papel fundamental. La inclusión de microcontroladores como el ATmega328P (Atmel Corporation, 2015), con una arquitectura RISC y capacidad de reprogramación, permite adaptarse a los cambios y ofrece flexibilidad en sistemas embebidos. Por otro lado, tecnologías avanzadas, como los chips FPGA (Field Programmable Gate Arrays), facilitan un diseño compacto y eficiente en el consumo energético, especialmente en aplicaciones de edificios inteligentes (Zhong Wu, 2015).

Como concluye Khalid, Ezzati y Beni-Hssane (2017), la inversión en hardware de alta calidad es clave para la durabilidad y confiabilidad en sistemas de seguridad, ya que estos componentes soportan las tareas intensivas de verificación de acceso y minimizan el riesgo de

fallas operativas. En resumen, la selección de hardware adecuado es notable para que el sistema funcione sin interrupciones y brinde una respuesta robusta en el control de accesos.

Software

El software en sistemas de control de acceso desempeña un rol crítico, ya que se encarga de la autenticación y autorización de usuarios mediante algoritmos de seguridad avanzados. Harmouch y El Kouch (2017) destacan que la implementación de algoritmos de cifrado es básico para proteger las comunicaciones de autenticación y prevenir ataques no autorizados. En sistemas más complejos, como los de control de elevadores, implementar redes neuronales recurrentes y aprendizaje profundo por refuerzo ha mostrado mejorar los tiempos de respuesta y la eficiencia operativa, al adaptar las decisiones del sistema según patrones históricos de tráfico (Liu, 2013)

Adicionalmente, la implementación de software que permita la administración de credenciales y la verificación en tiempo real asegura una operación ágil y sin vulnerabilidades. En un caso específico, se menciona el sistema RegistryUNAD, que utiliza un servidor Apache con PHP y una base de datos MySQL (Caldón Cuchimba, 2020), logrando una personalización elevada y optimización de la administración de permisos en entornos de alta demanda. Estos desarrollos permiten que los sistemas de control de acceso respondan ante intentos de acceso no autorizados en tiempo real, lo cual incrementa la seguridad general.

(Xie, 2014) señalan también la relevancia para los algoritmos de privacidad en sistemas RFID, donde el software debe estar diseñado para proteger los datos y evitar la interceptación o clonación de dispositivos. Esta condición en el diseño asegura que la información de los usuarios esté protegida, lo que es fundamental en sistemas donde la privacidad es una prioridad. La

constante mejora de los algoritmos y su capacidad de adaptación a las necesidades de cada instalación son claves para mantener una seguridad confiable.

Integración

La integración de sistemas de control de acceso con otros dispositivos de seguridad, como cámaras de vigilancia (CCTV), alarmas de incendio y sistemas de gestión de visitantes, es fundamental para la seguridad integral del edificio. Esta interoperabilidad facilita una respuesta centralizada y coordinada ante incidentes, permitiendo que cada subsistema contribuya a la seguridad global del entorno. Como afirman El Makkaoui y Ezzati (2017), la interoperabilidad mejora la respuesta ante emergencias y refuerza la capacidad de supervisión de las instalaciones.

El uso de tecnologías como CompactRIO, que permiten la comunicación y administración centralizada, es otra herramienta sustancial en entornos industriales y académicos (Ye, 2016). La capacidad de que el sistema de control de acceso se integre con otros dispositivos de seguridad permite una supervisión constante y reduce los tiempos de respuesta en caso de eventos de seguridad. En edificios inteligentes, por ejemplo, los sistemas pueden responder de manera automatizada a eventos sospechosos, incrementando así la seguridad y minimizando la dependencia de la intervención humana.

La implementación de sistemas interoperables también maximiza la funcionalidad de los sistemas RFID y biométricos, ya que se pueden vincular con tecnologías de vigilancia y control en un solo entorno centralizado (Sánchez Gómez, 2020).La interoperabilidad permite al sistema operar de manera fluida en un ecosistema de dispositivos conectados, lo cual es vital para garantizar una seguridad completa y coordinada en cualquier instalación.

Metodología

La metodología desarrollada para el diseño e implementación del sistema de control de acceso en la Clínica Medilink ha abordado diversos aspectos técnicos y funcionales. Se ha centrado en garantizar la seguridad y eficiencia operativa mediante un dispositivo basado en tecnología RFID, diseñado para priorizar el acceso en situaciones de emergencia. Estos dispositivos cuentan con una arquitectura distribuida y centralizada que permite la validación autónoma de usuarios en cada planta y el control del acceso a la cabina del ascensor. Los componentes seleccionados, como el microcontrolador ATmega328P y las tarjetas RFID de 13.56 MHz, han sido claves para cumplir con los requisitos de fiabilidad y precisión. Además, se ha diseñado un cronograma detallado de instalación y pruebas que minimiza las interrupciones operativas, asegurando la disponibilidad del ascensor para casos críticos durante la implementación. La integración final incluye capacitación del personal para garantizar el correcto uso y mantenimiento del sistema.

Diseño del Sistema de Control de Acceso

Para la elaboración del dispositivo para el control del acceso en el ascensor camillero de la clínica Medilink se pactaron las siguientes especificaciones y requisitos.

Especificaciones Técnicas y Requisitos Funcionales del Sistema

Los dispositivos para implementar, la función principal es desactivar el mando del ascensor hasta que se identifique un usuario autorizado portador de una tarjeta RFID habilitando los mandos en cada parada, lo que para términos se nombrará HALL.

La solicitud de la empresa Medilik, indica que necesita el uso exclusivo del ascensor para camilleros con pacientes en estado de emergencia, motivo por el cual debe estar disponible para el llamado desde cualquier HALL. Las especificaciones del control son:

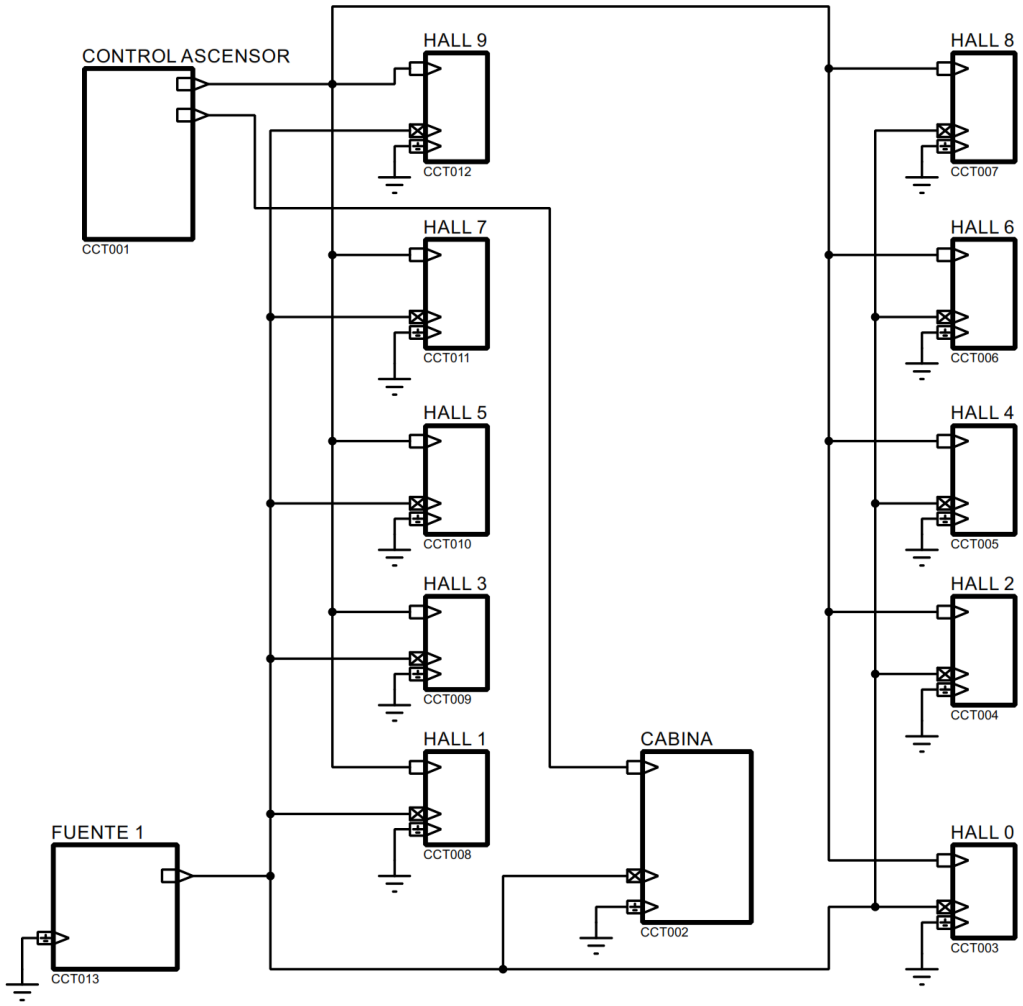
- 10 Hall
- Una Cabina con dos Puertas
- 6 plantas (Pisos)
- 120 volts Instalados
- 100 usuarios

Arquitectura del Sistema de Control de Acceso

El diagrama de la Figura 1, se observa la disposición de cada uno de los puntos donde se va a instalar los controladores para habilitar la función de llamado del carro viajero del ascensor.

Figura 1

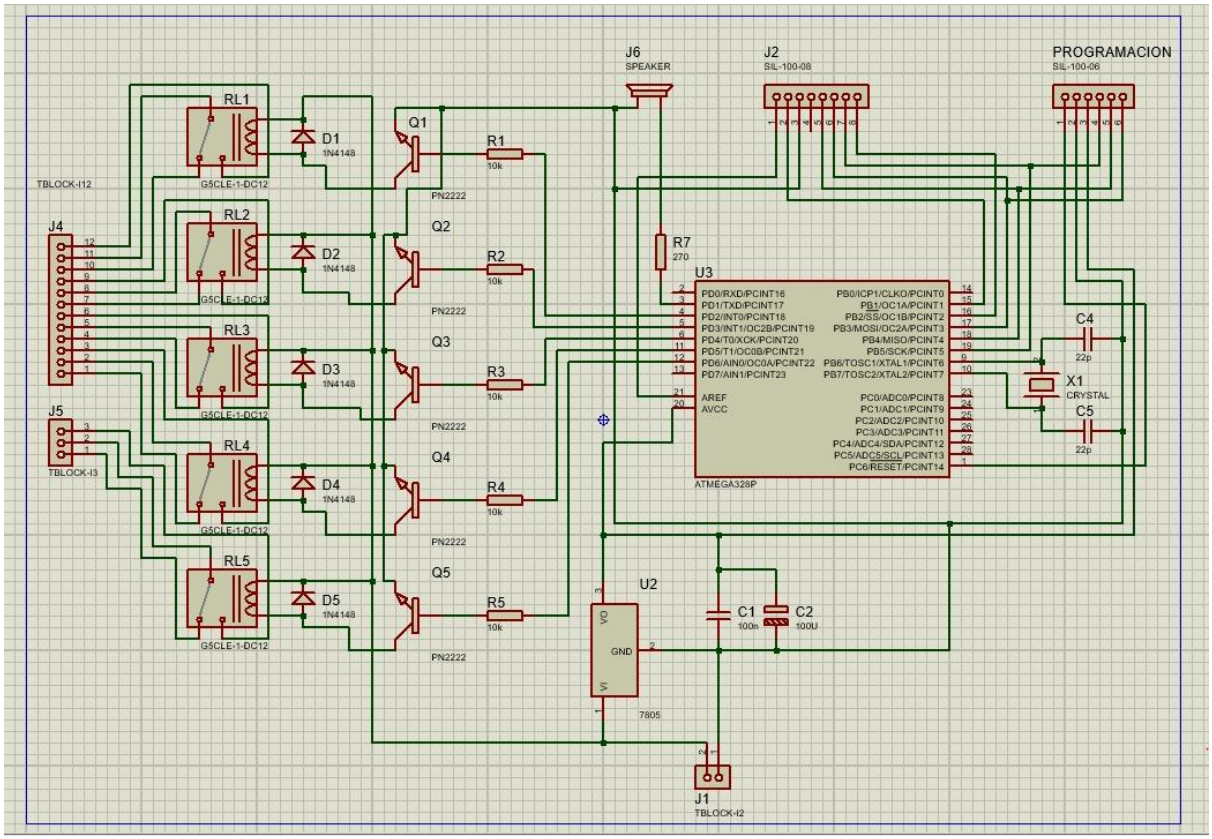
Diagrama de Conexiones del Sistema de Acceso en Cada Piso



Nota. Este diagrama que se observa en la **Figura 1**, resalta la arquitectura distribuida y centralizada del sistema de control de acceso, donde cada piso tiene autonomía para validar a los usuarios y enviar señales al ascensor. La conexión eficiente entre los puntos de acceso y la cabina garantiza un flujo seguro y controlado, facilitando el uso prioritario del ascensor en situaciones de emergencia, como el traslado de pacientes.

Figura 2

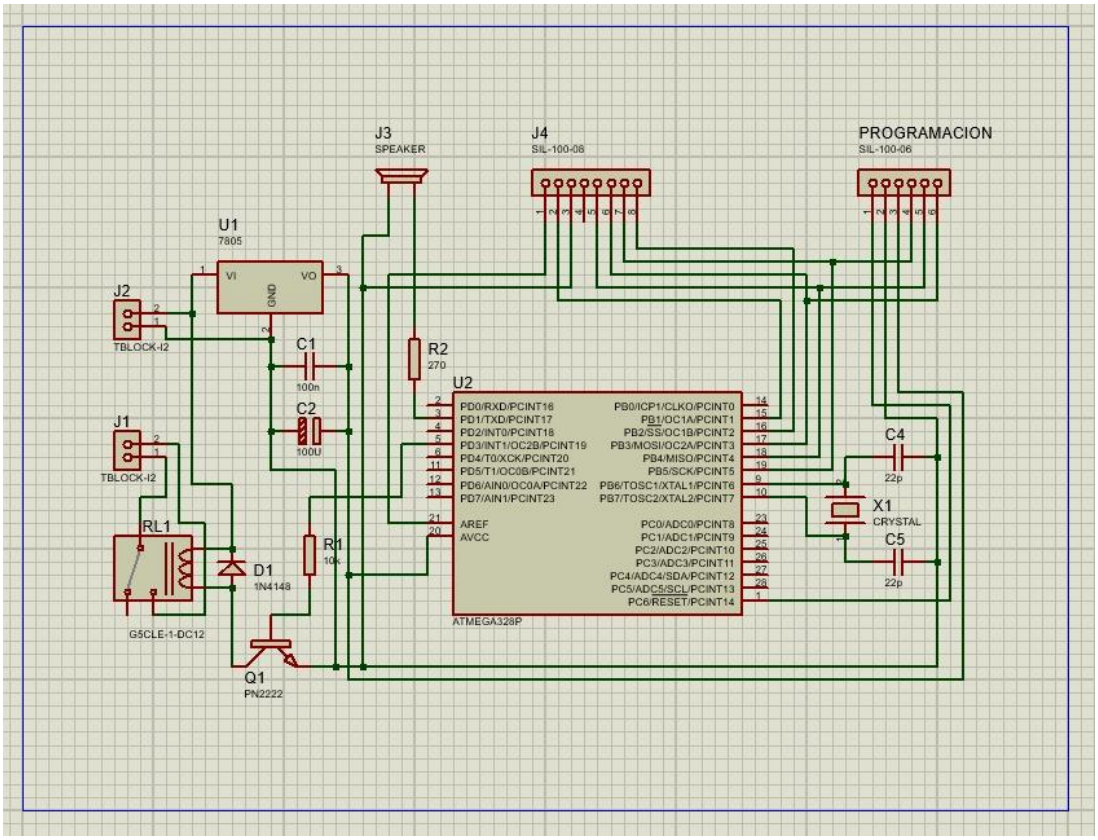
Diagrama Esquemático Circuito de Cabina



Nota. La Figura 2, muestra el diagrama esquemático del circuito electrónico dentro de la cabina del ascensor, el cual es clave para gestionar la interacción del usuario autorizado una vez que está dentro del ascensor. Este circuito se conecta a los botones físicos dentro de la cabina, permitiendo al usuario elegir el nivel al que desea ir. Los botones solo se habilitan después de que se valide una tarjeta RFID. Los relés permiten desactivar o activar los comandos de la cabina, garantizando que el sistema opere una vez se valide el usuario.

Figura 3

Diagrama Esquemático Circuito de HALL.



Nota. La Figura 3 presenta el circuito esquemático de los puntos de acceso (HALLs) ubicados en cada piso. Este circuito se encarga de gestionar la validación del usuario mediante el lector RFID y enviar la señal para llamar al ascensor. El lector instalado en cada hall es el encargado de escanear las tarjetas RFID. Si la tarjeta es válida, se envía una señal al controlador para permitir el llamado del ascensor. Una vez validada la tarjeta, el usuario puede pulsar el botón para solicitar el ascensor. Este circuito solo activa los controles si la autenticación ha sido exitosa. Los relés se encargan de activar/desactivar la botonera del hall en función de la autorización, asegurando que el acceso no autorizado sea bloqueado.

Selección de Componentes y Tecnologías

Para el proyecto se seleccionaron los siguientes Componentes:

Atmega328P

El ATmega328P es un microcontrolador CMOS de 8 bits basado en la arquitectura AVR de RISC mejorada. Este dispositivo se caracteriza por su bajo consumo de energía y alta eficiencia en la ejecución de instrucciones. El ATmega328P es parte de la familia de microcontroladores AVR y es ampliamente utilizado en estudios y desarrollos de control embebido debido a su capacidad de procesamiento eficiente y flexibilidad en la programación (Atmel Corporation, 2015).

A continuación, se presenta una lista con las principales características del microcontrolador ATmega328P:

Arquitectura

- Arquitectura RISC avanzada.
- 131 instrucciones potentes, la mayoría de las cuales se ejecutan en un ciclo de reloj.
- 32 registros de propósito general de 8 bits.
- Operación totalmente estática.

Memoria

- Memoria Flash autoprogramable en el sistema: 32KBytes.
- EEPROM: 1KByte.
- SRAM interna: 2KBytes.
- Ciclos de escritura/borrado: 10,000 para Flash y 100,000 para EEPROM.
- Retención de datos: 20 años a 85°C y 100 años a 25°C.

Capacidades de programación

- Programación en el sistema mediante programa de arranque en chip.
- Operación de lectura y escritura real.

Periféricos

- Dos temporizadores/contadores de 8 bits con prescaler y modo de comparación independientes.
- Un temporizador/contador de 16 bits con prescaler, modo de comparación y modo de captura independientes.
- Contador de tiempo real con oscilador separado.
- Seis canales PWM.
- Convertidor ADC de 8 canales y 10 bits (en paquetes TQFP y VQFN).
- Medición de temperatura.
- USART programable.
- Interfaz SPI en modo maestro/esclavo.
- Interfaz serial de 2 hilos (compatible con Philips I2C).
- Temporizador watchdog programable con oscilador en chip.
- Comparador analógico en chip.
- Interrupción y activación por cambio de pin.

Características especiales

- Reset por encendido y detección de brown-out programable.
- Oscilador calibrado internamente.
- Fuentes de interrupción internas y externas.

- Seis modos de sueño: Idle, reducción de ruido de ADC, ahorro de energía, apagado, espera y espera extendida.

Entradas/Salidas (I/O)

- 23 líneas de I/O programables.
- Paquetes disponibles: SPDIP de 28 pines, TQFP de 32 pines, VQFN de 28 pines y VQFN de 32 pines.
- Voltaje de operación: 1.8 - 5.5V.
- Rango de temperatura: -40°C a 85°C.

Consumo de energía:

- Modo activo a 1MHz, 1.8V, 25°C: 0.2mA.
- Modo de apagado: 0.1µA.
- Modo de ahorro de energía (incluyendo RTC de 32kHz): 0.75µA.

Tarjeta RFID 13.56 MHz

Tarjeta RFID 13.56 Mhz MFS50 (Identificación por Radiofrecuencia) para frecuencias de detección de 13.56MHz color blanco con memoria interna, para propósitos de transmisión de datos de forma remota, por ejemplo, identidad de objeto mediante ondas de radio.

- Tipo: Tarjeta RFID
- Modelo: MFS50
- Frecuencia: 13.56 MHz
- Protocolo: ISO/IEC 14443 Tipo A
- Bauds: 106 kbps
- Alcance de lectura/escritura: 0~5cm (aprox.)
- EEPROM: 1K Bytes

- Identificador único de 4 Bytes
- Tiempo de lectura: 100ms
- Ciclos de escritura: 100 000
- Dimensiones: 85.5mm x 54mm x 1mm
- Color: Blanco
- Material: PVC

Llavero RFID-RC522

El RC522 RFID está basado en el IC MFRC522 de NXP, es un lector/escritor altamente integrado para comunicación sin contacto a 13.56 MHz. El lector MFRC522 es compatible con los estándares ISO/IEC 14443 A/MIFARE y NTAG. Este permite la lectura y escritura de tarjetas y transpondedores compatibles con ISO/IEC 14443A, y está diseñado para ofrecer una implementación robusta y eficiente en la demodulación y decodificación de señales.

A continuación, se presenta una lista de verificación con las principales características del RC522.

RFID

Voltaje de operación: 2.5V~3.3V.

Consumo de corriente:

- En operación: 13~26mA.
- En modo de espera: 10~13mA.
- Frecuencia de operación: 13.56MHz.

Compatibilidad de estándares:

- Soporta comunicación de alta velocidad ISO/IEC 14443A hasta 848 kBd.

Interfaces de comunicación:

- SPI con velocidad de bus hasta 10Mbit/s.
- Interfaz I2C hasta 400 kBd en modo rápido y hasta 3400 kBd en modo de alta velocidad.
- UART serial RS232 hasta 1228.8 kBd, con niveles de voltaje dependientes del suministro de voltaje del pin.

Compatibilidad de tarjetas: Compatible con tarjetas MIFARE y ISO 14443A.

Distancia típica de operación:

- Hasta 50 mm en modo de lectura/escritura, dependiendo del tamaño y ajuste de la antena.

Aplicación con Arduino: Biblioteca RFID de miguelbalboa.

Pines de interfaz:

- SDA a Digital 10.
- SCK a Digital 13.
- MOSI a Digital 11.
- MISO a Digital 12.
- IRQ no conectado.
- GND a GND.
- RST a Digital 9.
- 3.3V a fuente de 3.3V.

Fuente alimentación conmutada S-100-24

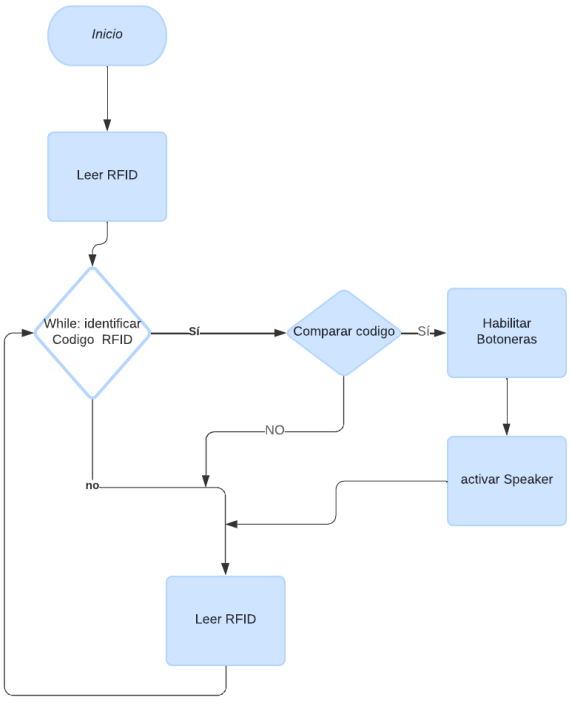
- tensión de salida: 24VDC ± 1%
- Voltaje de salida ajustable: 21,6~26,4V
- corriente de salida: 0.0 ~ 4,5 A

- rizado y ruido: 50mV
- potencia: 108W
- dimensiones: 159 x 97 x 38 mm
- tensión de entrada: 170 ~ 264VCA, 47 ~ 63Hz (conexiones L, N y a tierra)
- corriente in-rush (230VCA): 30A/115VAC 50A/230VAC (arranque en frío)
- temperatura de funcionamiento: -10°C ~ 60ºC

Diseño y Codificación de ATmega328P

Figura 4

Diagrama de Flujo Algoritmo de Permiso



Nota. La figura 4, se observa la lógica de la solución plantada para habilitar y deshabilitar el uso de las botoneras con el uso de un dispositivo RFID, indicado el permiso de uso a través de un sonido. Este diagrama de flujo ilustra un proceso sencillo pero eficaz para gestionar el control de

acceso. La combinación de la lectura RFID y la activación temporal de los controles del ascensor garantiza que solo usuarios autorizados puedan hacer uso del mismo, alineándose con los objetivos del proyecto de mejorar la seguridad y eficiencia operativa en la clínica Medilink.

Proceso de Fabricación de los Dispositivos de Control de Acceso

Figura 5

Layout Circuito de Cabina

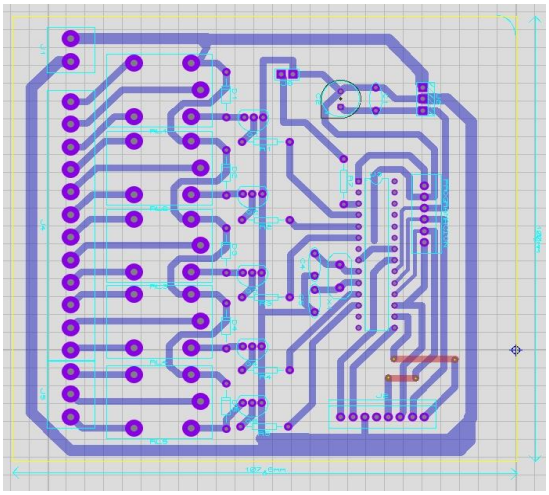
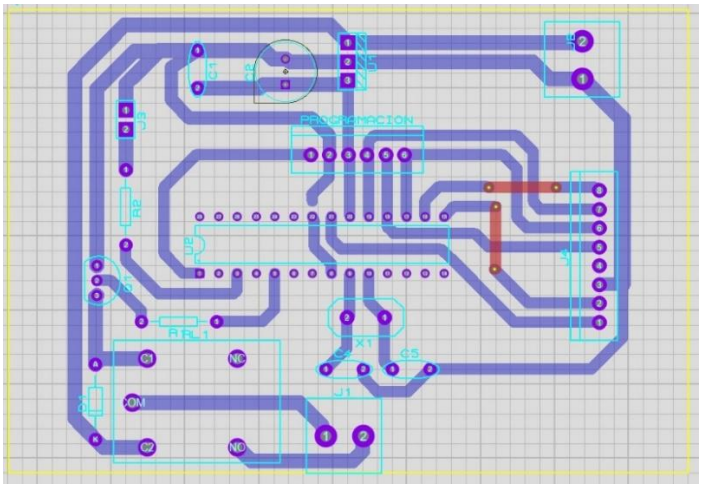


Figura 6

Layout Circuito de HALL

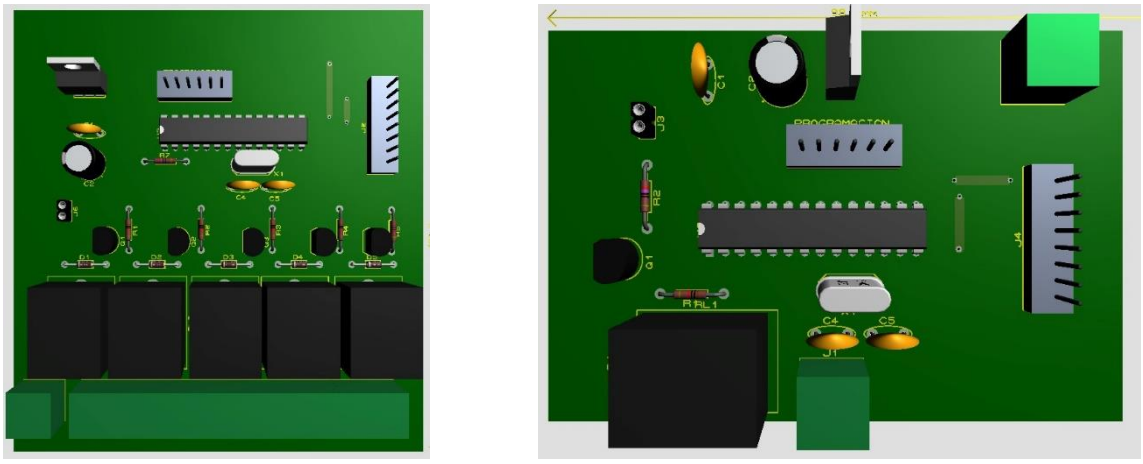


Nota. La Figura 5, muestra las rutas o conexiones de los componentes electrónicos que controlan la tarjeta de lectura RFID interna del ascensor (ubicada en la cabina). Esta parte del sistema es crítica porque permite que, una vez validada la tarjeta RFID, el usuario seleccione el piso al que desea ir. La Figura 6, ilustra el diseño del layout para los puntos de control externos del ascensor, es decir, los botones ubicados en cada planta o Hall que permiten llamar al ascensor. Estos puntos también están controlados mediante lectoras de RFID para garantizar que los usuarios puedan llamar el ascensor.

Integración de Componentes y Ensamblaje del Sistema

Figura 7

Vistas Superior Circuitos de Cabina y de Hall



(a) **(b)**

Nota. La figura 7a, ilustra cómo se disponen los componentes electrónicos y las pistas de conexión dentro del espacio de control ubicado en la cabina del ascensor. Este diseño es clave para gestionar las funciones internas del ascensor, permitiendo al usuario seleccionar el piso solo después de la autenticación exitosa con la tarjeta RFID. La figura 7b, representa el diseño para los controles externos del ascensor ubicados en cada planta o piso. Este circuito permite la

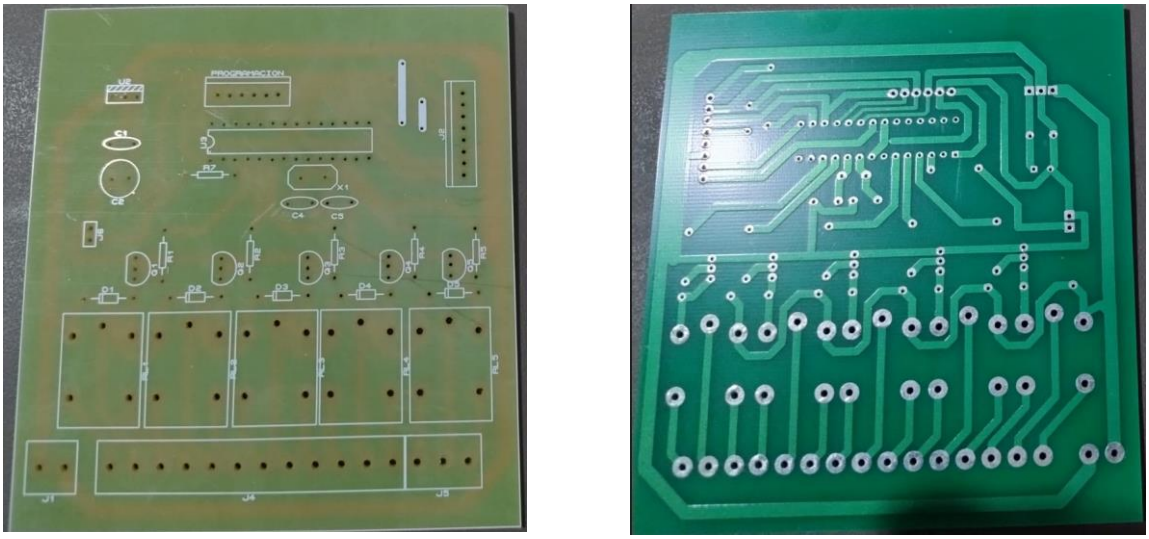
interacción del usuario desde fuera de la cabina, activando el llamado del ascensor tras verificar que el usuario tiene acceso autorizado.

Fabricación PCB

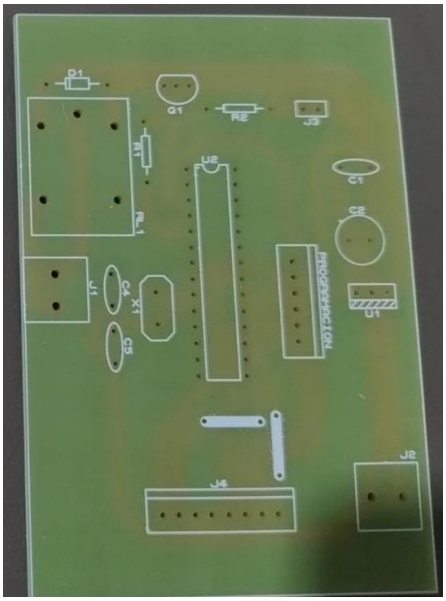
La Figura 8 presenta las vistas superior e inferior de las placas de circuito impreso (PCB) para la cabina y los halls del sistema de control de acceso en la clínica Medilink. Las imágenes 8a y 8b corresponden a la misma tarjeta utilizada en la cabina del ascensor, mostrando su diseño tanto por arriba como por debajo. Esta tarjeta gestiona los botones de selección de pisos, activados tras la autenticación exitosa mediante una tarjeta RFID. Su diseño optimiza el espacio y distribuye los componentes para evitar interferencias y facilitar la integración con los controles internos del ascensor.

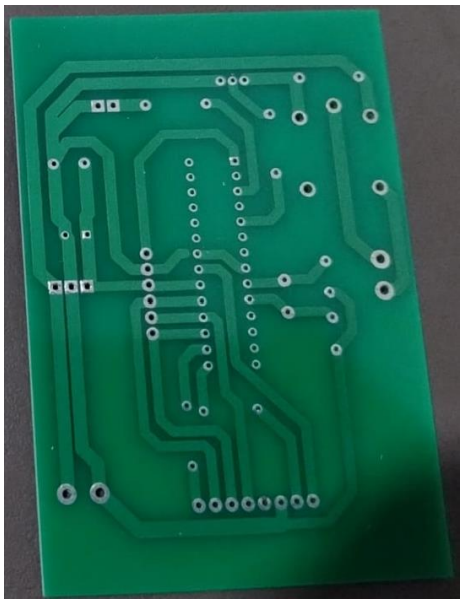
Figura 8

Vista Superior de PCBs de Cabina y Hall



(a) **(b)**





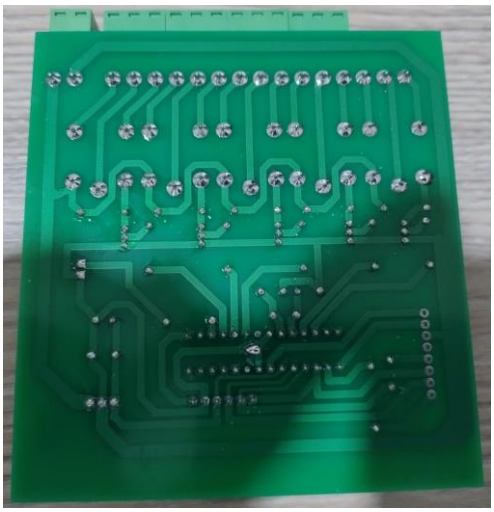
(c) **(d)**

Nota. De manera similar, las imágenes 8c y 8d corresponden a la misma tarjeta para los Halls, mostrando ambas caras de la placa. Esta tarjeta permite el control del llamado del ascensor desde cada planta, asegurando que las conexiones entre dispositivos se garanticen en los lectores RFID. La fabricación de estas placas fue realizada por una empresa especializada, lo que garantiza precisión y calidad en el ensamblaje. Finalmente, en el proceso de ensamble en la Figura 9, se muestra las tarjetas tanto de cabina como las de los Halls, en su forma final listas para ser instaladas en el ascensor.

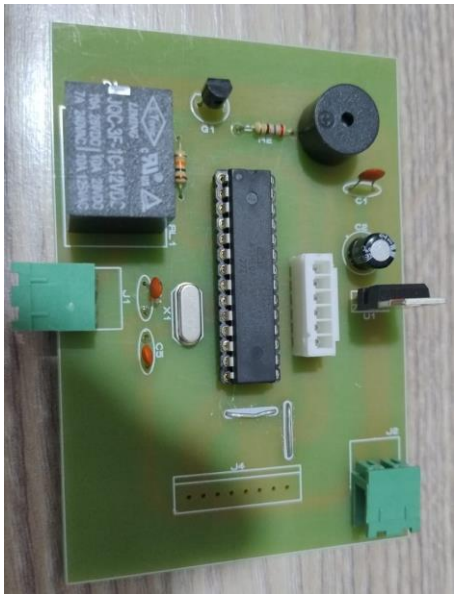
Figura 9

Tarjetas PCB de Cabina y de Hall (Integrada)

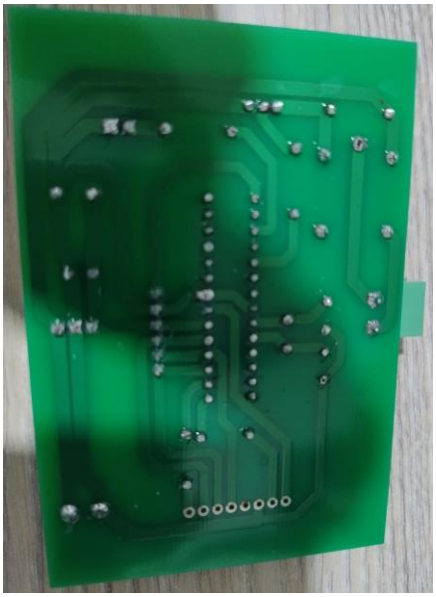
(a)



(b)



(c)



(d)

Nota. Ambas tarjetas han sido diseñadas con una disposición eficiente de componentes y una integración modular para facilitar su instalación y mantenimiento en el ascensor. El uso de relevadores asegura un control robusto de dispositivos de potencia, mientras que los

microcontroladores proporcionan flexibilidad en la programación y capacidad para realizar mejoras futuras en el sistema.

Además, la calidad del diseño del PCB es fundamental para evitar problemas de interferencia electromagnética (EMI) como la frecuencia de 60 Hz, y asegurar la durabilidad en condiciones de operación típicas del ascensor, como vibraciones y fluctuaciones de temperatura. Estas especificaciones garantizan que el desarrollo de las tarjetas sea confiable y fácilmente adaptable a diferentes escenarios de uso.

Implementación en la Clínica Medilink

Para implementar el sistema en el ascensor, se estableció un cronograma de paradas programadas, considerando estrictamente las políticas de la clínica. Debido a que el ascensor debe estar disponible las 24 horas del día, los 7 días de la semana, se diseñó una estrategia de interrupciones limitadas a los fines de semana, cuando el flujo de personal es bajo, ya que solo opera para urgencias y no para usuarios de consulta externa.

Estrategia de Paradas

- Duración de la parada: Cada parada programada tenía una duración de 24 horas.
- Frecuencia: Se realizaron dos paradas al mes.
- Objetivo por parada: Trabajar en dos botoneras de Hall por cada parada.

Tabla 2

Cronograma de Actividades para la Instalación

Mes	Actividad	Descripción	Duración
	Parada 1: Instalación de 2 botoneras de Hall	Desmonte, traslado, perforaciones, instalación y programación de las tarjetas	24 horas
Mes 1			
	Parada 2: Instalación de 2 botoneras de Hall	Desmonte, traslado, perforaciones, instalación y programación de las tarjetas	24 horas
	Parada 3: Instalación de 2 botoneras de Hall	Desmonte, traslado, perforaciones, instalación y programación de las tarjetas	24 horas
Mes 2			
	Parada 4: Instalación de 2 botoneras de Hall	Desmonte, traslado, perforaciones, instalación y programación de las tarjetas	24 horas
	Parada 5: Instalación de 2 botoneras de Hall	Desmonte, traslado, perforaciones, instalación y programación de las tarjetas	24 horas
	Parada 6: Instalación de la botonera de cabina	Desmonte, traslado, perforaciones, instalación y programación de las tarjetas	24 horas
Mes 3			
	Parada 7: Configuración y puesta en marcha del sistema	Ajustes finales, integración completa y pruebas de funcionamiento	24 horas
	Capacitación del personal y usuarios	Capacitación sobre el uso adecuado del sistema	4 horas

Nota. Se describe el proceso a realizar en cada botonera.

Instalación de los Dispositivos en los Ascensores y Áreas Relevantes

Para la instalación de los dispositivos se realizaron dos paradas al mes en los cuales, se trabajaron dos Halls Por parada, esto debido a las actividades que se debieron realizar para cada botonera:

Actividades realizadas:

1. Parada programada de 24 horas, previamente aprobada por la dirección del centro médico.
2. Desmonte de las botoneras a intervenir.
3. Traslado de las botoneras al taller de S&S Ingeniería S.A.S.
4. Acondicionamiento de las botoneras para realizar perforaciones y cortes.
5. Realización de perforaciones y cortes en el metal de las botoneras.
6. Acondicionamiento y fijación de los soportes para las tarjetas.
7. Instalación de las tarjetas electrónicas.
8. Programación inicial de las tarjetas en modo predeterminado (default).
9. Reinstalación de las botoneras en el ascensor.
10. Puesta en marcha del ascensor.

Control Durante las Paradas

Durante el tiempo en que el ascensor estuvo fuera de servicio, se asignó un técnico para operar el ascensor de forma manual, garantizando su disponibilidad inmediata en caso de atender pacientes de urgencias.

Duración Total la Instalación

- Duración: La instalación del sistema se llevó a cabo en un período de tres meses.
- Detalles del cronograma:

- 10 botoneras de Hall: Se trabajaron 4 botoneras por mes, distribuidas en dos paradas mensuales.
- Botonera de cabina: Se dedicó una parada exclusiva debido a su mayor complejidad.
- Configuración y puesta en marcha: Se asignó una parada adicional para la configuración final y la integración de todo el sistema.

Configuración y Puesta en Marcha del Sistema

Una vez instalados todos los dispositivos y realizada la integración del sistema, se procedió a:

- Configuración de las tarjetas electrónicas: Ajuste de parámetros finales para garantizar el correcto funcionamiento del sistema de control de acceso.
- Pruebas de funcionamiento: Verificación exhaustiva del sistema para garantizar su operatividad y seguridad.

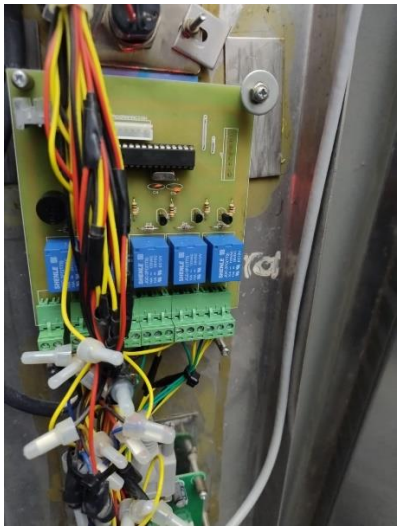
Figura 10

Proceso de Instalación

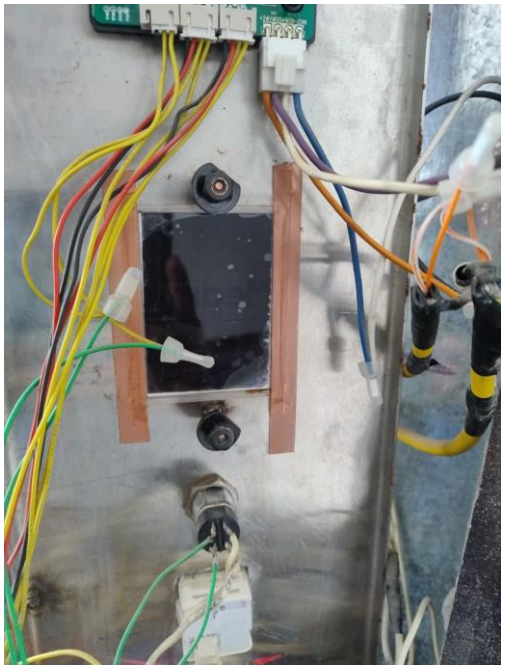
(a) Hall antes de la intervención, (b) Hall después de la instalación del sistema, (c) Tarjeta de Hall instalada, (d) Tarjeta de cabina Instalada, (e) Perforación y adecuación para instalar el lector de tarjetas RFID y (f) Botonera completa de Cabina con Tarjeta lectora de RFID Instalada.

a

b



c **d**



e **f**

Nota. La figura 10, muestra el proceso de instalación de un dispositivo de gestión de entradas y salidas mediante RFID en un ascensor de la Clínica Medilink en Yopal, Casanare, desarrollado por S&S Ingeniería. Inicialmente, se observa la botonera de Hall del ascensor antes de la intervención (a), con un panel básico sin funciones avanzadas de autenticación. Posteriormente, se evidencia el resultado tras la instalación del sistema (b), donde se incorpora un lector de tarjetas RFID junto con un diseño más moderno y funcional. En la fase técnica, se instaló una tarjeta electrónica en el panel del Hall (c), diseñada para gestionar las señales provenientes del lector RFID y los botones de llamada. En el interior de la cabina del ascensor, se integró la tarjeta electrónica de cabina (d) que controla los comandos internos, conectando el lector RFID con los sistemas operativos del ascensor mediante relés y circuitos específicos. Para ello, fue necesario realizar perforaciones y ajustes estructurales en el panel (e) para adecuar el espacio al hardware requerido. Finalmente, se observa la botonera completa de la cabina (f), donde se

integraron los botones tradicionales con el lector RFID, asegurando la interoperabilidad entre el sistema de control de acceso y las funciones originales del ascensor. Este proceso no solo optimizó la seguridad del ascensor mediante un acceso restringido y automatizado, sino que también mejoró la disponibilidad del ascensor para atender las urgencias de la clínica en el menor tiempo posible.

Capacitación del Personal y Usuarios Sobre el Uso del Sistema

Como parte del proyecto, se llevó a cabo la capacitación del personal y de los usuarios del ascensor, enfocada en:

- Uso adecuado del nuevo sistema de control de acceso.
- Resolución de posibles inconvenientes.
- Protocolos de operación en casos de emergencia.

De esta manera, se está garantizando la correcta adopción y el funcionamiento eficiente del sistema por parte de todos los involucrados, mediante una capacitación práctica dirigida especialmente al personal de seguridad del centro médico (Figura 11). En la imagen (a) se está explicando detalladamente el funcionamiento del sistema desde el interior de la cabina del ascensor, mientras que en la imagen (b) se está revisando el sistema de control desde el panel externo. El acta correspondiente y la lista completa de asistentes se encuentran disponibles para consulta en el Anexo 1 y Anexo 2 respectivamente.

Figura 11

Capacitando a Personal de Seguridad del Centro Médico

(a)

(b)

Resultados

El proyecto consistió en el diseño, fabricación e implementación de dispositivos de gestión de entradas y salidas mediante RFID para los ascensores de la Clínica Medilink en Yopal, Casanare. Este sistema tuvo como propósito controlar el uso del ascensor camillero y asegurar la disponibilidad del mismo, garantizando su disponibilidad para emergencias y optimizando el flujo de personas.

Diseño e Implementación del Sistema

El diseño incluyó la creación de un circuito modular basado en microcontroladores ATmega328P y lectores de tarjetas RFID de 13.56 MHz. Estos módulos fueron integrados en las botoneras del Hall y de la cabina del ascensor. Para cada parada (Hall), se implementaron tarjetas electrónicas que gestionan el acceso mediante la validación de tarjetas RFID. En la cabina, un circuito adicional se encargó de habilitar los botones solo para usuarios autorizados. Este diseño permite un control descentralizado y seguro, adecuado para entornos hospitalarios.

Fabricación y Ensamblaje

La fabricación del sistema incluyó el diseño y producción de las placas de circuito impreso (PCB), optimizadas para condiciones de vibración y de temperatura propias del entorno hospitalario. Se realizaron perforaciones y ajustes estructurales en las botoneras para integrar los nuevos dispositivos sin afectar la operación original del ascensor. Las pruebas iniciales en el taller de S&S Ingeniería S.A.S garantizaron la correcta operatividad antes de la instalación definitiva.

Instalación

La instalación se llevó a cabo en un período de tres meses, siguiendo un cronograma de paradas programadas que minimizó la interrupción de las operaciones de la clínica. Durante cada

parada, se trabajaron dos botoneras del hall o la cabina, y se implementaron las siguientes actividades:

Desmonte y Traslado de las Botoneras al Taller

- Acondicionamiento y perforaciones para el montaje de los lectores RFID.

Instalación y programación de las tarjetas electrónicas en modo predeterminado.

- Reinstalación y pruebas funcionales del sistema.
- El sistema fue configurado para controlar 10 puntos de Hall y una cabina con dos puertas, distribuidos en seis plantas, y gestionó el acceso de hasta 100 usuarios registrados.

Capacitación y Puesta en Marcha

Se capacitó al personal y usuarios sobre el uso adecuado del sistema y los protocolos en caso de emergencias. Finalmente, se realizaron pruebas de integración y ajustes finales, verificando que todas las funciones operativas estuvieran alineadas con los objetivos del proyecto.

Discusión

El desarrollo de este sistema de control de acceso alcanzó los objetivos propuestos, siendo un modelo exitoso para la integración de tecnología RFID en entornos hospitalarios. A continuación, se analizan los resultados conforme a los objetivos específicos y el alcance del proyecto:

Diseño del Sistema

El diseño se fundamentó en la modularidad, flexibilidad y escalabilidad del sistema. El uso del microcontrolador ATmega328P fue una elección estratégica debido a su bajo consumo energético y su capacidad de procesamiento eficiente. Este diseño permite futuras actualizaciones y modificaciones sin necesidad de reemplazar completamente el sistema, lo que lo hace escalable para otros clientes que puedan requerir más puntos de control o usuarios en el futuro.

La integración de lectores RFID en las botoneras del ascensor permitió simplificar el acceso, eliminando problemas asociados con métodos más convencionales, como códigos PIN o llaves físicas. Además, la implementación de algoritmos de control aseguró que únicamente usuarios con tarjeras RFID puedan manipular el ascensor camillero.

Fabricación y Calidad

La calidad de los materiales y procesos de fabricación es un factor decisivo en la fiabilidad del sistema. Las placas PCB fueron diseñadas para minimizar interferencias electromagnéticas y soportar condiciones de uso intensivo. Esto garantizó la durabilidad del sistema en un ambiente donde las vibraciones y los cambios de temperatura son comunes.

Instalación y Adaptación

El cronograma de instalación demostró ser efectivo para reducir al mínimo la interrupción en las operaciones de la clínica. Las paradas programadas durante los fines de semana permitieron implementar el sistema de forma ordenada y garantizar su disponibilidad durante la semana para atender emergencias médicas.

El proceso de perforaciones y ajustes estructurales en las botoneras permitió una integración estética y funcional, asegurando que las modificaciones no afectaran la apariencia profesional del ascensor. Esta atención al detalle refuerza la importancia de la integración armoniosa entre tecnología y diseño en aplicaciones reales.

Capacitación y Usabilidad

La capacitación del personal fue esencial para garantizar la adopción del sistema y minimizar la resistencia al cambio. El uso de los dispositivos es sencillo y el tiempo de respuesta rápido facilitaron que los usuarios se familiarizaran rápidamente con el sistema, debido a que la interacción es solo acercar la Tarjeta RFID al lector. Además, la capacitación incluyó protocolos para emergencias, aumentando la confianza en el uso del sistema.

Contribución a la Seguridad

El proyecto cumplió su objetivo principal de mejorar la seguridad en el acceso a los ascensores. La combinación de autenticación mediante RFID y registro de auditoría fortaleció el control del flujo de personas. Esto no solo benefició a los pacientes y al personal médico, sino que también aumentó la confianza de la institución en la tecnología implementada.

Impacto en el Entorno Hospitalario

El sistema se adaptó perfectamente al entorno hospitalario, donde la higiene, la rapidez y la seguridad son aspectos prioritarios. La tecnología RFID eliminó la necesidad de contacto

físico con los dispositivos de acceso, una ventaja significativa en la prevención de infecciones. Además, al priorizar el uso del ascensor camillero para emergencias, se mejoró el tiempo de respuesta en situaciones críticas, alineándose con los objetivos operativos de la clínica.

Finalmente, el sistema de control de acceso implementado en la Clínica Medilink representa un avance significativo en la gestión de recursos hospitalarios. Este modelo puede ser replicado y adaptado a otras instituciones que enfrenten desafíos similares, destacando la importancia de integrar tecnología avanzada en entornos donde la seguridad y la eficiencia son fundamentales. Aunque el sistema cumplió con los objetivos, futuras mejoras podrían incluir la implementación de autenticación multifactor y análisis de datos para mejorar aún más el rendimiento y la seguridad.

Conclusiones

El diseño, fabricación e implementación del sistema de control de acceso para ascensores en la Clínica Medilink permite gestionar y optimizar los recursos hospitalarios. El proyecto cumple los objetivos planteados, demostrando resultados en seguridad, fiabilidad y eficiencia operativa. La integración de tecnología RFID permite el acceso prioritario al personal médico y pacientes en emergencias, limita el uso no autorizado del ascensor camillero y reduce los tiempos de traslado. El diseño modular, basado en el microcontrolador ATmega328P, facilita la implementación y permite futuras expansiones. Las pruebas realizadas verifican el funcionamiento del sistema y su capacidad para responder a las necesidades del entorno hospitalario.

Las contribuciones de este estudio se observan tanto en el ámbito práctico como técnico. Se desarrolló un modelo replicable y escalable aplicable a otras instituciones de salud con necesidades similares en la gestión de acceso a áreas restringidas. El uso de tecnología RFID junto a un diseño integrado de hardware y software presentó una solución funcional para entornos hospitalarios. La capacitación del personal y usuarios facilitó la adopción del sistema, y los datos obtenidos en las auditorías permitieron ajustar la gestión de recursos. El proyecto fortaleció la seguridad en la Clínica Medilink y proporcionó bases para futuras implementaciones tecnológicas en áreas críticas.

No obstante, este trabajo presenta ciertas limitaciones que abren camino para trabajo futuro. Aunque el sistema cumplió con los objetivos propuestos, la implementación de autenticación multifactor, como la combinación de RFID y biometría, podría incrementar aún más los niveles de seguridad. Adicionalmente, la integración de análisis de datos mediante tecnologías de IoT (Internet de las Cosas) podrá mejorar el rendimiento del sistema y permitir

respuestas más rápidas a eventos inusuales. Por último, explorar materiales más resistentes para los componentes podría aumentar aún más la durabilidad del sistema en condiciones adversas. Estas áreas de mejora futura representan una oportunidad para evolucionar este proyecto y mantener su relevancia en un entorno hospitalario en constante cambio.

Recomendaciones

Es altamente recomendable que futuras investigaciones en el área de control de acceso exploren la integración de tecnologías avanzadas que incrementen la seguridad y funcionalidad de estos sistemas. En particular, la implementación de autenticación multifactor, que combine la tecnología RFID con biometría (reconocimiento facial, huella dactilar), ofrece un nivel superior de protección frente a accesos no autorizados. Adicionalmente, la incorporación de tecnologías de Internet de las Cosas (IoT) permitiría habilitar el monitoreo del sistema, ofreciendo ventajas como la detección de patrones de uso y la identificación de anomalías operativas. Estas iniciativas pueden complementarse con estudios orientados al desarrollo de algoritmos más robustos para la encriptación de datos, protegiendo la comunicación del sistema frente a posibles vulnerabilidades. Asimismo, es pertinente investigar cómo estos sistemas pueden adaptarse a diferentes ambientes, como el industrial o educativo, para extender su aplicabilidad.

Por otro lado, para garantizar la mejora continua del sistema implementado, se sugiere establecer un programa de actualizaciones periódicas tanto para el software como para el hardware, con el fin de mantener la compatibilidad tecnológica y ampliar las capacidades del sistema. Un enfoque modular y escalable debe ser considerado para facilitar la expansión del sistema a nuevos puntos de acceso o usuarios sin necesidad de cambios significativos en la infraestructura existente. Además, resulta crucial diseñar un plan de mantenimiento preventivo que abarque la revisión regular de los componentes electrónicos, como lectores RFID y tarjetas de control, garantizando la fiabilidad operativa a largo plazo. Finalmente, se recomienda fortalecer las actividades de capacitación para el personal y usuarios, asegurando una correcta utilización del sistema y promoviendo la adopción de sus funcionalidades avanzadas, lo que

incrementará la efectividad y aceptación del sistema en el entorno hospitalario y en otros escenarios potenciales de aplicación.

Referencia Bibliográfica

Aldana Porras, J. M. (2018). *Diseño de un sistema de reconocimiento facial como medio de control de acceso biométrico mediado por técnicas de inteligencia artificial como herramienta base de seguridad del CEAD Ibagué.* Ibague: Universidad Nacional Abierta y a Distancia (UNAD), Escuela de Ciencias Básicas, Tecnología e Ingeniería.

Atmel Corporation, .. (2015). *ATmega328P: 8-bit AVR Microcontroller with 32K Bytes In-System Programmable Flash.* Obtenido de https://www.microchip.com/wwwproducts/en/ATmega328P

Bagga, P. D. (2022). Blockchain-envisioned access control for internet of things applications: A comprehensive survey and future directions. Telecommunication Systems,. *Springer*. doi:https://doi.org/10.1007/s11235-022-00938-7

Bolle, R. M. (2020). Biometrics: Personal Identification in Networked Society. *Springer*.

Caldón Cuchimba, J. A. (2020). *Prototipo RegistryUNAD como estrategia de control de entrada y salida de usuarios en la Universidad Nacional Abierta y a Distancia UNAD UDR La Plata Huila.* Universidad Nacional Abierta y a Distancia (UNAD), Escuela de Ciencias Básicas, Tecnología e Ingeniería (ECBTI).

Charbel El Gemayel, K. C. (2021). Automated face detection and control system using computer vision-based video analytics to avoid the spreading of COVID-19. *International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies.* IEEE. doi:https://doi.org/10.1109/3ICT53449.2021.9581593

Cristaldo, F. (2023). Investigación en seguridad del paciente en entornos hospitalarios. Revista Boaciencia. Salud y Medio Ambiente. *Boaciencia. Salud y Medio Ambiente*, 54-57. doi:https://doi.org/10.59801/sma.v3i1.93

González. (2023). *Seguridad en entornos hospitalarios.* revista de salud pública.

Héctor Eduardo Alarcón Castro, J. D. (2017). *Control de acceso e integración CCTV en línea en el edificio JC, municipio de Fusagasugá.* Universidad Nacional Abierta y a Distancia (UNAD), Escuela de Ciencias Básicas, Tecnología e Ingeniería (ECBTI).

hen, H. &. (2020). Analyzing the Security of PIN-based Access Control Systems. *Journal of Information Security and Applications*.

Huseinbegovic, S. K. (2009). Design and implementation of the CAN-based elevator control system. En 2009 IEEE Conference on Industrial Electronics and Applications (ICIEA). *IEEE*. doi:https://doi.org/10.1109/ICIEA.2009.5138705

Hussain, A.-S. T. (2023). Automated RFID-based attendance and access control system for efficient workforce management. *International Symposium on Innovative Approaches in Smart Technologies (ISAS)*, (págs. 1-7). doi:https://doi.org/10.1109/ISAS60782.2023.10391615

Instituto Colombiano de Normas Técnicas y Certificación, .. (2021). *Revisión técnico-mecánica de sistemas de transporte vertical y puertas eléctricas. Parte 1: Ascensores electromecánicos e hidráulicos.* ICONTEC.

Kim, D. &. (2022). Evaluating the Security of Mobile Access Control Systems in Modern Office Environments. *Journal of Information Security and Applications*.

Kushwaha, R. &. (2019). PUG-FB: Person-verification using geometric and Haralick features of footprint biometric. Multimedia Tools and Applications. *Springer*. doi:https://doi.org/10.1007/s11042-019-08149-0

Liu, W. L. (2013). Dispatching algorithm design for elevator group control system with Q-learning based on a recurrent neural network. *25th Chinese Control and Decision*

Conference (CCDC) (págs. 3397–3402). IEEE. doi:https://doi.org/10.1109/CCDC.2013.6561509

Mehdipour, Y. &. (2013). Hospital Information System (HIS): At a Glance. *Asian Journal of Computer and Information Systems*. Obtenido de https://www.researchgate.net/publication/329029643

Mezzanotte, P. P. (2021). Innovative RFID sensors for Internet of Things applications. *IEEE Journal of Microwaves*, 55-64. doi:https://doi.org/10.1109/JMW.2020.3035020

Sánchez Gómez, J. J. (2020). *Biometría y la seguridad informática en los métodos de autenticación.* Universidad Nacional Abierta y a Distancia (UNAD), Escuela de Ciencias Básicas, Tecnología e Ingeniería (ECBTI).

Woo-Garcia, R. M.-D.-H. (2016). Design and implementation of a system access control by RFID. *IEEE*. doi:https://doi.org/10.1109/SYSTEM.2016.24582

Xie, L. Y. (2014). Managing RFID data: Challenges, opportunities and solutions. *EEE Communications Surveys & Tutorials*, 1294–1314. doi:https://doi.org/10.1109/SURV.2014.022614.00143

Ye, J. H. (2016). Design of Model Elevator Control System Based on NI CompactRIO and LabVIEW. *nternational Symposium on Computational Intelligence and Design (ISCID)* (págs. 68-73). IEEE. doi:https://doi.org/10.1109/ISCID.2016.23

Zhang, Y. &. (2021). Advancements in RFID Technology for Smart Access Control. *IEEE Transactions on Industrial Electronics*, 2424-2433.

Zhong Wu, C. (2015). Design of electrical control system elevator based on VVVF. *International Conference on Computational Intelligence and Communication Networks (CICN)* (págs. 1490–1492). IEEE. doi:https://doi.org/10.1109/CICN.2015.288

Apéndices

Apéndice A

Acta de Capacitación al Personal de Seguridad en la Clínica Medilink en Yopal Casanare

Ciudad y fecha: Yopal, Casanare, 24/09/2024]

REF: ACTA DE CAPACITACIÓN

Argemiro Eliecer Amezquita Jiménez, certifica que se realizó satisfactoriamente la capacitación dirigida al personal de seguridad del **Centro Médico Medilink** en la calle 13 N° 29 – 41 de la ciudad de Yopal, siendo las 4:30 pm se inicia la capacitación con los siguientes temas:

1. Seguridad en Ascensores.
2. Identificación de Fallas y canales de Comunicación.
3. Entrega, manejo y permisos del nuevo sistema de Control de Acceso mediante tarjetas RFID.

Durante la capacitación se entregaron tarjetas RFID, explicándose claramente el uso correcto, asignación de permisos y limitaciones de acceso según las funciones del personal.

La capacitación se realizó en las instalaciones de **Centro Médico Medilink** con una duración de 2 horas.

Firman a continuación como constancia del desarrollo y participación en la capacitación:

Capacitador:
Nombre: Argemiro Amezquita Jimenez
Firma:
Cargo: Capacitador

Responsable Centro Médico Medilink:
Nombre: Karina Gutierrez
Firma:
Cargo: Administradora / RL

Apéndice B

Control de Asistencia de la Capacitación en el Centro Médico Medilink en Yopal-Casanare

CONTROL DE ASISTENCIA

Fecha: 24 Septiembre 2024
Lugar: Centro Médico Medilink - Yopal
Tema: Seguridad en Ascensores, Fallas, Canales de Comunicación y Control de Acceso con tarjetas RFID

Nº	Nombre Completo	Cargo	Documento	Firma
1	Pedro Sanchez V.	Guarda de seguri		
2	ANDREA CASTAÑO G	RECEPCIÓN		
3	[illegible]	[illegible]		
4	[illegible]	[illegible]		
5				
6				
7				
8				
9				

Observaciones:

Firma del responsable de la Capacitación:

Nombre: Argenoro Amezquita Jimenez
Cargo: Capacitador
Firma: