Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), Noviembre-Diciembre 2025,
Volumen 9, Número 6.

https://doi.org/10.37811/cl_rcm.v9i6

DESARROLLO DE PROTOTIPO PARA CONTROL DE ACCESO VEHICULAR A ESTACIONAMIENTOS

DEVELOPMENT OF A PROTOTYPE FOR VEHICLE ACCESS CONTROL TO PARKING LOTS

Jorge Arturo López Salazar
Tecnológico Nacional de México

Ricardo Ussiel Flores López
Tecnológico Nacional de México

Diego César Castillo Hernández
Tecnológico Nacional de México

Juan Manuel Montoya Guel
Tecnológico Nacional de México

María Guadalupe Hernández-Sierra
Tecnológico Nacional de México

DOI: https://doi.org/10.37811/cl_rcm.v9i6.21542

Desarrollo de Prototipo para Control de Acceso Vehicular a Estacionamientos

Jorge Arturo López Salazar[1]
L23180543@slp.tecnm.mx
https://orcid.org/0009-0007-6231-6683
Tecnológico Nacional de México
Instituto Tecnológico de San Luis Potosí
México

Ricardo Ussiel Flores López
L21181192@slp.tecnm.mx
https://orcid.org/0009-0004-1131-2744
Tecnológico Nacional de México
Instituto Tecnológico de San Luis Potosí
México

Diego César Castillo Hernández
L21181190@slp.tecnm.mx
https://orcid.org/0009-0002-3577-9811
Tecnológico Nacional de México
Instituto Tecnológico de San Luis Potosí
México

Juan Manuel Montoya Guel
L21181198@slp.tecnm.mx
https://orcid.org/0009-0001-6457-9926
Tecnológico Nacional de México
Instituto Tecnológico de San Luis Potosí
México

María Guadalupe Hernández-Sierra
maria.hs@slp.tecnm.mx
https://orcid.org/0000-0002-2979-0523
Tecnológico Nacional de México
Instituto Tecnológico de San Luis Potosí
México

RESUMEN

El presente trabajo describe el desarrollo de un prototipo de sistema automatizado para el control de acceso vehicular en estacionamientos, con el propósito de optimizar los procesos de ingreso, fortalecer la seguridad institucional y reducir el impacto ambiental generado por los tiempos de espera. El sistema fue diseñado e implementado bajo el modelo de desarrollo en cascada, integrando componentes de software y hardware. La solución utiliza códigos QR para la validación rápida y segura de los usuarios, registrando en tiempo real los accesos y salidas. Durante su desarrollo se realizaron análisis de riesgos, pruebas alfa y beta, así como evaluaciones técnicas enfocadas en seguridad, rendimiento, usabilidad y compatibilidad. Los resultados obtenidos evidencian que el prototipo cumple con los objetivos planteados. Además, la ejecución del proyecto representó una experiencia formativa significativa para los estudiantes, al permitirles aplicar de manera integral los conocimientos adquiridos durante su formación académica y fortalecer sus competencias blandas. Este desarrollo demuestra la importancia de incorporar prácticas aplicadas en la formación de ingenieros informáticos, vinculando la teoría con la solución de problemáticas reales mediante el uso de tecnologías emergentes.

Palabras clave: control de acceso, código QR, desarrollo de software, ingeniería informática, automatización

[1] Autor principal
Correspondencia: maria.hs@slp.tecnm.mx

Development of a Prototype for Vehicle Access Control to Parking Lots

ABSTRACT

This paper describes the development of a prototype automated system for vehicle access control in parking facilities, with the aim of optimizing entry processes, strengthening institutional security, and reducing the environmental impact of waiting times. The system was designed and implemented using the waterfall development model, integrating software and hardware components. The solution utilizes QR codes for fast and secure user validation, recording entries and exits in real time. During its development, risk analyses, alpha and beta testing, and technical evaluations focused on security, performance, usability, and compatibility were conducted. The results obtained demonstrate that the prototype meets the stated objectives. Furthermore, the project provided a significant learning experience for the students, allowing them to comprehensively apply the knowledge acquired during their academic training and strengthen their soft skills. This development demonstrates the importance of incorporating applied practices into the training of computer engineers, linking theory with the solution of real-world problems through the use of emerging technologies.

***Keywords*:** access control, QR code, software development, computer engineering, automation

Artículo recibido 15 noviembre 2025
Aceptado para publicación: 15 diciembre 2025

INTRODUCCIÓN

Un sistema de acceso a estacionamientos privados es un sistema de control que gestiona quién puede entrar y salir de un aparcamiento restringido. Su objetivo principal es garantizar la seguridad, al permitir o denegar la entrada a vehículos o personas no autorizadas y se implementa mediante dispositivos físicos como barreras y guardias de seguridad, o con tecnología como puede ser lectores de tarjetas o matrículas, teclados y sistemas de videovigilancia.

El control de acceso vehicular en instituciones educativas de nivel superior (IES) constituye un aspecto esencial para garantizar la seguridad, la organización y la eficiencia en la gestión de los espacios destinados al estacionamiento. En diversos entornos, estos procesos aún se realizan de manera manual o mediante mecanismos poco eficientes, lo que genera demoras en el ingreso, congestión vehicular, pérdida de tiempo y vulnerabilidad ante accesos no autorizados. En este contexto, la incorporación de tecnologías digitales representa una alternativa viable para optimizar dichos procedimientos y fortalecer la seguridad institucional.

El presente estudio aborda el desarrollo de un sistema automatizado de control de acceso a los estacionamientos de la universidad, que son cuatro, basado en la lectura del código QR impreso en la credencial que identifica al estudiante como miembro activo y además, integra los datos de su vehículo los que han sido previamente registrados con la tarjeta de circulación del mismo en el departamento encargado de la seguridad de la IES: números de placa del vehículo e información de contacto (por ejemplo: correo electrónico o teléfono).

Este tipo de código debe su nombre a la abreviatura del inglés Quick Response o en español respuesta rápida, está conformado por barras bidimensionales que almacenan información y se accede a ella con una cámara lectora del teléfono inteligente, computadora u otros dispositivos (Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), 2025).

Este diseño es una solución tecnológica implementable en cualquier otro escenario. Permite validar de manera ágil y segura la identidad de los usuarios, registrar los accesos y salidas en tiempo real y disponer de información confiable y auditable sobre el uso del espacio.

Inicialmente, la institución contaba únicamente con un estacionamiento vehicular destinado al uso de docentes y personal administrativo. Con el paso de los años, el incremento en la matrícula estudiantil y la facilidad para poseer un vehículo propio propició la ampliación de la infraestructura mediante la creación de nuevos espacios para aulas y laboratorios, lo que a su vez hizo necesario habilitar más accesos y áreas de estacionamiento con el fin de ofrecer este servicio también al alumnado, que al ser mayor de edad puede transportarse en su propio automóvil. Esta situación requiere ahora de más guardias de seguridad que controlen las entradas y salidas y por supuesto, la vulnerabilidad crece.

Con este prototipo se busca mejorar la eficiencia operativa, reducir riesgos de seguridad y contribuir al fortalecimiento de una cultura institucional orientada a la innovación tecnológica y la gestión inteligente de recursos.

Otro factor que se pretende reducir, y hasta eliminar, es el congestionamiento generado al ingreso y egreso de los vehículos. Ya que, por el tiempo de espera en que el vigilante valida y anota la identidad del vehículo y luego libera la pluma, se origina fila de automóviles en marcha. Esto ocasiona pérdida de tiempo, daños a la salud, contaminación ambiental y acústica.

Cuando un vehículo permanece en marcha en vacío, emite gases contaminantes que deterioran la calidad del aire, llegando incluso a generar un impacto ambiental mayor que cuando se encuentra en movimiento. A ello se suma su contribución al aceleramiento del cambio climático y los efectos negativos sobre la salud humana, derivados de la disminución en la calidad del aire respirable (Edenred, 2025).

Por otra parte, los sonidos generados por los automóviles en marcha: motor, aceleración, frenadas, uso de bocinas a alto volumen, roce de llanta, entre otros producen contaminación acústica o sónica siendo factores que pueden generar irritabilidad y deterioro del entorno social, tanto en los ocupantes como en las personas que perciben el ruido (El Silencio Urbano: Importancia De Reducir El Ruido Vehicular, 2024).

Este problema ha sido ya objeto de estudio y propuesta de soluciones de varios autores, entre ellos estudiantes de nivel licenciatura, que aportan desarrollos para eliminar o subsanar la situación. Aunque son propuestas similares, tienen diferenciadores con este caso de estudio.

Por ejemplo, el presentado por De Ita et al. (2022), quienes diseñaron e implementaron un software para el control del ingreso vehicular a estacionamientos, el cual además incluye una interfaz gráfica que permite visualizar la ocupación del espacio. El propósito de esta solución fue reducir los congestionamientos derivados de la validación física de acceso, subsanar la falta de registros y optimizar el tiempo empleado en la búsqueda de cajones disponibles, además de generar reportes concentrados de información para una mejor gestión del estacionamiento.

Por su parte, los estudiantes de Ingeniería Mecatrónica, Gómez & Morales (2025) presentaron para su titulación el desarrollo de una aplicación móvil utilizando tecnología de identificación por Radiofrecuencia (RFID). La finalidad fue automatizar el acceso y contar con el registro de los usuarios a fin de tener una mayor seguridad y disminuir el congestionamiento derivado de la espera al ingreso. Sus resultados los sustentaron con datos estadísticos que demostraron la viabilidad de su desarrollo.

Otro caso es el desarrollo de Mora & Becerra (2022) quienes realizaron un sistema para el registro y validación de los vehículos que ingresan a su propia institución. Además, de la gestión de los lugares disponibles en el estacionamiento utilizando aplicación móvil para Android con un código QR, apoyándose en sensores ópticos, indicadores y actuadores.

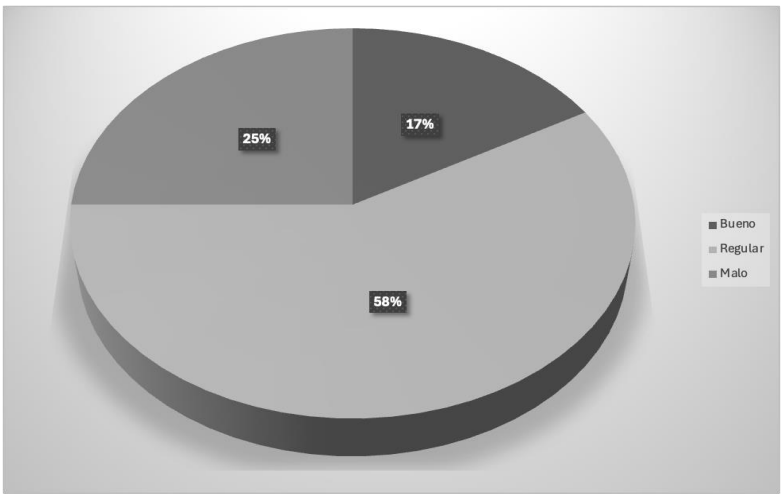
METODOLOGÍA

Para la elaboración del prototipo del proyecto, que integra componentes de software y hardware, se adoptó el modelo en cascada, correspondiente al ciclo clásico de desarrollo de sistemas. Este enfoque permitió organizar el proceso en etapas secuenciadas y estructuradas: análisis de requerimientos, definición de roles y privilegios, diseño del sistema y de base de datos, análisis de riesgos, verificación mediante pruebas alfa y beta y finalmente la puesta en marcha del prototipo (Delgado & Díaz, 2021). Con ello, se busca su futura implementación y funcionamiento integral en todos los puntos de acceso a los diferentes estacionamientos.

En la primera fase del proyecto se realizaron entrevistas tanto al personal de vigilancia como a los conductores de los vehículos que acceden al estacionamiento.

Referente a la percepción sobre la eficiencia del sistema actual en la entrada vehicular, a cargo del vigilante y con método manual, los usuarios indicaron su percepción de satisfacción, en su gran mayoría 58 por ciento calificaron el método como regular y 25 por ciento en la categoría de malo. Solo un 17 por ciento como bueno y ningún conductor como excelente. Estos resultados se observan en la Figura 1.

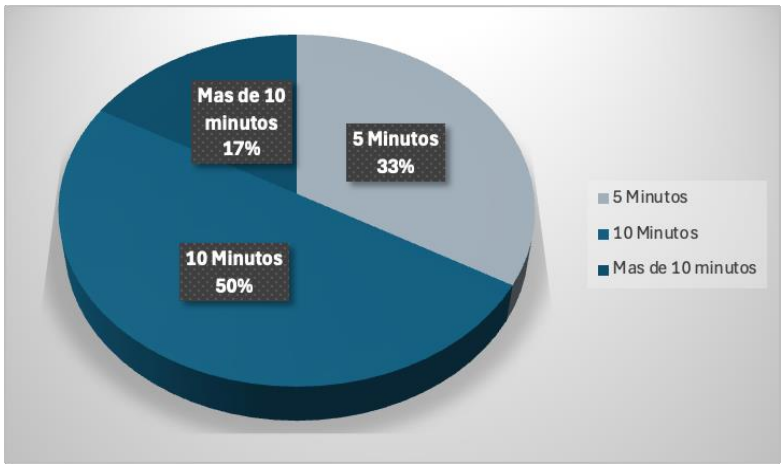
Figura 1 Apreciación sobre la eficiencia de vigilancia en el acceso al estacionamiento.



Nota. Elaboración propia.

También se cuestionó sobre el tiempo de espera al ingreso, es decir, en línea de espera. En la Figura 2 se aprecia que la mayoría, 50 por ciento, indica que son hasta 10 minutos y 33 por ciento contestaron 5 minutos. Es decir, mucho tiempo esperando acceder. Incluso los que se decantaron por 5 o menos minutos fueron sólo 17 por ciento y nadie señaló que tuvieran una entrada fluida, sin tiempo de espera, lo cual afirma que es demasiado ese lapso de tiempo. Lo indicado está graficado en la Figura2

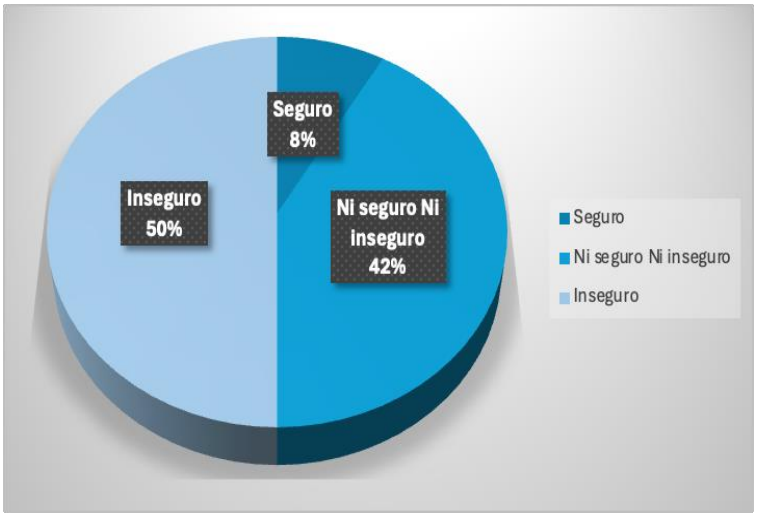
Figura 2 Tiempo en línea de espera para el ingreso al estacionamiento.



Nota. Elaboración propia.

Otro cuestionamiento importante fue el referente a la seguridad de los vehículos que permanecen estacionados dentro de la IES mientras los alumnos atienden sus actividades académicas. Al no contar con un control de acceso eficiente, pudiera darse el caso de que ingresen personas ajenas a la institución con fines maliciosos. En la Figura 3 los resultados demuestran que abrumadoramente el 50 por ciento manifiesta inseguridad, 42 por ciento ni seguro ni inseguro y solo el 8 por ciento seguro.

Figura 3 Percepción de seguridad en el estacionamiento institucional.



Nota. Elaboración propia.

En conclusión, estos resultados evidenciaron que el proceso manual existente era lento, obsoleto y carecía de las medidas para garantizar la seguridad necesarias.

Paralelamente, se llevó a cabo una investigación documental sobre soluciones tecnológicas aplicables, a partir de la cual se determinó la utilización de las credenciales con código QR, junto con su correspondiente lector para la validación del acceso.

La siguiente etapa consistió en identificar los diferentes roles de usuario, con el propósito de garantizar una interacción adecuada con el sistema según el nivel de responsabilidad e involucramiento de cada perfil. La personalización de pantallas y opciones no solo optimiza la eficiencia operativa, sino que también fortalece la seguridad al restringir el acceso a funciones críticas. Esta diferenciación no se limita a un recurso técnico, sino que constituye una estrategia integral orientada a equilibrar la eficiencia, la seguridad y la usabilidad. En entornos educativos, donde convergen diversos actores y se requiere alta precisión en los procesos, este enfoque asegura que cada interacción con el sistema se realice de manera fluida, segura y en coherencia con los objetivos institucionales.

En primer lugar, el usuario llamado vigilante, quien antes era crucial para la operación del acceso, ahora sus funciones se limitan a ser el responsable de encender el equipo, supervisar la seguridad física de manera visual y resolver incidencias, como por ejemplo fallo en lector de código QR teniendo que reiniciar la aplicación o bloquear accesos de manera temporal durante emergencias de seguridad. Estas acciones quedan fuera de la operación del sistema. A este rol solo le concierne prender y apagar el equipo lector o notificar incidencias.

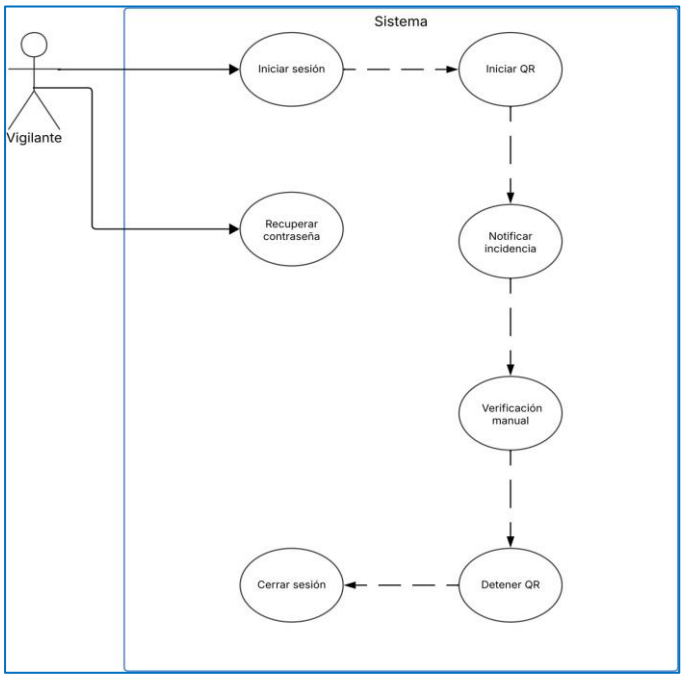
Los conductores tienen interacción únicamente cuando muestran el código QR de su credencial al lector a su ingreso y salida del estacionamiento.

El último rol corresponde al del administrador del sistema, cuya función principal es la obtención de reportes de acceso y egreso, gestión de usuarios y actividades de respaldo y restauración de la información.

Estas acciones se muestran en las Figuras 4, 5 y 6 donde se explican con un diagrama Unified Modelling Language (UML) de casos de uso las interacciones entre los actores y las funcionalidades del sistema.

La Figura 4 corresponde al vigilante quien solo es quien enciende la cámara lectora de código QR y en casos de falla regresa al método tradicional de verificación y registro manual.

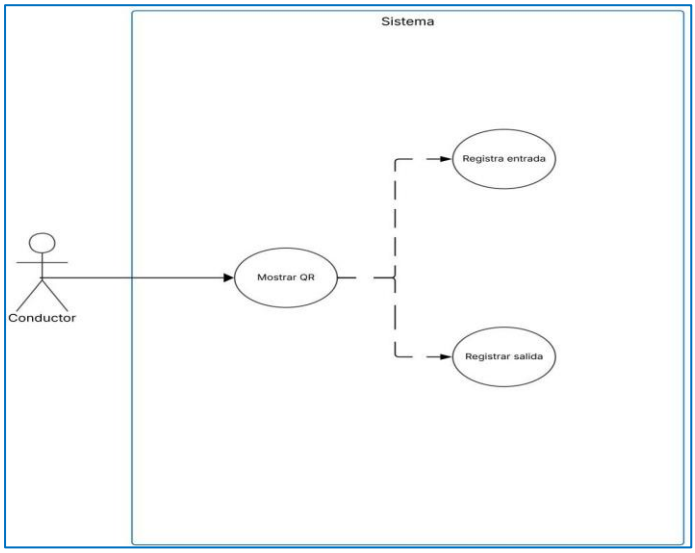
Figura 4 Diagrama UML de casos de uso: usuario vigilante



Nota. Elaboración propia.

La Figura 5 muestra las acciones de los conductores que ingresan y salen del aparcamiento: estudiantes, docentes, personal administrativo e invitados. Su intervención consiste solamente en mostrar su código QR para que sea escaneado y registrado por el sistema, tanto en el ingreso como el egreso.

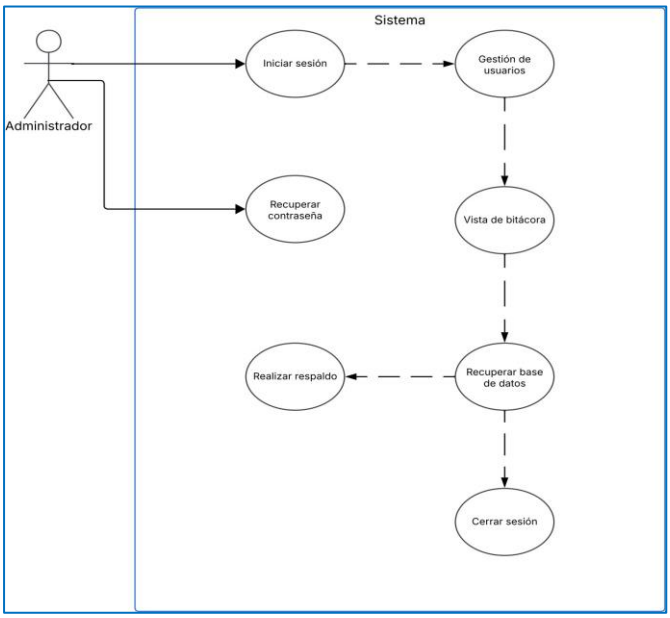
Figura 5 Diagrama UML de casos de uso: usuario conductor



Nota. Elaboración propia.

Por último, el actor administrador, como se indica en la Figura 6, es el encargado de gestionar los datos de los conductores y vigilantes, consulta la bitácora de accesos y realiza las funciones de respaldo y recuperación de la información almacenada.

Figura 6 Diagrama UML de casos de uso: usuario administrador



Elaboración propia.

Continuando con el diseño del sistema, se eligió como Sistema Gestor de Base de Datos (SGBD) el MySQL 8.0, Tkinter para la realización de la interfaz intuitiva, ya que permite el manejo de CRUD (Crear, Leer, Actualizar y Eliminar) y la gran potencia que tiene Lenguaje de Consulta Estructurado (SQL) para consultas e informes (OCI, 2024).

Para el desarrollo de código se apoyó en herramientas como Python 3.9+, como lenguaje de programación, ya que se utiliza frecuentemente para aplicaciones web al ser eficiente y con facilidad de aprendizaje y aplicación, además funciona en diversas plataformas y es de descarga gratuita (Amazon AWS, 2024).

Fue necesario realizar una aplicación lectora de código QR que fuera compatible con dispositivos móviles. La siguiente etapa del modelo de desarrollo, anterior de la implementación y liberación del sistema, corresponde a las pruebas de usuario. Esta fase es fundamental para garantizar el correcto funcionamiento y la confiabilidad de los resultados, lo cual conduce al proceso iterativo de la mejora continua. Estas acciones permiten detectar y corregir errores, evaluar el desempeño bajo diferentes condiciones y asegurar que el sistema cumpla con los requerimientos establecidos. De esta manera, se minimizan riesgos operativos y se incrementa la calidad y estabilidad del producto final (Piñero et al., 2021, 100).

Estos postulados se respaldan con investigaciones ya publicadas, como lo que indican (Gómez et al., 2024, 2) “La automatización de pruebas en las organizaciones es cada vez más frecuente por diversas razones, entre ellas, mayor reusabilidad, mejor cobertura de prueba y, por consiguiente, mayor calidad en el producto desarrollado.”

Se llevaron a cabo tres tipos de pruebas: detección de riesgos, pruebas alfa y pruebas beta.

Durante la programación, se realizó un análisis de riesgos, el cual permite comprender mejor las limitaciones del proyecto, asignar recursos de manera más precisa y crear planes de proyecto más realistas y detallados (Chaurasia & Guide, 2023). A partir de este, se integraron estrategias de protección y mitigación contra errores del usuario.

El riesgo en el desarrollo de software se refiere a la probabilidad de que suceda un suceso incierto que influya de manera negativa generalmente en el resultado del proyecto (McGrath & Jonker, 2025).

Para lo cual, se integró una matriz de riesgos con las siguientes categorías: fallos en la integración de sistemas, acceso no autorizado debido a vulnerabilidades en los mecanismos de autenticación y pérdida de datos personales.

Un fallo en la integración de sistemas se define como un error entre conexiones de los diferentes módulos del sistema, impidiendo que trabajen de manera conjunta, provocando problemas como fallos en la comunicación o bajo rendimiento (Britto, 2025). Para el desarrollo de este estudio, el riesgo podría manifestarse como fallo en la comunicación entre sensores, bases de datos de usuarios, interfaces de control, lo que generaría denegaciones de acceso no planificadas, congestión vehicular o pérdida de datos. En la Tabla 1 se aprecia la tabla de medición de dicho riesgo.

Tabla 1 Criterio de medición del riesgo: Fallos en integración de sistemas (app acceso estacionamiento)

Área de impacto	**Bajo**	**Moderado**	**Alto**
Funcionalidad del sistema	Fallos menores que causan retrasos ocasionales	Fallos recurrentes con colas/demoras significativas	Bloqueo total del acceso al estacionamiento
Impacto en usuarios	Molestias mínimas (resueltas en segundos)	Insatisfacción notable y tiempos de espera prolongada	Usuarios no acceden al servicio + reclamos masivos
Alcance del fallo	Afecta solo lecturas de placas	Afecta cobro automático y barreras	Colapso total del sistema

Nota. Elaboración propia.

El siguiente riesgo, identificado como acceso no autorizado debido a vulnerabilidades en los mecanismos de autenticación, se refiere a la existencia de posibilidades de accesos malintencionados o no autorizados que violen los mecanismos para verificación de identidad y por consecuencia ingresen y visualicen o manipulen información del sistema.

En la tabla 2 se identifican dichas vulnerabilidades y se enlistan las medidas de mitigación, asegurando que la aplicación cumpla su función sin comprometer la seguridad, operatividad o confianza de la comunidad escolar.

Tabla 2 Criterio de medición del riesgo: Acceso no autorizado por vulnerabilidades en autenticaciones (aplicación para automatizar el acceso al estacionamiento)

Área de impacto	Bajo	Moderado	Alto
Afectación a la imagen de la organización	Vulnerabilidades detectadas internamente, sin accesos no autorizados ni impacto a usuarios	Accesos no autorizados manejados internamente, sin difusión pública	Acceso no autorizado masivo/prolongado. Incidente público o reportado en medios, afectando la confianza de clientes.

Nota. Elaboración propia

Por último, se analizó el riesgo catalogado como pérdida de datos personales. Esta amenaza incluye la exposición o eliminación de los datos de identificación personal de un usuario, la cual existe almacenada dentro de la base de datos del sistema; número de control institucional o número de empleado, nombre del usuario, placas de circulación del vehículo, horarios de ingreso/egreso del estacionamiento, número de teléfono móvil y correo.

Las causas pueden ser variadas, desde fallos técnicos hasta intrusos por ataque cibernético. Sin embargo, pudieran generarse sanciones, a los desarrolladores o a la IES, administrativas o penales por incumplir normativas de privacidad hasta daños reputacionales (McKeinze, 2025).

En la Tabla 3 se puede observar las áreas de impacto de este riesgo de acuerdo a la ponderación del mismo.

Tabla 3 Criterio de medición del riesgo: pérdida de datos personales (aplicación de acceso al estacionamiento)

Área de impacto	Bajo	Moderado	Alto
Afectación a la privacidad y cumplimiento normativo	La pérdida involucra datos no sensibles y se limita a un equipo técnico interno	La pérdida incluye datos personales básicos y afecta a múltiples departamentos	La pérdida expone datos sensibles al público o terceros no autorizados
Impacto en la confianza del cliente	Impacto mínimo; los usuarios no identifican riesgos directos	Preocupación detectable; algunos usuarios cuestionan la seguridad de la app	Pérdida masiva de confianza; usuarios abandonan el servicio y exigen responsabilidades legales
Consecuencias legales y regulatorias	Sin sanciones; el incidente se resuelve internamente	Multas menores o requerimientos de notificación a autoridades locales	Sanciones graves, demandas colectivas y obligación de notificación pública

Nota. Elaboración propia.

Dando continuidad a la evaluación previa a la liberación, se realizaron pruebas alfa, las cuales constituyen la primera fase de verificación funcional de un sistema antes la prueba con usuarios externos. Su objetivo principal es identificar errores lógicos, de programación o de diseño en un entorno controlado, generalmente la realizan los mismos desarrolladores o un grupo interno de evaluación. En este caso, fueron conducidas por el docente-asesor del equipo en un ambiente controlado, simulando el escenario real. Los resultados se fueron registrando en una bitácora para darles seguimiento a las correcciones. Esta evaluación reveló errores en la validación de permisos y la estabilidad de la conexión, los cuales se corrigieron y entonces se pudo continuar con la siguiente etapa.

Para finalizar se llevaron a cabo pruebas beta. Previamente, los desarrolladores elaboraron una rúbrica de comprobación con enunciados sobre los diferentes ítems: usabilidad (experiencia de usuario), funcionalidad, rendimiento, seguridad, satisfacción general, portabilidad. Las respuestas se codificaron en escala de Likert. Se escogió a docentes de la IES con experiencia en el desarrollo de software, siendo una actividad a doble ciego para garantizar la calidad y confianza de los resultados.

El objetivo principal de esta fase es obtener información estimable sobre el rendimiento del software en condiciones reales de uso, con el fin de identificar y corregir errores que no se hayan detectado en la evaluación alfa y realizar mejoras basadas en las experiencias de los usuarios (*Beta Testing Meaning*, 2025). En la tabla 4 se exponen las retroalimentaciones de este grupo evaluador, así como las acciones llevadas a cabo para corregirlas o mitigarlas.

Tabla 4 Evaluación técnica y recomendaciones de mejora del sistema

Criterio evaluado	**Resultado observado**	**Retroalimentación**
Cifrado de datos en reposo y en tránsito	Cifrado en tránsito y reposo. No obstante, se identificó el uso de algoritmos criptográficos considerados débiles.	Se recomienda actualizar los mecanismos de cifrado a estándares robustos.
Respaldo automatizado con cifrado y retención	El sistema depende de un esquema de respaldo manual.	Es imprescindible migrar a un sistema de respaldo automatizado con políticas definidas de retención y cifrado uniforme.
Recuperación ante desastres	No se evidenció un plan formal de recuperación ante desastres.	Es urgente definir e implementar un plan de recuperación ante desastres.

Rendimiento en consultas a bases de datos	El sistema presenta un rendimiento eficiente, con consultas rápidas (menores a 500 ms) y uso apropiado de mecanismos de caché.	Este resultado es positivo. Se sugiere mantener prácticas de optimización y monitoreo continuo, así como implementar alertas proactivas que detecten degradaciones del rendimiento.
Estabilidad bajo carga alta	Se observaron picos en el uso de CPU y memoria RAM bajo cargas elevadas.	Se recomienda optimizar la gestión de recursos, mejorar procesos en segundo plano y considerar la implementación de escalamiento horizontal o vertical según la demanda.
Compatibilidad con sistemas operativos	El sistema actualmente opera únicamente en una versión específica del sistema operativo.	Para mejorar la portabilidad y escalabilidad, se aconseja ampliar la compatibilidad con múltiples versiones y plataformas.
Experiencia e interfaz de usuario (UX/UI)	El diseño de la interfaz es funcional, pero carece de elementos intuitivos que faciliten la interacción del usuario.	Se recomienda realizar una revisión basada en diseño centrado en el usuario, incorporando principios de accesibilidad, navegabilidad y diseño visual.
Actualización de dependencias y gestión de vulnerabilidades	Las actualizaciones	Se debe integrar una herramienta de análisis de vulnerabilidades para identificar riesgos antes del despliegue.
Tiempo de actividad (uptime) en pruebas de estrés	El sistema demostró una alta disponibilidad por la implementación de balanceo de carga.	Excelente desempeño.
Funcionamiento de respaldo y recuperación	No se implementaron procesos formales de validación post-recuperación.	Es necesario establecer un protocolo de verificación que garantice la integridad de los datos restaurados.
Soporte de arquitecturas multi-nube y on-premise	El sistema solo es funcional en un entorno específico, lo que limita su escalabilidad.	Se recomienda incorporar capacidades de interoperabilidad para operar tanto en entornos multi-nube.
Claridad en variables de entorno y parámetros de configuración	Las variables de entorno están presentes, pero carecen de documentación clara.	Se sugiere documentar exhaustivamente todos los parámetros de configuración en un archivo *README* o manual técnico.

Estos ciclos de evaluación, con sus respectivas correcciones, confirmaron la eficacia de la solución propuesta y avalaron que se puede poner en práctica

RESULTADOS Y DISCUSIÓN

El desarrollo del sistema de información para el control del estacionamiento institucional evidenció resultados favorables en cuanto a su funcionalidad, eficiencia y pertinencia para el entorno. Durante las pruebas de validación, el prototipo demostró una notable estabilidad operativa, reduciendo significativamente el tiempo de ingreso vehicular y mejorando el control de accesos. La automatización mediante el uso de códigos QR permitió agilizar los procesos y disminuir errores humanos, garantizando además la trazabilidad y seguridad de los registros. Este resultado confirma la viabilidad del producto de software como una herramienta tecnológica adaptable a diferentes contextos, capaz de optimizar recursos y fortalecer las políticas de seguridad de la institución.

Asimismo, la implementación de esta práctica académica resultó sumamente valiosa en la formación de los estudiantes, al propiciar la aplicación integral de conocimientos teóricos en un contexto real. La participación en un proyecto de desarrollo completo, desde el análisis de requerimientos hasta las pruebas de implementación, fortaleció competencias esenciales como el trabajo colaborativo, la resolución de problemas y la gestión técnica de sistemas. Estas experiencias prácticas contribuyen al aprendizaje significativo, al desarrollo de una visión profesional orientada a la innovación, la mejora continua y la responsabilidad tecnológica dentro del ámbito de la Ingeniería Informática.

La línea de investigación a la cual pertenece este proyecto se refiere a Ingeniería de software, parte esencial de la carrera mencionada.

CONCLUSIONES

El presente proyecto de desarrollo de software representa una solución tecnológica integral que responde de manera precisa y eficiente a una necesidad real de la comunidad educativa: el control seguro, automatizado y auditable del acceso vehicular en la IES. A lo largo del trabajo, se evidenció una planificación estructurada, un enfoque metodológico riguroso y una implementación técnica respaldada por principios sólidos de ingeniería informática.

El sistema desarrollado, sustentado en tecnologías como Python, MySQL, Tkinter y escaneo mediante códigos QR, no solo optimiza la gestión del estacionamiento institucional, sino que también fortalece

la seguridad, minimiza errores humanos y garantiza la trazabilidad de todos los accesos registrados. El diseño de base de datos, la gestión de usuarios por roles, las pruebas iterativas (alfa y beta), así como las funcionalidades de respaldo y recuperación de datos, demuestran un compromiso con la robustez, escalabilidad y sostenibilidad de la solución.

Además, la documentación generada a lo largo del ciclo de desarrollo incluyendo bitácoras de pruebas, análisis de riesgos, manuales de usuario y el acta formal de entrega del sistema refleja una comprensión profunda del proceso de desarrollo de software profesional, alineado con buenas prácticas y estándares del sector tecnológico.

En síntesis, el proyecto desarrollado trasciende la mera implementación técnica, consolidándose como una solución efectiva y funcional que responde a las necesidades reales de la institución.

REFERENCIAS BIBLIOGRÁFICAS

Amazon AWS. (2024). *¿Qué es Python? - Explicación del lenguaje Python - AWS. Amazon AWS.* Recuperado noviembre 4, 2025, de https://aws.amazon.com/es/what-is/python/

Beta Testing Meaning. (2025, marzo 4). Full Scale. Recuperado octubre 28, 2025, de https://fullscale.io/blog/beta-testing-meaning/

Britto, F. (2025, octubre 23). *Integración de sistemas: conoce su importancia, sus tipos y sus retos*. SYDLE. Recuperado octubre 27, 2025, de https://www.sydle.com/es/blog/integracion-de-sistemas- 6140d39a84679b13bf127a93

Chaurasia, N., & Guide, S. (2023, junio 12). *Master Project Risk Analysis: Tools, Techniques & Certifications*. Sprintzeal.com. Recuperado octubre 27, 2025, de https://www.sprintzeal.com/blog/project-risk-analysis

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef). (2025). *Códigos QR*. Revista Proteja su dinero. https://revista.condusef.gob.mx/usuario-inteligente/sabias-que/2025/01/fabre/

De Ita, A., Montiel, J., Carmona, M., & Larios, M. (2022). Modelo de sistema de control de acceso y gestión de operaciones de un estacionamiento privado. *Revista Iztatl Computación,*, *11*(2), 33-40. https://ingenieria.uatx.mx/docs/RevistaIztatlComputacionNo22.pdf#page=40

Delgado, L., & Díaz, L. (2021). Modelos de Desarrollo de Software. *Revista Cubana de Ciencias Informáticas*, *15*(1), 37-51. https://www.redalyc.org/journal/3783/378366538003/html/

Edenred. (2025, junio 25). *Contaminación vehicular: índices, causas y cómo resarcirla*. Edenred México. Recuperado octubre 14, 2025, de https://www.edenred.mx/blog/contaminacion-vehicular-indices-causas-y-como-resarcirla

El silencio urbano: importancia de reducir el ruido vehicular. (2024). Comaudi Industrial. Recuperado octubre 14, 2025, de https://www.comaudi-industrial.com/blog/importancia-de-reducir-el-ruido-vehicular/#:~:text=de%20la%20poblaci%C3%B3n.-,Efectos%20negativos%20del%20ruido%20vehicular%20en%20la%20calidad%20de%20vida,menor%20percepci%C3%B3n%20de%20bienestar%20comunitario.

Glorsario de términos de ISTQB®. (2025). International Software Testing Qualifications Board (ISTQB). Recuperado octubre 17, 2025, de https://glossary.istqb.org/es_ES/search?term=&exact_matches_first=true&page=3

Gómez, A., Sosa, M., Verona, S., & Delgado, M. (2023). Buenas prácticas de la ingeniería de software: pruebas de software. *Revista Cubana de Transformación Digital*, *4*(2), 1-13. https://rctd.uic.cu/rctd/article/view/205

Gómez, T., & Morales, R. (2025). Desarrollo de un prototipo para control de acceso vehicular de parqueaderos con tecnología RFID y aplicación móvil. *Repositorio Institucional de la Universidad Politécnica Salesiana*. https://dspace.ups.edu.ec/handle/123456789/30429

McGrath, A., & Jonker, A. (2025). *¿Qué es la gestión de riesgos?* IBM. Recuperado octubre 27, 2025, de https://www.ibm.com/mx-es/think/topics/risk-management

McKeinze, B. (2025). *Reguladores, prioridades de cumplimiento y sanciones*. Manual Glogal de datos y ciberseguridad. Recuperado octubre 28, 2025, de https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/latin-america/mexico/topics/regulators-enforcement-priorities-and-penalties

Mora, J.A., & Becerra, D.D. (2022). Sistema de control para registro y gestión de plazas de estacionamiento mediante cifrado en códigos QR. repositorio universitario. Universidad distrital Francisco José de Caldas. http://hdl.handle.net/11349/36589

OCI. (2024, agosto 29). *MySQL: qué es y cómo se usa*. Oracle. Recuperado noviembre 4, 2025, de https://www.oracle.com/latam/mysql/what-is-mysql/

Piñero, M., Marin, A., Trujillo, Y., & Buedo, D. (2021). Buenas prácticas para prevenir los riesgos de la eficiencia del desempeño en los productos de software. *Revista Cubana de Ciencias Informáticas*, *15*(1), 89-113. http://scielo.sld.cu/scielo.php?pid=S2227-18992021000100089&script=sci_arttext