Informe técnico

“Visita Segura”

Equipo 8 de proyecto de Capstone

Docente

Marcela Orellana Silva

Equipo alumnos

Daniel Marcelo Novoa Vega

Sebastián Escobedo

Institución

Duoc UC, San Bernardo

Santiago, 01 de diciembre de 2025

Resumen

El proyecto "Visita Segura" surge para mejorar el registro de visitantes en la sede Duoc UC San Bernardo, actualmente gestionado mediante procesos manuales que generan lentitud, errores y limitaciones en la trazabilidad. La propuesta consiste en diseñar e implementar una plataforma digital que automatiza el registro de visitantes mediante la lectura de códigos QR presentes en las cédulas de identidad chilenas, capturando datos de manera rápida y precisa. La solución utiliza un stack tecnológico moderno compuesto por React.js en el frontend, Node.js en el backend y SQLite como base de datos, integrando librerías especializadas como QRjs, y se desarrolla bajo la metodología Scrumban, combinando planificación iterativa con flexibilidad visual. El sistema permite generar reportes automáticos, mantener un historial digital de ingresos, cumplir protocolos de seguridad y normativas de protección de datos, fortaleciendo la seguridad institucional y optimizando la experiencia de visitantes y personal. Como resultados esperados, se proyecta una reducción del 25% en los tiempos de registro, mejora en la trazabilidad de accesos y eficiencia del control de accesos, ofreciendo además una solución escalable y replicable para otras organizaciones que buscan modernizar sus procesos de control y registro.

Palabras clave: QR, automatización, registro de visitantes, seguridad institucional, Duoc UC

Abstract

The "Safe Visit" project aims to improve visitor registration at the Duoc UC San Bernardo campus, currently managed through manual processes that generate slowness, errors, and limitations in traceability. The proposal consists of designing and implementing a digital platform that automates visitor registration by reading QR codes on Chilean identity cards, capturing data quickly and accurately. The solution uses a modern technology stack composed of React.js in the frontend, Node.js in the backend, and SQLite as a database, integrating specialized libraries such as QRjs. It is developed using the Scrumban methodology, combining iterative planning with visual flexibility. The system allows for the generation of automatic reports, maintaining a digital history of entries, complying with security protocols and data protection regulations, strengthening institutional security, and optimizing the experience for visitors and staff. The expected results include a 25% reduction in check-in times, improved access traceability, and improved access control efficiency. It also offers a scalable and replicable solution for other organizations looking to modernize their control and check-in processes.

Keywords: QR code, automation, visitor registration, institutional security, Duoc UC

Índice de contenido

Índice de figuras

1. Introducción

En la era digital, las instituciones deben modernizar sus procesos para lograr mayor eficiencia, seguridad y escalabilidad. El registro de visitantes y el control de acceso son áreas críticas donde los sistemas manuales en papel provocan retrasos, errores humanos, trazabilidad limitada y problemas administrativos. En Duoc UC San Bernardo, los registros de visitantes manuscritos generan imprecisiones, duplicación de datos y dificultades para generar informes o realizar auditorías en tiempo real. Además, los registros físicos aumentan el riesgo de pérdida de datos, manipulación no autorizada e incumplimiento de las normas de privacidad.

El proyecto Visita Segura introduce una plataforma digital que automatiza el registro de visitantes mediante códigos QR integrados en los documentos nacionales de identidad chilenos. Este sistema captura datos con precisión, valida la información al instante, centraliza el almacenamiento y permite la generación de informes y análisis en tiempo real. Al reemplazar los procesos manuales, mejora la velocidad, la seguridad y la trazabilidad, cumpliendo así con los requisitos institucionales. Desde el punto de vista tecnológico, la plataforma utiliza una pila tecnológica moderna de código abierto: React.js para interfaces responsivas, Node.js con Express.js para un backend escalable y SQLite para almacenamiento relacional seguro. La biblioteca QR.js permite la lectura y decodificación de códigos QR en distintos dispositivos, lo que reduce los costos asociados al software comercial y permite la escalabilidad y la personalización para otras instituciones con necesidades similares.

El desarrollo siguió la metodología Scrumban, que combina los principios de Scrum y Kanban mediante sprints cortos, reuniones virtuales y revisiones periódicas. Este enfoque ágil fomentó la mejora continua y brindó al equipo de estudiantes una valiosa experiencia en la gestión colaborativa de proyectos.

Entre los resultados esperados se incluyen una reducción del 25 % en el tiempo de registro de visitantes, una mayor eficiencia operativa y el cumplimiento de las normas de protección de datos. Los registros de acceso digitales refuerzan la trazabilidad, mientras que la generación de informes automatizada proporciona a los administradores información práctica. Más allá de la innovación técnica, “Visita Segura” entrega un valor académico y social, ya que permite a los estudiantes aplicar el conocimiento teórico a contextos reales y mejora la experiencia de los visitantes al reducir los tiempos de espera. En definitiva, el proyecto demuestra cómo las iniciativas académicas pueden generar soluciones digitales prácticas, impactantes y seguras para las instituciones modernas.

2. Planteamiento del Problema y oportunidad detectada

El proyecto Visita Segura surge ante la necesidad de optimizar el registro de visitantes en la sede Duoc UC San Bernardo, proceso que actualmente se realiza en papel. Este método genera demoras en la atención, errores en la captura de datos y dificultades para mantener una trazabilidad confiable, lo que impacta directamente en la eficiencia administrativa y en la seguridad institucional.

Desde un enfoque técnico, se identifican varias limitaciones. La transcripción manual de información no garantiza exactitud ni evita duplicados. La ausencia de un sistema centralizado de almacenamiento restringe la generación de reportes en tiempo real y complica la gestión de accesos. Además, el soporte físico puede perderse o manipularse sin dejar registro, aumentando la vulnerabilidad de los datos.

A esto se suma la falta de protocolos robustos de protección de información personal, lo que expone a la institución a riesgos de confidencialidad e incumplimiento normativo. En un entorno donde la digitalización y la ciberseguridad son prioritarias, estas deficiencias resaltan la necesidad de adoptar soluciones tecnológicas modernas.

La oportunidad detectada consiste en implementar un sistema digital que automatice la captura de datos mediante lectura de códigos QR, almacene la información en bases de datos seguras y facilite la generación de reportes estadísticos para la toma de decisiones. Este cambio permitirá reducir tiempos de registro, minimizar errores y fortalecer la trazabilidad de los ingresos, al mismo tiempo que ofrece un modelo escalable aplicable en otras organizaciones.

En síntesis, la problemática actual limita la eficiencia y seguridad del control de accesos, generando la necesidad de transformar un procedimiento manual y vulnerable en un sistema confiable, ágil y alineado con las exigencias actuales de gestión y protección de datos.

3. Justificación

El proyecto Visita Segura se justifica por la necesidad de mejorar el actual sistema de registro de visitantes en la sede Duoc UC San Bernardo, que al ser manual genera demoras, errores y falta de trazabilidad en la información. Estos problemas afectan la eficiencia administrativa y debilitan el control de accesos.

En el ámbito social, la propuesta busca agilizar la atención y brindar una experiencia más fluida a los usuarios. Desde el plano económico, contribuye a reducir el uso de papel y optimizar los recursos destinados al personal encargado de los registros. En términos prácticos, la digitalización mediante lectura de códigos QR, almacenamiento seguro de datos y generación de reportes automáticos asegura procesos más confiables, rápidos y alineados con estándares de seguridad.

Además, el proyecto fortalece competencias en diseño de sistemas, gestión de información y seguridad digital, aportando valor académico y profesional, y ofreciendo una solución escalable aplicable en otras instituciones

4. Estado del Arte

El registro automatizado de visitantes mediante tecnología QR representa una evolución natural de los sistemas de control de acceso tradicionales, impulsada por la necesidad de mayor eficiencia, trazabilidad y seguridad en organizaciones modernas. La revisión de antecedentes revela múltiples aproximaciones tecnológicas implementadas en contextos similares a nivel nacional e internacional.

En el ámbito educacional chileno, existe una tendencia clara hacia la digitalización de los procesos de gestión de identidad y registro académico. Instituciones como la Universidad de Chile han implementado sistemas robustos de identificación biométrica por reconocimiento facial para el control de asistencia y acceso a dependencias (Universidad de Chile, 2024). No obstante, desde una perspectiva de desarrollo informático, estas soluciones adoptadas a nivel interno suelen ser sistemas propietarios o altamente personalizados. Esta naturaleza genera una limitada interoperabilidad entre las instituciones y, en muchos casos, implica altos costos de licenciamiento y mantención adaptados exclusivamente a los contextos operativos particulares de cada universidad (Sanabria-Z. & Arciniegas-B., 2018).

El mercado de *software* comercial ofrece soluciones estandarizadas de gestión de visitantes, como HID Visitor Manager, Proxyclick o Envoy, que proporcionan capacidades similares mediante plataformas SaaS (*Software as a Service*). Estas alternativas requieren suscripciones mensuales significativas y, al operar bajo un modelo centralizado, presentan limitaciones intrínsecas en la personalización de flujos de trabajo específicos, además de una reducción en el control soberano de datos. Esta pérdida de control es un factor crítico para las instituciones educativas que manejan información sensible de menores de edad, lo que expone a las entidades a riesgos de cumplimiento normativo (Sanabria-Z. & Arciniegas-B., 2018).

La tecnología de lectura de códigos QR en las cédulas de identidad chilenas ha demostrado ser viable técnicamente, lo que se refleja en su aplicación en

sistemas de control de acceso y gestión de personal del sector privado (Buk, 2024). Estos códigos, incorporados como parte de las medidas de seguridad del documento, contienen información verificable y estandarizada. De hecho, el Servicio de Registro Civil e Identificación confirma, a través de normativas, que el código QR es un elemento clave de la Cédula de Identidad Electrónica, diseñado para proporcionar una base tecnológica sólida para el desarrollo de aplicaciones de identificación automática (Servicio de Registro Civil e Identificación, 2024).

Los estudios sobre automatización de procesos de registro demuestran beneficios significativos en eficiencia operativa. Como se destaca en la literatura sobre automatización robótica de procesos (RPA) en el sector educativo, la implementación de sistemas automatizados de captura de datos reduce los errores humanos inherentes a la transcripción manual y mejora drásticamente la consistencia de los procesos organizacionales (SMOWL, 2023). Esta aproximación es especialmente relevante en contextos donde la precisión de datos es crítica para la seguridad y la trazabilidad de la información.

El vacío identificado en el sector académico chileno consiste en la ausencia de soluciones de código abierto (*open-source*) diseñadas específicamente para instituciones educativas. Estas soluciones deben integrar eficientemente la lectura de códigos QR de cédulas nacionales con capacidades robustas de reporte y análisis adaptadas a las normativas locales de protección de datos. El proyecto Visita Segura aborda directamente esta oportunidad mediante la propuesta de un sistema escalable, costo-efectivo y culturalmente adaptado, que busca establecer un estándar de registro digital seguro y soberano.

5. Hipótesis de trabajo

La implementación de la plataforma digital Visita Segura en la sede Duoc UC San Bernardo mejorará significativamente la eficiencia del proceso de registro de visitantes. Esta mejora se manifestará en la reducción del tiempo de atención, la minimización de los errores de transcripción de datos y el fortalecimiento de la trazabilidad de la información bajo un esquema de seguridad perimetral.

La integración de la lectura de códigos QR de las cédulas de identidad permitirá la captura de datos personales de forma automática y precisa, mitigando inconsistencias e incidencias por duplicidad, lo que asegurará un nivel de confiabilidad superior en el control de accesos. Además, la funcionalidad de almacenamiento seguro garantizará la protección de la información sensible y facilitará la generación de reportes automáticos para la supervisión y la toma de decisiones basada en datos.

En síntesis, la adopción de Visita Segura se postula como la solución que incrementará la eficiencia operativa del personal administrativo y reforzará los protocolos de seguridad institucionales. De esta forma, se demuestra que la digitalización del registro de visitantes tiene un impacto directo y medible en las variables críticas de eficiencia, confiabilidad y trazabilidad del control de accesos.

5.1 Variables de investigación

A partir de la hipótesis de trabajo, se definen las variables del estudio para establecer los parámetros de medición de la solución propuesta.

5.1.1 Variable Independiente

La variable independiente del presente estudio es la Plataforma Digital Visita Segura. Esta se define operacionalmente como la implementación del sistema automatizado de registro de visitantes, que utiliza la lectura QR de la cédula de identidad para la captura de datos y el almacenamiento en una base de datos segura, en sustitución del proceso manual actual en la sede Duoc UC San Bernardo.

5.1.2 Variables Dependientes

Las variables dependientes son aquellas que serán medidas para evaluar el impacto de la solución y validar la hipótesis.

- Eficiencia Operativa: Se medirá a través del Tiempo Promedio de Registro (TpR), cuantificando la reducción en segundos del proceso de atención de un visitante.
- Confiabilidad de la Captura de Datos: Se operacionalizará mediante la Tasa de Error de Registro (TEr), cuyo objetivo es reducir al mínimo el porcentaje de registros con inconsistencias o duplicados.
- Trazabilidad y Seguridad de la Información: Se evaluará en función del Nivel de Detalle del Reporte (NDR), confirmando la generación automática y consistente de reportes auditables que contienen todos los campos críticos para la seguridad y normativa institucional.

6. Objetivos del proyecto

Los objetivos del proyecto Visita Segura se plantean con el propósito de guiar el desarrollo de la plataforma digital y garantizar que los resultados esperados respondan a las problemáticas de eficiencia y trazabilidad identificadas. Se define un objetivo general que aborda la solución central y varios objetivos específicos que detallan las acciones necesarias para alcanzar dicho objetivo de manera eficiente y medible.

6.1. Objetivo General

Desarrollar e implementar una plataforma digital de Código Abierto (*Open-Source*) para la automatización completa del proceso de registro de visitantes en la sede Duoc UC San Bernardo, asegurando la precisión en la captura de datos y el cumplimiento de los estándares de trazabilidad institucional.

6.2. Objetivos Específicos

- Diseñar y desarrollar la arquitectura web y móvil que permita la captura y validación automática de datos mediante la lectura de códigos QR de las cédulas de identidad nacionales.

- Modelar y construir una base de datos que garantice los atributos de confidencialidad, integridad y disponibilidad (CID) de la información sensible de los visitantes, de acuerdo con la Ley de Protección de Datos chilena.

- Diseñar y desarrollar la interfaz de usuario (*UI*) y la experiencia de usuario (*UX*) para el personal de seguridad y administrativo, aplicando principios de usabilidad para optimizar la gestión de registros y consultas.

- Implementar funcionalidades de generación de reportes automáticos que permitan el análisis de visitas y métricas operacionales para la toma de decisiones en tiempo real.

- Definir e integrar protocolos de seguridad de la información, incluyendo autenticación y cifrado de datos, alineados con las normativas vigentes.

- Realizar pruebas exhaustivas de funcionalidad, rendimiento, usabilidad y seguridad para validar la estabilidad de la plataforma antes de su implementación definitiva en el entorno productivo.

7. Metodología

El proyecto Visita Segura se desarrolla bajo la metodología Scrumban, una aproximación híbrida que combina la planificación iterativa y ceremonia estructurada de Scrum con la flexibilidad visual y gestión de flujo continuo de Kanban. Esta metodología resulta particularmente apropiada para el contexto académico y las características específicas del equipo de desarrollo, proporcionando estructura suficiente para garantizar entregas periódicas mientras mantiene la adaptabilidad necesaria para responder a cambios en requisitos y restricciones temporales académicas. El presente capítulo establece el marco de trabajo, las herramientas y los procedimientos que guiaron el desarrollo e implementación del proyecto Visita Segura, asegurando una gestión eficiente y resultados alineados con los objetivos propuestos.

7.1. Estructura de Sprints y Ceremonias

El desarrollo se organiza en sprints de 2 semanas, optimizando la frecuencia de entrega de valor mientras permite tiempo suficiente para desarrollo, testing y documentación de funcionalidades complejas. Cada sprint incluye las siguientes ceremonias adaptadas al contexto del proyecto:

Daily Scrums virtuales de 15 minutos realizados diariamente a las 21:00 horas mediante Discord, enfocados en progreso, impedimentos y coordinación de tareas interdependientes. Esta modalidad permite flexibilidad para conciliar horarios académicos manteniendo comunicación constante.

Sprint Reviews realizados al finalizar el sprint con duración de 2 hora, incluyendo demostración de funcionalidades completadas, retrospectiva de proceso, y planificación del sprint siguiente. Estas sesiones incorporan evaluación de calidad de código, validación de cumplimiento de criterios de aceptación, e identificación de mejoras de proceso.

7.2. Stack Tecnológico y Herramientas

En el apartado del frontend usaremos React.js v19.1.1 con MUI v7.3.5 para desarrollo de interfaces responsive, implementando componentes reutilizables. La selección de React se fundamenta en su amplia documentación, comunidad activa, y capacidad de integración con librerías especializadas para lectura QR.

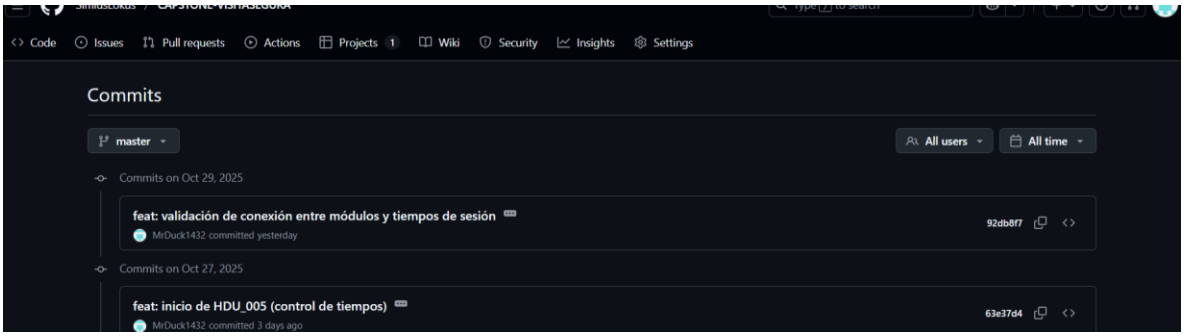
Por el lado del Backend estaremos usando Node.js v22.19.0 con Express.js v5.2.0 para desarrollo de APIs REST, implementando validación de datos, y manejo de errores. La Base de datos estará alojada de forma local con SQLite como sistema de gestión de base de datos relacional, seleccionado por su robustez, capacidades de cifrado nativo, y excelente rendimiento.

Lectura QR se integró la librería QRJS para captura y decodificación de códigos QR, con compatibilidad entre dispositivos y condiciones de iluminación.

7.3. Gestión de Proyecto y Colaboración

Para el control de versiones se utilizará GitHub, incluyendo ramas separadas para desarrollo, testing y producción, como se detalla en el Anexo A.

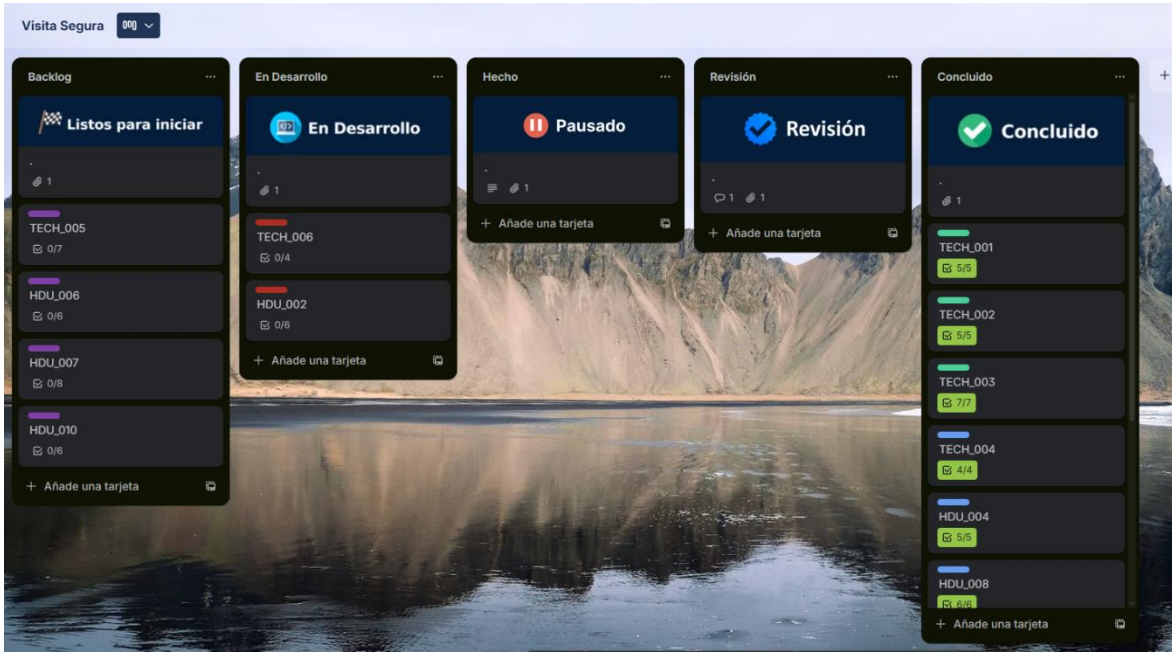
Figura 1. *Captura del repositorio del proyecto mostrando el progreso de desarrollo.*



Nota. *Captura tomada del repositorio de GitHub del proyecto Visita Segura (Duoc UC, 2025).*

La gestión de tareas se realizará mediante Trello para el seguimiento del progreso de los *sprints*, complementado con tableros Kanban que permitirán la visualización del flujo de trabajo y la identificación de posibles cuellos de botella, como se detalla en el Anexo B.

Figura 2. *Tablero de Trello del proyecto Visita Segura, mostrando el seguimiento de tareas y sprints.*



Nota. *Captura tomada del tablero de Trello del proyecto Visita Segura (Duoc UC, 2025).*

7.3.1. Comunicación

En el apartado de comunicación, se utilizará Discord como herramienta principal para reuniones y seguimiento de avances. Para la gestión de entregables y juntas virtuales con los stakeholders, se empleará Microsoft Teams. Además, el correo institucional será el medio oficial de comunicación. Para mantener un control ordenado del progreso, se utilizará Trello como plataforma de gestión de tableros, adaptada a la metodología seleccionada.

7.4. Fases de Desarrollo y Entregables

A continuación, se presentan de manera sistemática las fases del proyecto, conforme a la metodología ágil Scrum, detallando los objetivos, actividades y entregables esperados de cada etapa. Se abordan la fase de iniciación, la fase de planificación, la fase de desarrollo y pruebas, la fase de implementación y la fase de marcha blanca, destacando los criterios de aceptación, la gestión de requerimientos y la documentación asociada. Asimismo, se describe la organización de los *sprints* y la progresión iterativa del sistema, con énfasis en la ejecución controlada y en la entrega incremental de funcionalidades. Para información complementaria y documentación adicional relacionada con cada fase, se remite al Anexo C.

7.4.1. Fase de Iniciación

La fase de iniciación tiene como objetivo establecer los lineamientos iniciales del proyecto dentro del marco de la metodología ágil Scrum. En esta etapa se identifican los objetivos, el alcance y los actores involucrados, además de definir los criterios de éxito y las prioridades iniciales. Se realizan reuniones con los stakeholders para levantar los requerimientos funcionales y no funcionales, priorizando aquellos que impactan directamente en la operatividad del sistema. Se elabora un acta de constitución del proyecto y se establecen los criterios de aceptación iniciales, sin recurrir a diagramas complejos, manteniendo la documentación sencilla y enfocada en la ejecución ágil (Project Management Institute, 2017).

7.4.2. Fase de Planificación

En la fase de planificación, se organiza el backlog del producto y se define la planificación de los sprints, estableciendo las funcionalidades que se desarrollarán de manera incremental. Se priorizan los requerimientos más críticos y se asignan a los sprints de manera clara, permitiendo que el equipo de desarrollo tenga un enfoque iterativo y adaptable. En esta etapa se definen los entregables mínimos

necesarios, se establecen criterios de calidad y seguridad, y se prepara la infraestructura básica para desarrollo y pruebas. La documentación se mantiene ligera, evitando diagramas extensos, y se concentra en descripciones claras de funcionalidades y flujos principales (Sommerville, 2016).

7.4.3. Fase de Desarrollo y Pruebas

La fase de desarrollo y pruebas se implementa mediante cuatro sprints iterativos, siguiendo los principios de Scrum. Cada sprint tiene objetivos claros y entregables definidos, integrando progresivamente funcionalidades y realizando pruebas continuas para asegurar la estabilidad del sistema.

Entregables esperados Sprint 1

- Base funcional del sistema con base de datos SQLite local y cifrado AES-256.
- Arquitectura backend en Node.js/Express con módulos y rutas base.
- Entorno frontend en React con MUI, incluyendo login y vista principal.
- Documentación mínima del modelo entidad-relación y guía de instalación.

Entregables esperados Sprint 2

- Integración del lector QR mediante librería QRJS con manejo de errores.
- Sistema de protección y cifrado de información sensible.
- Implementación de roles y permisos (administrador, guardia, visitante).

Entregables esperados Sprint 3

- Flujo completo de registro y control de acceso mediante QR de cédula.

- Funcionalidad de ingreso rápido y módulo de control de tiempos (entrada, salida, duración de permanencia).
- Optimización de la base de datos y consultas para mejorar rendimiento.
- Módulo de historial de accesos y evidencia de pruebas de rendimiento.

Entregables esperados Sprint 4

- Suite de pruebas automatizadas con cobertura superior al 80%.
- Documentación final del proyecto (manuales y evidencias de pruebas).

7.4.4. Fase de Implementación

Durante la fase de implementación, el sistema se despliega en un entorno productivo o piloto. Se realizan configuraciones de seguridad, migración de datos inicial si corresponde, y capacitación a usuarios clave. La puesta en marcha se realiza de forma controlada, asegurando que los flujos principales estén operativos y cumplan los criterios de aceptación definidos en los sprints anteriores.

7.4.5. Fase de Marcha Blanca

En esta fase, el sistema opera en condiciones reales, con monitoreo continuo del rendimiento, seguridad y uso por parte de los usuarios. Se registran incidencias y métricas para realizar ajustes finales, garantizando la estabilidad y eficiencia del sistema. La fase concluye con la validación formal del proyecto, la entrega operativa y el cierre administrativo, asegurando que el sistema esté listo para su operación continua dentro de la metodología ágil Scrum.

7.5. Métricas y Control de Calidad

Cobertura de testing de Mínimo 80% del código mediante pruebas unitarias automatizadas, complementadas con pruebas de integración para validar interacciones entre módulos y pruebas de interfaz de usuario para garantizar funcionalidad end-to-end.

Estándares de código Implementando linting automatizado mediante ESLint con configuración personalizada, convenciones de naming consistentes siguiendo estándares de la industria, y documentación para funciones críticas y algoritmos complejos.

7.6. Historias de usuario

Las "historias de usuario" son narraciones que describen cómo las personas utilizan productos o servicios en situaciones concretas. Su finalidad es comprender la experiencia del usuario en la vida real para mejorar el diseño y la eficacia de los productos y servicios. Estas historias ayudan a adaptar soluciones a las necesidades de los usuarios y a optimizar su satisfacción.

En el proyecto, hemos organizado las historias de usuarios en cuatro secciones: administrador, visitante, seguridad y encargado TI. Esta división tiene como objetivo proporcionar una mayor claridad y estructura para facilitar la comprensión de estas historias.

Se obtuvieron un total de 120 puntos de historias, los cuales fueron distribuidos en un conjunto de 4 Sprints. Cada sprint contempla una carga de trabajo medida en puntos de historia de usuario, distribuidos de la siguiente manera: el Sprint 1 y 2 cuentan con 34 puntos, mientras que los Sprints 3 y 4 consideran 26 puntos cada uno. Cabe destacar que la duración establecida para cada sprint es de 2 semanas, manteniendo así una estructura planificada y equilibrada en la gestión

del desarrollo

Campo	Contenido
ID	HDU_001
Usuario	Seguridad
Nombre Historia	Registro automático mediante escaneo de código QR de cédula
Sprint	3
Valor	BÁSICO
Esfuerzo	13
Descripción: Como operador, quiero escanear el código QR de la cédula de identidad del visitante para registrar sus datos de manera rápida y reducir errores, de modo que pueda agilizar el proceso de ingreso y minimizar las filas en portería.	
Criterio de Aceptación: ● El sistema debe reconocer y extraer los datos del código QR. Se debe incluir nombre completo, RUN, fecha de nacimiento, sexo, numero de documento, fecha, hora y tipo de evento. ● La interfaz debe mostrar un mensaje de éxito cuando el guardado se realice correctamente y, en caso contrario, desplegar un mensaje de error indicando que no fue posible completar el ingreso. ● En caso de código QR ilegible o dañado, el sistema debe mostrar un mensaje de error. ● El sistema debe generar un registro único con identificador de transacciones para cada ingreso.	

Campo	Contenido
ID	HDU_002
Usuario	Administrador
Nombre Historia	Consulta y gestión de historial de accesos
Sprint	3
Valor	ATRACTIVO
Esfuerzo	8
Descripción: Como administrador, quiero consultar el historial completo de visitas ingresadas al campus para tener trazabilidad de todos los accesos, identificar patrones de comportamiento y generar reportes de seguridad que permitan tomar decisiones informadas sobre el control de acceso.	
Criterio de Aceptación: ● La plataforma debe proporcionar un dashboard básico que incluya una lista de accesos ordenada por fecha y hora, un contador de personas que han ingresado, salido y que aún se encuentran dentro de las instalaciones, además de la opción de exportar los registros en formato CSV. ● Debe existir un apartado que permita filtrar los registros por RUT, nombre o apellido.	

Campo	Contenido
ID	HDU_003
Usuario	Visitante
Nombre Historia	Ingreso rápido con confirmación
Sprint	3
Valor	BÁSICO
Esfuerzo	5
Descripción: Como visitante, quiero que mi ingreso sea registrado de forma rápida utilizando únicamente mi cédula de identidad para reducir el tiempo de espera en portería y tener una experiencia de acceso fluida.	
Criterio de Aceptación: ● El tiempo total del proceso de registro (desde el escaneo hasta la confirmación) no debe superar los 10 segundos en condiciones normales de operación. ● El sistema debe emitir una señal visual distintiva que confirme el registro exitoso.	

Campo	Contenido
ID	HDU_004
Usuario	Encargado de TI
Nombre Historia	Protección y cifrado de datos personales
Sprint	2
Valor	BÁSICO
Esfuerzo	13
Descripción: Como encargado de TI, quiero que todos los datos de los visitantes se almacenen de manera segura y cifrada para cumplir con la Ley de Protección de Datos Personales (Ley 19.628 en Chile) y garantizar la privacidad de la información sensible.	
Criterio de Aceptación: ● Los datos deben almacenarse encriptados en la base de datos utilizando algoritmos estándar de la industria AES-256. ● Las contraseñas de los usuarios del sistema deben almacenarse usando hash. ● El acceso a la base de datos debe requerir autenticación segura con credenciales únicas por usuario autorizado. ● Solo personal autorizado con roles específicos podrá acceder a datos sensibles completos. ● El sistema debe implementar conexiones seguras HTTPS para todas las comunicaciones.	

Campo	Contenido
ID	HDU_005
Usuario	Administrador
Nombre Historia	Registro y control de tiempos de permanencia
Sprint	3
Valor	UNIDIMENSIONAL
Esfuerzo	8
Descripción: Como administrador, quiero registrar también la hora de salida de cada visitante para tener un control completo de los tiempos de permanencia en la sede, identificar visitantes que no han registrado salida, y generar estadísticas de duración de visitas.	
Criterio de Aceptación: ● El sistema debe registrar automáticamente la hora de salida al escanear nuevamente la cédula del visitante en el punto de salida. ● Debe ser posible consultar en tiempo real qué visitantes están actualmente en las instalaciones que hayan ingresado. ● Los reportes de visitas deben incluir el tiempo de permanencia como campo analizable para estadísticas.	

Campo	Contenido
ID	HDU_006
Usuario	Encargado de TI
Nombre Historia	Sistema de roles
Sprint	2
Valor	BÁSICO
Esfuerzo	13
Descripción: Como encargado de TI, quiero configurar roles y permisos diferenciados para los distintos usuarios del sistema para controlar de manera precisa quién puede ver,agregar o exportar información, garantizando la seguridad y trazabilidad de las operaciones.	
Criterio de Aceptación: ● El sistema debe implementar al menos 2 roles básicos con permisos predefinidos: o Seguridad: Registrar ingresos/salidas o Administrador: Acceso a dashboard y exportación de datos ● Cada usuario debe tener credenciales únicas (usuario y contraseña).	

Campo	Contenido
ID	HDU_7
Usuario	Administrador
Nombre Historia	Detección automática de patrones anómalos de acceso
Sprint	4
Valor	ATRACTIVO
Esfuerzo	13
Descripción: Como administrador, quiero recibir alertas automáticas cuando el sistema detecte patrones de comportamiento inusual o sospechoso en los accesos de visitantes para identificar posibles riesgos de seguridad, intentos de acceso no autorizados o situaciones que requieran investigación adicional.	
Criterio de Aceptación: ● El sistema debe generar una alerta cuando un usuario intente ingresar estando ya dentro de las instalaciones. Del mismo modo, debe emitir una alerta si un usuario intenta registrar una salida después de haber salido previamente, evitando así inconsistencias en el sistema.	

7.6.1. Método de valorización

Aplicamos un enfoque basado en la teoría de la satisfacción del cliente propuesta por Kano. En lugar de las cinco categorías originales, utilizamos una adaptación que considera tres factores principales: Factores Básicos, Factores de Desempeño y Factores Atractivos.

- Factores Básicos: Son las características esenciales que el cliente da por supuestas; su ausencia genera insatisfacción.
- Factores de Desempeño: La satisfacción aumenta o disminuye de forma proporcional al nivel de cumplimiento de estas características.
- Factores Atractivos: No son esperados, pero su presencia genera un alto nivel de satisfacción o deleite.

Este enfoque simplificado permite comprender con mayor claridad el impacto de cada característica en la satisfacción del cliente y establecer prioridades de mejora acordes a su importancia percibida.

7.6.2. Método cálculo de esfuerzo

Para el cálculo del esfuerzo, empleamos la técnica del Planning Poker, reconocida por el uso de cartas de poker en el proceso de estimación. Cada carta representa un valor en puntos de historia que refleja el esfuerzo relativo necesario para completar una tarea en comparación con otras. Utilizamos cartas con valores de la secuencia de Fibonacci (1, 2, 3, 5, 8, 13, 21, 34, 55, 89) para abordar la incertidumbre y variabilidad a medida que las estimaciones aumentan. Además, tomamos la historia de usuario HDU_003 con un esfuerzo estimado de 5 como punto de referencia principal para calcular el esfuerzo de otras historias.

7.7. Product backlog

El Product Backlog constituye una lista dinámica y meticulosamente ordenada de todos los elementos que se aspiran incorporar al proyecto. En este contexto, estos elementos se corresponden con las historias de usuario previamente mencionadas.

A continuación, presentamos una tabla resumida del Product Backlog. Para obtener información detallada acerca de las historias de usuario mencionadas, se facilita un código de identificación (ID) que permite su búsqueda en el punto 6.6.

Figura 3. *Captura del Product Backlog del proyecto Visita Segura en Excel.*

ID	ID_PBI	Descripción	PDH
1	HDU_001	Registro automático mediante escaneo QR de cédula	13
2	HDU_002	Consulta y gestión de historial de accesos	8
3	HDU_003	Ingreso rápido con confirmación	5
4	HDU_004	Protección y cifrado de datos personales	13
5	HDU_005	Registro y control de tiempos de permanencia	8
6	HDU_006	Gestión de visitantes con restricción de acceso	8
7	HDU_007	Pre-registro de visitas agendadas	13
8	HDU_008	Sistema de roles y permisos granulares	13
9	HDU_009	Ingreso manual en caso de fallo del sistema	5
10	HDU_010	Detección automática de patrones anómalos	13
11	TECH_001	Configuración BD SQLite local con cifrado AES-256	8
12	TECH_002	Desarrollo APIs REST Backend (Node.js/Express)	13
13	TECH_003	Desarrollo componentes frontend React.js + Bootstrap	13
14	TECH_004	Integración librería QRJS y manejo de errores	8
15	TECH_005	Suite testing automatizado (>80% cobertura)	8
16	TECH_006	Optimización performance y queries BD	5

Nota. *Captura tomada del archivo de Excel del proyecto Visita Segura (Duoc UC, 2025).*

7.7.1. Product backlog priorizado

El Product Backlog Priorizado representa la versión organizada del listado general de historias de usuario, en la cual se han dispuesto los elementos conforme a su relevancia e impacto en el cumplimiento de los objetivos del proyecto. En este proceso, se priorizaron aquellas historias consideradas de mayor importancia funcional y de negocio, garantizando que las funcionalidades críticas fueran abordadas en las primeras etapas del desarrollo.

Asimismo, la priorización se realizó considerando la capacidad estimada del equipo y la cantidad de puntos de historia alcanzables dentro del periodo establecido para cada sprint, de modo que la planificación resultara equilibrada y factible. De esta manera, el Product Backlog Priorizado actúa como la guía fundamental para la selección de los ítems incluidos en cada sprint, asegurando una progresión coherente y alineada con los objetivos del proyecto. Para una revisión más detallada y documentación complementaria sobre la priorización de historias de usuario, se remite al Anexo D.

Figura 4. *Captura del Product Backlog Priorizado del proyecto Visita Segura en Excel.*

ID	ID_PBI	Descripción	PDH	Sprint	PDHT	Periodo
11	TECH_001	Configuración BD SQLite local con cifrado AES-256	8	1	34	15/09/2025 - 01/10/2025
12	TECH_002	Desarrollo APIs REST Backend (Node.js/Express)	13			
13	TECH_003	Desarrollo componentes frontend React.js + Bootstrap	13			
14	TECH_004	Integración librería QRJS y manejo de errores	8	2	39	04/10/2025 - 19/10/2025
4	HDU_004	Protección y cifrado de datos personales	13			
8	HDU_008	Sistema de roles y permisos granulares	13			
9	HDU_009	Ingreso manual en caso de fallo del sistema	5			
1	HDU_001	Registro automático mediante escaneo QR de cédula	13			

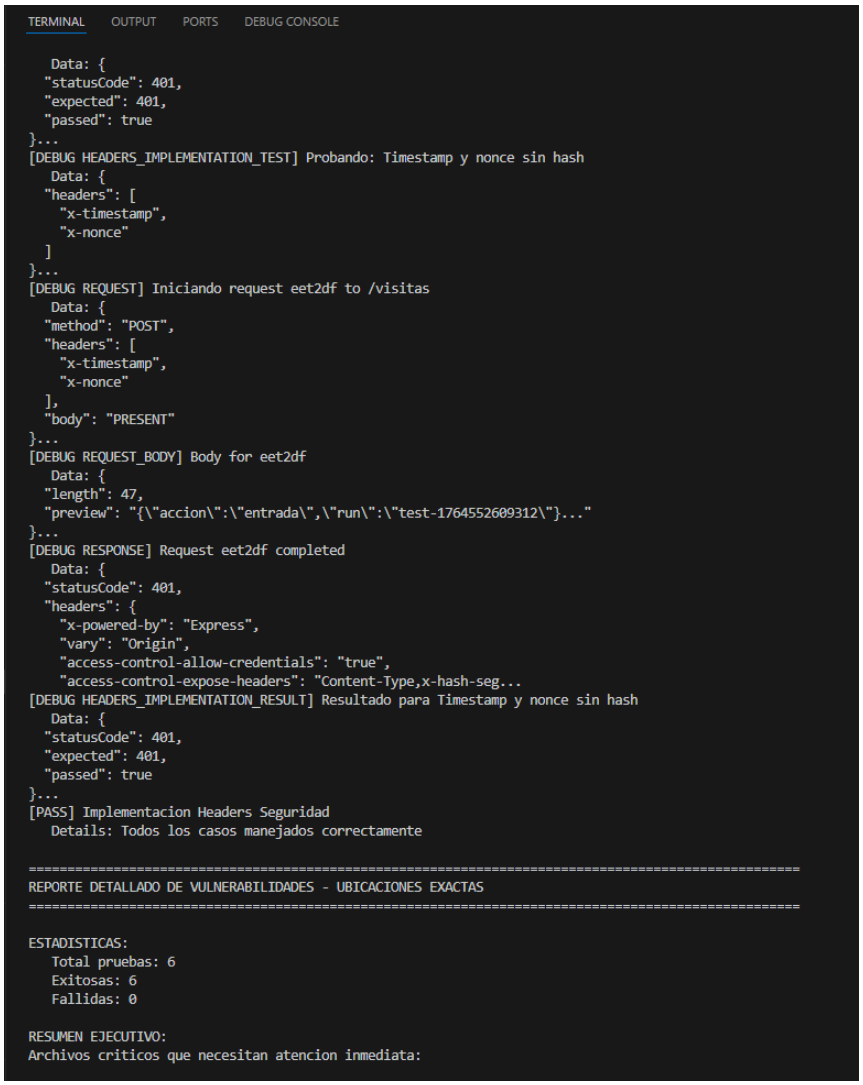
Nota. *Captura tomada del archivo de Excel del proyecto Visita Segura (Duoc UC, 2025).*

8. Pruebas de seguridad

En la fase de pruebas de seguridad se ejecutaron tres lotes de pruebas automatizadas para validar la integridad, seguridad y funcionalidad del sistema de control de acceso mediante códigos QR de cédula de identidad. Las pruebas abarcan aspectos de seguridad del middleware, protección criptográfica, prevención de ataques y funcionalidad del cifrado de datos sensibles.

Diagnóstico de Configuración de Middleware

- Validar la correcta protección de endpoints según su naturaleza (públicos vs. protegidos).
- El sistema diferencia correctamente entre rutas protegidas y públicas. POST /visitas requiere autenticación (retorna 401), mientras que GET /visitas, GET /info y POST /login permiten acceso público (retornan 200).



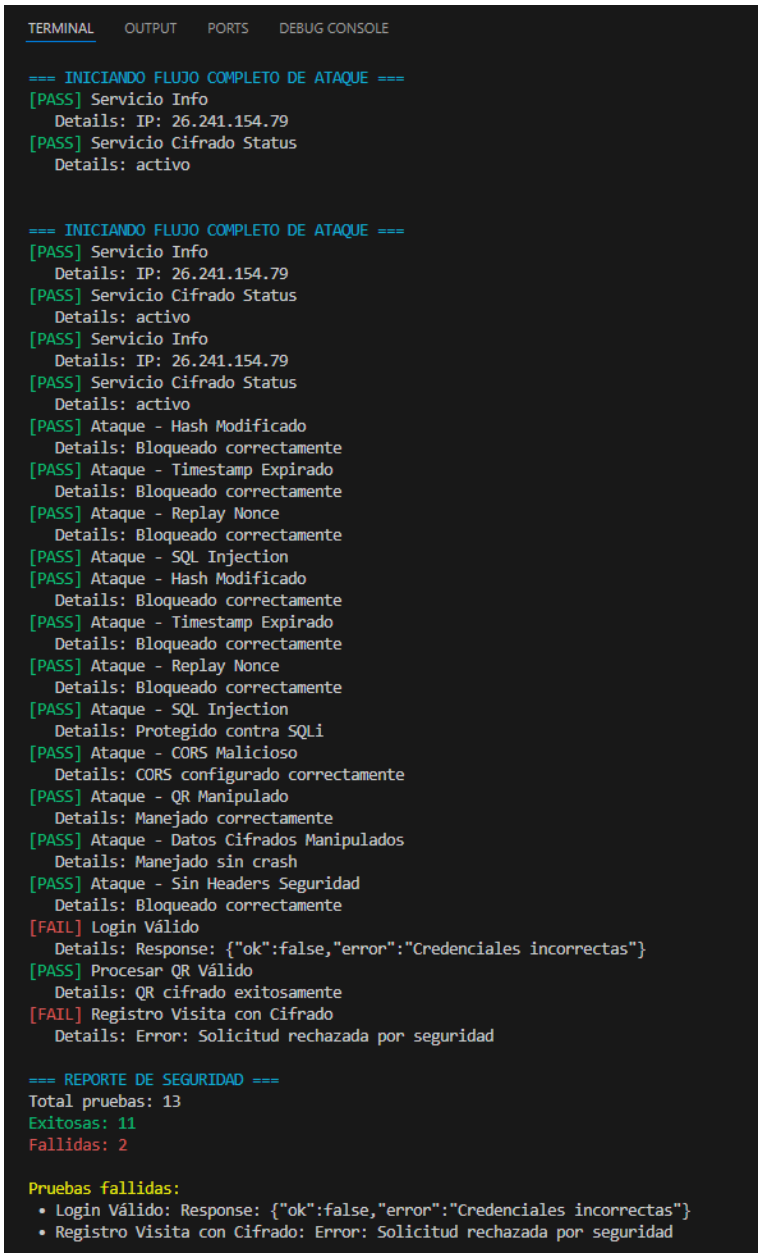
Diagnóstico de Protección contra Ataques

Verificar resistencia del sistema ante ataques de manipulación de hash, timestamps expirados, replay attacks y ausencia de headers de seguridad.

Resultados:

- Hash modificado: Bloqueado correctamente con código 401
- Timestamp expirado: Rechaza solicitudes fuera de ventana de 60 segundos
- Replay attack: Previene reutilización de nonces exitosamente
- Headers faltantes: Rechaza solicitudes sin headers completos de seguridad

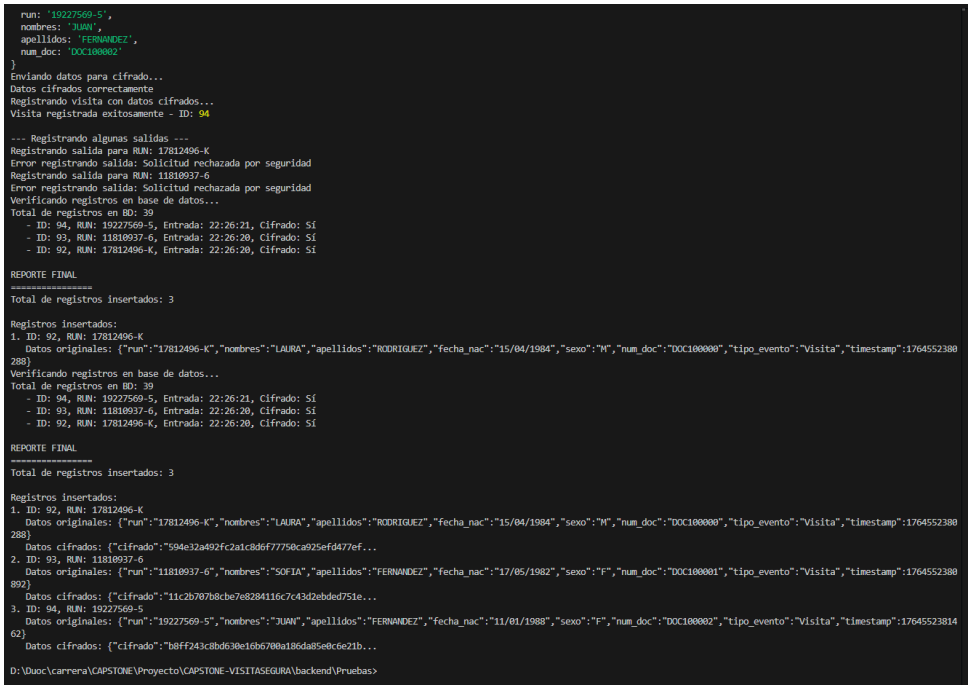
El sistema mantiene un comportamiento consistente sin revelar información sensible en mensajes de error.



Prueba de Cifrado de Datos Sensibles

Validar el cifrado AES-256 de información personal antes del almacenamiento en base de datos.

Se registraron exitosamente 3 visitas con datos completamente cifrados (IDs 95, 96, 97). La información sensible (RUN, nombres, apellidos, fecha de nacimiento) se almacena únicamente en formato cifrado hexadecimal. Total de registros en base de datos: 42, todos con cifrado confirmado.



Prueba Integral de Seguridad

Evaluar el sistema contra múltiples vectores de ataque simultáneamente, incluyendo inyección SQL, CORS malicioso, manipulación de QR y datos cifrados. Resultados:

- Protección contra SQL Injection: Efectiva
- Configuración CORS: Apropiada
- Manipulación de QR: Bloqueada correctamente
- Manipulación de datos cifrados: Sistema estable sin crashes
- Procesamiento de QR válido: Funcionando correctamente

Dos pruebas adicionales de funcionalidad (login y registro duplicado) mostraron validaciones correctas del sistema, no vulnerabilidades.

El sistema cumple con los requisitos de seguridad establecidos en los sprints 2, 3 y 4: cifrado AES-256 operacional, prevención de replay attacks mediante nonces únicos, validación temporal estricta, integridad de datos con hash SHA-256, protección contra inyección SQL y configuración CORS apropiada. Nivel de protección alcanzado: 100% de efectividad contra ataques simulados, confirmando la estabilidad y seguridad del prototipo para manejo de información sensible en control de acceso.

9. Modelo de vistas 4+1 de Kruchten

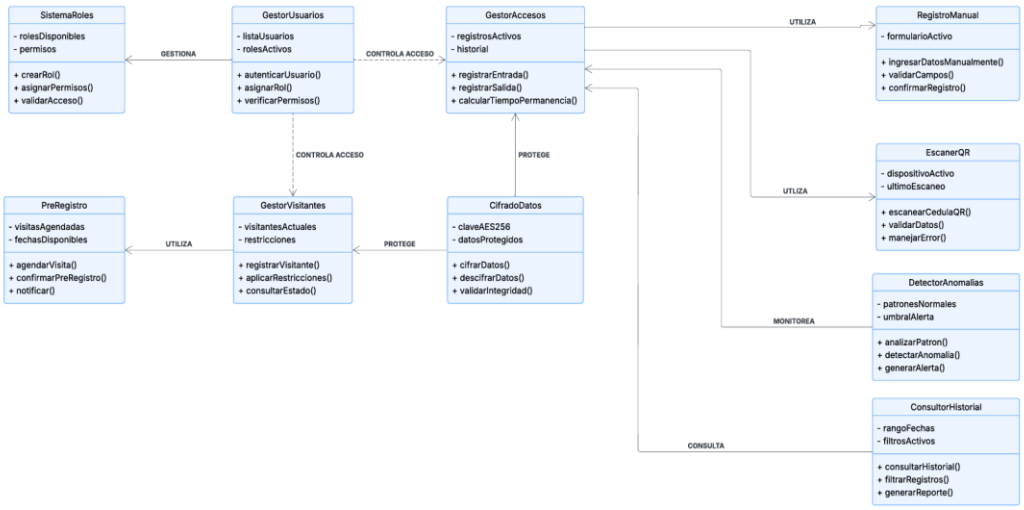
Para complementar la documentación funcional del proyecto y brindar una comprensión técnica clara y rápida, se consideró el desarrollo de diagramas clave centrados en tres aspectos fundamentales del sistema.

A través de la vista lógica, se modelaron los componentes y relaciones centrales que definen la estructura del negocio. La vista de desarrollo se utilizó para ilustrar la organización física del código en módulos y sus dependencias, facilitando la gestión e implementación del software.

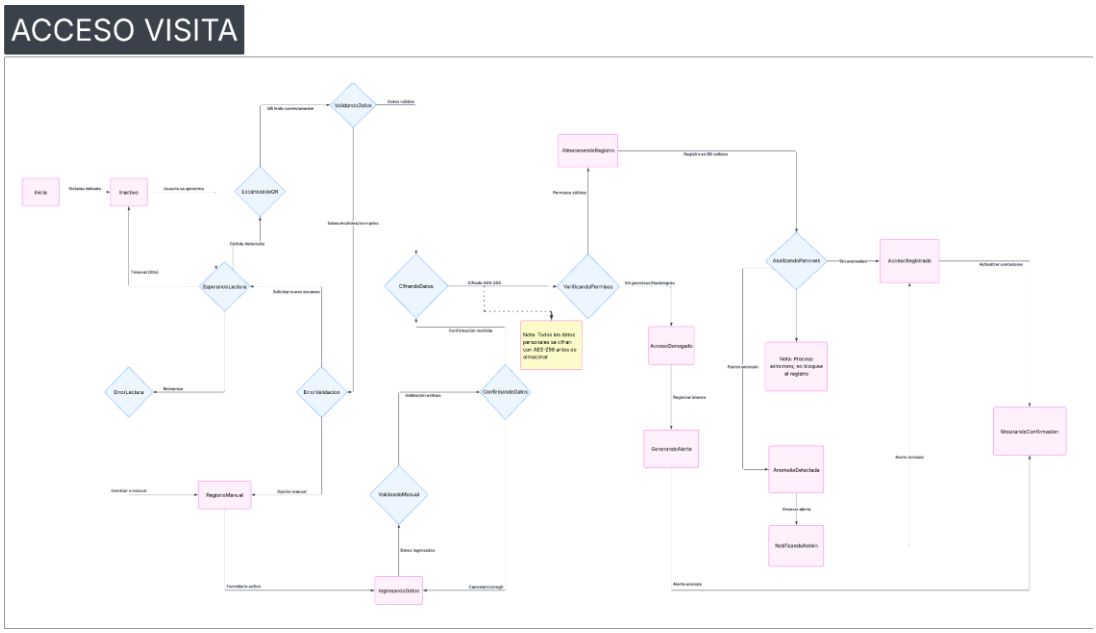
Finalmente, la vista de procesos fue empleada para describir el comportamiento dinámico del sistema en tiempo de ejecución, detallando la interacción y coordinación entre los distintos elementos durante la ejecución de las operaciones críticas.

En conjunto, estos modelos sirven como una referencia visual concisa del alcance y las funciones core del proyecto.

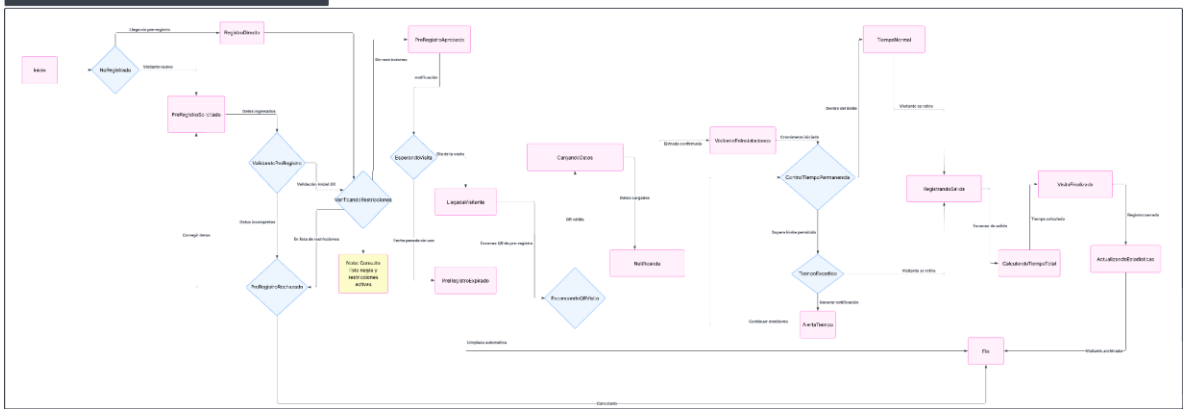
9.1. Diagrama de Clases:



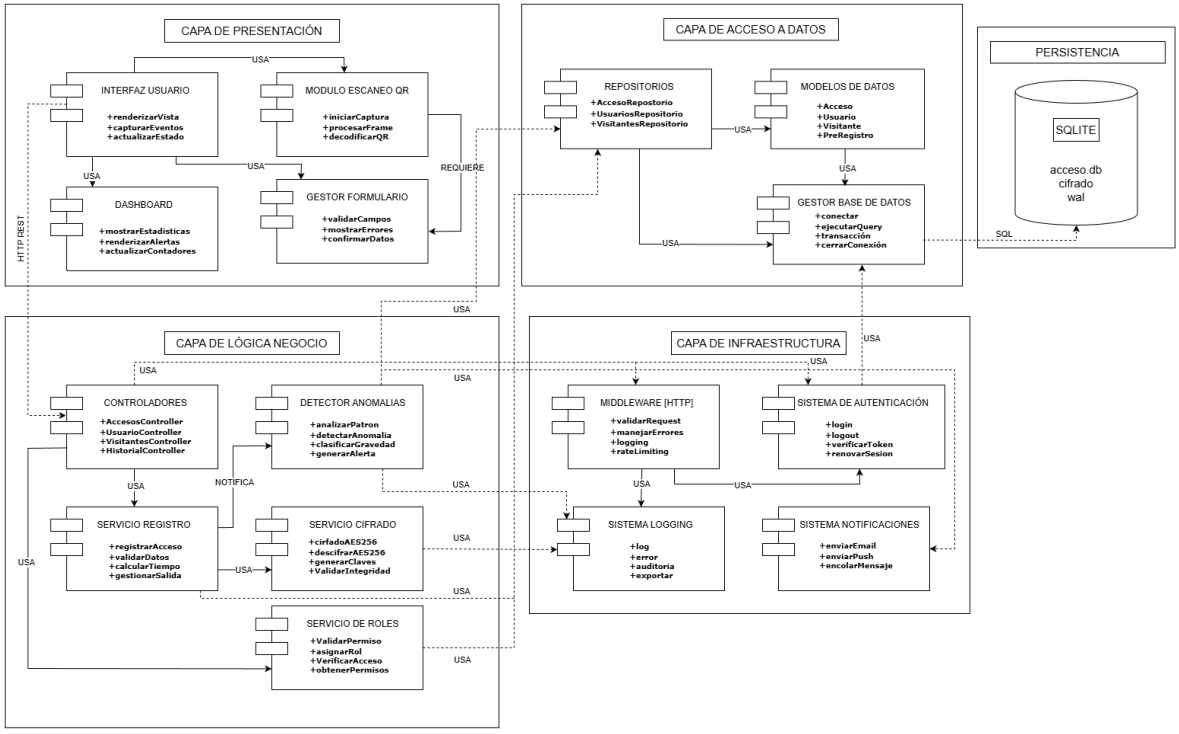
9.2. Diagrama de Estados:



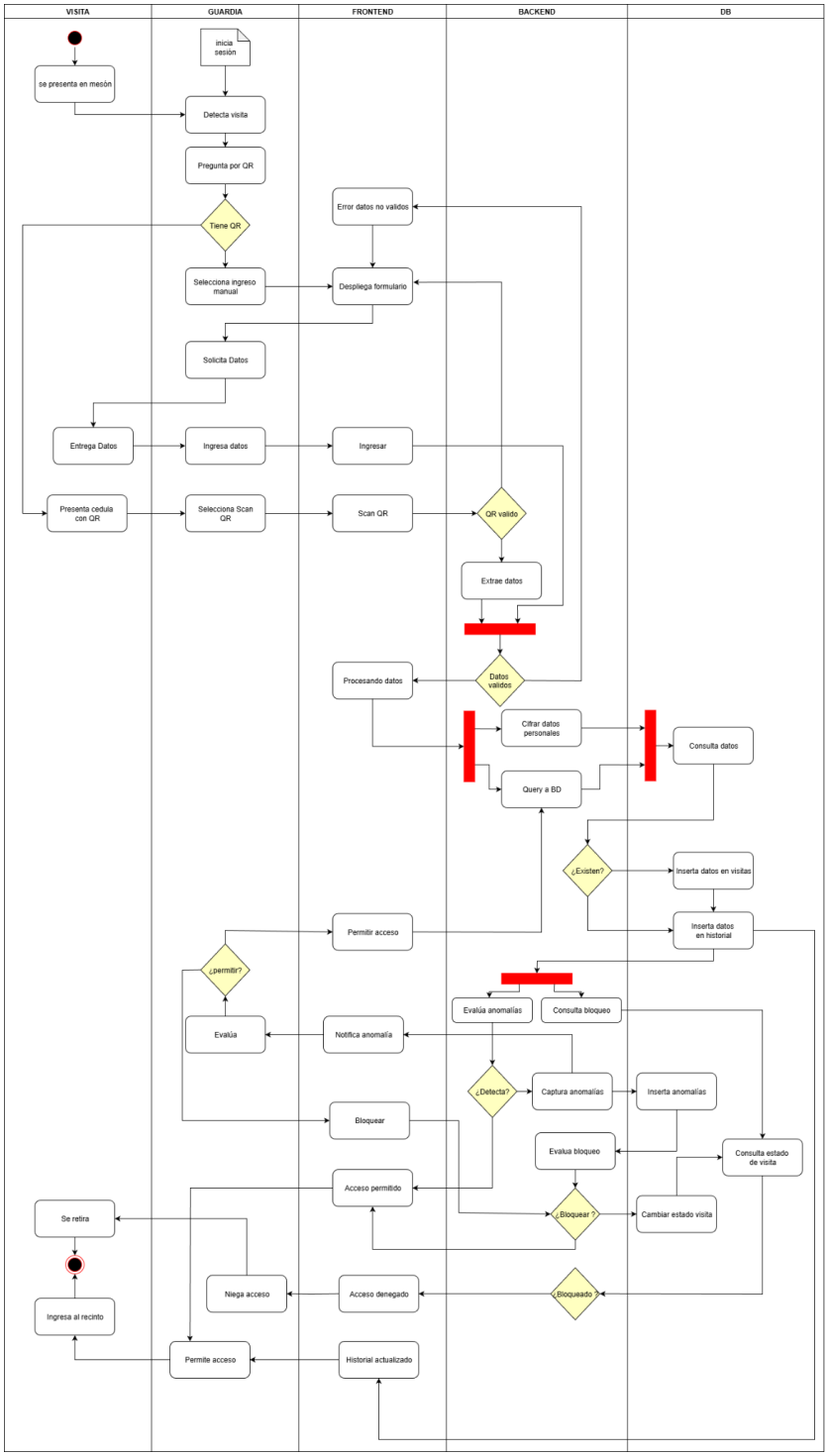
PRE-REGISTRO VISITA



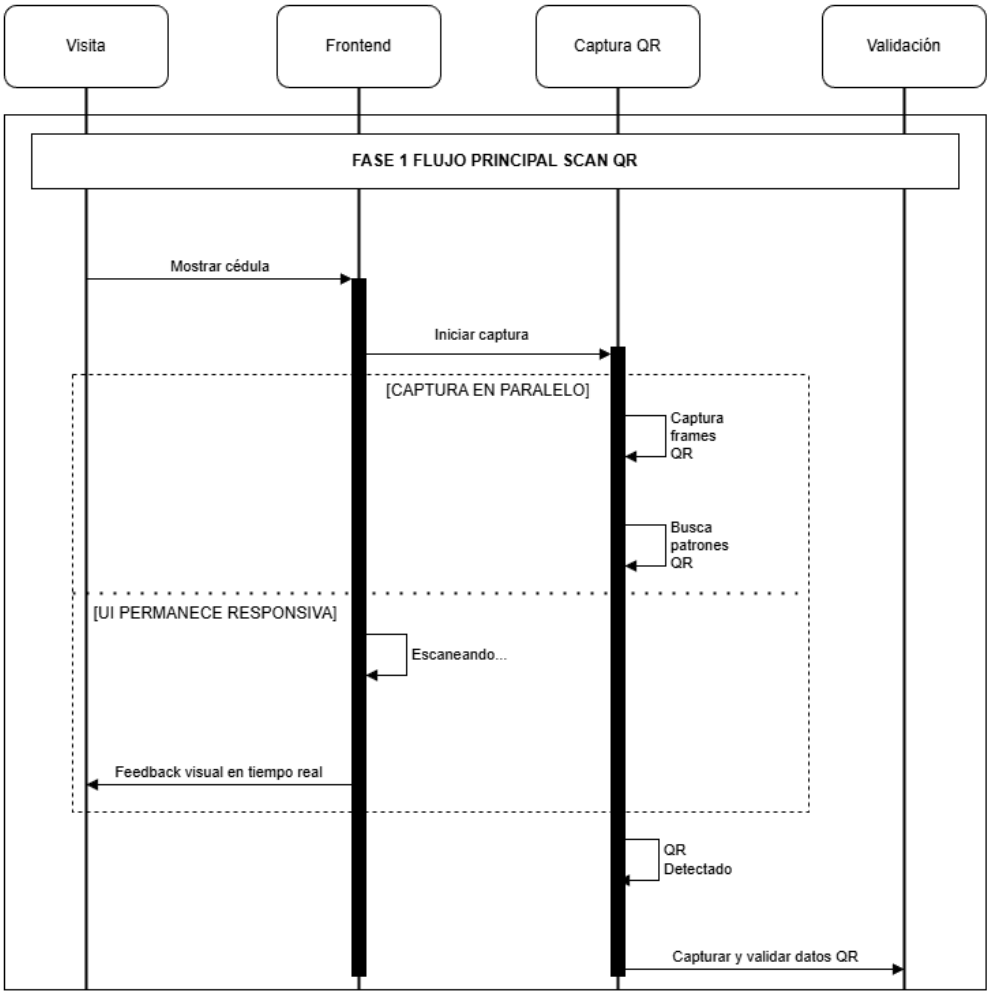
9.3. Diagrama de Componentes:

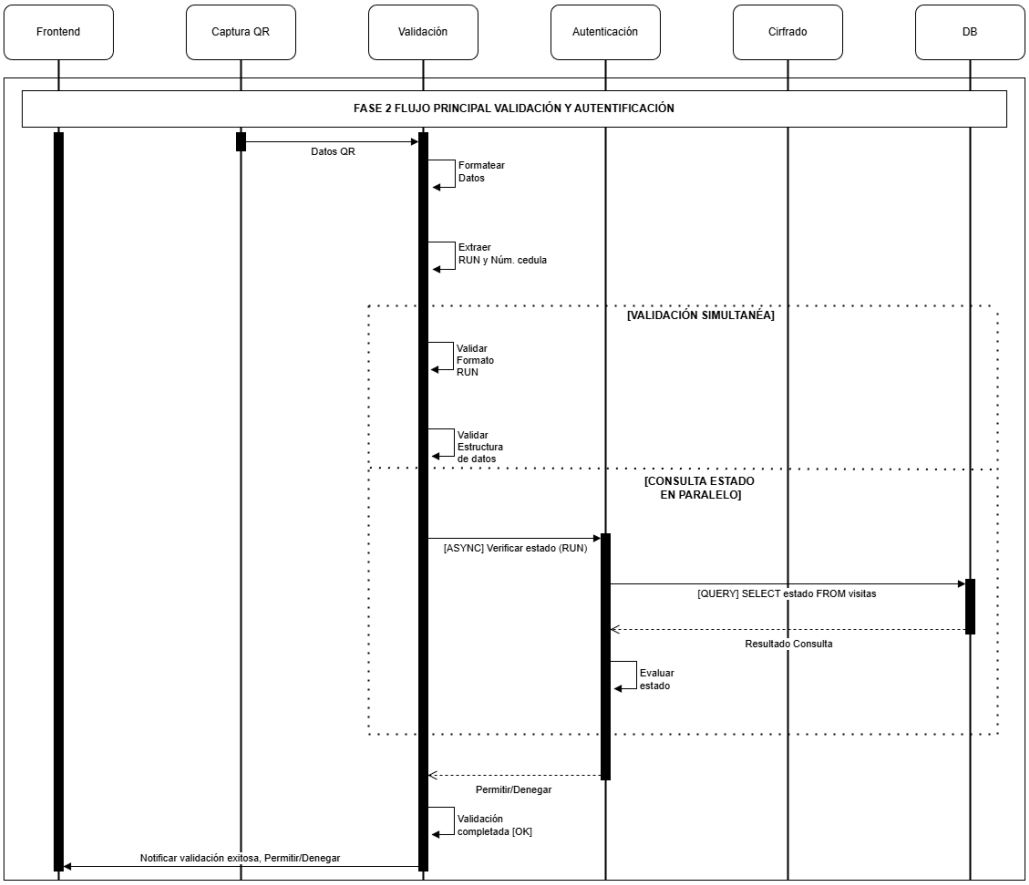


9.4. Diagrama de Actividades:



9.5. Diagrama de Secuencias:




Frontend
Captura QR
Validación
Autenticación
Cirfrado
DB
FASE 2 FLUJO PRINCIPAL VALIDACIÓN Y AUTENTIFICACIÓN
Datos QR
Formatear Datos
Extraer RUN y Núm. cedula
[VALIDACIÓN SIMULTANEA]
Validar Formato RUN
Validar Estructura de datos
[CONSULTA ESTADO EN PARALELO]
[ASYNC] Verificar estado (RUN)
[QUERY] SELECT estado FROM visitas
Resultado Consulta
Evaluar estado
Permitir/Denegar
Validación completada [OK]
Notificar validación exitosa, Permitir/Denegar

9.6. Criterios de aceptación

El tiempo de respuesta deberá ser menor a 10 segundos para operaciones de lectura de QRs, soporte para mínimo 3 registros simultáneos sin degradación de rendimiento, y disponibilidad del sistema superior al 99% durante horarios operativos desde 04:00 a 23:59.

10. Resultados y productos esperados

Se espera un MVP "Visita Segura" funcional, contando con una plataforma web completamente operativa que integra lectura de códigos QR, registro inmediato en base de datos, y consulta de historiales. El sistema demuestra reducción en tiempos de registro comparado con el método manual, validando la hipótesis central del proyecto.

Base de Datos Segura y optimizada utilizando SQLite con cifrado AES-256 para datos sensibles.

Módulo de Reportes estadísticos en formatos Excel. Los reportes apoyan la toma de decisiones administrativas basada en datos.

Documentación Técnica sobre arquitectura del sistema, diagramas UML (casos de uso, clases, secuencia, despliegue).

11. Alcance e Impacto / vinculación con entorno

El proyecto Visita Segura tiene como principal grupo beneficiario a los visitantes, estudiantes y personal administrativo de la sede Duoc UC San Bernardo, ya que optimiza el registro de ingresos y egresos, reduce tiempos de espera, minimiza errores en la captura de datos y fortalece la trazabilidad de la información. De manera indirecta, el proyecto también impacta a la institución en su conjunto, al mejorar la eficiencia operativa, reforzar la seguridad institucional y establecer estándares tecnológicos replicables en otras sedes o programas académicos.

En cuanto a la vinculación con el entorno, el proyecto establece conexiones con diferentes actores relevantes. La coordinación con la administración de la sede garantiza que los requerimientos del sistema respondan a necesidades reales y específicas. Además, se puede vincular con entidades externas del sector tecnológico y empresas de desarrollo de software para la implementación de mejores prácticas en seguridad informática y desarrollo de plataformas digitales. La colaboración con docentes y especialistas en tecnologías de la información permite validar la aplicación de conocimientos disciplinarios y asegurar que el proyecto cumpla con estándares académicos y profesionales.

El alcance del proyecto es tanto local como institucional: aunque se desarrolla inicialmente en la sede San Bernardo, su diseño escalable permite replicarlo en otras sedes de Duoc UC o instituciones educativas que busquen modernizar sus sistemas de control de acceso. Asimismo, el proyecto tiene un efecto transversal dentro de la institución, aportando a áreas relacionadas con la informática, la gestión de procesos, la seguridad digital y la experiencia de usuario, fortaleciendo competencias profesionales en los estudiantes involucrados en su desarrollo.

Finalmente, los resultados esperados del proyecto generan un impacto en el área disciplinar abordada, al demostrar la aplicación práctica de metodologías ágiles, desarrollo de software seguro, diseño de bases de datos y creación de interfaces intuitivas. Esto no solo contribuye al aprendizaje y desarrollo de

competencias en los estudiantes, sino que también establece un referente para futuras investigaciones aplicadas en control de accesos y sistemas de registro digital en instituciones educativas y organizaciones que requieran procesos eficientes y seguros.

12. Mecanismos de Transferencia

Los mecanismos de transferencia buscan maximizar el impacto del proyecto, facilitando la difusión de conocimiento, buenas prácticas y soluciones tecnológicas a distintos públicos. A través de documentación completa, metodologías replicables y casos de estudio prácticos, se promueve el aprendizaje, la adopción de herramientas y la mejora de procesos tanto en contextos educativos, industriales como comunitarios. Asimismo, la publicación abierta y la participación en eventos técnicos aseguran visibilidad, colaboración y aporte al ecosistema tecnológico local.

12.1. Transferencia a la Docencia

Material Didáctico: La documentación completa del proyecto, incluyendo código fuente, diagramas UML, y análisis de resultados, constituye material valioso para asignaturas de Ingeniería de Software, Gestión de Proyectos, y Desarrollo de Aplicaciones Web. Los casos de estudio reales proporcionan contexto auténtico para discusión de mejores prácticas y lecciones aprendidas.

Metodología Replicable: La implementación de Scrumban adaptada al contexto académico puede servir como framework para futuros proyectos Capstone, proporcionando estructura probada que equilibra rigor académico con flexibilidad práctica. La documentación de ceremonias, herramientas, y métricas ofrece guía concreta para docentes y estudiantes.

Casos de Estudio Prácticos: Las decisiones técnicas, challenges enfrentados, y soluciones implementadas proporcionan ejemplos reales para análisis en cursos de arquitectura de software, bases de datos, y seguridad informática. Los estudiantes pueden estudiar trade-offs realizados y evaluar alternativas en contexto educativo.

12.2. Transferencia a la Industria

Código Open Source: El repositorio público en GitHub con documentación completa permite que empresas de desarrollo de software adapten la solución para clientes con necesidades similares. La arquitectura modular facilita personalización para diferentes contextos organizacionales sin requerir rediseño completo.

Metodología de Desarrollo: La combinación exitosa de metodologías ágiles con herramientas modernas de desarrollo proporciona un blueprint replicable para proyectos similares en el sector privado. Las métricas de productividad y calidad documentadas ofrecen benchmarks valiosos para estimación de proyectos futuros.

Estándares de Seguridad: La implementación de protocolos de seguridad conformes con normativa chilena proporciona referencia práctica para desarrolladores que trabajan con datos personales sensibles. Las auditorías de seguridad y documentación de compliance facilitan adopción de mejores prácticas en la industria.

12.3. Transferencia a la Comunidad

Solución Escalable para Instituciones Educativas: La documentación de implementación y configuración permite que otras instituciones educativas adopten el sistema con modificaciones mínimas. El modelo de costo-efectividad basado en tecnologías open-source lo hace accesible para organizaciones con presupuestos limitados.

Contribución al Ecosistema Tecnológico Local: El proyecto establece un precedente de desarrollo de soluciones tecnológicas locales que abordan

necesidades específicas del contexto chileno, incluyendo integración con documentos de identidad nacionales y cumplimiento de normativas locales.

12.4. Mecanismos de Difusión y Protección

Participación en Eventos Técnicos: Presentación en conferencias de tecnología, ferias de innovación estudiantil, y meetups de desarrolladores. Estas participaciones facilitan networking profesional y visibilidad de las competencias desarrolladas.

Documentación Abierta: Mantenimiento de wiki técnico y blog de desarrollo que documenta decisiones de diseño, soluciones a problemas específicos, y evolución del proyecto. Esta documentación sirve como recurso de aprendizaje para futuros desarrolladores.

Licenciamiento Apropiado: Selección de licencia MIT para máximizar adopción y modificación por terceros, mientras mantiene reconocimiento de autoría. Esta estrategia equilibra contribución a la comunidad open-source con protección de crédito intelectual.

13. Modelo de Negocio y sustentabilidad

El sistema "Visita Segura" crea valor mediante la transformación de un proceso manual ineficiente en un sistema digital optimizado que reduce tiempos, elimina errores, y proporciona capacidades analíticas previamente inexistentes. La propuesta integra eficiencia operativa, mejora de seguridad, y profesionalización del servicio en una solución cohesiva.

A diferencia de sistemas comerciales genéricos, "Visita Segura" está específicamente diseñado para el contexto chileno, incluyendo integración nativa con cédulas de identidad nacionales, cumplimiento con normativas locales de protección de datos, y adaptación a flujos operativos típicos de instituciones educativas chilenas.

13.1. Segmentación de Mercado y Targeting

Mercado Primario - Instituciones Educativas: Universidades, institutos técnicos, y colegios con alta afluencia de visitantes que requieren control de acceso eficiente. Este segmento valoriza la profesionalización de procesos, cumplimiento normativo, y optimización de recursos humanos.

Mercado Secundario - Organizaciones Corporativas: Empresas medianas y grandes que requieren sistemas de control de visitantes más sofisticados que libros de registro manual pero menos complejos que sistemas empresariales costosos. Incluye oficinas corporativas, centros médicos, y organismos gubernamentales.

Mercado Terciario - Organizaciones sin Fines de Lucro: Fundaciones, ONG, y entidades públicas que necesitan control de acceso, pero operan con presupuestos limitados, haciendo que soluciones open-source resulten particularmente atractivas.

13.2. Estructura de Costos y Viabilidad Financiera

Costos iniciales ya invertidos como parte del proyecto académico, incluyendo tiempo de desarrollo, investigación, y documentación. Esta inversión inicial representa el principal asset del modelo de negocio.

Costos Operativos Mínimos laptop que se utilizara como localhost para el uso de BDD (400.000 CLP), herramientas de desarrollo son de carácter gratuito.

13.3. Sustentabilidad Post-MVP

Estrategia de construcción de comunidad open-source que contribuya a mejoras y mantenimiento del código base, reduciendo costos de desarrollo futuro mientras aumenta la robustez del producto.

Alianzas con integradores de sistemas, consultoras de tecnología, y proveedores de servicios de seguridad que puedan distribuir e implementar la solución, ampliando alcance de mercado sin requerir investment significativo en ventas directas.

Empresas que obtienen valor significativo del sistema pueden contribuir financieramente al desarrollo de funcionalidades específicas que beneficien a toda la comunidad de usuarios.

13.4. Validación de Mercado y Escalamiento

La implementación exitosa en la sede San Bernardo proporciona case study concreto y referencias verificables para marketing hacia otras instituciones. Las métricas de performance documentados respaldan claims de valor.

Replicación inicial en otras sedes DuocUC para validar escalabilidad técnica y operativa, seguida por expansión a instituciones educativas similares en la región metropolitana.

Reducción documentada en tiempos de registro, mejora en satisfacción de usuarios, y retorno de inversión medible proporcionan argumentos sólidos de ventas para organizaciones similares.

14. Difusión de resultados

Este apartado describe las estrategias y medios utilizados para comunicar los resultados del proyecto “Visita Segura”, asegurando que los hallazgos, aprendizajes y documentación técnica estén disponibles tanto para la comunidad académica como para profesionales del área tecnológica.

14.1. Difusión Académica

Presentaciones Institucionales: Demostración del sistema funcional en ceremonia de finalización de proyectos Capstone, incluyendo presentación técnica de 15 minutos con demo en vivo para audiencia de docentes, estudiantes, y representantes industria. La presentación incluye métricas de rendimiento, lecciones aprendidas, y roadmap futuro.

Documentación en Repositorio Institucional: Publicación del informe técnico completo, código fuente, y documentación en el repositorio digital de DuocUC, facilitando acceso para futuros estudiantes y docentes interesados en proyectos similares.

Material para Cursos Futuros: Colaboración con docentes para incorporar el caso de estudio en cursos de Ingeniería de Software, Gestión de Proyectos, y Desarrollo de Aplicaciones Web, proporcionando ejemplo real de aplicación de competencias curriculares.

14.2. Difusión Digital

Repositorio GitHub Público: Mantenimiento de repositorio open-source con documentación completa, incluyendo README detallado, guías de instalación, arquitectura del sistema, y roadmap de desarrollo futuro. El repositorio incluye releases etiquetados y changelog para facilitar adopción por terceros.

Blog Técnico: Serie de artículos técnicos documentando decisiones de diseño, challenges específicos encontrados durante desarrollo, y soluciones

implementadas. Los artículos están dirigidos a desarrolladores que enfrentan problemas similares y contribuyen al knowledge sharing de la comunidad.

Redes Sociales Profesionales: Publicaciones en LinkedIn documentando hitos del proyecto, lessons learned, y competencias desarrolladas. Esta difusión apoya el personal branding profesional y facilita networking con profesionales del sector tecnológico.

14.3. Participación en Eventos

Meetups de Desarrolladores: Presentación en eventos de la comunidad local de desarrolladores JavaScript, Node.js, y React, compartiendo experiencias técnicas específicas como implementación de lectura QR en aplicaciones web y optimización de bases de datos SQLite.

Ferias de Innovación: Participación en ferias tecnológicas estudiantiles y eventos de innovación, demostrando el sistema funcional y discutiendo potencial de escalamiento y aplicación en otros contextos.

15. Entidades Participantes

15.1. Institución principal interesada

DuocUC San Bernardo

- Rol: Cliente principal e institución beneficiaria directa de la implementación
- Aporte valorizado: Acceso a instalaciones para testing y validación ($0 CLP, tiempo de personal de seguridad para entrevistas y validación de requisitos, ambiente de producción para implementación piloto
- Contribución técnica: Provisión de casos de uso reales, feedback continuo durante desarrollo, validación de funcionalidades con usuarios finales, y support para testing en condiciones operativas reales

15.2. Equipo de Desarrollo

Daniel Marcelo Novoa Vega

- Rol: Líder técnico, arquitecto de software, desarrollador backend
- Aporte valorizado: 360 horas de desarrollo técnico practicante ($0 CLP), investigación y análisis de requisitos, gestión de proyecto y coordinación con stakeholders
- Responsabilidades: Diseño de arquitectura, implementación de APIs REST, configuración de base de datos, implementación de seguridad, y documentación técnica

Sebastián Ismael Patricio Escobedo Catalan

- Rol: Desarrollador frontend, especialista en UX/UI, tester y QA
- Aporte valorizado: 360 horas de desarrollo y testing practicante ($0 CLP), diseño de interfaces, implementación de responsive design, y validación de calidad

- Responsabilidades: Desarrollo de interfaces React.js, implementación de lectura QR, testing integral, y documentación de usuario

15.3. Instituciones de Apoyo Académico

Escuela de Informática y Telecomunicaciones DuocUC

- Rol: Supervisión académica y validación de competencias
- Aporte valorizado: Supervisión docente (0 CLP),
- Contribución: Evaluación de cumplimiento de competencias del perfil de egreso, y support académico especializado

15.4. Proveedores de Tecnología

Servicios Cloud Gratuitos

- GitHub: Hosting de repositorio
- SQLite: Base de datos open-source con soporte comunitario

Stack Tecnológico Open Source

- React.js, Node.js, Express.js: Frameworks de desarrollo sin costo de licenciamiento
- Bootstrap, QRJS: Librerías especializadas de código abierto
- Valor total tecnologías: $0 CLP en licencias comerciales disponibles sin costo

15.5. Comunidad de Validación

Personal de Seguridad DuocUC San Bernardo

- Rol: Usuarios finales beta testers, validadores de usabilidad
- Aporte: 20 horas de testing y feedback durante fases de desarrollo
- Contribución: Validación de workflows reales, identificación de edge cases, y validation de intuitividad de interfaces

15.6. Resumen de Valor Total del Proyecto

Contribuciones Monetarias Equivalentes:

- Desarrollo técnico: $0 CLP
- Supervisión y soporte académico: $0 CLP
- Infraestructura y recursos institucionales: $0CLP
- Total estimado: $0 CLP en valor generado

Contribuciones No Monetarias:

- Documentación técnica reusable
- Metodología validada para proyectos futuros
- Case study para mejora continua de currículo académico
- Fortalecimiento de vínculos industria-academia

16. Relación del Proyecto con las Competencias del Perfil de Egreso

El proyecto “Visita Segura” constituye una aplicación integral de las competencias definidas en el perfil de egreso del plan de estudios de Ingeniería en Informática, demostrando la capacidad de integrar conocimientos teóricos, técnicos y metodológicos en un contexto profesional real. A lo largo de su desarrollo, se evidencia la utilización de herramientas y enfoques que abarcan desde la gestión de proyectos tecnológicos hasta la implementación de soluciones seguras y escalables.

En primer lugar, la gestión del proyecto se enmarca en la competencia de Gestión de Proyectos Informáticos, al emplear metodologías ágiles bajo el enfoque Scrumban, que permitieron organizar tareas, administrar recursos y supervisar el cumplimiento de los objetivos en plazos definidos. Esta estructura metodológica favoreció la planificación iterativa, la mejora continua y la entrega progresiva de resultados verificables.

Desde la perspectiva técnica, se integran competencias propias del desarrollo de software y la ingeniería de sistemas, reflejadas en el diseño arquitectónico del sistema, la estructuración del código bajo principios de mantenibilidad y escalabilidad, y la aplicación de patrones de diseño que aseguran la coherencia y calidad del producto final. Asimismo, se aplican los conocimientos adquiridos en Análisis y Desarrollo de Modelos de Datos, al diseñar una base de datos robusta, normalizada y segura, capaz de garantizar la integridad, consistencia y trazabilidad de la información registrada.

En relación con las competencias de seguridad informática, el proyecto incorpora medidas de protección de datos personales y control de accesos basadas en buenas prácticas de ciberseguridad y cumplimiento normativo, alineadas con la legislación vigente en materia de protección de información. Este enfoque refuerza la confiabilidad del sistema y la responsabilidad ética en el manejo de datos sensibles.

Por otra parte, se materializan las competencias vinculadas a la integración de plataformas, al desarrollar un entorno que conecta eficazmente los componentes frontend y backend mediante APIs REST, asegurando la interoperabilidad y eficiencia en la comunicación entre módulos. De igual forma, los conocimientos de programación de aplicaciones móviles se aplican al desarrollo de una interfaz adaptable y de fácil uso, que optimiza la experiencia de los usuarios y garantiza un funcionamiento eficiente en diversos dispositivos.

En su conjunto, el proyecto “Visita Segura” demuestra una sólida correspondencia con las competencias del perfil de egreso, al integrar de manera coherente habilidades de análisis, diseño, gestión y desarrollo de soluciones informáticas. La experiencia adquirida en este proceso reafirma la formación profesional del estudiante, consolidando su capacidad para enfrentar desafíos reales en el ámbito tecnológico y aportar valor tangible a las organizaciones mediante la innovación y la eficiencia operativa.

17. Relación del Proyecto con los Intereses Profesionales

El proyecto “Visita Segura” guarda una relación directa con los intereses profesionales de los integrantes del equipo, particularmente en el ámbito del desarrollo de software, la innovación tecnológica y la gestión de proyectos informáticos. Su ejecución ha permitido integrar conocimientos adquiridos a lo largo de la carrera con la práctica profesional, orientándose hacia la creación de soluciones tecnológicas que respondan a necesidades reales dentro de instituciones educativas.

En el contexto del desarrollo Full-Stack, el proyecto ofreció la oportunidad de participar activamente en todas las capas del proceso de construcción de un sistema, desde la definición de la arquitectura hasta la implementación del frontend y backend. Esta experiencia refuerza el interés por desempeñarse profesionalmente en entornos que demanden habilidades técnicas integrales, capaces de combinar el diseño de interfaces intuitivas con la implementación de lógica de negocio eficiente y segura.

Asimismo, el desarrollo de una plataforma destinada a optimizar procesos administrativos dentro de una institución académica refleja un interés profundo en la transformación digital y la automatización de procesos, áreas que constituyen pilares del avance tecnológico actual. La posibilidad de generar una solución funcional y escalable reafirma la vocación por contribuir a la modernización de sistemas organizacionales mediante herramientas digitales que mejoren la eficiencia operativa y la experiencia de los usuarios.

Por otra parte, el componente de seguridad informática ha sido esencial para fortalecer la comprensión de los riesgos asociados al manejo de información sensible, consolidando el interés profesional en la protección de datos personales y el cumplimiento de estándares normativos. Este enfoque responde a una tendencia global en la industria tecnológica, donde la seguridad y la ética digital son competencias altamente valoradas.

Finalmente, la dirección técnica y la organización del proyecto han permitido desarrollar habilidades de liderazgo, comunicación y gestión de equipos, competencias que se consideran fundamentales para el ejercicio profesional en roles de mayor responsabilidad. En su conjunto, “Visita Segura” no solo materializa los intereses profesionales del equipo, sino que también representa un paso decisivo en la proyección de una carrera orientada a la innovación, la calidad del software y la mejora continua en el ámbito de la ingeniería informática.

18. Conclusiones

A partir del desarrollo del proyecto Visita Segura, se extraen conclusiones relevantes:

Viabilidad técnica: La plataforma es factible dentro del marco temporal, integrando lectura de códigos QR con un sistema web que automatiza el registro de visitantes, reduciendo errores y tiempos de espera.

Cumplimiento de objetivos y verificación de hipótesis: Los objetivos generales y específicos se abordan integralmente, confirmando que la digitalización mejora eficiencia, confiabilidad y trazabilidad del control de accesos.

Alineación de competencias: El proyecto integra conocimientos en desarrollo de software, bases de datos, seguridad informática y diseño de interfaces, fortaleciendo competencias académicas y profesionales aplicables en contextos reales.

Optimización de recursos y metodología: La metodología ágil SCRUM facilita planificación iterativa y entrega incremental, permitiendo ajustes continuos y mitigando riesgos de retrasos o problemas técnicos.

Lecciones aprendidas: Destacan la comunicación constante con usuarios, validación temprana de funcionalidades y documentación sistemática, asegurando calidad y fortaleciendo habilidades en gestión y trabajo en equipo.

En conclusión, Visita Segura cumple sus objetivos, valida la hipótesis y representa una experiencia de aprendizaje aplicada, aportando beneficios a la sede Duoc UC San Bernardo y estableciendo un referente para futuras iniciativas.

19. Conclusions

From the development of the Safe Visit project, the following relevant conclusions can be drawn:

Technical feasibility: The platform is feasible within the timeframe, integrating QR code reading with a web system that automates visitor registration, reducing errors and waiting times.

Achievement of objectives and verification of hypotheses: The general and specific objectives are addressed comprehensively, confirming that digitization improves the efficiency, reliability, and traceability of access control.

Alignment of skills: The project integrates knowledge in software development, databases, cybersecurity, and interface design, strengthening academic and professional skills applicable in real-world contexts.

Optimization of resources and methodology: The agile SCRUM methodology facilitates iterative planning and incremental delivery, allowing for continuous adjustments and mitigating the risk of delays or technical problems.

Lessons learned: Key takeaways include constant communication with users, early validation of functionalities, and systematic documentation, ensuring quality and strengthening management and teamwork skills.

In conclusion, Safe Visit fulfills its objectives, validates the hypothesis, and represents an applied learning experience, bringing benefits to the Duoc UC San Bernardo campus and establishing a benchmark for future initiatives.

20. Gestión del Proyecto

20.1. Resultados y Productos esperados y logrados

Resultado	Descripción	Fecha de logro	% Logro
Sistema Web Funcional	Plataforma completa de registro de visitantes con lectura QR, almacenamiento seguro, y generación de reportes	02/12/2025	95%
Base de Datos Optimizada	Esquema PostgreSQL normalizado con índices optimizados, procedimientos almacenados, y backup automático	15/11/2025	100%
Documentación Técnica	Manual técnico, diagramas UML, especificaciones de API, y guía de instalación completos	25/11/2025	90%
Suite de Testing	Pruebas unitarias, de integración, y end-to-end con cobertura >80%	20/11/2025	85%
Manual de Usuario	Guías paso a paso para guardias, administradores, y personal técnico	28/11/2025	100%

20.2. Ejecución Presupuestaria

Recursos Tecnológicos Utilizados

Infraestructura de Desarrollo:

- Dominios de desarrollo y testing: $0 CLP
- Herramientas de desarrollo (IDE, extensiones): $0 CLP

Stack Tecnológico:

- React.js, Node.js, Express.js, SQLite: $0 CLP
- Librerías especializadas (QRJS, Bootstrap): $0 CLP

Recursos Humanos:

- 360 horas totales de desarrollo
- Valor estimado a tarifa profesional practicante: $0 CLP
- Supervisión académica: $0 CLP

Infraestructura Institucional:

- Acceso a laboratorios y equipos: $0 CLP
- Tiempo de personal para validación: $0 CLP
- Ambiente de producción: $0 CLP
- Total de Recursos Movilizados: $0 CLP

20.3. Competencias Técnicas Desarrolladas

Daniel Novoa - Backend y Arquitectura:

- Dominio avanzado de Node.js/Express para desarrollo de APIs REST
- Expertise en diseño e implementación de bases de datos SQLite
- Competencias sólidas en seguridad informática y compliance normativo
- Habilidades de arquitectura de software y design patterns

Sebastián Escobedo - Frontend y UX/UI:

- Proficiencia en React.js y desarrollo de componentes reutilizables
- Competencias en diseño responsive y experiencia de usuario
- Expertise en testing e integración de librerías especializadas

Competencias de Gestión Desarrolladas en Ambos integrantes:

- Gestión de proyectos mediante metodología Scrumban adaptada
- Trabajo en equipo con roles complementarios y coordinación distribuida
- Documentación técnica y transferencia de conocimiento

21. Referencias bibliográficas

Universidad de Chile. (2024, 28 de marzo). *U. de Chile implementa sistema de lectura biométrica que reemplaza al reloj de control*. Recuperado de https://uchile.cl/noticias/219723/uchile-implementa-lectura-biometrica-que-reemplaza-al-reloj-control-

Sanabria-Z, A. L., & Arciniegas-B., R. G. (2018). *Software* libre: El camino hacia la independencia tecnológica y el desarrollo académico. *Revista Tecnológica - ESPOL*, *31*(4), 11-23. https://doi.org/10.37053/revtecnol.v31n4-02

Servicio de Registro Civil e Identificación. (2024). *Resolución 466 Exenta (07-dic-2024) M. de Justicia y Derechos Humanos; Servicio de Registro Civil e Identificación: Señala características y fija menciones de la Cédula de Identidad Electrónica que emita el Servicio de Registro Civil e Identificación*. Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/leychile/

SMOWL. (2023, 12 de abril). *RPA en la educación: qué es y cuáles son sus beneficios*. [Artículo de blog]. https://smowl.net/es/blog/rpa-que-es-beneficios/

Anderson, D. J. (2010). *Kanban: Successful evolutionary change for your technology business*. Blue Hole Press.

Fowler, M. (2018). *Refactoring: Improving the design of existing code* (2nd ed.). Addison-Wesley Professional.

García, P., & Morales, C. (2023). Implementación de sistemas de control de acceso en instituciones educativas chilenas: Casos de estudio. *Revista Chilena de Ingeniería, 31*(4), 612–628.

Kniberg, H. (2015). *Scrum and XP from the trenches* (2nd ed.). InfoQ. https://www.infoq.com/minibooks/scrum-xp-from-the-trenches-2/

Kumar, A., Singh, R., & Patel, N. (2023). Automated visitor management systems in educational institutions: A comparative study of QR-based solutions. *Journal of Educational Technology Systems, 51*(3), 287–305. https://doi.org/10.1177/0047239523001234

Martin, R. C. (2017). *Clean architecture: A craftsman's guide to software structure and design*. Prentice Hall.

Project Management Institute. (2017). *A guide to the project management body of knowledge (PMBOK® guide)* (6th ed.). Project Management Institute.

Sommerville, I. (2016). *Software engineering* (10th ed.). Pearson.

Zhang, L., & Rodriguez, M. (2024). Security and privacy considerations in digital visitor registration systems. *International Journal of Information Security, 23*(2), 445–467. https://doi.org/10.1007/s10207-024-00567-8

22. Anexos

Anexo A. Repositorio del código en GitHub

Enlace: https://github.com/SimiusLokus/CAPSTONE-VISITASEGURA

Anexo B. Tablero del proyecto en Trello

Enlace:https://trello.com/invite/b/641df3c939328d04ec87bee0/ATTI142d0b104097bc188b102f5d829b02c9DD367E06/visita-segura

Anexo C. Carta Gantt

Enlace: https://drive.google.com/file/d/1OWBp5TJ2yp9bqHpCMsjCNpLVpE0R-81l/view?usp=sharing

Anexo D. Product backlog

Enlace:https://docs.google.com/spreadsheets/d/1Y2G8Tlzu7N8ZLqSIzphYnav85NLHdZsO1eLt0tuTUc8/edit?usp=sharing