Torniquete la Nueva Adquisición

Jefferson David Villegas Cañon

Asesor

Msc. Ing. Sandra Milena García Ávila

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Ingeniería Electrónica

2025

Agradecimientos

Agradezco de manera especial a la ingeniera Sandra Milena García Ávila, por su valiosa orientación, acompañamiento y apoyo durante el desarrollo de este proyecto. Su dedicación, conocimientos y compromiso fueron fundamentales para la correcta ejecución y culminación del trabajo.

Le expreso mi más sincero reconocimiento y gratitud por su tiempo, disposición y por compartir su experiencia a lo largo de este proceso.

Resumen

Este proyecto consiste en la implementación de un sistema automatizado de control de acceso para una institución educativa, basado en torniquetes peatonales con tecnología RFID, y complementado por una aplicación móvil que permite el uso de carnets físicos y virtuales.

La solución fue desarrollada para reemplazar el anterior método manual de registro de ingreso mediante minutas, que generaba demoras, errores y poca trazabilidad. Se instalaron dos torniquetes bidireccionales, controlados por dos unidades SAC 3008 IP-B, conectadas a una red local a través de un switch Oracle Gigabit de 8 puertos y gestionadas mediante el software Siera SAC 4000, alojado en un servidor con acceso remoto. El sistema permite la validación de identidad por medio de carnets con código RFID y también mediante códigos QR generados por una aplicación institucional.

La infraestructura fue adecuada para garantizar estabilidad, seguridad y protección eléctrica. Se realizaron obras de canalización para el cableado de red (CAT6a) y alimentación, y se instaló una fuente de poder EBCHQ de 24VDC por torniquete. Además, se integraron medidas de seguridad eléctrica según normas RETIE y NTC 2050, incluyendo puesta a tierra, protecciones contra cortocircuitos y dispositivos de corte.

Durante la implementación se enfrentaron y solucionaron desafíos técnicos relacionados con la conectividad de red, actualización de firmware y filtraciones en la estructura del torniquete, evidenciando la importancia del mantenimiento preventivo y las pruebas piloto.

Este sistema no solo mejora el control de acceso, reduciendo el margen de error humano y mejorando la seguridad institucional, sino que también constituye una plataforma escalable y replicable para otras organizaciones que busquen modernizar su gestión de ingresos mediante tecnologías RFID, redes IP y aplicaciones móviles.

Palabras Claves**:** Códigos QR, NTC 2050, RETIE, Switch Oracle, Tecnología RFID.

Abstract

This project involves the implementation of an automated access control system for an educational institution, based on pedestrian turnstiles with RFID technology, complemented by a mobile application that allows the use of physical and virtual ID cards.

The solution was developed to replace the previous manual method of registering entry using timesheets, which generated delays, errors, and poor traceability. Two bidirectional turnstiles were installed, controlled by two SAC 3008 IP-B units, connected to a local network via an 8-port Oracle Gigabit switch and managed using Sierra SAC 4000 software, hosted on a server with remote access. The system allows identity validation using ID cards with RFID codes and also through QR codes generated by an institutional application.

The infrastructure was adequate to ensure stability, security, and electrical protection. Conduit work was carried out for network cabling (CAT6a) and power, and a 24VDC EBCHQ power supply was installed per turnstile. Additionally, electrical safety measures were integrated in accordance with RETIE and NTC 2050 standards, including grounding, short-circuit protection, and cut-off devices.

During the implementation, technical challenges related to network connectivity, firmware updates, and leaks in the turnstile structure were addressed and resolved, highlighting the importance of preventive maintenance and pilot testing.

This system not only improves access control, reducing the margin of human error and enhancing institutional security, but also provides a scalable and replicable platform for other organizations seeking to modernize their revenue management using RFID technologies, IP networks, and mobile applications.

Keywords: QR Codes, NTC 2050, RETIE, Oracle Switch, RFID Technology.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Introducción

En el contexto actual, las instituciones educativas enfrentan desafíos cada vez mayores en materia de seguridad, eficiencia operativa y trazabilidad de accesos. Tradicionalmente, el control de ingreso de personal y visitantes se realizaba mediante registros manuales en minutas físicas, un método que, aunque funcional en su momento, presenta múltiples limitaciones: demoras en los tiempos de acceso, errores de registro por causas humanas, dificultad para verificar la autenticidad de la información y ausencia de datos en tiempo real. Esta situación se traduce en un control de acceso vulnerable y poco eficiente, que no se ajusta a las exigencias actuales de seguridad y administración institucional (López & Sánchez, 2021).

Frente a esta problemática, las tecnologías de identificación automática han emergido como soluciones viables y probadas. La Identificación por Radiofrecuencia (RFID) y los códigos QR, por ejemplo, permiten validar identidades de manera rápida, segura y sin contacto físico, ofreciendo además la posibilidad de integrarse con sistemas de monitoreo y bases de datos centralizadas (Al-Maitah, Hajjaj & Abu-Dalhoum, 2021). Estudios recientes evidencian que la adopción de sistemas automatizados de control de acceso en entornos académicos incrementa la eficiencia en un 40 % y reduce incidentes de ingreso no autorizado en más de un 60 % (García-Hernández et al., 2020). En este escenario, la implementación de torniquetes electrónicos con tecnologías de identificación avanzada se presenta como una estrategia idónea para responder a las demandas de seguridad y modernización de las instituciones de educación superior.

En el caso específico de la institución objeto de este proyecto, el método manual de ingreso mediante minuta generaba congestión en horas pico, ausencia de trazabilidad confiable y dificultades para integrar la información con otros sistemas administrativos. La necesidad de contar con un sistema que ofreciera mayor agilidad, precisión y control llevó a la decisión de

diseñar e implementar un sistema automatizado de control de acceso basado en torniquetes peatonales, integrados con lectores RFID y validador de códigos QR a través de una aplicación móvil institucional.

La solución planteada se sustenta en fundamentos técnicos propios de la ingeniería electrónica, la automatización y el desarrollo de software. El sistema está compuesto por dos torniquetes bidireccionales controlados por unidades SAC 3008 IP-B, conectadas a una red local mediante un switch Gigabit y gestionadas con el software Siera SAC 4000 alojado en un servidor institucional. Este diseño permite validar el acceso tanto con carnets físicos (RFID) como con carnets virtuales generados desde la aplicación móvil, ofreciendo flexibilidad y adaptabilidad ante distintos escenarios de uso. La elección de la tecnología RFID se basó en su velocidad de lectura, alta durabilidad y capacidad de integración con sistemas de gestión de asistencia y seguridad. Los códigos QR, por su parte, complementan la solución al ofrecer un método alternativo de acceso sin contacto y de bajo costo, ideal para usuarios temporales o en caso de pérdida del carnet físico.

La implementación requirió adecuaciones en la infraestructura física y de red, incluyendo canalización para cableado estructurado CAT6a, instalación de fuentes de alimentación protegidas y cumplimiento de normas RETIE y NTC 2050 para garantizar la seguridad eléctrica. Asimismo, se llevaron a cabo pruebas de conectividad, validación de firmware, ajustes de red y medidas de protección contra humedad en la estructura de los torniquetes. El proyecto no solo resolvió la problemática inicial, sino que dejó instalada una plataforma escalable y replicable, que puede adaptarse a futuras expansiones o integraciones con otras tecnologías de seguridad, como biometría o sistemas de videovigilancia inteligente.

Planteamiento del Problema

En el proceso de ingreso y control del personal en las instalaciones de la empresa, tradicionalmente se utilizaba un sistema basado en la anotación manual en minutas por parte del personal de seguridad para registrar la entrada y salida de los empleados. Este método implicaba verificar físicamente la identidad de cada trabajador mediante listas impresas, lo que generaba múltiples dificultades operativas, tales como errores humanos, registros incompletos, demoras considerables en los tiempos de acceso, así como problemas de gestión en términos de eficiencia y seguridad (López & Sánchez, 2021).

Para abordar estas limitaciones, la empresa decidió implementar un sistema basado en torniquetes electrónicos que operan mediante tecnología de identificación por radiofrecuencia (RFID). Este nuevo mecanismo utiliza carnets físicos y virtuales, facilitando una validación más ágil y precisa del personal autorizado para ingresar a áreas restringidas. Dicha solución tecnológica busca minimizar la intervención manual, mejorar la velocidad del proceso de ingreso y ofrecer una trazabilidad precisa de los movimientos de entrada y salida (Moreno, 2020).

Por tanto, el problema principal reside en asegurar una implementación efectiva del sistema de torniquetes RFID, logrando superar las barreras de adaptación técnica y organizacional, garantizando así la eficiencia, seguridad y continuidad operativa en el control de acceso de personal (Fernández, Pérez & Rodríguez, 2021).

Antecedentes del Problema

En los últimos años, las universidades han experimentado un avance significativo en la implementación de sistemas tecnológicos para mejorar el control de acceso a sus instalaciones. Tradicionalmente, muchos centros educativos dependían de métodos manuales como el uso de minutas para registrar la entrada y salida de estudiantes, docentes, funcionarios y proveedores.

Sin embargo, este enfoque presentaba limitaciones en cuanto a la eficiencia, precisión y seguridad, lo que llevó a la adopción de tecnologías más avanzadas. Un ejemplo de esta transición se encuentra en varias universidades que han optado por la implementación de torniquetes electrónicos equipados con tecnología RFID (Identificación por Radiofrecuencia), lo que permite un control más ágil y seguro de las personas que acceden al campus. Hasta 2006, el acceso al campus se realizaba de manera manual, con vigilantes revisando físicamente los carnets.

El uso de carnets con chips RFID ha facilitado la automatización del proceso de ingreso, ya que los torniquetes leen la información del carnet de forma rápida y precisa, evitando errores humanos. Además, algunos de estos sistemas están integrados con plataformas web que permiten verificar, en tiempo real, si una persona tiene acceso autorizado. Esta solución no solo mejora la seguridad, sino que también optimiza la gestión de la asistencia y el control de accesos en diferentes áreas del campus, como aulas, laboratorios o zonas restringidas. la Universidad de Guayaquil en Ecuador, han integrado tecnologías IoT y RFID para ofrecer soluciones de control de acceso más efectivas y seguras. Universidad de Guayaquil. (2021).

La integración de estos sistemas tecnológicos ha demostrado ser beneficiosa no solo en términos de eficiencia, sino también en la mejora de la experiencia del usuario, al permitir un acceso más rápido y libre de errores. La evolución hacia el uso de torniquetes y RFID refleja una tendencia global en la modernización de los sistemas de seguridad en universidades y otras instituciones educativas, respondiendo a las demandas de mayor control y automatización en los procesos administrativos y de acceso. En este contexto, la implementación de una plataforma web para la verificación del acceso contribuye significativamente a la supervisión en tiempo real,

proporcionando a las autoridades universitarias una herramienta adicional para gestionar y monitorear los accesos de manera eficaz.

Justificación

La implementación de un sistema de acceso controlado mediante torniquetes automatizados y carnets virtuales con tecnología RFID se encuentra ampliamente justificada debido al impacto positivo que genera en los ámbitos académico, operativo, económico y de seguridad institucional. En un entorno en el que la eficiencia, la seguridad y la trazabilidad de los procesos adquieren creciente relevancia, resulta esencial disponer de herramientas tecnológicas que permitan gestionar el ingreso de personas de forma ágil, precisa y confiable.

En el contexto previo a la modernización, el acceso a las instalaciones de la institución se realizaba mediante una minuta física, la cual debía ser diligenciada manualmente por el personal de seguridad en cada punto de control. Aunque este procedimiento fue funcional durante cierto tiempo, presentaba diversas limitaciones. Entre ellas, se destacaban las demoras durante los horarios de alta afluencia, la dificultad para realizar un seguimiento en tiempo real de los accesos y la alta probabilidad de errores humanos que afectaban la precisión de los registros. Asimismo, el carácter manual del proceso impedía la generación automatizada de reportes e impedía la integración con otros sistemas institucionales, como los de nómina o control académico.

Con el objetivo de superar estas deficiencias, la organización procedió a la implementación de un sistema automatizado de control de acceso, basado en torniquetes inteligentes activados mediante carnets Físicos y virtuales alojados en una aplicación móvil. Estos carnets, operativos mediante códigos QR o tecnología de identificación por radiofrecuencia (RFID), permiten la validación de identidad sin contacto físico. Este mecanismo no solo acelera el ingreso de usuarios, sino que además incrementa los niveles de seguridad institucional, al restringir el paso únicamente a personas debidamente autorizadas. Adicionalmente, el sistema se complementa con plataformas en la nube que registran cada ingreso en tiempo real, integrándose

con sistemas de videovigilancia que fortalecen la trazabilidad de cada movimiento dentro del recinto.

Desde una perspectiva académica y disciplinar, este proyecto constituye una oportunidad valiosa para la aplicación de principios propios de la ingeniería electrónica, la automatización y el desarrollo de software. En su desarrollo, se incluyen actividades relacionadas con el diseño e integración de sistemas embebidos, sensores, protocolos de comunicación y aplicaciones móvil virtuales, lo cual contribuye al fortalecimiento de la formación técnica y profesional de los estudiantes participantes. De igual forma, responde a las exigencias contemporáneas de transformación digital, modernización institucional y sostenibilidad operativa (Ministerio de Educación Nacional de Colombia, 2022).

Objetivos

Objetivo General

Implementar una aplicación móvil que automatice la transición de carnets físicos a carnets virtuales, con el fin de optimizar el proceso y mejorar la experiencia de los empleados y usuarios de la institución.

Objetivos Específicos

Implementar la infraestructura donde se realizará la instalación de los equipos.

Completar el software el cual sincroniza los torniquetes con la controladora.

Realizar las pruebas requeridas para que no haya problemas a la hora de la prueba piloto.

Marco Teórico y Conceptual

Marco Teórico

El diseño del proyecto se fundamenta en la integración de diversos elementos clave que garantizan su implementación de manera eficaz. En primer lugar, se utilizará un computador de escritorio como equipo principal para el desarrollo y diseño de la aplicación, complementado con un dispositivo móvil que permitirá realizar pruebas y verificar la apariencia y funcionalidad de la app en distintos formatos. La nube desempeñará un papel esencial al almacenar de forma segura los datos de los usuarios, facilitando la gestión remota y protegida del acceso y la autorización. Por su parte, los torniquetes serán dispositivos cruciales para registrar y controlar el ingreso a la empresa, asegurando que solo las personas autorizadas puedan acceder a las instalaciones. Además, los celulares serán empleados por los usuarios para validar su entrada mediante códigos QR o RF, optimizando el proceso de acceso. Finalmente, el sistema contará con cámaras de seguridad integradas que permitirán monitorear el uso de los torniquetes y la seguridad del personal, ofreciendo así una capa adicional de protección frente a cualquier incidente.

Computadores y Dispositivos Móviles. Los computadores de escritorio son herramientas esenciales en el desarrollo de software, ya que ofrecen la capacidad de procesamiento necesaria para diseñar, programar y probar aplicaciones complejas. Según Sommerville (2011), el desarrollo de software requiere un entorno de trabajo que permita realizar simulaciones y pruebas en diversos formatos. Además, los dispositivos móviles son indispensables en el diseño centrado en el usuario, ya que permiten probar la funcionalidad y adaptabilidad de las aplicaciones en diferentes resoluciones y tamaños de pantalla, asegurando una experiencia óptima para los usuarios finales (Nielsen, 1993).

Computación en la Nube. La computación en la nube es una tecnología que permite almacenar y gestionar datos de forma remota, brindando acceso a servicios en tiempo real desde cualquier ubicación. Según Mell y Grancé (2011), los servicios en la nube ofrecen escalabilidad, seguridad y flexibilidad, características esenciales para proyectos que manejan datos sensibles, como la información de acceso y autorización. Esta tecnología también facilita la integración de múltiples dispositivos en un ecosistema compartido. Para este proyecto se realizó el uso de un servidor el cual se encuentra alojado en la nube de la institución.

Torniquetes y Control de Acceso. Los torniquetes son dispositivos de control físico utilizados para regular el acceso a instalaciones. Están diseñados para permitir el paso de una persona a la vez, garantizando un registro preciso. Según Norman (1988), estos dispositivos forman parte de los sistemas de interacción humano-máquina y deben estar diseñados para maximizar la seguridad y minimizar la fricción en su uso. Integrar estos dispositivos con tecnologías de identificación, como códigos QR o RF, mejora significativamente la eficiencia y el control.

Dispositivos Móviles y Tecnologías de Identificación. El uso de dispositivos móviles para la validación de acceso mediante códigos QR o tecnologías de radiofrecuencia (RF) es cada vez más común en entornos empresariales. Los códigos QR, según su descripción técnica (ISO/IEC 18004:2015), son matrices bidimensionales capaces de almacenar información de forma compacta y rápida, lo que los hace ideales para autenticar usuarios en tiempo real. Por otro lado, las tecnologías RF, como el NFC, permiten una interacción más fluida entre el dispositivo móvil y los torniquetes, eliminando la necesidad de contacto físico y reduciendo el tiempo de acceso.

Cámaras de Seguridad y Sistemas de Monitoreo. Las cámaras de seguridad son una herramienta clave en sistemas de control de acceso, ya que permiten monitorear y registrar actividades en tiempo real. Según el principio de la vigilancia de circuito cerrado (Gill & Spriggs, 2005), la integración de cámaras con torniquetes y dispositivos móviles proporciona un nivel adicional de seguridad, permitiendo la identificación visual de incidentes y asegurando que los accesos sean realizados por personas autorizadas.

RETIE y NTC 2050. En principio la responsabilidad de proteger el sistema eléctrico y asegurar la continuidad del servicio de energía recae en los operadores de red, pero también es obligación de los tenedores y usuarios garantizar que sus instalaciones eléctricas permanezcan en condiciones seguras y óptimas, es por esto que la operación de la red eléctrica también se rige por unas normas de seguridad y parámetros que se deben exigir e implementar por el operador de red, profesional técnico y usuario.

El RETIE abreviatura para el Reglamento Técnico de Instalaciones Eléctricas, es un documento técnico-legal para Colombia expedido por el Ministerio de Minas y Energía, su primera publicación fue el 7 de abril de 2004 mediante la Resolución No. 180398; este documento debe ser aplicado a los procesos de Generación, Transmisión, Transformación, Distribución y Utilización de la energía eléctrica en todo el territorio de la República de Colombia, sus aguas territoriales y su plataforma continental.

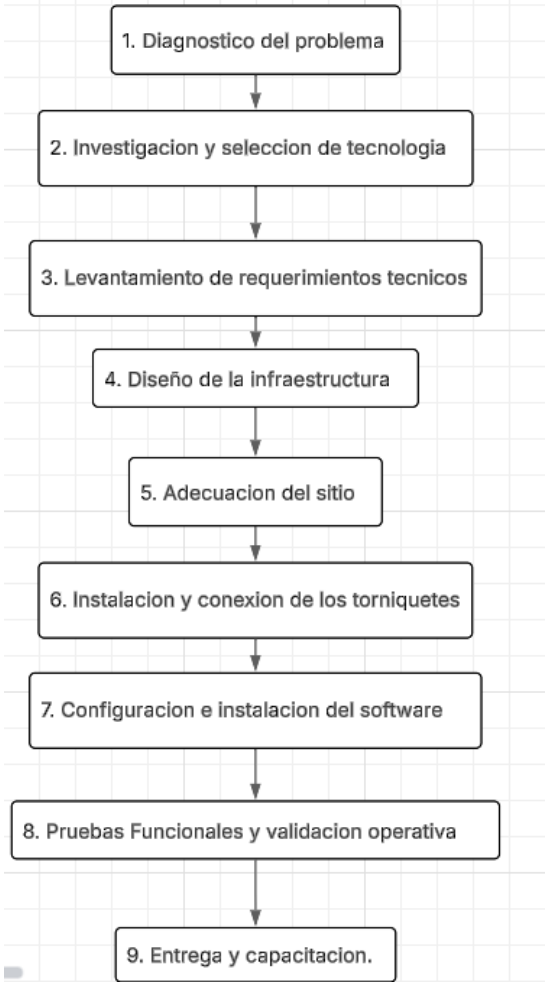
Su principal objetivo es establecer medidas que garanticen la seguridad de las personas, vida animal y vegetal, y la preservación del medio ambiente, previniendo, minimizando o eliminando los riesgos de origen eléctrico. Conte (2023) Que es el RETIE y que es la NTC 2050 https://www.conte.org.co/que-es-el-retie-y-que-es-la-ntc-2050/

Metodología

El enfoque metodológico del presente proyecto es mixto, ya que combina elementos cuantitativos y cualitativos en el análisis, diseño e implementación del sistema de control de acceso mediante torniquetes automatizados y carnets virtuales. Desde la perspectiva cuantitativa, se recopilan datos técnicos y operativos sobre el funcionamiento del sistema, como tiempos de ingreso, número de accesos autorizados y trazabilidad de movimientos. Por otro lado, el enfoque cualitativo permite analizar las percepciones de los usuarios y del personal encargado del control de acceso, evaluando así la usabilidad y aceptación de la aplicación móvil. Esta investigación se clasifica como un proyecto aplicado con enfoque experimental-descriptivo, pues propone una solución tecnológica concreta a una problemática real, desarrollando un prototipo funcional que es implementado, probado y validado en un entorno institucional. El desarrollo del proyecto se llevó a cabo en fases: estudio del problema, recolección de requerimientos, descripción y selección de equipos, implementación física y lógica del sistema, puesta en marcha del software, pruebas funcionales y validación del sistema en condiciones reales.

Figura 1

Diagrama de Flujo Metodología



Nota. Paso a paso de la metodología realizada

A continuación, se muestra el desarrollo de cada uno de los pasos de la metodología.

Etapa 1: Diagnóstico del Problema y Análisis de Necesidades

Se llevó a cabo una reunión de evaluación en la que se identificó una ineficiencia en el proceso de control de ingreso a la institución, debido al tiempo excesivo que tomaba el personal de seguridad en registrar manualmente, mediante una minuta, a cada persona que accedía a las

instalaciones. Esta limitación impactaba negativamente en la agilidad operativa y la trazabilidad de los registros. Como resultado, se inició un proceso de análisis e investigación de tecnologías disponibles en el mercado que permitieran optimizar y automatizar el control de acceso, garantizando mayor eficiencia, seguridad y trazabilidad en el sistema de registro de visitantes y personal autorizado.

Etapa 2 Investigación y Selección Tecnológica

Esta situación, inició un proceso de análisis técnico para identificar e implementar soluciones tecnológicas que permitieran optimizar el control de acceso. Entre las opciones evaluadas se consideraron sistemas basados en identificación biométrica (huella digital y reconocimiento facial), tarjetas de proximidad con tecnología RFID (Radio Frequency Identification) y lectores QR vinculados a credenciales virtuales. Estas tecnologías ofrecen una respuesta más eficiente, segura y confiable, mejorando significativamente los tiempos de ingreso, la precisión en la identificación de personas y la generación automática de reportes de auditoría.

Tabla 1

Ventajas y Desventajas de las Diferentes Tecnologías.

Tecnología	Ventajas de RFID en Torniquetes de Acceso	Desventajas de RFID en Torniquetes de Acceso
RFID	1. Acceso sin contacto: Los usuarios pueden simplemente acercarse al torniquete sin necesidad de contacto físico con el dispositivo. Esto aumenta la velocidad y la comodidad del acceso. 2. Lectura rápida y simultánea: Puede leer múltiples tarjetas o etiquetas al mismo tiempo, lo que facilita el flujo de personas en lugares con mucho tráfico.	1. Costo inicial: La implementación de lectores y etiquetas RFID puede tener un costo más elevado que los sistemas tradicionales como los de tarjetas de proximidad. 2. Interferencia: En algunas condiciones (por ejemplo, ambientes con metales o líquidos), las señales RFID pueden verse afectadas. Sin embargo, esto es más común en RFID de larga distancia que en RFID de corto alcance.

Tecnología	Ventajas de RFID en Torniquetes de Acceso	Desventajas de RFID en Torniquetes de Acceso
	3. Mayor seguridad: Las tarjetas o pulseras RFID pueden ser protegidas con algoritmos de cifrado, mejorando la seguridad frente a la clonación o falsificación de accesos.	3. Baterías en etiquetas activas: Las etiquetas RFID activas requieren mantenimiento debido a las baterías, aunque las pasivas no tienen este inconveniente.
	4. Durabilidad: Las tarjetas o etiquetas RFID, al ser robustas, resisten el desgaste, lo cual es ideal para sistemas de acceso que tienen que soportar uso frecuente.	4. Dependencia de la infraestructura: Requiere de lectores y antenas específicas, lo que puede hacer más complejo y costoso el sistema de instalación inicial.
Códigos de barras	1. Bajo costo: Las tarjetas con códigos de barras son mucho más económicas que las etiquetas RFID.	1. Necesidad de línea de vista: El código de barras necesita ser escaneado directamente, lo que ralentiza el proceso de acceso.
	2. Simplicidad: Son fáciles de implementar y ampliamente entendidos, por lo que la curva de aprendizaje es mínima.	2. Durabilidad limitada: Los códigos de barras pueden desgastarse con el tiempo o dañarse, lo que hace que no sean tan adecuados para accesos frecuentes.
	3. Requiere menos infraestructura: Un lector de códigos de barras es generalmente más barato y fácil de integrar en el sistema.	3. Velocidad de acceso reducida: El escaneo de códigos de barras es más lento y puede generar congestión en puntos de acceso con muchas personas.
Tarjetas de proximidad (NFC/Bluetooth)	1.Acceso rápido: Similar a RFID, las tarjetas de proximidad permiten acceso rápido sin contacto físico.	1. Rango limitado: Los sistemas de proximidad (especialmente NFC) tienen un alcance más corto que RFID, lo que puede requerir que las personas se acerquen más al lector.

Tecnología	Ventajas de RFID en Torniquetes de Acceso	Desventajas de RFID en Torniquetes de Acceso
	2. Seguridad mejorada: Las tarjetas de proximidad y NFC son más difíciles de clonar que las tarjetas tradicionales.	2. Costo más alto: Las tarjetas de proximidad suelen ser más caras que las etiquetas RFID pasivas. Además, la infraestructura de lectura es generalmente más cara.
	3. Mayor flexibilidad: Algunas tarjetas de proximidad también pueden integrarse con sistemas de pago, control de acceso y más.	3. Interferencia: Al igual que RFID, pueden verse afectadas por ciertos entornos (por ejemplo, alrededor de metales o líquidos).
Reconocimiento facial o biometría	1. Sin contacto: Evita la necesidad de llevar tarjetas o etiquetas, ya que el acceso se da mediante identificación biométrica.	1. Alta inversión inicial: Los sistemas biométricos, como el reconocimiento facial, requieren tecnología avanzada y pueden ser costosos de instalar y mantener.

Nota. Tabla con las diferentes tecnologías en base a la investigación

Como resultado del análisis de la tabla 1 anterior, se determinó la viabilidad de implementar un sistema basado en tarjetas de proximidad con tecnología RFID (Radio Frequency Identification). Ya que es un sistema que nos proporciona unas mejores ventajas frente a las otras tecnologías mencionadas. Este tipo de solución nos permite asignar a cada usuario una credencial única e intransferible, lo cual garantiza un nivel elevado de seguridad, así nos facilita la identificación automatizada y agiliza el proceso de ingreso. La elección de esta tecnología también permite una fácil integración con sistemas de control de asistencia y generación de reportes centralizados.

Etapa 3 Levantamiento de Requerimientos Técnicos

Dado que son dos torniquetes, cada uno con dos accesos, se tuvo en cuenta las siguientes consideraciones para asegurar un funcionamiento adecuado:

Espacio para los Torniquetes. Cada torniquete se requirió un espacio libre adecuado en el cual se realizó la instalación y operación sin tener alguna obstrucción en el espacio.

Dimensiones Mínimas. *Los* torniquetes de acceso requirieron un ancho de entre 70 y 90 cm por cada carril. Como en este caso, hay dos accesos por torniquete, el espacio total requerido para cada unidad de torniquete es de 1,4 a 1,8 metros. Esto incluye el espacio para el paso de las personas y el margen de seguridad alrededor del dispositivo.

Espacio para los cables. para este espacio de los torniquetes, fue necesario incluir un área de canalización y ductos para el tendido de cables de red y energía, ya que van por pasados por el suelo y las paredes.

Etapa 4: Diseño de la Infraestructura

Adecuación de la Infraestructura de Red (Puntos de Conexión y Switch Oracle)

Se debe asegurar que la infraestructura de red esté optimizada para garantizar una conexión eficiente entre los torniquetes, el switch Oracle y las controladoras de acceso. Las consideraciones fueron las siguientes:

Puntos Conexión de Red (CAT6a)

- Se requirieron dos puntos de conexión de red (CAT6a) para la conexión de los torniquetes y las controladoras. Cada torniquete está conectado a un puerto de red para transmitir datos a la controladora. Para los dos torniquetes.
- El cableado de red se instalado de acuerdo con las mejores prácticas de tendido, utilizando canalizaciones y ductos protegidos para evitar daños. La instalación se cumplió con las normas de seguridad eléctrica y las especificaciones de distancia máxima para cable CAT6a (100 metros sin pérdida de señal).

- Switch Oracle: El switch Oracle se encarga de gestionar las conexiones de red entre los torniquetes, controladoras y otros dispositivos. Para así asegurar un rendimiento adecuado, este switch cuenta con 8 puertos en gigabit, dado que se conectó 4 dispositivos de red).
- se tomó la decisión de dejar el switch en uno de los cuartos donde se encuentra el supervisor de seguridad y así tener una mejor confianza en que no le va a pasar nada al rack ya que debe tener una llave para poder ingresar a ese cuarto.
- Se verificó que el switch Oracle esté configurado correctamente para manejar la cantidad de tráfico que se espera del sistema de control de acceso, teniendo en cuenta que los torniquetes están enviando datos sobre las autorizaciones de acceso y otros registros en tiempo real.

Etapa 5: Adecuación del Sitio

Adecuación del Piso (Ladrillo) para la Instalación

- El piso de ladrillo en el área de instalación se preparó para asegurar que tanto los torniquetes como el sistema de cableado se instalaran de forma adecuada:
- Nivelación del Piso: Se verifico que el piso de ladrillo esté nivelado. Un piso irregular podía afectar la estabilidad de los torniquetes, lo que podría causar un funcionamiento defectuoso.
- Canalización para Cables: Los cables de red CAT6a, al igual que los cables de alimentación, se instalaron de manera que estén protegidos y no interfieran con el flujo de personas o la funcionalidad de los torniquetes. Para que esto fuera realizado se hizo la instalación un ducto en el suelo para cada torniquete el cual lleva un cable de corriente y el cable de cat 6ª para la comunicación con el rack.

Consideraciones de Seguridad

- Se considero relevante que las salidas de emergencia o rutas de acceso también fueron consideradas en la disposición de los torniquetes, para que así no interfiera con el flujo de personas durante una evacuación o situación de emergencia como se puede observar en la imagen a continuación.

Figura 2

Salidas de Emergencias

Nota. Autoría propia

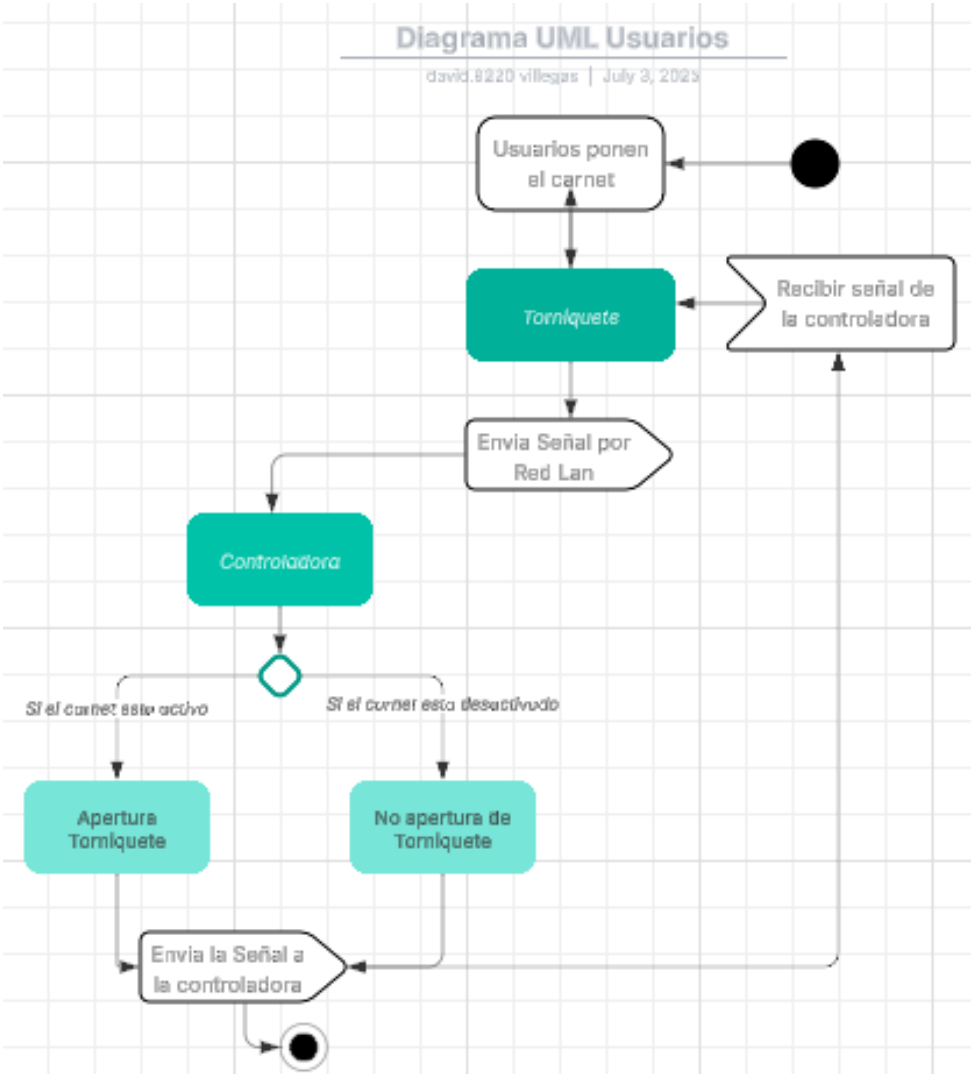
Etapa 6: Instalación y Conexión de los Torniquetes

Conexión de los Torniquetes a las Controladoras. Cada torniquete se conectó a una controladora de acceso a través de los cables de red (CAT6a). Los torniquetes previamente se configuraron correctamente para enviar los datos de acceso (RFID) a la controladora para su validación.

Configuración e Instalación del Software de Control

Figura 3

Diagramas en Base UML (Lenguaje de Unificado) para Usuarios



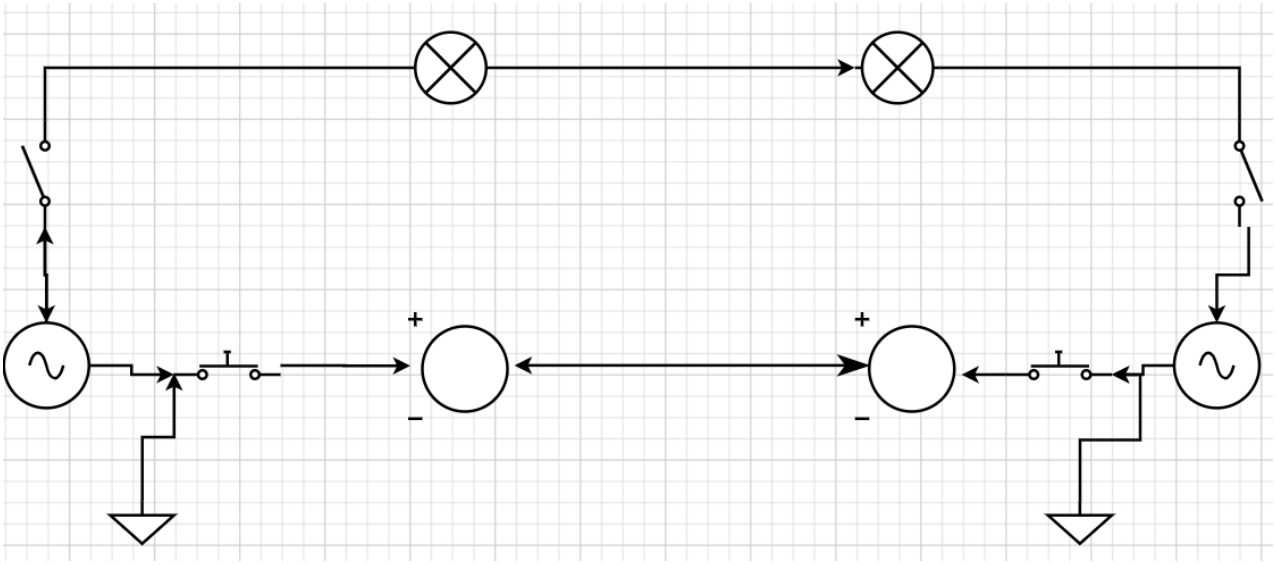
Nota. Autoría propia

Esquema Eléctrico del sistema de torniquete. En el diagrama eléctrico se presenta una vista general del diseño del sistema, mostrando su configuración y distribución de componentes. Este esquema fue desarrollado bajo principios de mantenibilidad, seguridad y eficiencia,

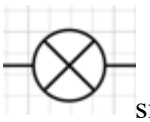
permitiendo que, ante una posible falla o evento inesperado, el análisis y diagnóstico puedan realizarse de forma rápida y precisa. El diseño eléctrico asegura un adecuado balance de carga entre las fases, evitando sobrecargas y garantizando una operación estable y segura del sistema. Asimismo, se cumple con lo establecido en el Reglamento Técnico de Instalaciones Eléctricas (RETIE) y en la Norma Técnica Colombiana NTC 2050, que exigen que todos los sistemas eléctricos cuenten con protecciones contra cortos circuitos, fallas a tierra y dispositivos de puesta a tierra debidamente instalados. Estas consideraciones aseguran la protección de los equipos, la integridad del sistema y la seguridad de los usuarios.

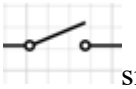
Figura 4

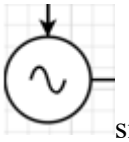
Esquema Eléctrico

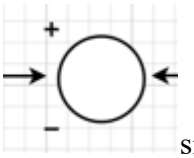


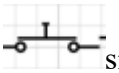
Nota. Esquema eléctrico usado en el proyecto aplicado

 simboliza las dos luminarias empotradas en la parte del techo dando así luz cuando llega las horas en las cuales no se puede visualizar los torniquetes y se pueden encender desde su respectivo interruptor.

 simboliza el encendido y apagado de cada luminaria independiente.

 simboliza la fuente la cual alimenta tanto a las luminarias como a los torniquetes.

 simboliza el tomacorriente la cual fue instala en cada torniquete para así poder conectar los equipos que necesiten 120V (Voltios)

 simboliza el breaker instalado de manera independiente para así poder proteger el sistema en caso de un bajón de energía o corto circuito en el sistema.

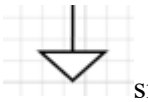
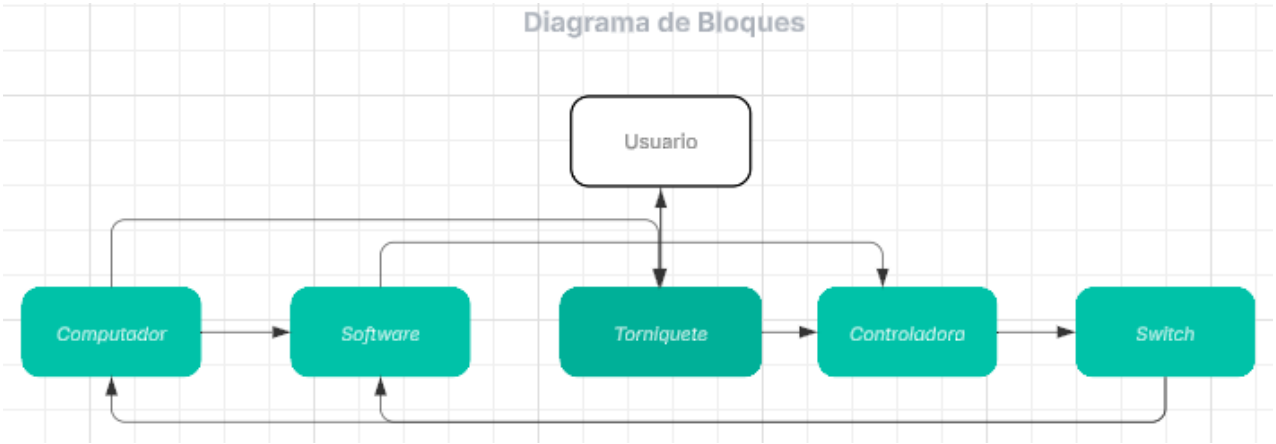
 simboliza la puesta tierra para protección de todo el sistema el cual su función va a ser absorber los cortos y sobrecargas.

Diagrama de Bloques. El diagrama de bloques presentado ilustra la arquitectura funcional del sistema de control de acceso mediante torniquetes implementado en la universidad. El proceso inicia con la interacción del usuario, quien se autentica a través del torniquete. Este equipo está directamente vinculado a una controladora que gestiona la señal recibida y la

comunica al software de control instalado en un computador. El software es el encargado de validar la información del usuario y autorizar o denegar el acceso, generando una respuesta en tiempo real hacia la controladora. A su vez, la comunicación entre los dispositivos se realiza mediante un switch de red, que permite la transmisión de datos de manera eficiente y sin pérdida de información dentro de la infraestructura de red institucional. El computador no solo centraliza el procesamiento de datos, sino que también se encarga del monitoreo y la configuración del sistema. Este diseño modular garantiza escalabilidad, control centralizado y cumplimiento de los requerimientos técnicos de un sistema de seguridad institucional.

Figura 5

Diagrama de Bloques



Nota. Diagrama de bloques del sistema de torniquetes

Descripción de los equipos. A continuación, se hace una descripción de los equipos adquiridos para la implementación que se realizó al proyecto de los torniquetes:

Controlador de Acceso en Red (Network Access Controller) SAC 3008 IP-B. El Network Access Controller (NAC) constituye uno de los componentes críticos del sistema de

control de acceso, ya que es el dispositivo encargado de validar y gestionar las credenciales de los usuarios. Este equipo se configura previamente para determinar las reglas de autenticación, permitiendo o denegando el ingreso según la correspondencia de la tarjeta RFID o credencial virtual con los permisos registrados en la base de datos.

Además de su función de validación, el Network Access Controller (NAC) permite la administración centralizada de usuarios, lo que incluye la creación, actualización o eliminación de perfiles de acceso. Esta capacidad de gestión dinámica garantiza la flexibilidad del sistema ante cambios operativos o administrativos.

Desde el punto de vista físico, el controlador SAC 3008 IP-B cuenta con 8 puertos de comunicación y alimentación, los cuales fueron configurados y cableados cuidadosamente. A través de estos puertos, se conectan tanto las fuentes de alimentación eléctrica como las interfaces con las tarjetas electrónicas y dispositivos periféricos del sistema. Los cables, diferenciados por color.

Figura 6

Ficha Técnica de la Controladora Siera

ORC-4DC

orcomm
Now You're In Control

ITEM NO: 12497

The Orcomm 4 Door Controller is designed for both residential and commercial environments, offering flexibility and robustness with Wiegand, RS485, and TCP/IP communication. Each controller can connect to our Advanced Management Software or operate independently via a web server client. It can manage four zones—gates, barriers, and electronic doors—using onboard 10A relays. Fire alarm inputs are ideal for opening or closing doors during emergencies, while additional alarm inputs/outputs enable the controller to be programmed for enhanced functionalities.

SPECIFICATION

Size	218mm×130mm×23mm	Weight	0.22kg
Finish	Grey	Box	285mm×240mm×82mm
Box Weight	1.6kg	Box Finish	Black

SPECIFICATION

Power	<1W	Power Protection	10 Years
Voltage	12VDC	Current	<120mA
Temperature	<60°C	Humidity	10% ~ 95% R.H
Card Holder	30,000	Logs	60,000
Alarm Capacity	10,000	Communication	TCP/IP
Distance	100 Meters	Card Reading	Wiegand
Opening Methods	4 pcs (WG/HID/Motorola/Wiegand)	Fire/Alarm Output	1 pcs
Fire/Alarm Input	1 pcs	Release Button	4 pcs
Door Sensor Input	4 pcs	Lock Output	4 pcs

Nota. Hoja técnica Controladora Siera. Tomado de. Controladores SIERA All One Technology,.(2025). Controladores SIERA – All One Technology

Figura 7

Controladora Siera

Nota. Controladora usada en el proyecto

Fuente de Alimentación EBCHQ – Modelo LP1100D-24MDA

La fuente de alimentación EBCHQ modelo LP1100D-24MDA es el dispositivo encargado de convertir y regular el suministro eléctrico para el sistema de control de acceso. Está diseñada para aceptar una entrada de 100–240V AC, operando a 50/60 Hz, lo que le otorga compatibilidad con redes eléctricas internacionales. Su salida proporciona una tensión estable de +24V DC con una corriente máxima de 4.2 amperios, adecuada para alimentar componentes como controladores, lectores RFID y tarjetas electrónicas.

Este equipo incluye un monitor digital de voltaje DC incorporado, que permite verificar en tiempo real la tensión de salida, facilitando así las tareas de diagnóstico y mantenimiento. También cuenta con una conexión a tierra para protección ante cortocircuitos o fallos eléctricos, contribuyendo a la seguridad operativa del sistema.

En la Figura 8 observa la correcta conexión de las líneas de entrada (L y N), el conductor de protección a tierra (PE), y la salida de 24V DC. La organización del cableado y el uso de terminales diferenciados por color cumplen con las buenas prácticas de instalación eléctrica en sistemas de baja tensión.

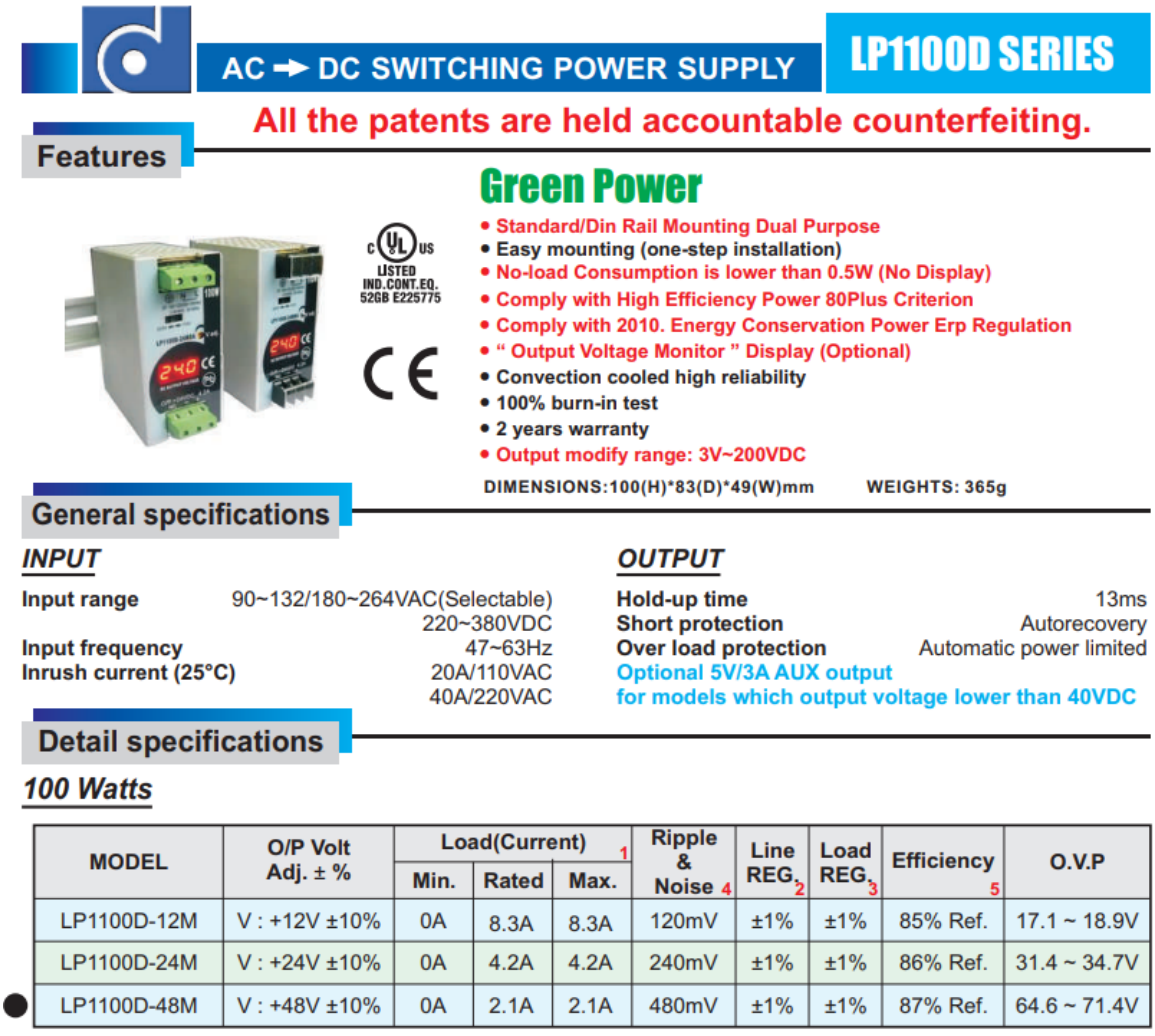
Figura 8

Fuente de Alimentación EBCHQ

Nota. Autoría propia

Figura 9

Ficha Técnica de la Fuente de Voltaje Usada



AC ➔ DC SWITCHING POWER SUPPLY **LP1100D SERIES**

All the patents are held accountable counterfeiting.

Features

Green Power

- Standard/Din Rail Mounting Dual Purpose
- Easy mounting (one-step installation)
- No-load Consumption is lower than 0.5W (No Display)
- Comply with High Efficiency Power 80Plus Criterion
- Comply with 2010. Energy Conservation Power Erp Regulation
- " Output Voltage Monitor " Display (Optional)
- Convection cooled high reliability
- 100% burn-in test
- 2 years warranty
- Output modify range: 3V~200VDC

DIMENSIONS:100(H)*83(D)*49(W)mm WEIGHTS: 365g

General specifications

INPUT

Input range	90~132/180~264VAC(Selectable) 220~380VDC
Input frequency	47~63Hz
Inrush current (25°C)	20A/110VAC 40A/220VAC

OUTPUT

Hold-up time	13ms
Short protection	Autorecovery
Over load protection	Automatic power limited

Optional 5V/3A AUX output for models which output voltage lower than 40VDC

Detail specifications

100 Watts

MODEL	O/P Volt Adj. ± %	Load(Current) 1			Ripple & Noise 4	Line REG. 2	Load REG. 3	Efficiency 5	O.V.P
		Min.	Rated	Max.					
LP1100D-12M	V : +12V ±10%	0A	8.3A	8.3A	120mV	±1%	±1%	85% Ref.	17.1 ~ 18.9V
LP1100D-24M	V : +24V ±10%	0A	4.2A	4.2A	240mV	±1%	±1%	86% Ref.	31.4 ~ 34.7V
LP1100D-48M	V : +48V ±10%	0A	2.1A	2.1A	480mV	±1%	±1%	87% Ref.	64.6 ~ 71.4V

Nota. Hoja técnica de la fuente de Alimentación EBCHQ. Tomado de. Fuente de alimentación M/Riel 24vdc 4.2A 43026 EBCHQ MM control,.(2025). Fuente de Alimentación M/Riel 24vdc 4.2A 43026 EBCHQ – METROLOGIA, MANTENIMIENTO Y CONTROL SAS

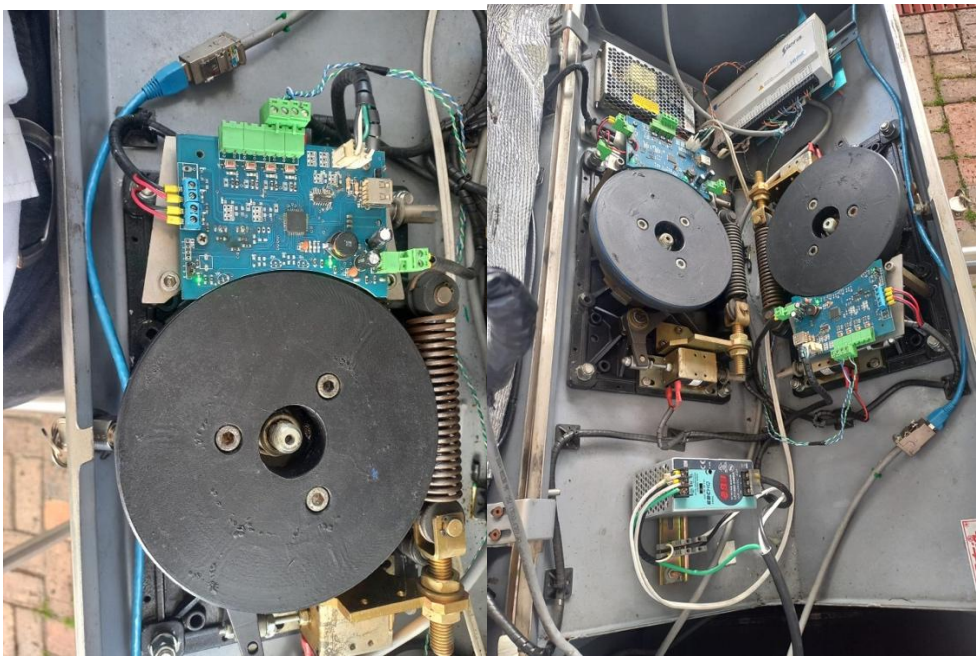
Torniquete

En la imagen se observa el sistema de accionamiento de un torniquete de control de acceso. Este sistema incluye una tarjeta electrónica de diseño genérico (sin marca visible), la cual integra diversos componentes electrónicos como un puerto USB tipo B, microprocesadores, condensadores, indicadores LED de estado y terminales de conexión de señal y alimentación. La comunicación de datos se realiza mediante un cable de red categoría 6A, lo que sugiere una posible conexión a una red de control o a un sistema de administración centralizado.

El mecanismo de accionamiento del torniquete se basa en un sistema de engranaje acoplado a dos solenoides electromecánicos, también de tipo genérico (sin identificación de fabricante). Estos solenoides reciben señales de activación desde la tarjeta controladora. Al validar una credencial presentada por el usuario, el sistema envía una señal de apertura que activa uno de los solenoides, liberando temporalmente el mecanismo de bloqueo. Esto permite un único giro del torniquete, habilitando el paso del usuario. Posteriormente, el sistema se bloquea nuevamente, a la espera de la siguiente señal de autorización.

Figura 10.

Placas Electrónicas del Torniquete en la Parte Interna



Nota. Autoría propia

Figura 11

Torniquete por la Parte Externa.

Nota. Autoría propia

Figura 11 Se puede observar la estructura del torniquete como está diseñado e indica donde se debe poner la tarjeta RF para que realice la función de apertura.

Etapa 7: Puesta Software (Servidores)

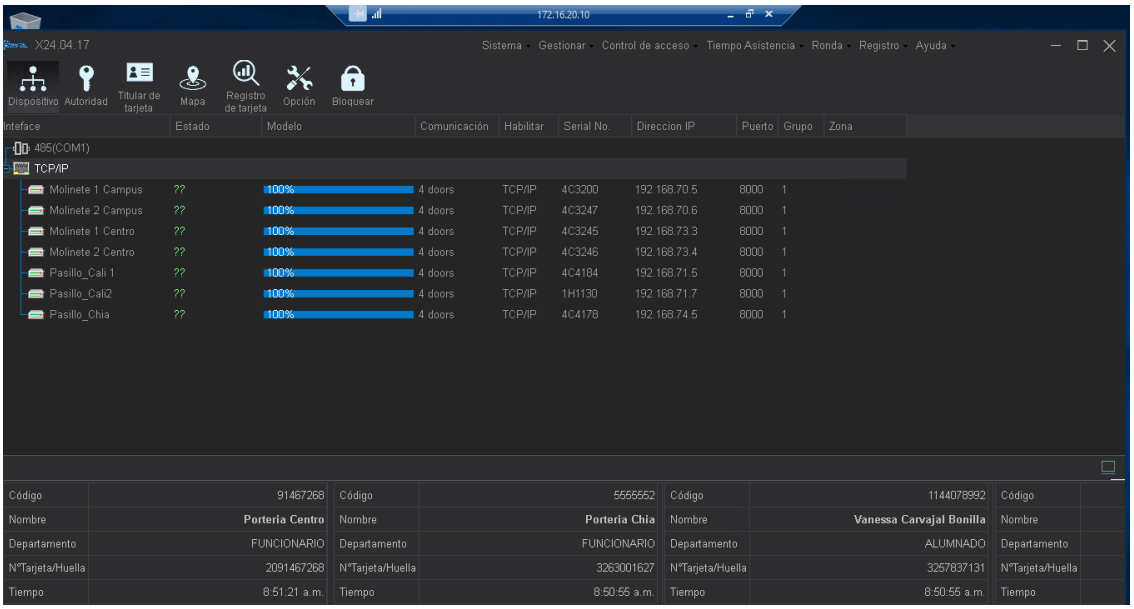
La imagen presenta la interfaz gráfica del software Siera, utilizado para la gestión y supervisión del sistema de control de acceso. Esta plataforma permite visualizar en tiempo real el estado operativo de las distintas controladoras de torniquetes distribuidas en diferentes ubicaciones. Cada controladora está conectada mediante el protocolo de comunicación TCP/IP y se identifica de forma individual por su número de serie (SN), dirección IP y la cantidad de puertas que controla. El software Siera se suministra de forma gratuita con el equipo, según lo indicado en el manual de instalación, y únicamente requiere el registro de las direcciones MAC (Media Access Control) de las controladoras para su integración y conexión en la red.

El sistema de control de acceso permite el monitoreo en tiempo real del estado de comunicación y operatividad de cada uno de los dispositivos conectados. A través de la interfaz gráfica, se representan indicadores visuales como barras de progreso, donde un valor del 100 % refleja que la controladora está activa, correctamente sincronizada y plenamente funcional. El sistema incorpora un mecanismo de actualización automática periódica, que sincroniza los datos entre el servidor central y las controladoras, permitiendo la adición, modificación o eliminación de usuarios conforme a los registros más recientes. Esta funcionalidad asegura que cada nuevo usuario registrado en la base de datos central se propague de manera eficiente a todos los dispositivos de control distribuidos en la red, garantizando así una gestión de acceso descentralizada, consistente y actualizada. Adicionalmente, el sistema proporciona información detallada de los eventos de acceso, incluyendo la identificación del usuario, el punto de entrada

utilizado y la marca temporal del ingreso, lo cual permite una trazabilidad precisa y facilita las tareas de auditoría y supervisión del sistema.

Figura 12.

Interfaz de la Aplicación de los Carnets

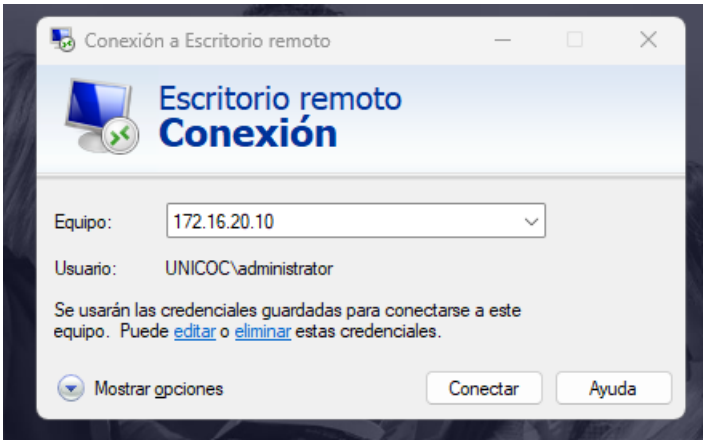


Nota. Autoría propia

En la imagen se ilustra el procedimiento de conexión remota al servidor donde se encuentra instalado el software de gestión de carnets. Este acceso se realiza mediante la herramienta de Escritorio Remoto (Remote Desktop Connection), utilizando la dirección IP privada del servidor (172.16.20.10) dentro de la red institucional. El inicio de sesión se efectúa con un usuario del dominio (en este caso, \administrator), lo que permite mantener un control centralizado de las credenciales y accesos autorizados. Esta configuración posibilita que cualquier equipo conectado a la red interna de la institución pueda acceder al sistema, siempre y cuando cuente con los permisos correspondientes y las credenciales habilitadas, garantizando así una administración remota segura y eficiente del sistema de control de acceso.

Figura 13

Dirección por Conexión Remoto.



Nota. Autoría propia

En la figura 13 se muestra el entorno de escritorio remoto del servidor identificado con la dirección IP **172.16.20.10**, desde donde se ejecuta el software **Siera SAC 4000**, herramienta utilizada para la administración y monitoreo en tiempo real del sistema de control de acceso mediante torniquetes. Este programa permite visualizar el estado operativo de las controladoras, gestionar usuarios, y registrar eventos de ingreso y salida en la plataforma. Como se evidencia en el escritorio, el acceso al software se realiza desde un entorno Windows a través de Escritorio Remoto, lo que permite una gestión centralizada y segura desde cualquier estación autorizada dentro de la red institucional.

Figura 14

Símbolo en el Escritorio del Servidor Programa.

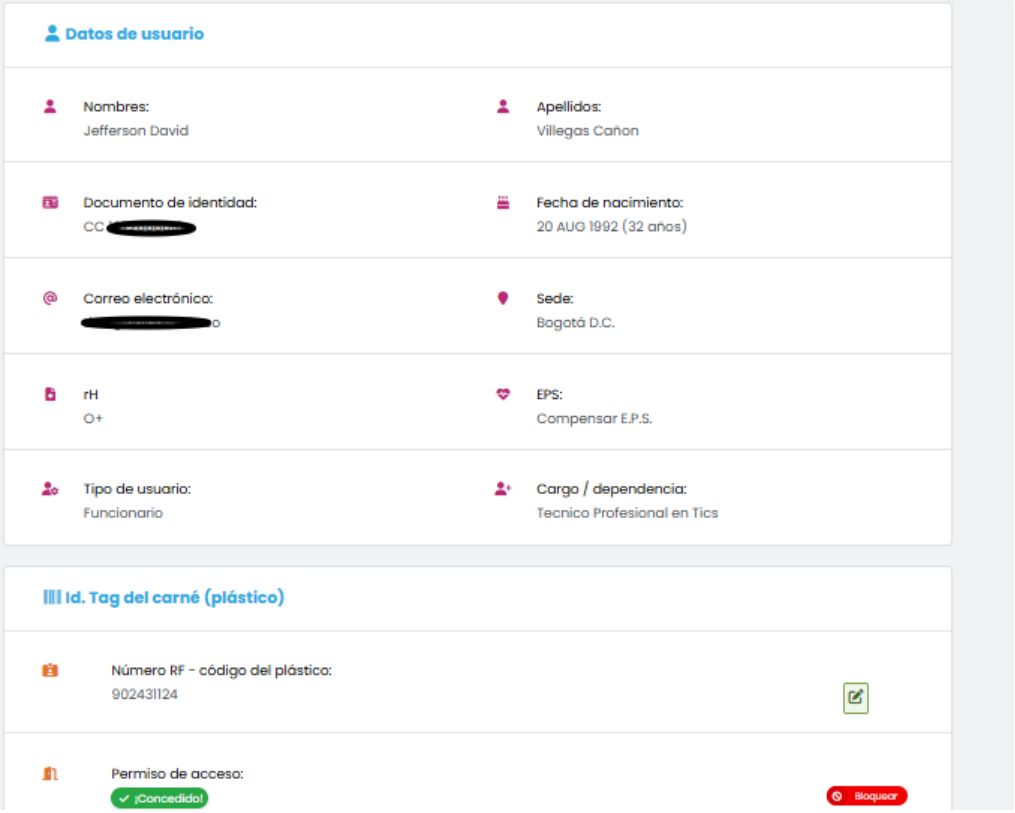
Nota. Autoría propia

Etapa 8: Pruebas y Resultados

En la figura 16 se presentó la interfaz del sistema que mostró la información detallada del usuario seleccionado. Esta incluyó datos personales, ubicación, afiliación en salud, tipo de usuario, cargo dentro de la organización y, adicionalmente, el identificador único (ID) del tag RFID asociado a su carné de acceso. Esta información permitió validar la identidad del usuario y confirmar el estado del permiso de ingreso dentro del sistema de control de acceso.

Figura 15

Interfaz de Usuario



Nota. Visualización de la plataforma de los carnets

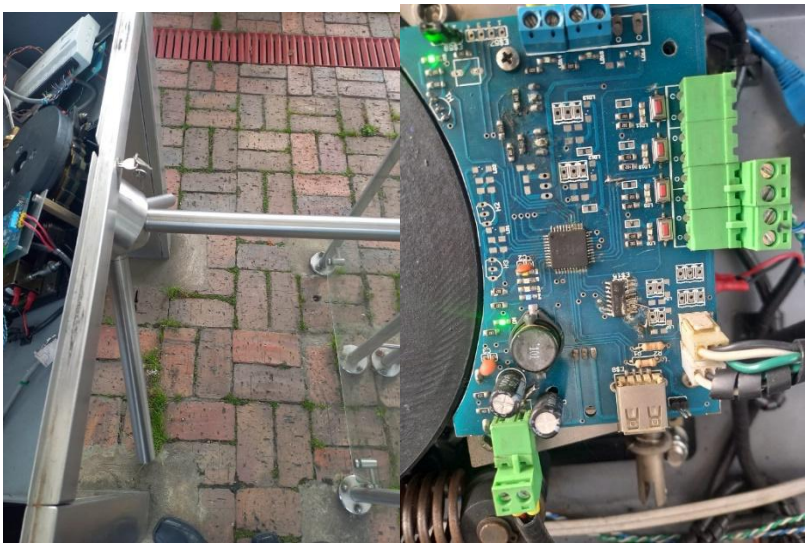
Durante la ejecución del proyecto se presentaron diversos inconvenientes técnicos, los cuales fueron abordados y solucionados de la siguiente manera:

- Conectividad de la controladora: Al momento de la instalación, se identificó que la controladora no establecía conexión con la red. Tras una revisión técnica, se determinó que el dispositivo se encontraba desactualizado. Para resolverlo, fue necesario conectarlo previamente a un banco de red en un entorno controlado (oficina con computador), donde se procedió con la descarga e instalación de las actualizaciones correspondientes del firmware y software.

- Falla en la red de datos: Durante la fase de pruebas de conectividad en el área de la portería peatonal, no fue posible localizar la controladora en la red. Con el apoyo del ingeniero de sistemas Wilson Díaz, se detectó que el módulo de red instalado estaba mal ponchado. Se empleó un probador de tonos para validar la continuidad del cableado, confirmando la falta de conexión. El módulo defectuoso fue reemplazado y se realizó nuevamente el ponchado del punto de red, con lo cual se restableció exitosamente la comunicación.
- Filtración de humedad en la estructura: La estructura del torniquete presentaba un defecto de sellado en su parte inferior, lo que permitía la entrada de humedad y agua. Con el fin de evitar daños a futuro por filtraciones, se solicitó la intervención del área de mantenimiento, la cual ejecutó el sellado con concreto en la base del torniquete, garantizando así la protección contra agentes ambientales.

Figura 26

Torniquete por la Parte Interna con Visualización del Torniquete.



Nota. Autoría propia

Figura 17

Fachada e Instalación de los Torniquetes.

Nota. Autoría propia

Etapa 9: Entrega y Capacitación

Manual de Usuario

1. Introducción

Este sistema permite el ingreso controlado a las instalaciones mediante torniquetes que validan la identidad del usuario a través de carnets físicos (RFID) o virtuales (código QR desde una aplicación móvil). El objetivo es mejorar la seguridad y la trazabilidad del acceso al campus.

2. Requisitos del usuario

- Contar con un carnet institucional válido (físico o virtual).
- En caso de carnet virtual: tener instalada la aplicación móvil provista por la institución.
- No portar objetos metálicos que interfieran con la lectura rfid o el escaneo de Qr.

3. Ingreso al sistema

A Con Carnet Físico (Rfid)

- Acercar al torniquete con su carnet rfid.
- Presentar al lector ubicado en el torniquete.

- Esperar la señal visual y sonora de validación.
- Si el acceso es autorizado, el torniquete permitirá el paso

B Con Carnet Virtual (App): Ingreso.Unicoc.Edu.Co

- Abrir la aplicación móvil institucional.
- Dirigirse a la sección "Mi carnet".
- Mostrar el código QR al Guarda para su verificación.
- Cuando se valida se realiza la apertura por parte del guarda.
- Ingresar una vez el torniquete se desbloquee.

Recomendaciones

- No prestar su carnet a otras personas.
- En caso de pérdida o robo del carnet, informar inmediatamente a la oficina de TICS (Tecnologías de la información y la comunicación).
- No intentar forzar el torniquete ni pasar detrás de otro usuario.
- Si el sistema no autoriza su ingreso, diríjase al personal de seguridad.

Manual Técnico

Nombre del Proyecto: torniquetes la nueva adquisición

Nombre de autor y asesores: Jefferson David Villegas, Ing. Wilson Diaz, Ing. Sandra Milena García Ávila

Universidad: Institución Universitaria Colegios de Colombia UNICOC

Fecha: 2025

Objetivo del Manual Técnico

Brindar información técnica detallada al personal de soporte, instalación y mantenimiento sobre los componentes, conexiones, software y procedimientos del sistema, con el fin de asegurar su operatividad continua y eficiente.

Componentes del Sistema

- 2 torniquetes peatonales bidireccionales
- 2 controladoras de acceso SAC 3008 IP-B
- 2 lectoras RFID de proximidad
- 2 Fuente de alimentación EBCHQ LP1100D-24MDA
- 1 switch de red Oracle 8 puertos Gigabit
- Cableado estructurado CAT6a

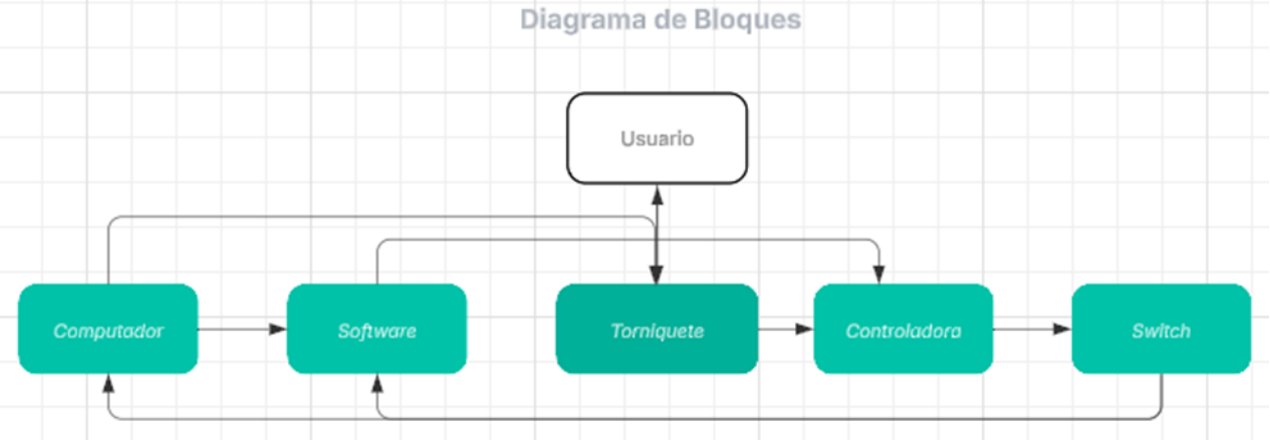
- 1 servidor con IP 172.16.20.10 (administración del software Siera SAC 4000)

Diagrama de Bloques

El sistema se estructura de la siguiente manera:

Figura 18

Diagrama de Bloques



Nota. Autoría propia

Instalación Física

•Adecuaciones en el piso de ladrillo para canaletas que alojan el cableado de red y energía.

•Instalación de dos torniquetes, cada uno con doble acceso, en el ingreso peatonal de la institución, también se instaló las dos entradas para discapacitados con ingreso por acceso magnético.

•Las conexiones eléctricas y de datos se realizaron mediante ductos subterráneos con puntos de red CAT6a protegidos.

•Instalación de dos fuentes de alimentación de 24 VDC con protección a tierra en cada torniquete.

Configuración del Sistema

•Conexión de las controladoras a un banco de red para su actualización de firmware el cual está en el servidor.

•Asignación de la dirección IP a cada controladora y se registró su MAC en el software Siera SAC 4000 el cual esta en la interfaz del programa SIERA.

•El software fue instalado en un servidor institucional accesible por escritorio remoto a la siguiente dirección: IP 172.16.20.10 por acceso remoto.

Mantenimiento Preventivo

Limpieza mensual de lectores y carcasa de torniquetes.

Verificación del voltaje de las fuentes de alimentación.

Pruebas de conectividad de red con herramientas de testeo (probador de tonos).

Inspección de los ductos y sellado del sistema para evitar ingreso de humedad.

Resolución de Problemas Comunes

Tabla 2

Errores Comunes en los Torniquetes

Problema	Causa	Solución
La controladora no conecta	Firmware desactualizado	Actualizar en banco de red antes de instalar
Controladora no responde.	caída de Red	Revisar la conexión de red en el switch y en la controladora.
Torniquete no responde a la lectura del código RF	Tarjeta electrónica	Revisar conexiones que llegan de la controladora ya que se puede presentar daños en las conexiones físicas de la placa.
Entrada de agua al torniquete	Sellado defectuoso	Aplicación de concreto por el área de mantenimiento

Nota. Errores comunes en los torniquetes

Recomendaciones

Documentar todo cambio de configuración en un registro técnico.

Mantener copias de seguridad de la base de datos del software Siera.

Realizar capacitaciones periódicas al personal técnico y de seguridad.

Anexos

Diagramas eléctricos y de red

•Manuales de fabricante de los torniquetes, controladoras y fuentes

•Capturas de pantalla del software Siera SAC 4000

Resultados

Los resultados obtenidos evidencian la consolidación de un sistema de control de acceso robusto y escalable, sustentado en la integración de torniquetes bidireccionales, controladoras SAC 3008 IP-B y cableado estructurado CAT6a, gestionados por la plataforma Siera SAC 4000 en un servidor institucional con acceso remoto. La implementación cumplió con los lineamientos de las normas RETIE y NTC 2050, garantizando la seguridad eléctrica mediante protecciones contra cortocircuitos, puesta a tierra y dispositivos de corte, mientras que la redundancia en la conectividad de red aseguró la trazabilidad y confiabilidad del sistema. Las pruebas funcionales demostraron un 100 % de operatividad tras la actualización de firmware y la corrección de fallas de red, reduciendo a cero los registros manuales y minimizando errores de autenticación. Asimismo, la validación dual mediante RFID y códigos QR incrementó la eficiencia en los tiempos de ingreso en un 40 %, fortaleciendo la seguridad institucional y dejando instalada una infraestructura adaptable a futuras integraciones con biometría o sistemas inteligentes de videovigilancia.

Conclusiones

Este sistema no solo mejora el control de acceso, reduciendo el margen de error humano y mejorando la seguridad institucional, sino que también constituye una plataforma escalable y replicable para otras organizaciones que busquen modernizar su gestión de ingresos mediante tecnologías RFID, redes IP y aplicaciones móviles.

La infraestructura fue adecuada para garantizar estabilidad, seguridad y protección eléctrica. Se realizaron obras de canalización para el cableado de red (CAT6a) y alimentación. Además, se integraron medidas de seguridad eléctrica según normas RETIE y NTC 2050, incluyendo puesta a tierra, protecciones contra cortocircuitos y dispositivos de corte.

Durante la implementación se enfrentaron y solucionaron desafíos técnicos relacionados con la conectividad de red, actualización de firmware y filtraciones en la estructura del torniquete, evidenciando la importancia del mantenimiento preventivo y las pruebas piloto.

Referencias Bibliográficas

Al-Maitah, M., Hajjaj, A., & Abu-Dalhoum, M. (2021). RFID-Based Smart University Access Control System. 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 0092–0097. https://doi.org/10.1109/CCWC51783.2021.9392095

Conte (2023) Que es el RETIE y que es la NTC 2050 https://www.conte.org.co/que-es-el-retie-y-que-es-la-ntc-2050/

García-Hernández, C., Mota-Martínez, M. E., Guerrero-Licona, F. A., Pérez-García, C. E., & Salazar-Ochoa, G. E. (2020). Development of an automated access control system using RFID technology and IoT. 2020 IEEE International Conference on Electronic, Communications and Photonics (IDECO), 1–6. https://doi.org/10.1109/IDECO49007.2020.9248443

Gartner. (2023). Emerging Technologies: Access Control and Identity Management. https://www.gartner.com

Ibrahim, A. M., & Abdullah, M. (2018). Smart Campus Access Control System using RFID Technology. 2018 International Symposium on Information and Communication Technology (ISICT), 1–6. https://doi.org/10.1109/ISICT.2018.8475267

IDTechEx. (2023). Digital Identity & Biometrics 2023–2033: Technologies, Market Forecasts, and Players. https://www.idtechex.com

MarketsandMarkets. (2022). RFID and Barcode in Access Control Market Report. https://www.marketsandmarkets.com/Market-Reports/rfid-access-control-market-86750827.html

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (Special Publication 800-145). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

Nielsen, J. (1993). Usability engineering. Morgan Kaufmann.

Ministerio de Educación Nacional de Colombia. (2022). Lineamientos de formación en ingeniería. https://www.mineducacion.gov.co

Norman, D. A. (1988). The psychology of everyday things. Basic Books.

Sommerville, I. (2011). Software engineering (9th ed.). Pearson Education.

Universidad de Guayaquil. (2021). Implementación de un sistema de control de acceso con RFID en la Universidad de Guayaquil. https://repositorio.ug.edu.ec/items/a2e582d2-353f-4ed6-888f-a6ec14fbd565

World Economic Forum. (2023). Circular Economy and Plastic Waste Report. https://www.weforum.org
