Plataforma Digital para la Gestión Segura de la Cédula de Ciudadanía: Bloqueo y Desbloqueo con CARD ID, Autenticación Biométrica y Validación ANI

Yudy Pahola Buitrago León

Morelia Díaz Hernández

Geovanny Alonso Munar Sotelo

Universidad EAN

Facultad de ingeniería

Ingeniería Industrial Optimizado

Bogotá D.C, Colombia

03 de junio de 2025

Plataforma Digital para la Gestión Segura de la Cédula de Ciudadanía: Bloqueo y Desbloqueo con CARD ID, Autenticación Biométrica y Validación ANI

Yudy Pahola Buitrago León

Morelia Díaz Hernández

Geovanny Alonso Munar Sotelo

Trabajo de grado presentado como requisito para optar al título de

Ingenieros Industriales

Director

John Jairo Porras

Proyecto de Integración – Pregrado

Grupo 4 – Virtual – Primer Semestre

Universidad EAN

Facultad de ingeniería

Ingeniería Industrial Optimizado

Bogotá D.C, Colombia

03 de junio de 2025

Nota de aceptación:

Firma del jurado

Firma del jurado

Firma del director del trabajo de grado

Bogotá, 03 de junio de 2025

Dedicatoria

Dedicamos este proyecto a nuestras familias, quienes han sido nuestro mayor apoyo durante este proceso. A ellas, que comprendieron y aceptaron con amor el tiempo que les restamos para poder estudiar, avanzar y cumplir con cada etapa de esta formación. Gracias por su paciencia, por acompañarnos en silencio, por alentarnos en los días difíciles y celebrar con nosotros cada pequeño logro.

También dedicamos este trabajo a todas las personas que creen en la educación como motor de transformación, y en la ingeniería como una disciplina capaz de generar soluciones reales para los desafíos sociales. A nuestros docentes, mentores y guías, que con sus enseñanzas nos impulsaron a pensar con visión crítica, técnica y humana.

Este proyecto es el reflejo del esfuerzo compartido, de las noches largas, los desafíos superados y el compromiso por construir una herramienta útil al servicio de la ciudadanía. Porque creemos firmemente que la tecnología debe ser un medio para proteger y empoderar a las personas.

Que la tecnología esté siempre al servicio de la ciudadanía, y nunca por encima de ella.

Resumen Ejecutivo

El presente proyecto de grado tiene como objetivo desarrollar una solución web para la Registraduría Nacional del Estado Civil que permita a los ciudadanos reportar la pérdida o el robo de su cédula de ciudadanía, bloqueando el uso del plástico mediante su número único (CARD ID). Actualmente, no existe un mecanismo que valide si el documento físico presentado por un ciudadano es el último expedido o si ha sido reportado como perdido, lo que genera un alto riesgo de suplantación de identidad física en Colombia.

La solución propuesta busca integrar esta funcionalidad con la base de datos del Archivo Nacional de Identificación (ANI), permitiendo a las entidades que consultan dicha base verificar el estado del documento. Se desarrollará un prototipo funcional de la plataforma, para evaluar su impacto y viabilidad en la mejora de la seguridad ciudadana y en la reducción de fraudes relacionados con la identidad.

Este proyecto aporta un mecanismo innovador para fortalecer la autenticación de identidad en el país y mejorar los procesos de verificación en instituciones públicas y privadas.

Palabras clave: suplantación de identidad, bloqueo de documentos, CARD ID, seguridad ciudadana, identificación oficial, Registraduría Nacional del Estado Civil, plataforma digital.

Abstract

The objective of this degree project is to develop a digital platform for the National Registry of Civil Status that allows citizens to report the loss or theft of their identity document, blocking the use of the plastic by means of its unique number (CARD ID). Currently, there is no mechanism to validate whether the physical document presented by a citizen is the last one issued or if it has been reported as lost, which generates a high risk of physical identity theft in Colombia.

The proposed solution seeks to integrate this functionality with the database of the National Identification Archive (ANI), allowing the entities that consult this database to verify the status of the document. A functional prototype of the platform will be developed, with web and mobile versions, to evaluate its impact and viability in improving citizen security and reducing identity-related fraud.

This project provides an innovative mechanism to strengthen identity authentication in the country and improve verification processes in public and private institutions.

Keywords: identity theft, document blocking, CARD ID, citizen security, official identification, National Civil Registry, digital platform.

Tabla de contenido

Índice de Tablas

Índice de Ilustraciones

Índice de Anexos

Introducción

La suplantación de identidad constituye uno de los problemas de seguridad más críticos en la sociedad actual, generando consecuencias económicas, sociales y legales tanto para los individuos como para las instituciones en Colombia. Este fenómeno no solo afecta la vida cotidiana de los ciudadanos, sino también la integridad y confiabilidad del sistema nacional de identificación administrado por la Registraduría Nacional del Estado Civil. Diversos estudios evidencian la creciente incidencia de casos relacionados con la suplantación de identidad física y digital, destacando la vulnerabilidad actual frente al uso indebido de documentos de identificación extraviados, hurtados o falsificados. Según la Policía Nacional de Colombia, en los últimos años se han incrementado notablemente las denuncias relacionadas con delitos de suplantación de identidad, reflejando así la magnitud y relevancia de este problema en la actualidad (Policía Nacional de Colombia, 2023).

En Colombia, la Registraduría Nacional del Estado Civil es la entidad encargada de administrar y salvaguardar los datos de identidad mediante el Archivo Nacional de Identificación (ANI). Sin embargo, aunque este sistema permite verificar la validez de un número de identificación específico, actualmente carece de herramientas tecnológicas para gestionar el estado activo o inactivo del documento físico (Gimeno, 2010). Esto genera una ventana temporal en la que personas inescrupulosas pueden cometer delitos de suplantación antes de que las autoridades correspondientes reaccionen adecuadamente, generando impactos negativos significativos sobre las víctimas y sobre la confianza general en los procesos institucionales (Garcia & Mazon, 2024).

Ante esta problemática, surge la necesidad de diseñar una solución tecnológica que permita a los ciudadanos reportar rápida y fácilmente la pérdida o el robo de sus documentos, posibilitando la actualización inmediata del estado del documento físico en la base de datos del ANI. Este proyecto tiene como objeto de estudio desarrollar e implementar una plataforma

digital que habilite el bloqueo eficiente del documento físico a través de su número único (CARD ID), evitando así su uso fraudulento posterior al reporte realizado por el ciudadano afectado. El funcionamiento de esta plataforma implicará que el ciudadano que pierda o desee activar su documento deberá ingresar datos personales específicos, los cuales serán validados directamente con la base de datos ANI. Posteriormente, si esta validación es exitosa, se realizará una autenticación biométrica facial para asegurar al cien por ciento la titularidad del documento.

De acuerdo con los lineamientos establecidos por estándares internacionales como la norma ISO 27001, relacionada con la seguridad de la información y protección de datos personales, la implementación de esta plataforma contribuirá a fortalecer los mecanismos de seguridad en la gestión documental y autenticación de identidad en Colombia (Sánchez, 2020). Asimismo, la incorporación de tecnologías biométricas ha demostrado ser altamente efectiva para mejorar la seguridad y reducir significativamente los riesgos asociados a la suplantación de identidad (Pedroza, 2019; Sánchez Gómez, 2020).

La ingeniería industrial desempeña un rol fundamental en este proyecto, debido a su capacidad para integrar técnicas y metodologías que optimizan procesos complejos, aumentando la eficiencia operativa y la productividad. Mediante el uso de herramientas de análisis y diseño de sistemas, la ingeniería industrial permite evaluar e implementar soluciones tecnológicas estratégicas que responden eficazmente a las necesidades sociales y organizacionales actuales. Además, su enfoque integral facilita la gestión eficiente de recursos y la adopción efectiva de innovaciones tecnológicas, garantizando la sostenibilidad y la mejora continua del sistema propuesto (Flórez & Camelo, 2023).

La pregunta central que guía esta investigación es: ¿Cómo la implementación de una plataforma digital para bloquear documentos de identificación física extraviados o hurtados,

mediante el número único de identificación (CARD ID), puede contribuir a reducir significativamente los riesgos de suplantación de identidad física en Colombia?

Para abordar integralmente el estudio, el informe final del proyecto de grado se estructurará en varias secciones, que incluirán aspectos fundamentales como la contextualización del problema, antecedentes y justificación del estudio, un marco teórico sustentado por referentes normativos y tecnológicos, una metodología detallada del diseño y desarrollo de la plataforma propuesta, el análisis de resultados obtenidos durante la implementación del prototipo y, finalmente, las conclusiones generales, recomendaciones y posibles líneas futuras de acción para la Registraduría Nacional del Estado Civil. Esta estructura permitirá guiar al lector a través del desarrollo lógico del proyecto, facilitando una comprensión clara y ordenada del trabajo realizado.

Antecedentes

La suplantación de identidad es un fenómeno que ha cobrado relevancia mundial en los últimos años debido al aumento de delitos informáticos y al uso indebido de documentos físicos de identificación. En Colombia, esta problemática ha sido reconocida por instituciones como la Registraduría Nacional del Estado Civil y la Dirección de Investigación Criminal e Interpol (DIJIN), quienes han reportado un crecimiento significativo de casos, especialmente durante la pandemia (DIJIN, 2020).

A pesar de los avances en digitalización, el sistema de identificación colombiano aún presenta vacíos críticos. Actualmente, no existe un mecanismo oficial que permita a los ciudadanos bloquear su cédula de ciudadanía de forma inmediata ante pérdida o robo. El Archivo Nacional de Identificación (ANI), aunque permite validar si un número de cédula está vigente, no ofrece información sobre el estado físico del documento, como si ha sido extraviado o anulado (Registraduría Nacional del Estado Civil, 2023).

Estudios recientes destacan la importancia de integrar mecanismos de verificación biométrica y tecnologías digitales en procesos de autenticación, como es el caso de países como Estonia, México y Alemania, que han implementado sistemas seguros para proteger la identidad de los ciudadanos (Galvis, 2023; RENIEC, 2015).

En respuesta a esta necesidad, el presente proyecto propone el diseño de una plataforma digital para la gestión segura de la cédula de ciudadanía, que permita el bloqueo y desbloqueo del documento mediante el número único CARD ID, validaciones con el ANI y autenticación biométrica facial. Esta solución se alinea con estándares internacionales de ciberseguridad y protección de datos personales, como la norma ISO/IEC 27001.

Definición del problema

La suplantación de identidad es una problemática relevante en la sociedad actual, especialmente en el contexto de documentos de identificación como la cédula de ciudadanía. Cuando un ciudadano pierde o le roban su documento, no existe un mecanismo oficial que le permita bloquearlo de manera inmediata, lo que incrementa el riesgo de que sea utilizado de forma fraudulenta. En la actualidad, la Registraduría Nacional del Estado Civil no cuenta con un sistema que permita a los ciudadanos bloquear o desbloquear su cédula de ciudadanía en caso de pérdida o robo.

Esto significa que, al extraviar el documento, no hay un registro accesible para las entidades que consultan la base de datos del Archivo Nacional de Identificación (ANI) que indique si un documento ha sido reportado como perdido. Esta situación genera una vulnerabilidad en la seguridad ciudadana, ya que facilita la comisión de delitos relacionados con la suplantación de identidad y el fraude.

Además, la ausencia de un mecanismo de bloqueo limita la efectividad de las verificaciones de identidad que realizan diversas instituciones públicas y privadas. Si bien el ANI valida si un número de cédula está vigente, no permite comprobar si el plástico que porta un ciudadano es el último expedido o si ha sido reportado como extraviado. Esto genera una brecha de seguridad que expone a los ciudadanos a posibles fraudes.

Por lo tanto, se hace necesario desarrollar una solución tecnológica que permita a los ciudadanos gestionar el estado de su documento de identidad de forma segura y eficiente. Una aplicación que integre el uso del CARD ID, autenticación biométrica y validaciones a través del ANI contribuiría a minimizar los riesgos asociados a la suplantación de identidad y fortalecería la seguridad en los procesos de verificación documental en el país.

¿Cómo puede una plataforma digital basada en el bloqueo del plástico de la cédula de ciudadanía mediante CARD ID y autenticación biométrica mejorar la seguridad en la verificación de identidad y reducir el riesgo de suplantación en Colombia?

Objetivos

Objetivo General

Desarrollar una aplicación web para la Registraduría Nacional del Estado Civil que permita a los ciudadanos reportar de manera rápida y segura la pérdida o el robo de su cédula de ciudadanía, gestionando eficazmente su bloqueo y desbloqueo, con el propósito de prevenir la suplantación de identidad y fortalecer la confianza en la autenticación de documentos.

Objetivos Específicos

1. Diseñar e implementar un prototipo funcional de un aplicativo web que permita a los ciudadanos registrar su cédula y gestionar su estado de bloqueo y desbloqueo, priorizando la seguridad y una experiencia de usuario eficiente.
2. Implementar un sistema de autenticación que utilice biometría facial y preguntas de seguridad para verificar con certeza la identidad del usuario antes de gestionar cualquier cambio en el estado del documento.
3. Habilitar la verificación en tiempo real del estado del documento de identidad para entidades autorizadas, asegurando su integración efectiva con las bases de datos oficiales.
4. Realizar pruebas piloto que permitan la evaluación respecto a la usabilidad y seguridad de la aplicación, facilitando así la identificación de mejoras continuas para optimizar su eficacia en la prevención de fraudes por suplantación de identidad

Justificación

La suplantación de identidad constituye un problema creciente que compromete la seguridad y confianza en los sistemas de identificación., Según datos de la Dijin, la suplantación de identidad en el país durante la pandemia en el año 2020 aumentó un 409%, en paralelo con el año 2019, donde se causaron únicamente 300 casos (Dijin, 2020).

La identificación segura y confiable de los ciudadanos es un pilar fundamental para la seguridad y el desarrollo de la sociedad. La ausencia de un mecanismo que permita bloquear y desbloquear la cédula de ciudadanía en caso de pérdida o robo expone a los ciudadanos a riesgos significativos de suplantación de identidad. Este problema no solo afecta a los individuos directamente involucrados, sino que también tiene repercusiones en instituciones públicas y privadas que dependen de procesos de verificación de identidad para la prestación de servicios.

De acuerdo con el Proyecto de Ley radicado en el año 2022, se ha identificado la necesidad de fortalecer los mecanismos de protección de la identidad para evitar fraudes y reportes injustificados a centrales de riesgo (Congreso de la República de Colombia, 2022). Además, investigaciones previas han señalado que la suplantación de identidad ha aumentado exponencialmente en los últimos años, afectando a múltiples sectores, incluyendo el financiero, donde las entidades han tenido que asumir grandes pérdidas por fraudes relacionados con este delito (Galvis, 2023).

El presente proyecto es necesario porque contribuye a la modernización y seguridad del sistema de identificación en Colombia. La implementación de una plataforma digital que permita la gestión del estado del documento de identidad mediante un proceso seguro, basado en CARD ID, autenticación biométrica y validaciones con el ANI, ofrecerá una herramienta eficaz para mitigar los riesgos asociados a la suplantación de identidad.

Los beneficios de este proyecto incluyen:

- Reducción del riesgo de fraude y delitos relacionados con la suplantación de identidad.
- Mayor eficiencia en los procesos de verificación de documentos de identidad por parte de entidades públicas y privadas.
- Protección de los ciudadanos ante el uso indebido de sus documentos extraviados.
- Contribución a la modernización de la Registraduría Nacional del Estado Civil mediante el uso de tecnologías avanzadas en la identificación y autenticación de ciudadanos.

Dado el impacto y la relevancia de esta problemática en la seguridad ciudadana, este proyecto se presenta como una solución viable y necesaria para fortalecer la confianza en los mecanismos de identificación y protección de la identidad en Colombia.

Análisis de Requerimientos

El diseño e implementación de la plataforma digital para la gestión segura de la cedula de Ciudadanía, tiene una serie de requerimientos técnicos, normativos y funcionales que garanticen la eficiencia de la plataforma de una manera viable y sostenible, el análisis correcto de estos requerimientos permitirá optimizar recursos y minimizar los riesgos que puedan surgir en el desarrollo de la plataforma.

Intención del producto

La intención del producto es proporcionar mecanismos de control seguros y eficientes a los ciudadanos para que puedan de manera rápida, sencilla y en tiempo real, bloquear o desbloquear su documento de identidad o cedula de ciudadanía ante un evento de pérdida o hurto, esto con el fin de evitar que sean víctimas de delitos como la suplantación de identidad. Esta herramienta busca dar solución al alto índice de delitos generados por suplantación de identidad ya que en la actualidad en Colombia no es posible identificar si un documento físico

fue reportado como extraviado o robado, mediante un sistema de bloqueo digital basado en el CARD ID de la cedula que genere una alerta en la Registraduría Nacional del Estado Civil y que sea visible en validaciones en la base de datos del Archivo Nacional de Identificación (ANI), se podrá advertir a entidades privadas y estatales que el documento en consulta se encuentra marcado como bloqueado lo por lo que podrían estarse viendo ante una situación de suplantación de identidad, de esta manera se busca proteger a la ciudadanía garantizando el derechos a la protección en la vulnerabilidad de autenticación de identidad .

Parámetros de Diseño

En el complejo panorama tecnológico actual, la creación de sistemas que no solo sean funcionales, sino también seguros, interconectados y centrados en el usuario, se ha convertido en una prioridad. Para garantizar la correcta funcionalidad del sistema, se deben evaluar diversos parámetros de diseño en relación con la seguridad, interoperabilidad y experiencia del usuario (Lerma Kirchner, 2017). Esta evaluación es fundamental para construir sistemas que no solo cumplan con sus objetivos primarios, sino que también generen confianza y faciliten una adopción exitosa. En los parámetros para el diseño del proyecto se tendrá en cuenta:

- Seguridad y protección de datos: Con mecanismos de cifrado de extremo a extremo se buscará tener un almacenamiento y tratamiento de información seguro, que cumpla con los requerimientos de la Ley 1581 de 2012 sobre la protección de datos, y que se integre con los sistemas de seguridad existentes en la Registraduría Nacional del Estado Civil.
- Interoperabilidad y conectividad: Se diseñará una plataforma que este integrada en tiempo real con la base de datos ANI, para esto es importante garantizar que sea compatible y su operatividad de alcance a los dispositivos

móviles y navegadores web, esto con el fin de garantizar respuesta rápidas, oportunas y eficientes a los usuarios.

- Accesibilidad y Experiencia del usuario: La interfaz bajo la cual opere la plataforma debe ser intuitiva y de fácil manejo para los diferentes tipos de usuarios que la operarían, debe ser adaptable a diferentes sistemas operativos, con la finalidad de tener un mayor alcance.

Características del diseño y especificación del producto

Tabla 1. Características del diseño y especificación del producto

Tipo de Característica	Requerimiento	Descripción	Detalle técnico
Características Técnicas	Plataforma web y móvil	Desarrollo en un entorno multiplataforma compatible con Android, iOS y navegadores web.	Aplicación Móvil o plataforma virtual con enlace a la Registraduría Nacional de Estado Civil
	Autenticación Biométrica	Implementación de reconocimiento facial con un margen de error menor al 5%, garantizado	Algoritmos de IA con redes neuronales
	Validación con CARD ID	Uso de un identificador único	Integración con bases de datos

Tipo de Característica	Requerimiento	Descripción	Detalle técnico
		definido como mecanismo de seguridad y protección de usuario	Registraduría Nacional de Estado Civil
Seguridad y Protección contra Fraudes	Actualización en tiempo real	Permite a las entidades validar la información de los usuarios en tiempo real	Sincronización en la nube con bases de datos Registraduría Nacional de Estado Civil
	Mecanismo de doble validación	Combinación de autenticación biométrica y preguntas de seguridad personalizadas.	
Requerimientos de Infraestructura	Servidores con alta disponibilidad	Garantizar la estabilidad del sistema ante un alto volumen de usuarios simultáneos	Servidores en la nube con escalabilidad automática y redundancia geográfica
	Migración	Implementación en una infraestructura	Uso de tecnologías como AWS

Tipo de Característica	Requerimiento	Descripción	Detalle técnico
		con certificaciones de seguridad para el resguardo de datos sensibles.	GovCloud, Microsoft Azure Government
	Sistemas de respaldo y redundancia	Evita la pérdida de información en caso de un ataque cibernético o daño en los servidores	Copias de seguridad automáticas y almacenamiento distribuidas en varias

Marco Teórico

Identidad y suplantación de identidad en Colombia

La identidad se define como el conjunto de atributos únicos e irrepetibles que permiten reconocer y diferenciar a una persona de otra dentro de un contexto determinado. Estos atributos abarcan características físicas, psicológicas y sociales que proporcionan una base sólida para la identificación individual en distintos ámbitos de la vida social (Huerta & Rodríguez, 2014). En este sentido, la identidad no es solamente un elemento individual, sino también una construcción social y jurídica que adquiere especial relevancia en contextos institucionales y legales.

En Colombia, la identidad se materializa mediante un proceso civil claramente definido según las etapas de vida de cada persona. Este proceso establece que los menores de 7 años

deben contar con un registro civil de nacimiento, los ciudadanos entre los 7 y 17 años poseen una tarjeta de identidad, mientras que los mayores de 18 años tienen la obligación de portar la cédula de ciudadanía. Finalmente, cuando la persona fallece, se registra un documento denominado registro civil de defunción. Este documento se enfoca particularmente en la cédula de ciudadanía, dado que representa el principal documento oficial que acredita la identidad de los ciudadanos colombianos, siendo obligatorio para múltiples trámites administrativos, legales y sociales (Congreso de la República de Colombia, 2022).

No obstante, pese a la clara estructuración de este proceso, la identificación en Colombia ha enfrentado históricamente desafíos significativos. La evolución desde métodos manuales basados en registros parroquiales hasta sistemas digitales avanzados gestionados por la Registraduría Nacional del Estado Civil no ha logrado erradicar del todo las vulnerabilidades existentes (Registraduría Nacional del Estado Civil, 2023). Estas debilidades, en especial las asociadas a la autenticación y validación del estado del documento físico facilitan la ocurrencia de delitos como la suplantación de identidad.

En consecuencia, la suplantación de identidad en Colombia, entendida como el uso fraudulento de los datos personales y especialmente de la cédula de ciudadanía, se ha convertido en un problema de gran impacto social, económico y jurídico. Este fenómeno se presenta en dos modalidades principales: suplantación física y digital. La suplantación física implica el uso no autorizado del documento físico original o falsificado para acceder a servicios presenciales como apertura de cuentas bancarias, créditos, o adquisición indebida de bienes y servicios. Por otra parte, la suplantación digital se refiere al uso fraudulento de la información personal a través de medios electrónicos, incluyendo la obtención ilícita de datos para realizar actividades ilegales a nombre de la víctima. El uso indebido del plástico físico de la cédula para cometer fraudes financieros y acceder a servicios representa una problemática creciente que

afecta significativamente a ciudadanos y organizaciones, causando pérdidas económicas y daños reputacionales considerables (Buitrago, Díaz & Munar, 2023).

Los estudios recientes indican un incremento significativo en los casos reportados de suplantación de identidad, subrayando la urgencia de implementar mecanismos efectivos de prevención (Buitrago, Díaz & Munar, 2023). Esta situación crítica evidencia la necesidad imperiosa de adoptar soluciones tecnológicas robustas como sistemas biométricos y plataformas digitales seguras, que permitan no solo verificar la autenticidad del documento, sino también brindar una respuesta preventiva eficaz frente a la creciente amenaza de la suplantación de identidad en el contexto colombiano.

Actualmente, en Colombia existen dos tipos principales de cédula de ciudadanía: la tradicional física con hologramas y la cédula digital. La cédula física tradicional está fabricada con material plástico e incorpora medidas de seguridad avanzadas como hologramas, códigos QR, microtextos, impresión digital y fotografía, que dificultan su falsificación y garantizan la autenticidad del documento

Ilustración 1. Cédula de Ciudadanía de Hologramas

Imagen obtenida de la Registraduría Nacional del Estado Civil

Por otro lado, la cédula digital, recientemente implementada, está diseñada en policarbonato e incorpora elementos modernos de seguridad, como el código QR, hologramas personalizados, biometría facial y una versión digital que puede portarse en dispositivos móviles. Estas características la convierten en un documento más seguro frente a intentos de falsificación y uso indebido.

Ilustración 2. Cédula de Ciudadanía Digital

Imagen obtenida de la Registraduría Nacional del Estado Civil

Sin embargo, el sistema actual presenta vulnerabilidades significativas en términos de autenticación, particularmente porque no existe un mecanismo eficiente para validar si un documento de identidad es el último expedido o si se encuentra activo o bloqueado (Registraduría Nacional del Estado Civil, 2023). Estos vacíos permiten que documentos reportados como extraviados o robados puedan ser utilizados de manera fraudulenta antes de que se genere una alerta efectiva a las instituciones pertinentes.

Frente a estas limitaciones, tradicionalmente en Colombia los mecanismos de validación de identidad han dependido principalmente de métodos convencionales basados en datos personales y documentos físicos, lo cual genera riesgos importantes de fraude debido a la

dificultad para asegurar su autenticidad y vigencia de forma inmediata y efectiva (Registraduría Nacional del Estado Civil, 2023).

Para mitigar estos riesgos, el Archivo Nacional de Identificación (ANI), permite validar la identidad de los ciudadanos mediante su número de cédula. A pesar de ello, la necesidad de actualizar y fortalecer los mecanismos integrados con tecnologías más avanzadas continúa siendo una prioridad urgente para mejorar la seguridad en los procesos de validación y autenticación de la identidad en Colombia (Registraduría Nacional del Estado Civil, 2023).

Archivo Nacional de Identificación (ANI)

El Archivo Nacional de Identificación (ANI) es una base de datos administrada por la Registraduría Nacional del Estado Civil de Colombia, que almacena y gestiona la información personal de los ciudadanos colombianos. Esta base de datos es fundamental para validar la identidad de las personas mediante su número de cédula, facilitando procesos de autenticación en diversas entidades públicas y privadas (ReconoSER ID, 2023).

El ANI permite a entidades públicas y privadas que cumplen funciones públicas y han suscrito convenios institucionales, acceder a la información contenida en la base de datos para consultas y validaciones que no estén sujetas a reserva legal. Este acceso se realiza conforme a lo establecido en el Decreto 019 de 2012, la Ley 1753 de 2015 y la Resolución 5633 de 2016 (Registraduría Nacional del Estado Civil, 2023).

Los estados de la cédula de ciudadanía registrados en el ANI incluyen:

- Vigente: El documento está activo y habilitado para su uso.
- Cancelada por muerte: El titular ha fallecido y el documento ha sido anulado.
- Pérdida o suspensión de derechos políticos: El ciudadano ha perdido temporal o permanentemente sus derechos políticos, afectando la validez del documento.

- Anulada: El documento ha sido invalidado por razones administrativas o legales.
- En trámite: El documento está en proceso de expedición o renovación (Registraduría Nacional del Estado Civil, 2023).

La información pública disponible en el ANI abarca datos biográficos básicos de los ciudadanos, como nombres, apellidos, número de cédula, fecha y lugar de nacimiento, entre otros. Esta información es utilizada para validar la identidad en procesos que requieren autenticación confiable (Registraduría Nacional del Estado Civil, 2023).

Es importante destacar que, aunque el ANI es una herramienta valiosa para la validación de identidades, su acceso está restringido y regulado para proteger la privacidad y seguridad de la información personal de los ciudadanos. Solo las entidades autorizadas y que cumplen con los requisitos legales pueden acceder a esta base de datos, garantizando así un uso adecuado y seguro de la información (Registraduría Nacional del Estado Civil, 2023).

La implementación y gestión del ANI reflejan los esfuerzos del Estado colombiano por modernizar y asegurar los sistemas de identificación, buscando minimizar riesgos asociados a la suplantación de identidad y otros delitos relacionados. Sin embargo, es fundamental continuar fortaleciendo estos sistemas y garantizar que las entidades que acceden a la información lo hagan bajo estrictos protocolos de seguridad y confidencialidad.

Complementando la información almacenada en el ANI, cada documento físico de la cédula de ciudadanía expedido por la Registraduría Nacional del Estado Civil posee un número único conocido como CARD ID. Este número identifica inequívocamente el plástico específico del documento y, aunque actualmente no es utilizado de manera generalizada para procesos de autenticación, representa un potencial significativo para reforzar la seguridad en la validación de documentos en tiempo real. La combinación del ANI y el uso efectivo del CARD ID podría convertirse en una herramienta clave en la prevención de la suplantación de

identidad, ya que la validación inmediata de este número único permitiría detectar rápidamente documentos que hayan sido reportados como extraviados o robados, reduciendo sustancialmente el riesgo de uso indebido y fraude asociado a la identidad (Madrigal, 2009).

CARD ID y su funcionalidad

El CARD ID es un número único asignado específicamente a cada plástico de la cédula de ciudadanía emitido por la Registraduría Nacional del Estado Civil de Colombia. A pesar de que este número se encuentra impreso en cada documento físico, actualmente no se aprovecha su potencial para procesos de autenticación o verificación de identidad. No obstante, el CARD ID posee características distintivas y exclusivas, lo que permite identificar cada documento de manera inequívoca. Por tanto, su utilización en procesos de validación podría resultar fundamental para evitar casos de suplantación, falsificación o fraude asociado al documento físico.

En este sentido, la integración efectiva del CARD ID con la base de datos del ANI proporcionaría un nivel adicional de seguridad, permitiendo verificar rápidamente si un documento específico ha sido reportado como perdido, robado o anulado. Esto podría contribuir de manera decisiva a la reducción del riesgo de fraude mediante la detección inmediata del uso indebido del documento físico. Por consiguiente, el CARD ID, utilizado en conjunto con otros mecanismos como la autenticación biométrica, podría consolidarse como una herramienta estratégica para fortalecer significativamente los procesos de identificación y autenticación en el país (Madrigal, 2009).

Autenticación y métodos biométricos

La autenticación biométrica es un método avanzado de verificación de identidad que emplea características físicas y conductuales únicas e intransferibles de cada individuo, tales

como huellas dactilares, reconocimiento facial y escaneo del iris, entre otras. En Colombia, la implementación de la biometría representa una herramienta clave para enfrentar los desafíos asociados a la autenticación tradicional basada en contraseñas o documentos físicos, métodos que han demostrado ser vulnerables frente a situaciones de extravío, robo o falsificación. Las características biométricas, al ser intrínsecas y permanentes en el tiempo, proporcionan un nivel superior de seguridad y confianza en los procesos de validación de identidad (De Janasz, Dowd & Schneider, 2015).

La relevancia de la autenticación biométrica para la identificación colombiana radica en su capacidad para prevenir y reducir significativamente los casos de fraude y suplantación, delitos que se han incrementado notablemente en el país. Por esta razón, la Registraduría Nacional del Estado Civil ha venido promoviendo la adopción de sistemas biométricos en diversas instituciones públicas y privadas, con el fin de fortalecer la integridad del sistema de identificación nacional y proteger adecuadamente los datos personales de los ciudadanos (Registraduría Nacional del Estado Civil, 2023).

Adicionalmente, la autenticación biométrica facilita procesos más ágiles, seguros y eficientes, minimizando errores humanos y generando mayor confianza en las transacciones y procesos administrativos. Esta tecnología permite identificar de manera rápida y precisa a los individuos mediante atributos físicos difíciles de replicar o falsificar, incrementando así la seguridad en sectores críticos como el financiero, sanitario y gubernamental (Buitrago, Díaz & Munar, 2023).

En definitiva, la implementación de la autenticación biométrica no solo representa un avance tecnológico importante para Colombia, sino que también es una medida estratégica necesaria para enfrentar y mitigar las vulnerabilidades y riesgos asociados al proceso actual de identificación nacional, consolidando un sistema robusto que garantice la protección efectiva de la identidad ciudadana.

Entre los métodos más destacados de autenticación biométrica se encuentran la huella dactilar, el reconocimiento facial y el escaneo del iris. La huella dactilar es uno de los métodos más antiguos y utilizados debido a la singularidad y estabilidad de las crestas papilares que forman patrones únicos en los dedos de cada individuo, siendo difícilmente replicables y ampliamente aceptados en múltiples plataformas tecnológicas (Biometría y Seguridad Informática, 2023).

El reconocimiento facial utiliza puntos nodales del rostro del individuo para autenticar su identidad mediante el análisis detallado de las proporciones y características únicas de la cara. Este método es particularmente valorado por su carácter no invasivo y natural para el usuario, permitiendo validaciones rápidas y eficientes en diversos entornos, desde dispositivos móviles hasta sistemas de video vigilancia (Buitrago, Díaz & Munar, 2023).

Por otro lado, el escaneo del iris ofrece una precisión extremadamente alta gracias a la singularidad del patrón del iris en cada ojo, captado mediante cámaras especializadas que utilizan tecnología infrarroja. Este método biométrico es considerado uno de los más seguros y confiables debido a la complejidad y estabilidad del iris, haciendo casi imposible su falsificación o imitación (Biometría y Seguridad Informática, 2023).

Plataformas digitales y seguridad en la información

Las plataformas digitales son aplicaciones o sistemas informáticos accesibles desde internet que permiten realizar diversas tareas de manera eficiente y segura. En el contexto de la identificación ciudadana, estas plataformas resultan fundamentales para gestionar trámites críticos que involucran información personal altamente sensible.

La seguridad informática en estas plataformas es esencial y se refiere a todas las prácticas destinadas a proteger la información digital contra accesos no autorizados, alteraciones, robos o daños. Uno de los métodos fundamentales para garantizar esta seguridad

es el cifrado de datos, un procedimiento que transforma la información legible en un código incomprensible que solo puede ser descifrado utilizando una clave específica. Para realizar este proceso, se emplean algoritmos criptográficos avanzados, como AES (Advanced Encryption Standard), que es conocido por su robustez y eficacia en la protección de datos; RSA (Rivest-Shamir-Adleman), que utiliza un sistema de claves pública y privada para asegurar la comunicación; y ECC (Elliptic Curve Cryptography), que emplea curvas elípticas para generar claves criptográficas más eficientes y seguras (Cardona et al., 2007).

Además del cifrado, las plataformas digitales también deben implementar protocolos seguros para proteger la información durante su transmisión en internet. Ejemplos de estos protocolos son HTTPS (Hypertext Transfer Protocol Secure), que encripta la información intercambiada entre el usuario y el servidor, y SSL/TLS (Secure Socket Layer/Transport Layer Security), que asegura que los datos no sean interceptados o manipulados durante su envío.

Asimismo, la autenticación multifactor (MFA) es una medida de seguridad que requiere que el usuario verifique su identidad mediante al menos dos métodos distintos. Estos métodos pueden incluir algo que el usuario conoce (como contraseñas o respuestas a preguntas de seguridad), algo que el usuario posee (como un teléfono móvil o una tarjeta inteligente) y algo que el usuario es (como una característica biométrica). En esta propuesta específica, el usuario inicialmente responderá preguntas de seguridad validadas por la información registrada en el ANI. Una vez superada esta validación, se realizará una autenticación biométrica facial, garantizando un alto nivel de seguridad y reduciendo significativamente el riesgo de fraude o suplantación.

Actualmente, en Colombia no existe una plataforma digital específica para gestionar el bloqueo y desbloqueo de la cédula de ciudadanía en casos de pérdida o hurto, por lo que esta propuesta representa una innovación tecnológica relevante para proteger eficazmente la identidad ciudadana.

Normativa de identificación en Colombia

En Colombia, la regulación legal relacionada con la protección de datos personales y la autenticación de identidad está principalmente contemplada en la Ley Estatutaria 1581 de 2012, conocida como Ley de Protección de Datos Personales. Esta ley establece principios fundamentales tales como finalidad, libertad, veracidad, transparencia, acceso restringido, seguridad y confidencialidad en el tratamiento de información personal, garantizando así los derechos de los ciudadanos al habeas data, que consiste en conocer, actualizar, rectificar y eliminar los datos personales almacenados en bases de datos públicas o privadas (Congreso de la República de Colombia, 2012).

Complementando esta ley, el Decreto 1377 de 2013 reglamenta de manera específica los procedimientos para obtener el consentimiento informado de los titulares de los datos personales, y establece claramente la responsabilidad y obligaciones que tienen las entidades públicas y privadas en la implementación de medidas de seguridad adecuadas para proteger esta información frente a cualquier riesgo o amenaza (Congreso de la República de Colombia, 2013).

Adicionalmente, la Ley 1273 de 2009, conocida como Ley de Delitos Informáticos, tipifica penalmente las conductas delictivas relacionadas con el acceso abusivo a sistemas informáticos, interceptación ilegal de datos, daño informático, uso de software malicioso y otras acciones ilícitas relacionadas con la información digital, estableciendo sanciones severas para proteger la información personal y la infraestructura tecnológica en Colombia (Congreso de la República de Colombia, 2009).

Asimismo, la Ley 1341 de 2009, denominada Ley de Tecnologías de la Información y las Comunicaciones (TIC), establece principios y conceptos fundamentales sobre la organización de las TIC en Colombia, promoviendo el acceso seguro y confiable a la

información digital, lo que fortalece la protección de datos personales y la seguridad informática en diversas plataformas digitales empleadas para la gestión pública y privada (Congreso de la República de Colombia, 2009).

Normas de seguridad en autenticación

A nivel internacional, existen estándares técnicos claramente definidos que proporcionan lineamientos para garantizar la seguridad de la información y la adecuada protección de los datos personales en las plataformas digitales. Entre estas normativas destacan particularmente las Normas ISO (International Organization for Standardization).

La norma ISO/IEC 27001 es una de las más relevantes en este ámbito, pues especifica los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema incluye controles específicos destinados a proteger la confidencialidad, integridad y disponibilidad de la información mediante una efectiva gestión de riesgos y mecanismos de protección tecnológica robustos (International Organization for Standardization [ISO], 2023).

Por otra parte, la norma ISO/IEC 27005 ofrece directrices detalladas para la gestión del riesgo en seguridad de la información, facilitando la identificación, evaluación y tratamiento de amenazas y vulnerabilidades en sistemas informáticos, fortaleciendo así significativamente las estrategias de seguridad en autenticación y protección de datos personales (ISO, 2023).

Estas normas internacionales, al ser adoptadas por organizaciones públicas y privadas, garantizan un alto estándar de seguridad informática y protección efectiva frente a riesgos cibernéticos, lo cual es fundamental en el contexto colombiano para prevenir y mitigar delitos relacionados con la suplantación de identidad y el manejo inapropiado de datos personales.

Casos de uso de autenticación en otros países

A nivel internacional, varios países han implementado sistemas avanzados para proteger la identidad ciudadana mediante métodos robustos de autenticación y bloqueo de documentos, ofreciendo modelos exitosos que pueden servir como referencia para Colombia. Finlandia es un ejemplo notable en la implementación de sistemas digitales avanzados para la autenticación y protección de documentos de identidad. En este país, los ciudadanos pueden bloquear de forma inmediata su tarjeta de identidad electrónica (Henkilökortti) en caso de pérdida o robo, a través de una plataforma gubernamental integrada en línea (Galvis, 2023). Este sistema permite la activación automática de alertas hacia diversas instituciones financieras y gubernamentales, evitando así el uso fraudulento del documento en trámites sensibles.

Otro caso relevante es Estonia, reconocido mundialmente por su sistema digital de identidad. Este país ha desarrollado una plataforma de identidad digital basada en tarjetas inteligentes que integran la firma digital y biometría facial, lo que permite no solo la autenticación segura, sino también la capacidad de bloquear y desbloquear documentos digitales en tiempo real mediante aplicaciones móviles y portales web gubernamentales (Galvis, 2023).

Asimismo, México ha implementado un sistema integral llamado RENAPO (Registro Nacional de Población), que utiliza autenticación biométrica, particularmente huellas dactilares y reconocimiento facial, para garantizar la identidad de los ciudadanos en trámites críticos como la emisión y renovación de documentos oficiales. Este sistema ha reducido considerablemente los casos de fraude relacionados con la suplantación de identidad, gracias a la capacidad inmediata de verificar la autenticidad de los usuarios (Galvis, 2023).

Estos casos internacionales ilustran cómo la integración efectiva de tecnologías avanzadas, plataformas digitales seguras y protocolos claros pueden contribuir

significativamente a la reducción de delitos relacionados con la identidad, proporcionando ejemplos concretos que podrían orientar el desarrollo y la implementación exitosa de un sistema similar en Colombia.

Análisis de restricciones

El desarrollo del proyecto del desarrollo de una plataforma digital para la gestión segura de la cédula de ciudadanía, al contener la implementación de plataformas digitales, cuenta con diversas restricciones de diferente tipo, que influyen en el alcance, la viabilidad y el éxito del proyecto, por tanto desde una mirada crítica y tomando en cuenta a Bernal Torres (2016),quien indica que la investigación y el desarrollo de proyectos requieren una metodología rigurosa que considere las limitaciones y los obstáculos que puedan surgir.

La finalidad de este análisis de restricciones es anticipar y mitigar posibles problemas que puedan afectar el desarrollo del proyecto y la funcionalidad de la plataforma planteada, esto implica analizar las limitaciones tecnológicas, legales, económicas, ambientales y sociales lo que es fundamental desde la etapa de diseño del proyecto según Cruz (2001).

Restricciones Ambiental

El desarrollo e implementación de una plataforma digital, implica desafíos técnicos y normativos, al igual y sin ser menos importantes que desafíos que deben ser considerados que impactan a nivel ambiental por tanto deben ser considerados en el análisis de restricciones, según Lerma Kirchner (2017), cualquier proceso de innovación tecnológica debe evaluar los efectos ambientales asociados a su ciclo de vida, desde la infraestructura utilizada hasta el consumo energético del sistema.

Consumo Energético de servidores y centros de datos

El funcionamiento de las plataformas digitales requiere servidores y bases de datos que tengan la capacidad de almacenar y procesar información en tiempo real. De acuerdo con Ardito et al. (2021), los centros de datos representan una de las principales fuentes de consumo energético en la industria tecnológica, contribuyendo significativamente a la huella de carbono. Teniendo en cuenta lo anterior es importante considerar estrategias de eficiencia energética, como optimización del uso de servidores, o uso de centros de datos que cumplan con certificados ambientales como estrategia para reducir el impacto ambiental.

Desarrollo y Mantenimiento de infraestructura tecnológica

El proyecto implica el uso de hardware especializado para el procesamiento de datos y uso de herramientas de autenticación biométrica, enlazados con la base de datos ANI de la Registraduría Nacional del Estado Civil. El uso de esta plataforma esta dado para el uso en aplicaciones móviles en aparatos celulares de los cuales la producción y diseño genera residuos electrónicos denominados (e-waste), estos residuos según la Organización de las Naciones Unidas (ONU, 2022), representan uno de los problemas ambientales de mayor crecimiento a nivel mundial debido a la falta de reciclaje adecuado. Para minimizar el impacto ambiental de estos residuos se debe promover la reutilización y reciclaje de los equipos obsoletos.

Uso de Energía en Dispositivos Móviles y Equipos del Usuario

El acceso a la plataforma digital por parte de los ciudadanos podría implicar un mayor uso de dispositivos móviles y computadores, esto podría incrementar el consumo energético a nivel individual. Como señalan Golembiewski y Sick (2020), la digitalización de servicios tiende a aumentar la demanda de energía en los hogares, debido al tiempo de uso prolongado de los equipos electrónicos. Por este motivo es importante optimizar algoritmos de procesamiento de datos y minimizar la cantidad de información transmitida innecesariamente, esto contribuiría al

desarrollo de una aplicación ligera y eficiente que reduzca el consumo de recursos en los dispositivos móviles.

Restricciones Económicas

Durante el desarrollo de este proyecto deben ser evaluadas una serie de restricciones económicas que puedes influir directamente en la viabilidad del proyecto, según Bernal Torres (2016), todo proyecto tecnológico debe considerar todos los costos asociados a el diseño, desarrollo y mantenimiento de cara a garantizar la sostenibilidad del proyecto a largo plazo.

Costos de Desarrollo, Implementación e infraestructura tecnológica

El desarrollo de una plataforma digital segura implica que se integre un sistema de autenticación biométrica, validación con enlace directo a la ANI y sistemas de bloqueo y desbloqueo, todas estas herramientas pueden tener un costo económico significativo que van desde el desarrollo del software y hardware, pasando por los costos asociados a la infraestructura de servidores y almacenamiento de datos, hasta los costos que se asocian a la integración con bases de datos existentes y de uso institucional como la ANI.

Costos de Seguridad y Cumplimiento Normativo

Los estándares de seguridad en las plataformas digitales se rigen bajo un marco de exigencia que corresponde a encriptación, monitoreo de amenazas y cumplimiento de normativas a nivel local y a nivel internacional lo que en palabras de Bieser y Hilty (2018), Puede aumentar los costos operativos del proyecto todo esto con la única finalidad de garantizar la protección de datos, lo impacta directamente en la credibilidad de la ciudadanía con respecto al uso de la herramienta, sanciones económicas hasta de 2.000 salarios mínimos legales vigentes ,suspensión de actividades o cierre de operaciones de acuerdo con el cumplimiento de la ley 1581 de 2012.

Costos de Mantenimiento y Actualización

La implementación y puesta en marcha de la plataforma trae con sigo una serie de actividades indispensables para su correcto funcionamiento, como lo son el mantenimiento permanente y realizado periódicamente y actualizaciones que garanticen la seguridad de la plataforma y de los datos de los ciudadanos, esto implica tener en cuenta costos asociados a personal técnico especializado, que se encargue de dar el mantenimiento necesario a la plataforma. Las actualizaciones de software si bien son indispensables para mitigar las brechas en seguridad y vulnerabilidades que pueda tener la herramienta, no deja de tener costos significativos tanto en su adquisición como en su implementación de acuerdo con Golembiewski y Sick (2020), los costos de mantenimiento y soporte técnico pueden representar hasta un 30% del presupuesto anual de un proyecto digital.

Accesibilidad Económica para los Usuarios

Aunque la plataforma está diseñada para aumentar la seguridad en la identificación de las personas, es posible que no todos puedan usarla fácilmente debido a problemas económicos. No todos tienen acceso a internet o a los dispositivos necesarios, y si usar la plataforma tiene algún costo, esto podría ser un obstáculo para muchos. La Organización de las Naciones Unidas (ONU, 2022) nos recuerda que la falta de acceso a la tecnología es un gran problema cuando se trata de usar servicios del gobierno. Por eso, es muy importante pensar en cómo hacer que la plataforma sea accesible para todos, sin importar su situación.

Restricciones Legales

El marco normativo del proyecto abarca esencialmente y de manera estricta algunas leyes como la de protección de tratamiento de datos, autenticación biométrica, o ley de ciberseguridad que deben ser abordadas de manera detallada a fin de garantizar el cumplimiento normativo en el proyecto, si bien la suplantación de identidad es un delito que se

encuentra en aumento Congreso de la República de Colombia (2022), las restricciones nombradas a igual que este proyectos están encaminadas en proteger a la ciudadanía.

Protección de Datos Personales Ley 1581 de 2012

En Colombia, la Ley 1581 de 2012 establece el marco legal para la protección de datos personales, esta ley impone estrictas restricciones en la recolección, almacenamiento y tratamiento de dicha información (Congreso de la República de Colombia, 2012). Por lo tanto, la plataforma deberá garantizar la confidencialidad, integridad y disponibilidad de los datos, lo que exige la implementación de rigurosos estándares de seguridad.

En las restricciones principales de la ley se encuentra su fundamentación en los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, adicionalmente se debe contar con el consentimiento expreso e informado del titular para el caso de nuestro proyecto se establecen restricciones más estrictas ya que se estaría haciendo uso de lo que la ley denomina datos sensibles en los que se encuentran datos como origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, pertenencia a sindicatos, organizaciones sociales, datos relativos a la salud, vida sexual y datos biométricos, los últimos siendo requeridos para el desarrollo del proyecto propuesto. La ley hace énfasis en los deberes de quienes manejan dichos datos, en estos deberes podemos encontrar garantizar la seguridad de los datos, informar a los titulares sobre sus derechos y atender sus solicitudes al igual que implementar medidas de seguridad para proteger los datos de accesos no autorizados, pérdidas o alteraciones.

Autenticación Biométrica Ley 1266 de 2008

El uso de reconocimiento facial y huellas dactilares para la autenticación debe cumplir con lineamientos específicos de privacidad y consentimiento informado. Según la Ley 1266 de 2008 su almacenamiento debe, el uso de datos biométricos debe ser autorizado explícitamente

por el titular, y su almacenamiento debe garantizar medidas de seguridad avanzadas para evitar suplantaciones (Congreso de la República de Colombia, 2008). Además, estándares internacionales, como la ISO/IEC 24745, establecen prácticas recomendadas para la protección de datos biométricos en sistemas digitales. El almacenamiento de datos biométricos requiere la implementación de medidas de seguridad robustas, como el cifrado de datos, el control de acceso estricto y la detección de intrusiones.

Ciberseguridad y Protección contra Fraudes Ley 1928 de 2019

La ley 1928 de 2019 está diseñada para regular el desarrollo y uso de plataformas digitales, también determina que puede ser tomado como un delito informático y establece los parámetros de seguridad en cuanto a la responsabilidad de las plataformas digitales de tener mecanismo de defensa frente a los ciberataques y fraudes electrónicos, adicionalmente teniendo en cuenta la implementación del CARD ID como identificador único para bloqueo y desbloqueo del documento de identificación, esto implica que se debe contar con mecanismo de encriptación robustos y protocolos de seguridad que minimicen las amenazas.

Regulación del Uso de Documentos de identificación

Si bien esta restricción no es de carácter legal, sí corresponde a un aspecto normativo que debe ser cuidadosamente considerado, ya que el desarrollo de la plataforma está directamente vinculado con la Registraduría Nacional del Estado Civil. Esta entidad, como única autoridad competente para la expedición y validación de la cédula de ciudadanía en Colombia, establece los lineamientos normativos y técnicos que deben cumplir todos los sistemas externos que interactúen con su infraestructura, en especial con el Archivo Nacional de Identificación (ANI).

Según su marco normativo, cualquier plataforma que busque conectarse con el ANI debe garantizar el cumplimiento de una serie de requisitos legales y técnicos para asegurar la

integridad, trazabilidad y confidencialidad de la información consultada. Entre estos requisitos se destacan:

- Estricto cumplimiento de la Ley 1581 de 2012 (Protección de datos personales).
- Estricto cumplimiento de la Ley 1266 de 2008 (Habeas Data).
- Adopción de estándares de Seguridad de la Información alineados a la norma ISO/IEC 27001.
- Estricto cumplimiento de la Ley 594 de 2000 (Ley General de Archivos).
- Estricto cumplimiento del Decreto 1080 de 2015, el cual reglamenta aspectos relacionados con la gestión de documentos electrónicos.

Asimismo, es necesario considerar las limitaciones en la responsabilidad legal, conforme a lo establecido por la Ley 527 de 1999, la cual regula el comercio electrónico en Colombia. Esta norma establece que las plataformas digitales pueden ser responsables por errores en la autenticación o bloqueos irregulares si no cuentan con mecanismos adecuados para la validación y rectificación de datos. Por tanto, cualquier sistema de identificación electrónica debe incorporar procesos sólidos de validación, trazabilidad y corrección, que minimicen el riesgo de suplantación o errores administrativos.

Adicionalmente, y como parte de las restricciones del presente trabajo, es importante aclarar que, por tratarse de un proyecto de carácter académico, no se cuenta con acceso a bases de datos oficiales como el ANI, el número CARD ID ni el sistema de biometría facial, ya que esta información es clasificada como sensible y está bajo custodia exclusiva de la Registraduría Nacional del Estado Civil. Solo las personas jurídicas que establezcan un contrato formalmente suscrito y supervisado por la entidad pueden tener acceso legítimo a estas fuentes de datos. En el caso de entidades privadas no estatales, se establece además el pago por consulta, cuyo valor varía según el tipo de servicio y volumen de solicitudes.

Esta condición representa una restricción crítica dentro del desarrollo y validación del sistema, ya que impide realizar pruebas reales con datos oficiales. Por esta razón, el prototipo construido en el marco del proyecto se basa en simulaciones técnicas, diseñadas para representar el comportamiento esperado de las bases de datos oficiales sin comprometer la legalidad ni la seguridad de la información. No obstante, es importante destacar que la Registraduría sí cuenta con la capacidad técnica, legal y operativa para llevar a cabo una implementación real del sistema, ya que es la propietaria legítima de las bases de datos requeridas y dispone del marco institucional necesario para la integración segura de esta plataforma en un entorno oficial.

Restricciones Socioculturales

Para llevar a cabo el proyecto con éxito se debe tener en consideración además del desarrollo técnico y tecnológico de la plataforma alineada al marco normativo y legal, debe ser considerado la aceptación en la sociedad, en la cual factores con el desconocimiento, el miedo o la falta de recursos pueden representar barreras que limiten el alcance de la plataforma.

Acceso a la Tecnología

En el desarrollo de herramientas y plataformas digitales sigue siendo un desafío importante la dificultad que tienen algunas poblaciones en Colombia, para acceder a dispositivos electrónicos e internet, según la Comisión Económica para América Latina y el Caribe (CEPAL, 2022), cerca del 40% de la población en zonas rurales aún no tiene acceso estable a internet, esto sin lugar a duda dificulta el uso de la plataforma en comunidades alejadas quienes de cierta manera estarían siendo excluidas vulnerando su derecho a la identidad y autenticación segura.

Desconfianza en la Seguridad de la información

Un estudio reciente de la Universidad de los Andes, realizado por Galvis en 2023, nos da una idea clara de cómo se siente la gente en Colombia. Resulta que un porcentaje importante de los colombianos desconfía bastante de estos sistemas de identificación digital, fundamentado principalmente por antecedentes en los que se han conocido casos de filtración de datos y vulnerabilidades en plataformas gubernamentales. Esta percepción puede dificultar el desarrollo de la plataforma, ya que muchas personas podrían evitar su uso por miedo a que su información sea comprometida.

Analfabetismo Digital

Según el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC, 2021), aún existe un porcentaje significativo de la población adulta mayor y personas de bajos recursos con limitaciones en el manejo de plataformas digitales. Lo que claramente limitaría el uso de la plataforma, esto en cierta medida también podría ser visto como exclusión social y económica ya que las personas sin acceso a las plataformas digitales pueden tener dificultades para acceder a servicios gubernamentales, buscar empleo y participar en la economía digital. Esto puede llevar a una mayor desigualdad social y económica, aunque entidades como el MinTIC ha implementado diversas iniciativas para reducir la brecha digital, como programas de capacitación en habilidades digitales y subsidios para el acceso a internet también es necesario el apoyo y compromiso del sector privado.

Resistencia al cambio y Transformación Cultural

En Colombia, persiste una marcada preferencia por los procesos presenciales en la gestión de documentos oficiales, a pesar de la creciente disponibilidad de plataformas digitales. Esta tendencia refleja una resistencia arraigada al cambio, un fenómeno que Lerma Kirchner (2017) identifica como un factor clave que obstaculiza la adopción de nuevas tecnologías. En un contexto donde los trámites burocráticos han sido tradicionalmente presenciales, la

transición hacia lo digital se enfrenta a inercias culturales y hábitos arraigados. La adopción lenta de plataformas digitales puede retrasar la modernización de los servicios públicos, aumentar los costos operativos y limitar el acceso a trámites para aquellos que no pueden desplazarse físicamente. La adopción exitosa de la digitalización en la gestión de documentos oficiales requiere un cambio cultural. Es necesario construir confianza en las nuevas tecnologías y demostrar que pueden ofrecer un servicio más eficiente, ágil y accesible para todos los colombianos.

Metodología para la selección y desarrollo de la solución

La generación de soluciones y la búsqueda de la mejor alternativa, una vez conocidas las restricciones, implica los siguientes aspectos:

1. Soluciones ilógicas La solución propuesta, que consiste en una plataforma digital para la gestión segura de la cédula de ciudadanía, no atenta contra ningún principio físico o ley natural. La implementación del bloqueo y desbloqueo de la cédula a través de autenticación biométrica y validación con el Archivo Nacional de Identificación (ANI) es factible desde el punto de vista técnico. Además, el uso de tecnologías digitales y bases de datos en tiempo real es viable y está alineado con las tendencias actuales de seguridad e identificación digital.

2. Comparación con hechos conocidos

En Colombia, no hay un mecanismo que permita verificar en tiempo real si una cédula física ha sido reportada como perdida o robada, lo que genera vulnerabilidades en el proceso de identificación. Comparado con sistemas internacionales, como los de Estonia o la validación de identidad digital en bancos, la propuesta de la plataforma digital representa una mejora significativa en términos de seguridad y acceso.

La implementación de sistemas de autenticación biométrica y plataformas digitales para la gestión de documentos de identidad ha demostrado ser efectiva en diversos países y

sectores. A continuación, se presentan ejemplos detallados que ilustran cómo estas tecnologías han mejorado la seguridad y eficiencia en la identificación ciudadana:

México: Modernización de la CURP

En marzo de 2025, el Gobierno de México anunció la implementación de una versión mejorada de la Clave Única de Registro de Población (CURP) que incorpora fotografía y huellas dactilares. Esta iniciativa tiene como objetivo facilitar la búsqueda de personas desaparecidas y mejorar la precisión en la identificación de ciudadanos y residentes legales en el país. La nueva CURP permitirá una identificación más rápida y precisa, apoyando investigaciones y reduciendo tiempos de respuesta en casos de desapariciones.

Unión Europea: Pasaportes Biométricos

Desde 2004, los 27 Estados miembros de la Unión Europea han adoptado el uso del pasaporte electrónico o pasaporte biométrico. Este documento incorpora datos personales y físicos de los ciudadanos almacenados en un chip, incluyendo información sobre viajes realizados. La implementación de esta tecnología ha permitido un mayor control y seguridad en las fronteras, dificultando la falsificación de documentos y mejorando la eficiencia en los procesos migratorios.

Perú: Documento Nacional de Identidad Electrónico (DNIe)

El Registro Nacional de Identificación y Estado Civil (RENIEC) de Perú comenzó a emitir el DNI electrónico en julio de 2013. Este documento, fabricado en policarbonato y con formato de tarjeta de crédito, contiene un chip que almacena información biométrica del titular, como huellas dactilares y fotografía. Además, permite a los ciudadanos firmar digitalmente documentos electrónicos con la misma validez que una firma manuscrita, facilitando el acceso a servicios estatales y privados de manera segura y eficiente.

África: Autenticación Biométrica en el Sector Bancario

En países como Nigeria, Malawi, Sudáfrica, Ghana, Kenia y Botsuana, las instituciones bancarias han adoptado sistemas de autenticación biométrica para verificar la identidad de sus clientes. Esta implementación ha resultado en una reducción significativa de casos de robo de identidad y ha hecho que las transacciones sean más seguras, rápidas y convenientes para los consumidores africanos.

Alemania: Documento de Identidad Electrónico

Desde noviembre de 2010, Alemania emite el documento de identidad electrónico (Elektronischer Personalausweis), que contiene un chip RFID donde se almacenan datos personales, incluyendo información biométrica como huellas dactilares y fotografía. Este documento permite la autenticación en línea y la firma electrónica, facilitando múltiples aplicaciones gubernamentales y comerciales, y mejorando la seguridad en la identificación de los ciudadanos.

La adopción de tecnologías biométricas y plataformas digitales en la gestión de documentos de identidad ha demostrado mejorar la seguridad, eficiencia y confianza en los sistemas de identificación a nivel global. La experiencia internacional respalda la implementación de soluciones similares, como la plataforma digital propuesta para la Registraduría Nacional del Estado Civil en Colombia, orientada a la gestión segura de la cédula de ciudadanía

3. Evaluación de las soluciones Debido a los costos asociados, no es factible evaluar todas las posibles soluciones. Por ello, se prioriza el análisis de alternativas viables y específicas. La plataforma digital se destaca por su enfoque en la seguridad y la prevención del fraude.

- Se han considerado otras soluciones, como la emisión de documentos con chips de seguridad o la vinculación con aplicaciones gubernamentales existentes, pero estas opciones presentan mayores costos de implementación y logística.
- La solución digital permite una implementación progresiva y escalable, lo que la hace competitiva.
- Se podría reconsiderar la incorporación de tecnologías adicionales, como inteligencia artificial para detección de fraudes o integraciones con otras entidades de seguridad.

Desde un enfoque de ingeniería, la solución seleccionada es rentable en términos económicos (reducción de fraudes y costos administrativos), ambientales (disminución del uso de documentos físicos) y sociales (mayor seguridad para los ciudadanos).

Diseño Metodológico

El desarrollo del presente proyecto de grado se fundamenta en una metodología de tipo aplicada, con enfoque cualitativo y proyectivo, orientada a la solución de un problema específico de la realidad colombiana: la suplantación de identidad mediante el uso indebido del documento físico de la cédula de ciudadanía. Desde esta perspectiva, el trabajo se orienta a generar una propuesta tecnológica viable que permita mitigar dicha problemática mediante una plataforma digital diseñada para el bloqueo y desbloqueo del documento, utilizando el número único CARD ID, validaciones con el Archivo Nacional de Identificación (ANI) y mecanismos de autenticación biométrica.

Ilustración 3. Fases Metodológicas

Elaboración propia

El enfoque metodológico combina la revisión documental, el análisis normativo y el desarrollo técnico de un prototipo funcional. Se parte de la observación del contexto actual, sin manipular variables directamente, lo que ubica este estudio dentro de un diseño no experimental y transeccional, ya que la información fue recolectada en un momento específico del tiempo, con el fin de describir y comprender un fenómeno social y tecnológico que requiere intervención.

Inicialmente, se realizó una revisión exhaustiva de fuentes secundarias: leyes nacionales, estándares internacionales de seguridad de la información, artículos académicos, informes técnicos y experiencias exitosas en otros países. Esta etapa permitió comprender el alcance del problema y establecer el marco legal y teórico sobre el cual se fundamenta la

propuesta. A partir de este análisis, se levantaron los requerimientos técnicos, funcionales y legales que debe cumplir la plataforma, así como las restricciones que podrían afectar su desarrollo e implementación.

Tabla 2. Requerimientos Técnicos

Código	Requerimiento
RT-1	El sistema debe ser desarrollado con tecnologías web seguras (ej. HTTPS, cifrado de datos).
RT-2	Debe integrarse o simular una base de datos que emule el comportamiento del ANI.
RT-3	La autenticación biométrica debe usar una librería de reconocimiento facial confiable y precisa.
RT-4	El sistema debe almacenar temporalmente los datos con cifrado y cumplir con políticas de retención segura.
RT-5	Debe tener capacidad de escalabilidad modular para futuras integraciones con bases de datos reales.
RT-6	Debe presentar altos niveles de disponibilidad y tolerancia a fallos para garantizar el acceso continuo.

Tabla 3. Requerimientos Funcionales

Código	Requerimiento
RF-1	El sistema debe permitir a los ciudadanos registrar su cédula de ciudadanía y asociarla a su CARD ID.
RF-2	Debe ofrecer la funcionalidad de bloqueo del documento físico en caso de pérdida o robo.

Código	Requerimiento
RF-3	Debe permitir el desbloqueo del documento por parte del usuario, previa validación biométrica.
RF-4	Debe mostrar el estado del documento (vigente, bloqueado) consultado desde la base del ANI.
RF-5	El sistema debe contar con autenticación biométrica facial para verificar la identidad del usuario.
RF-6	Debe generar un registro de cada transacción (bloqueo/desbloqueo) con fecha y hora para trazabilidad.
RF-7	Debe contar con una interfaz sencilla, accesible desde dispositivos móviles y navegadores web.

Tabla 4. Requerimientos Legales

Código	Requerimiento
RL-1	Debe cumplir con la Ley 1581 de 2012 sobre protección de datos personales en Colombia.
RL-2	El usuario debe dar su consentimiento informado para el tratamiento de datos personales y biométricos.
RL-3	Debe cumplir con la Ley 1266 de 2008 (Habeas Data) y la Ley 1273 de 2009 sobre delitos informáticos.
RL-4	El sistema debe adoptar principios de transparencia, seguridad y confidencialidad en todo el ciclo de datos.
RL-5	Debe permitir al usuario acceder, modificar o eliminar sus datos según el principio de autodeterminación.

Posteriormente, se avanzó en el diseño conceptual y técnico de la solución, elaborando los esquemas de arquitectura del sistema, interfaces de usuario y flujos operativos.

Desarrollo del Prototipo Funcional

Product Backlog

A continuación, se presenta el Product Backlog del proyecto, el cual reúne las principales historias de usuario que guiaron el desarrollo del prototipo funcional de la plataforma Cédula Segura. Este backlog fue construido bajo una perspectiva orientada al usuario, identificando los roles, necesidades y criterios de aceptación para cada funcionalidad priorizada.

Esta herramienta permitió mantener un enfoque claro sobre las funcionalidades esperadas, facilitando su implementación dentro de una arquitectura modular y segura.

Tabla 5. Product Backlog

Código HU	Rol	Requerimiento	¿Para qué?	Criterios de Aceptación
HU-01	Ciudadano	Quiero registrarme ingresando mi cédula y expedición	Para crear una cuenta segura y personal	Se valida con ANI. Si los datos coinciden, se permite crear una contraseña. Si falla 3 veces, se bloquea el intento.
HU-02	Ciudadano	Quiero iniciar sesión con mi contraseña	Para acceder a mi cuenta de manera segura	El sistema acepta credenciales válidas y rechaza las inválidas. Se genera token de sesión.
HU-03	Ciudadano	Quiero bloquear mi cédula si la pierdo	Para evitar suplantación física	El sistema solicita motivo, confirma identidad y cambia el estado del documento a “bloqueado”.
HU-04	Ciudadano	Quiero desbloquear mi cédula	Para poder volver a usarla normalmente	El sistema valida identidad biométrica y permite desbloquear si no hay alertas de seguridad activas.

Código HU	Rol	Requerimiento	¿Para qué?	Criterios de Aceptación
HU-05	Ciudadano	Quiero ver el historial de bloqueos/desbloqueos	Para revisar si alguien más ha intentado manipular mi documento	El sistema muestra una lista con fecha, hora y tipo de acción (bloqueo/desbloqueo).
HU-06	Administrador	Quiero ver estadísticas de uso del sistema	Para evaluar su adopción y funcionalidad	Se accede a un panel que muestra cantidad de bloqueos, usuarios activos y validaciones por mes.
HU-07	Ciudadano	Quiero recuperar mi cuenta si olvido la contraseña	Para restablecer el acceso sin riesgo	El sistema envía un código de verificación al correo registrado. Solo si el código es correcto, se puede crear una nueva contraseña.

Elaboración propia.

La tabla presenta las historias de usuario identificadas para el desarrollo de la plataforma Cédula Segura, organizadas según su prioridad, rol asociado, propósito funcional y criterios de aceptación definidos.

Tecnologías empleadas

El desarrollo de la plataforma Cédula Segura se fundamentó en una arquitectura modular e interoperable que, si bien fue construida bajo simulaciones propias del entorno académico, está diseñada para integrarse de manera realista al ecosistema tecnológico de la Registraduría Nacional del Estado Civil.

La solución se compone de varios elementos tecnológicos principales. En el núcleo de la plataforma se encuentra la aplicación web (App CC Segura), desarrollada en un entorno web responsivo, orientado a ofrecer una experiencia intuitiva al ciudadano. Esta aplicación está conectada directamente a una base de datos (BD CC Segura), la cual se encarga de almacenar temporalmente la información relacionada con las solicitudes de bloqueo y desbloqueo de documentos, así como los logs de autenticación biométrica y los estados de cada transacción.

Uno de los pilares fundamentales del sistema es la validación biométrica facial, la cual permite autenticar la identidad del ciudadano antes de ejecutar cualquier cambio sobre el estado del documento. Aunque en el entorno de desarrollo se utilizó una simulación con librerías de reconocimiento facial, la plataforma está diseñada para integrarse con soluciones biométricas reales que maneja actualmente la Registraduría.

Asimismo, la arquitectura contempla la conexión con el Web Service del Archivo Nacional de Identificación (WS ANI). Esta integración permite validar, en tiempo real, los datos ingresados por el ciudadano (número de cédula y fecha de expedición) con los registros oficiales. Esta validación se convierte en el primer filtro de seguridad antes de proceder con la autenticación biométrica y posterior gestión del documento.

Otro componente clave en la arquitectura del sistema es la interacción con los servicios internos de la RNEC. Esta conexión, representada como una “caja negra” desde el punto de vista de Cédula Segura, permite que una vez se apruebe una acción (bloqueo o desbloqueo), esta información se sincronice con los demás sistemas y bases de datos oficiales de la entidad. De esta forma, se asegura que el estado del documento se actualice de manera consistente y trazable dentro de todo el entorno institucional.

En términos de interoperabilidad, Cédula Segura se apoya en componentes que ya existen dentro de la infraestructura de la Registraduría Nacional del Estado Civil, tales como el sistema de validación facial, el servicio de consulta ANI, y las bases de datos de gestión documental. En este sentido, la plataforma no busca reemplazar servicios actuales, sino complementarlos, unificarlos y presentarlos al ciudadano mediante una interfaz segura, usable y enfocada en la prevención de la suplantación de identidad.

Finalmente, para efectos del desarrollo y pruebas, se emplearon tecnologías web estándar como HTML5, CSS3 y JavaScript, junto con librerías de simulación facial como Face

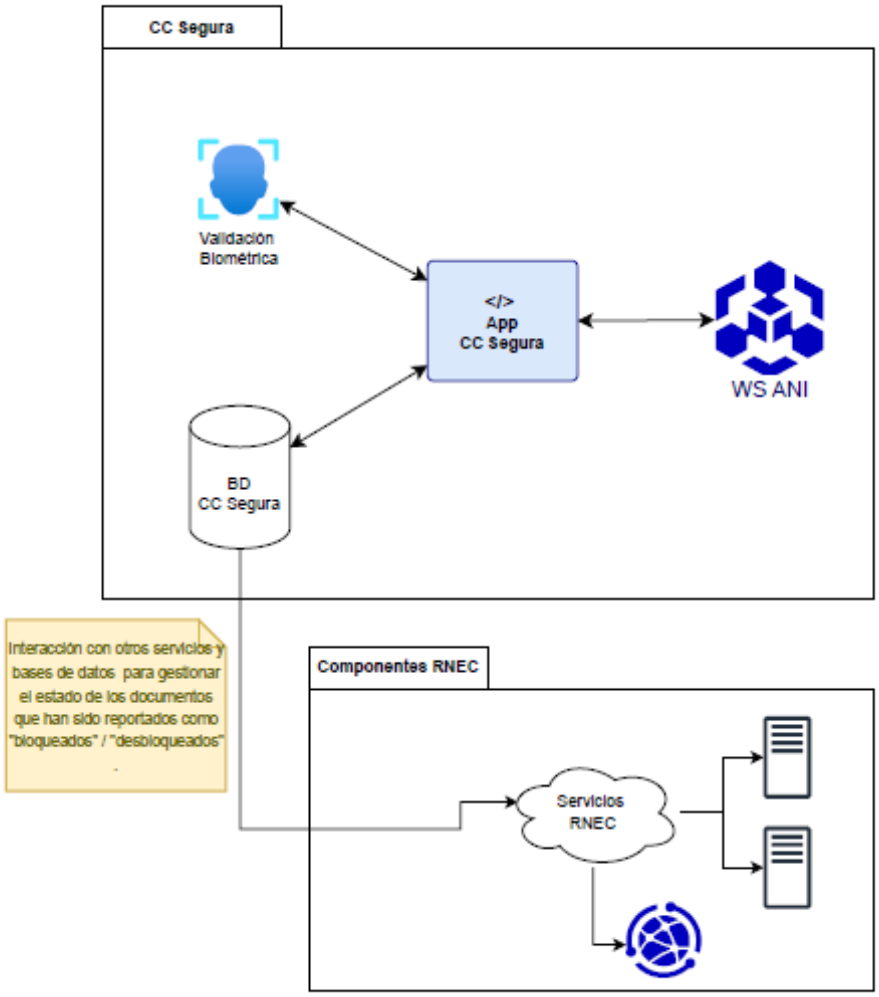
API (basada en TensorFlow.js) para demostrar la viabilidad de la autenticación biométrica. Las estructuras de datos fueron gestionadas en formato JSON y alojadas en entornos locales, respetando las restricciones legales de acceso a información sensible y de carácter confidencial.

Arquitectura del sistema

La plataforma Cédula Segura fue diseñada bajo una arquitectura modular que permite articular los diferentes procesos necesarios para gestionar, en tiempo real, el estado de la cédula de ciudadanía en caso de pérdida o hurto. Esta arquitectura contempla tanto los componentes desarrollados específicamente para el prototipo como la interacción con los servicios existentes en la infraestructura tecnológica de la Registraduría Nacional del Estado Civil.

A continuación, se presenta la arquitectura técnica del sistema *Cédula Segura* utilizando el modelo C4. Este modelo permite representar la estructura del software en múltiples niveles de abstracción. Se incluyen los diagramas de contexto, contenedores y componentes, los cuales facilitan la comprensión del sistema desde la visión externa hasta la lógica interna del prototipo funcional. interoperabilidad con las bases de datos y servicios oficiales de la entidad.

Ilustración 4. Diagrama de Contexto (C4) de la Plataforma Cédula Segura



Elaboración Propia
Nota: Representa la interacción entre el ciudadano, la plataforma, el ANI y servicios RNEC.

Tal como se muestra en la parte superior del diagrama, la arquitectura central de la solución está compuesta por los principales módulos de la plataforma Cédula Segura. En el corazón del sistema se encuentra la aplicación web (App Cédula Segura), que representa la interfaz con la que interactúa el ciudadano. Esta aplicación permite ingresar, consultar y ejecutar el proceso de bloqueo o desbloqueo del documento.

La aplicación se conecta directamente a una base de datos (BD Cédula Segura), la cual almacena de forma segura los registros temporales de transacciones, usuarios autenticados, intentos de validación, logs del sistema y estados de cada documento reportado.

Uno de los aspectos más relevantes en esta arquitectura es la integración de un componente de validación biométrica facial, que se encuentra alineado con los estándares de autenticación exigidos por la Registraduría. Esta validación se realiza previo a cualquier acción sobre el documento, lo que fortalece la seguridad del sistema y garantiza que las operaciones sean efectuadas por el titular del documento.

En paralelo, la aplicación realiza una consulta directa al Web Service del Archivo Nacional de Identificación (WS ANI). Esta consulta permite validar que los datos proporcionados por el ciudadano (número de cédula y fecha de expedición) coincidan con los registros oficiales. Si esta validación es exitosa, se permite avanzar al proceso de autenticación biométrica y gestión del estado del documento.

En la parte inferior del diagrama se representa la interacción entre la base de datos de Cédula Segura y los servicios internos de la RNEC, encargados de gestionar el estado oficial del documento dentro del sistema institucional. Esta conexión actúa como una caja negra desde la perspectiva de la plataforma, ya que el acceso a estos servicios se encuentra bajo control exclusivo de la Registraduría. Sin embargo, la arquitectura está diseñada para que una vez se confirme una operación de bloqueo o desbloqueo, esta sea registrada y sincronizada automáticamente en los sistemas internos de la entidad, asegurando coherencia y trazabilidad institucional.

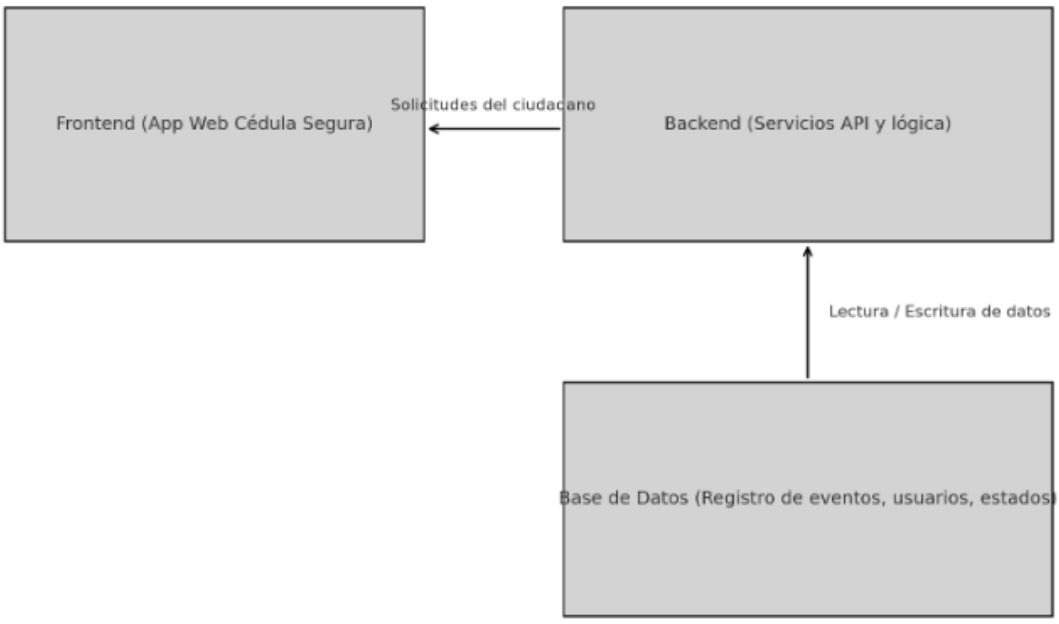
Esta arquitectura garantiza que la plataforma no actúe de manera aislada, sino que funcione como un canal ciudadano que aprovecha las capacidades ya existentes dentro de la Registraduría, tales como el sistema de identificación ANI, la base del número CARD ID y la

infraestructura de autenticación biométrica. En lugar de duplicar funciones o estructuras, Cédula Segura propone un enfoque complementario que unifica servicios dispersos y los pone a disposición del ciudadano para proteger su identidad de manera rápida, segura y eficiente.

Como parte del modelo C4, se incluye a continuación el Diagrama de Contenedores, el cual representa la estructura interna del sistema a nivel de aplicaciones y servicios. Este diagrama detalla cómo se organiza la solución en términos de frontend (interfaz web del ciudadano), backend (lógica de negocio y validaciones) y base de datos, evidenciando la comunicación entre estos elementos y su rol dentro del flujo operativo de la plataforma *Cédula Segura*.

Este nivel de abstracción permite entender cómo los diferentes contenedores trabajan de forma coordinada para cumplir con los procesos de validación, autenticación, consulta y gestión del estado de la cédula de ciudadanía.

Ilustración 5. Diagrama de Contenedores (C4) - Plataforma Cédula Segura

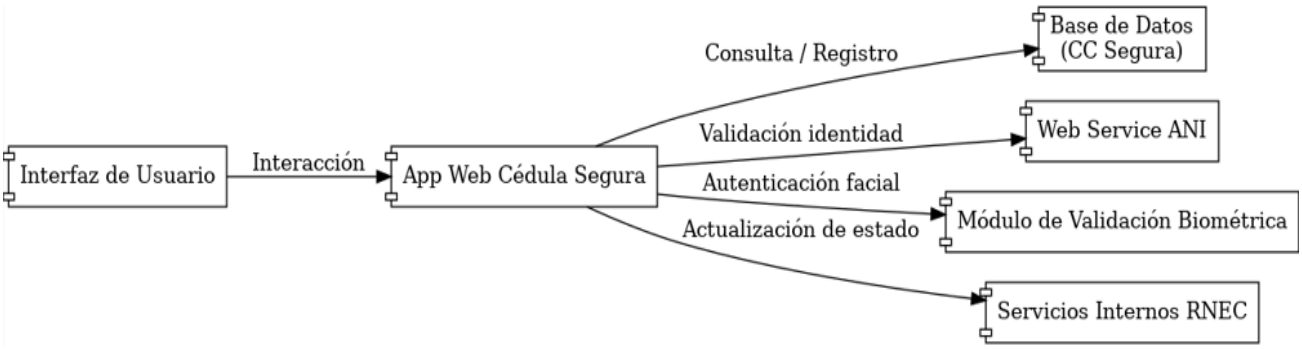


Elaboración Propia
Nota. Representa los contenedores principales de la arquitectura del sistema: la interfaz web para el ciudadano (frontend), los servicios API con lógica de negocio (backend) y la base de datos que almacena los estados e interacciones del documento.

Complementando la arquitectura general del sistema presentada anteriormente, se incluye a continuación el diagrama de componentes de la plataforma digital Cédula Segura. Este diagrama representa los principales bloques funcionales de software que conforman la solución tecnológica, así como su interconexión con servicios internos y externos necesarios para su funcionamiento.

El objetivo este diagrama es evidenciar la modularidad del sistema, su escalabilidad y la forma en que se organizan los distintos componentes de la aplicación, tales como la interfaz de usuario, el servicio web, la base de datos, el módulo de autenticación biométrica y la integración con los servicios institucionales como el ANI y los sistemas RNEC. Ver ilustración 5.

Ilustración 6. Diagrama de Componentes (C4) de la Plataforma Cédula Segura

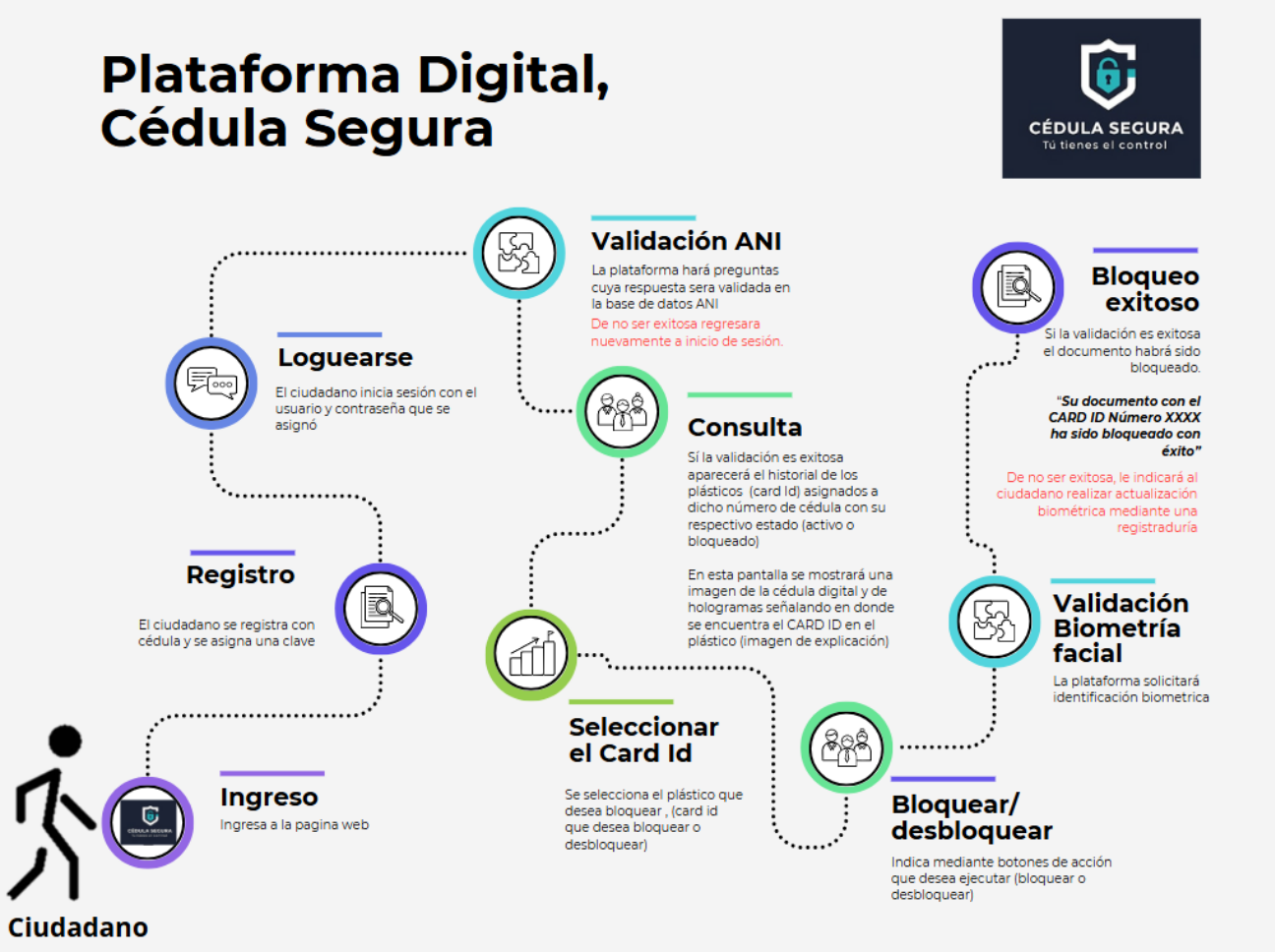


Elaboración Propia

Nota: Describe los módulos funcionales que conforman el backend y frontend del sistema, así como su integración con servicios externos.

El siguiente flujograma ilustra el recorrido que realiza un ciudadano dentro de la plataforma Cédula Segura, desde el ingreso inicial hasta la validación biométrica y la ejecución del bloqueo o desbloqueo del documento. Cada etapa ha sido diseñada para garantizar seguridad, trazabilidad y facilidad de uso:

Ilustración 7. Flujograma del Ciudadano



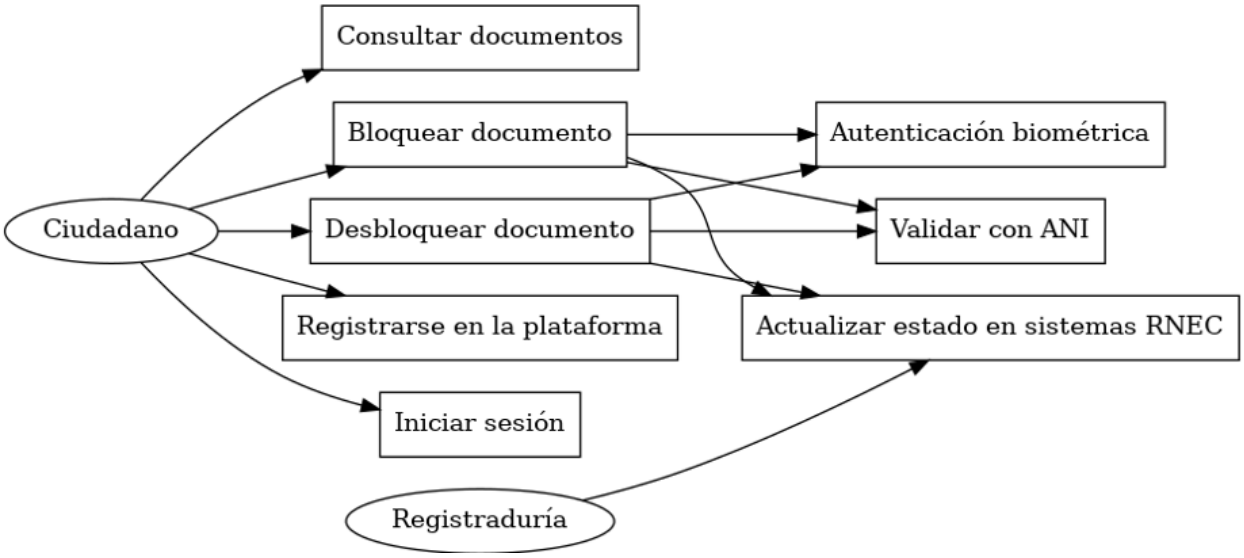
Elaboración Propia

Además del recorrido secuencial que realiza el ciudadano dentro de la plataforma, se presenta a continuación el diagrama de casos de uso. Este diagrama permite identificar, de forma estructurada, las principales funciones que puede ejecutar el usuario dentro del sistema,

así como la interacción con los módulos internos encargados de validar, autenticar y gestionar el estado del documento de identidad.

El propósito de este recurso es mostrar las funcionalidades clave desde la perspectiva del usuario, enmarcadas dentro del alcance del sistema *"Cédula Segura"*, incluyendo procesos como el registro, inicio de sesión, consulta de documentos, y acciones de bloqueo o desbloqueo con validación previa. Ver Ilustración 7.

Ilustración 8. Diagrama Casos de Uso UML



Elaboración Propia

Diccionario de Datos de la Plataforma Cédula Segura

Como parte del desarrollo técnico del prototipo funcional de la plataforma Cédula Segura, se presenta a continuación el diccionario de datos, el cual describe detalladamente los principales campos que integran la estructura de información del sistema.

Este instrumento permite documentar los atributos de cada dato que circula entre los distintos módulos, como registro, validación de identidad, autenticación biométrica, gestión de

bloqueos y recuperación de cuenta, proporcionando una guía clara sobre su tipo, longitud, origen, finalidad funcional y obligatoriedad.

Tabla 6. Diccionario de Datos - Cédula Segura

Nombre del Campo	Tipo de Dato	Longitud	Descripción	Origen	Módulo/Función	Requerido
cedula usuario	Numérico	10	Número de cédula del ciudadano	Usuario	Registro / Validación ANI	Sí
fecha expedición	Fecha	10	Fecha de expedición de la cédula	Usuario	Validación ANI	Sí
contraseña	Texto	64	Contraseña creada por el usuario (hash en BD)	Usuario	Registro / Inicio Sesión	Sí
token_sesion	Texto	128	Token único generado para sesión segura	Sistema	Seguridad / Login	Sí
resultado validación	Texto	15	Resultado de la validación ANI (válido / inválido)	WS ANI	Validación ANI	Sí
imagen biométrica	BLOB	-	Imagen facial capturada para autenticación	Usuario	Autenticación facial	Sí
resultado biometría	Texto	15	Resultado del análisis biométrico	Módulo biométrico	Validación de identidad	Sí
estado documento	Texto	20	Estado del documento: bloqueado / desbloqueado	Usuario / Sistema	Actualización estado	Sí
fecha actualización	FechaHora	-	Fecha y hora del último cambio de estado	Sistema	Auditoría / Registro	Sí
ip_dispositivo	Texto	45	IP del dispositivo usado por el ciudadano	Sistema	Seguridad / Auditoría	No
email_usuario	Texto	100	Correo electrónico asociado a la cuenta	Usuario	Recuperación de cuenta / Contacto	Sí
codigo_verificacion	Numérico	6	Código temporal enviado por email o SMS	Sistema	Verificación / Recuperación	Sí
intentos fallidos	Numérico	2	Cantidad de intentos fallidos de acceso	Sistema	Seguridad / Login	No
motivo bloqueo	Texto	100	Motivo declarado por el usuario para el bloqueo	Usuario	Gestión de bloqueos	No
historial bloqueo	Texto	-	Registro de bloqueos/desbloqueos con fecha	Sistema	Auditoría / Historial	No

Elaboración Propia

Nota: Todos los datos han sido estructurados de acuerdo con los requerimientos técnicos y de seguridad del sistema.

Implementación

La siguiente tabla describe los principales componentes de software que conforman el prototipo funcional de la plataforma Cédula Segura. Cada componente ha sido diseñado con base en una arquitectura modular, permitiendo su integración con servicios externos, como la base de datos del ANI y el sistema de autenticación biométrica.

La tabla clasifica cada componente según su ubicación en la arquitectura del sistema (frontend o backend) y resume su funcionalidad dentro del flujo operativo de la plataforma, asegurando trazabilidad, escalabilidad y cumplimiento de los requisitos definidos en el diseño del sistema.

Tabla 7. Implementación del Sistema Cédula Segura

Componente de Software	Arquitectura	Funcionalidad
Rutas para vistas (/routes)	Backend	Gestiona el enrutamiento entre las diferentes solicitudes y controladores del sistema.
Controlador de autenticación	Backend	Valida credenciales, gestiona sesiones seguras y genera tokens de acceso.
Módulo de validación ANI	Backend	Se comunica con el servicio web oficial del ANI para validar cédula y expedición.
Servicio de autenticación biométrica	Backend	Procesa la imagen facial capturada, compara con datos registrados y entrega respuesta.
API REST	Backend	Expone los servicios de la plataforma para ser consumidos desde el frontend.
Interfaz de usuario (/views)	Frontend	Presenta al ciudadano los formularios y pantallas de interacción.
Módulo de estado de documento	Backend	Permite bloquear o desbloquear el documento, según solicitud del usuario.
Registro de actividad (bitácora)	Backend	Almacena eventos importantes como intentos fallidos, bloqueos y accesos.
Validación de código de verificación	Backend	Verifica los códigos enviados al correo electrónico para recuperación de cuenta.
Almacenamiento en base de datos	Backend	Guarda de forma segura los datos del ciudadano, historial de bloqueo, etc.
Estilos e interfaz responsiva	Frontend	Mejora la experiencia del usuario en dispositivos móviles y navegadores.

Presentación del prototipo

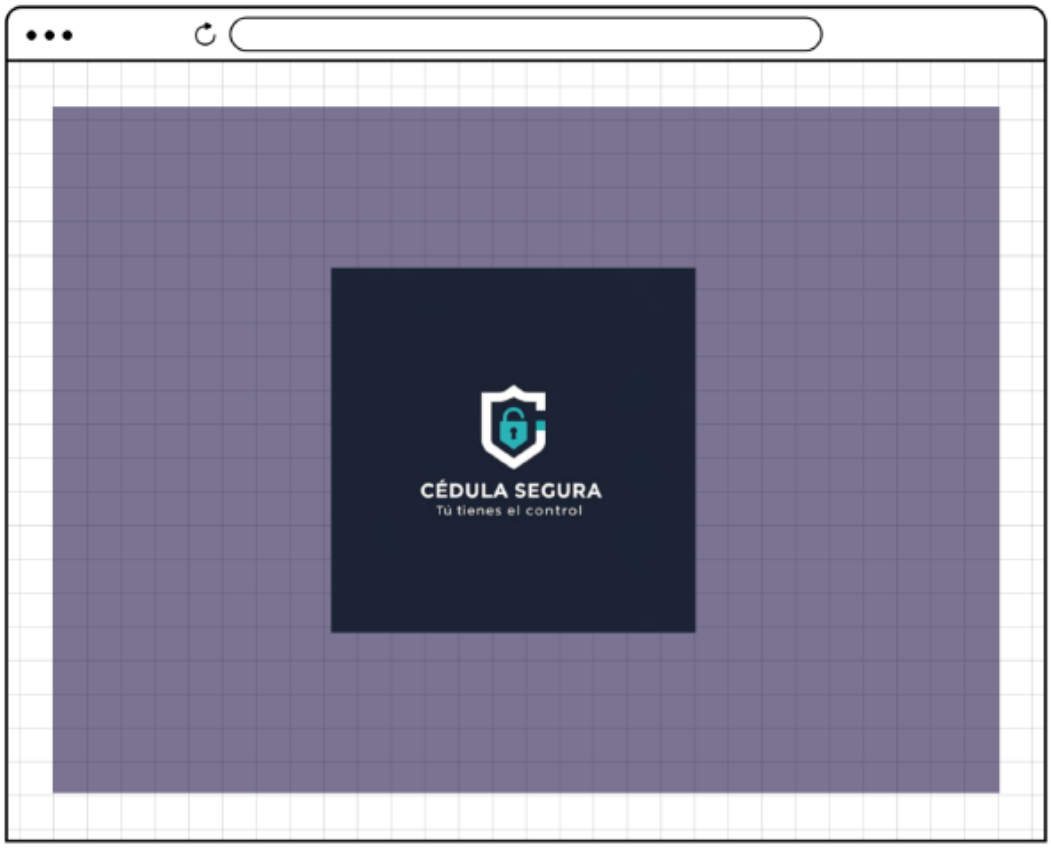
Como resultado del diseño e implementación del sistema Cédula Segura, se desarrolló un prototipo funcional que simula el flujo completo que seguiría el ciudadano para bloquear o desbloquear su documento de identidad en caso de pérdida o hurto. Este prototipo se diseñó con el objetivo de representar visualmente la interacción del usuario con la plataforma, y de demostrar la viabilidad técnica, funcional y de experiencia de uso de la solución propuesta.

A través de los siguientes mockups, se presenta una simulación visual del comportamiento esperado de la plataforma en cada una de sus etapas clave:

La interfaz inicia con una pantalla de presentación institucional, donde se visualiza el logotipo y el nombre oficial de la plataforma digital Cédula Segura.

Ver https://cedulasegura.site/ccsegura

Ilustración 9. Mockup 1 - Pantalla de Inicio – Cédula Segura



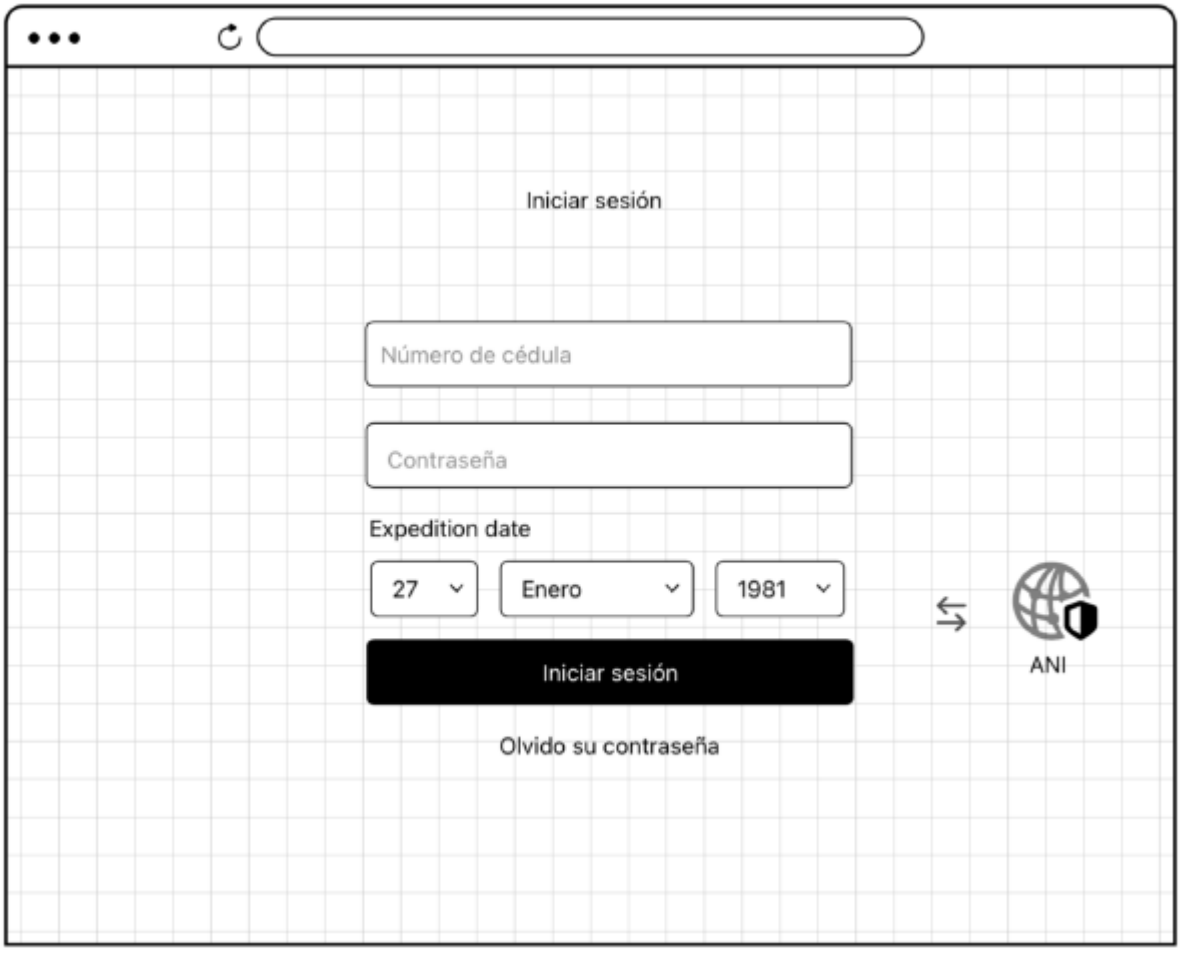
A continuación, se despliega el formulario de registro, en el cual el ciudadano debe ingresar su número de cédula y la fecha de expedición del documento, datos que serán validados directamente con la base de datos del Archivo Nacional de Identificación (ANI). Esta validación constituye el primer filtro de seguridad del sistema, y, en caso de que los datos no coincidan tras tres intentos, se bloquea el proceso y se solicita al ciudadano que se acerque a una sede física de la Registraduría para realizar la validación presencial.

Ilustración 10. Mockup 2 - Formulario de Registro

Una vez superado el registro, se habilita la pantalla de inicio de sesión, donde el ciudadano accede con su número de documento y la contraseña previamente asignada. En

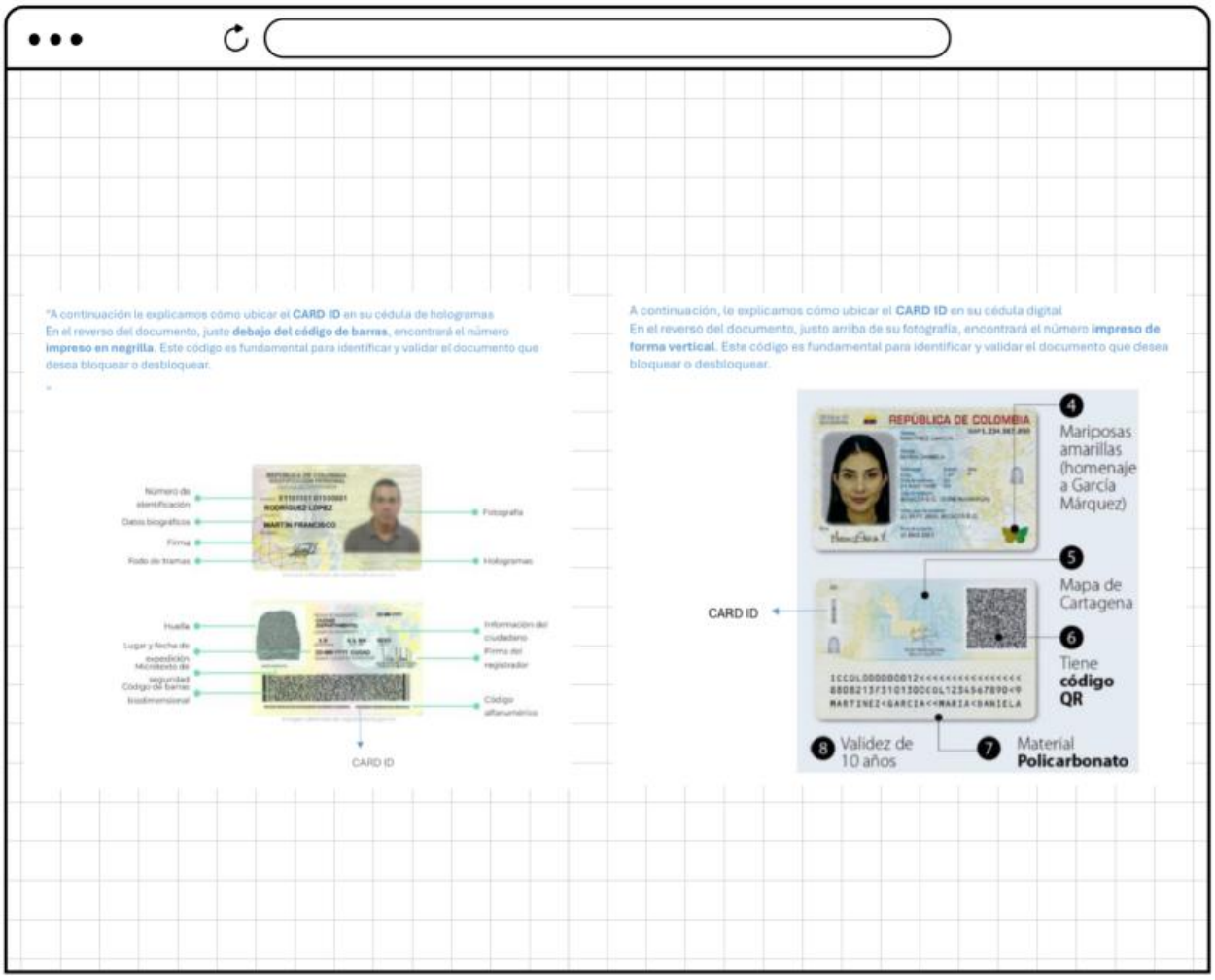
esta sección se incorpora un botón adicional para recuperación de contraseña en caso de olvido, lo que garantiza accesibilidad y continuidad en el uso del sistema.

Ilustración 11. Mockup 3 - Inicio de Sesión



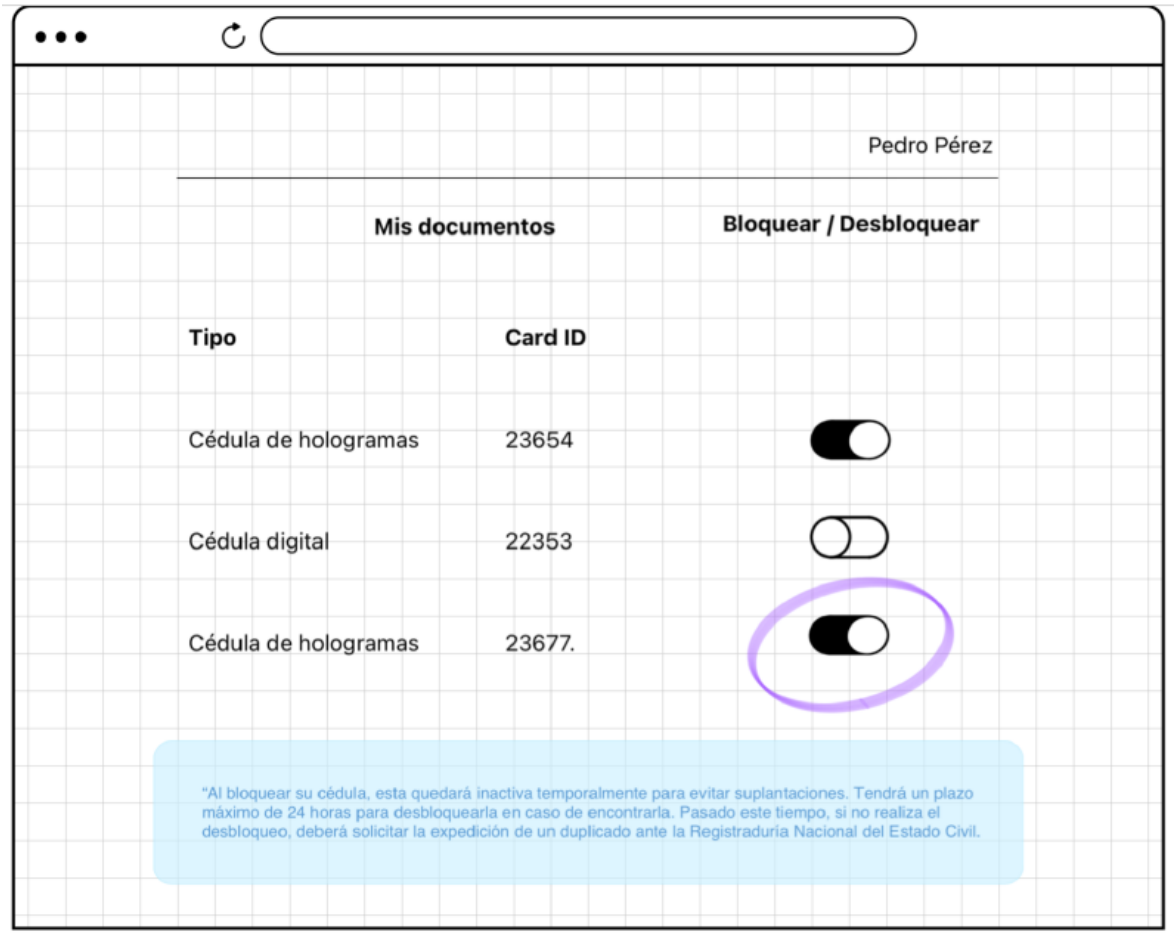
Posteriormente, se presenta una pantalla informativa con imágenes explicativas que orientan al usuario sobre cómo ubicar el número CARD ID en su cédula física. Esta orientación es esencial para continuar con el proceso, ya que el CARD ID es el elemento clave que identifica el plástico específico del documento que se desea gestionar.

Ilustración 12. Mockup 4 - Imágenes Explicativas



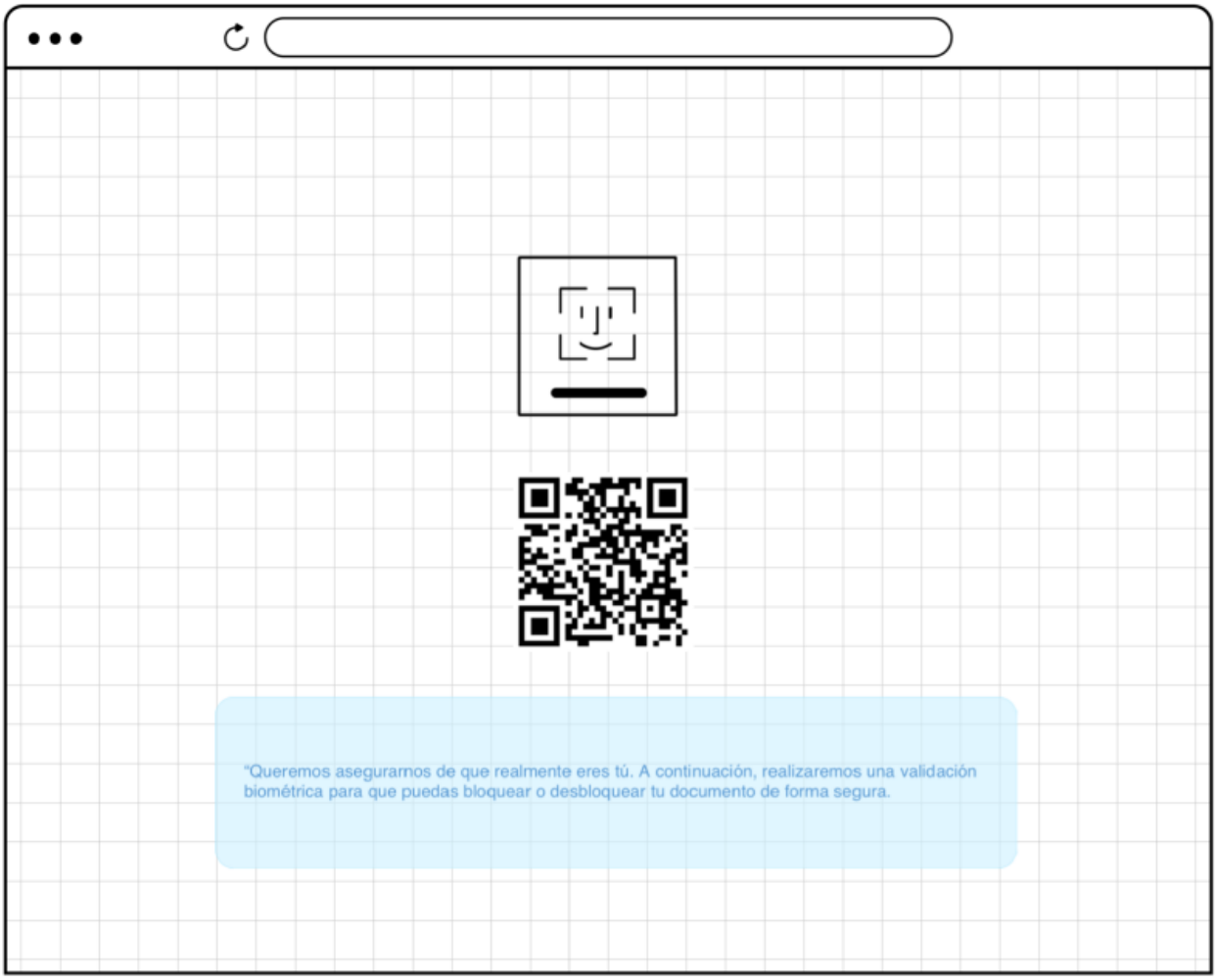
Una vez identificado el CARD ID, el sistema despliega el listado de documentos asociados al ciudadano, permitiéndole visualizar el tipo de documento (por ejemplo, cédula de hologramas o cédula digital), el número CARD ID correspondiente, y el estado actual del documento (activo o bloqueado). Junto a cada documento, el usuario encuentra los botones para ejecutar la acción deseada: bloquear o desbloquear. Esta pantalla también incluye un mensaje preventivo que indica que, una vez bloqueado el documento, el ciudadano dispondrá de un plazo de 24 horas para desbloquearlo en caso de recuperación. De lo contrario, deberá solicitar el duplicado del documento ante la Registraduría.

Ilustración 13. Mockup 5 - Listado de Documentos Asociados al Ciudadano



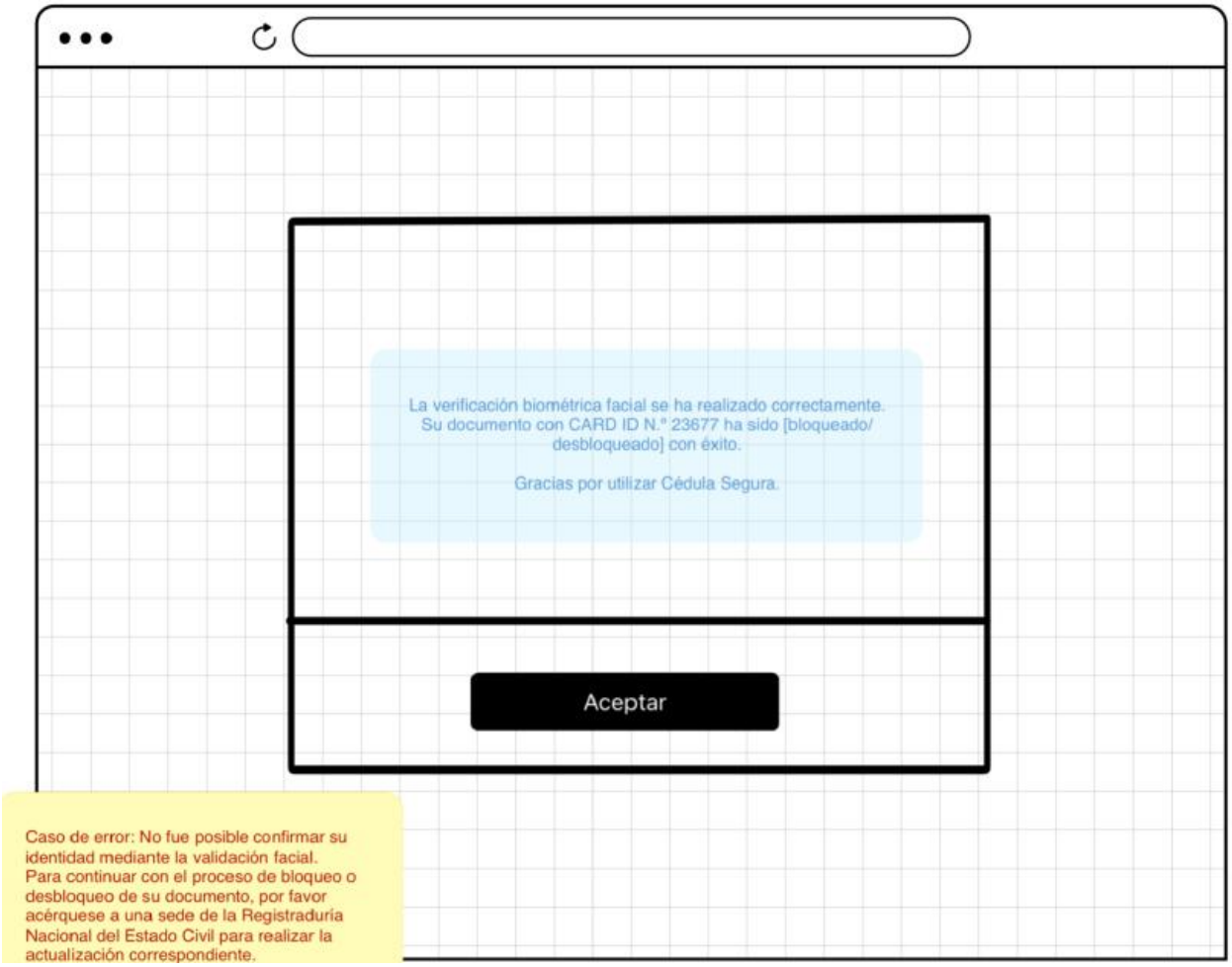
Una vez seleccionada la acción, el sistema activa el módulo de validación biométrica facial, solicitando al ciudadano que permita el acceso a su cámara para proceder con el reconocimiento facial. Esta etapa es fundamental para garantizar que solo el titular legítimo del documento pueda efectuar cambios sobre el estado de este.

Ilustración 14. Mockup 6 - Validación Biométrica



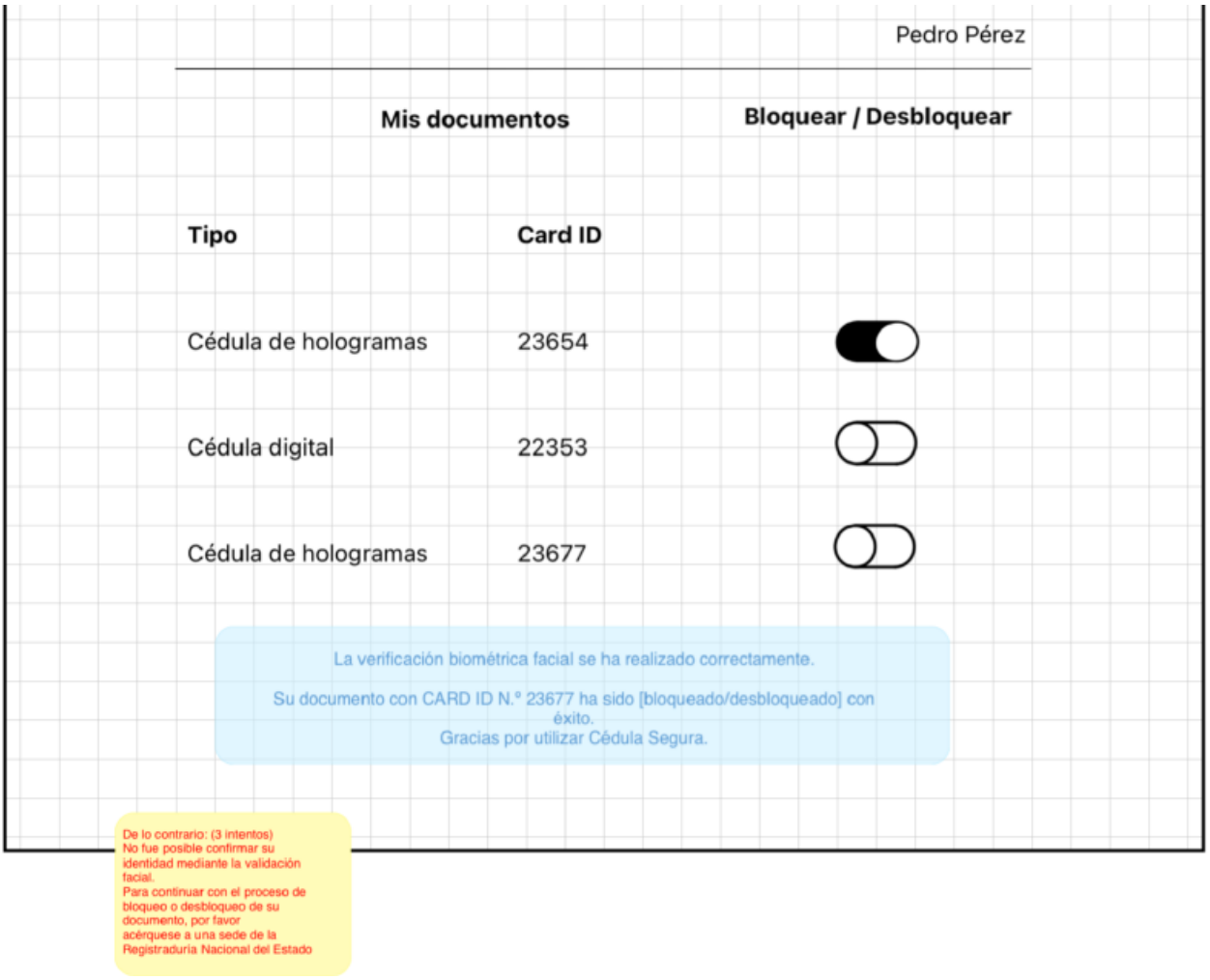
Si la validación es exitosa, se presenta un mensaje confirmando que el documento con el número CARD ID correspondiente ha sido bloqueado o desbloqueado exitosamente. En caso de fallos consecutivos en la validación, se informa al ciudadano que debe acudir a una sede de la Registraduría para realizar la actualización de sus datos biométricos.

Ilustración 15. Mockup 7 - Respuesta Validación Biométrica



Finalmente, el sistema retorna al usuario al listado de sus documentos, ya con el estado actualizado reflejado en tiempo real. Este flujo completo no solo representa una solución funcionalmente viable, sino que también garantiza una experiencia de usuario clara, segura y centrada en la prevención de la suplantación de identidad.

Ilustración 16. Mockup 8 - Listado de Documentos con su Estado Actualizado

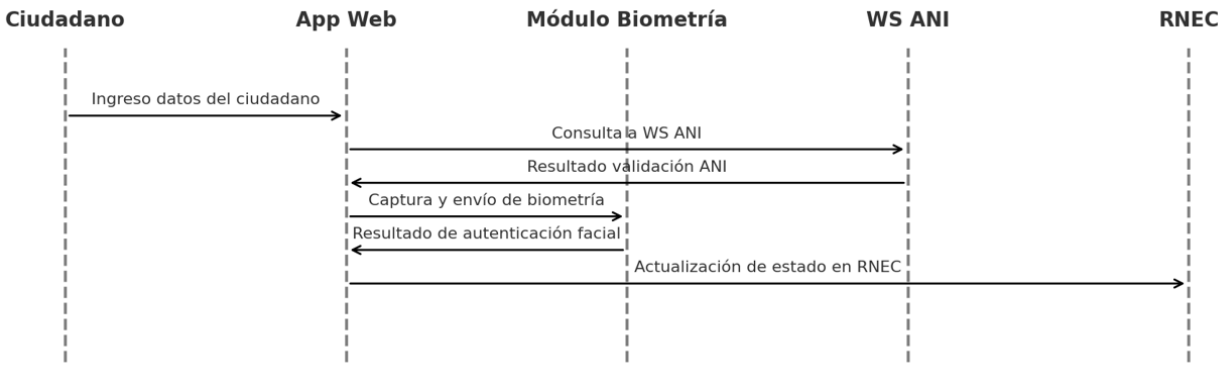


El prototipo desarrollado constituye un insumo visual y técnico clave para proyectar la viabilidad de implementación de la plataforma en un entorno real. Aunque fue construido en un contexto académico y simulado, los componentes, validaciones y flujos representados están diseñados para integrarse con los sistemas reales de la Registraduría Nacional del Estado Civil.

Para complementar la presentación del prototipo funcional y evidenciar la lógica operativa que sustenta cada uno de sus procesos, se presenta a continuación el diagrama de secuencia UML del sistema *Cédula Segura*. Este recurso gráfico ilustra, paso a paso, la

interacción entre el ciudadano, la plataforma digital, el servicio de validación biométrica facial, el Archivo Nacional de Identificación (ANI) y los sistemas internos de la Registraduría Nacional del Estado Civil. El diagrama permite visualizar el flujo lógico que sigue una solicitud de bloqueo o desbloqueo del documento, destacando los puntos clave de validación, autenticación y actualización del estado de este dentro del ecosistema institucional.

Ilustración 17. Diagrama de Secuencia UML



Pruebas Piloto y Validación

Durante el desarrollo del proyecto Cédula Segura se llevaron a cabo diversas validaciones funcionales y pruebas simuladas con el objetivo de evaluar el comportamiento del prototipo en condiciones cercanas al uso real. Estas pruebas se realizaron en un entorno académico, con usuarios de prueba y datos ficticios, respetando las restricciones legales en cuanto al acceso a bases institucionales como el Archivo Nacional de Identificación (ANI) y el sistema oficial de autenticación biométrica de la Registraduría Nacional del Estado Civil.

Las validaciones se centraron en comprobar la correcta ejecución del flujo completo del ciudadano dentro de la plataforma, desde el registro inicial y la verificación de datos personales, hasta el acceso al sistema, la autenticación biométrica facial y la posterior gestión del estado del documento. También se evaluó el sistema ante situaciones de error o uso

incorrecto, como el ingreso de información inválida o la omisión de pasos obligatorios. Los resultados funcionales demostraron que el prototipo opera de acuerdo con los requerimientos establecidos, ofreciendo un flujo claro, seguro y controlado.

Complementando las pruebas técnicas, se aplicó una encuesta de validación de experiencia de usuario a las personas que participaron en las pruebas piloto. Esta encuesta tuvo como propósito medir la percepción del ciudadano respecto a la facilidad de uso, claridad de los mensajes, diseño visual y utilidad general de la solución. Los resultados fueron altamente satisfactorios: más del 90 % de los participantes consideraron que la plataforma es fácil de usar y cumple con su propósito de forma clara y eficiente. Además, destacaron la utilidad de la solución como un mecanismo de prevención frente a la suplantación de identidad, y valoraron positivamente la experiencia de interacción con el sistema.

Este resultado no solo valida técnicamente el prototipo, sino que también confirma que su diseño está alineado con los principios de usabilidad, accesibilidad y confianza digital. La integración de esta retroalimentación en el proceso de validación permitió identificar oportunidades de mejora menores, que ya fueron consideradas en la fase de ajuste posterior a la prueba. Con base en estas pruebas funcionales y en la opinión directa de los usuarios, se concluye que la solución es viable y cumple con los criterios requeridos para una eventual implementación institucional.

Tabla 8. Bitácora de Pruebas

Fecha	Escenario de prueba	Resultado esperado	Resultado obtenido	Observaciones
20/05/2025	Registro con cédula y fecha válidas	El sistema valida con el ANI simulado y permite la creación de contraseña	La validación fue exitosa, se habilitó el campo para asignar contraseña	Se confirmó que el primer filtro de verificación funciona correctamente
21/05/2025	Ingreso de datos erróneos tres veces	Sistema bloquea el intento de registro y muestra mensaje indicando que debe acudir a una sede	Tras el tercer intento fallido, el flujo fue cerrado con mensaje preventivo	El bloqueo funciona correctamente como medida de seguridad
22/05/2025	Acceso al sistema y visualización de documentos	El ciudadano visualiza los documentos asociados, el estado y el CARD ID	La tabla se cargó correctamente con datos simulados	Flujo adecuado, se confirma que el sistema puede manejar múltiples documentos por usuario
23/05/2025	Bloqueo de documento con validación biométrica facial	El sistema solicita reconocimiento facial y actualiza el estado a 'Bloqueado'	Autenticación facial simulada fue exitosa y el estado cambió correctamente	Se validó el flujo completo con interacción de múltiples módulos
24/05/2025	Desbloqueo sin autenticación biométrica	El sistema deniega la acción e informa que se requiere validación facial previa	El intento fue rechazado con mensaje preventivo	Se confirmó que no es posible ejecutar acciones sensibles sin validación previa

Documentación y evaluación final

En la fase final del proyecto se procedió a la documentación integral y evaluación del desarrollo de la plataforma digital Cédula Segura, con el propósito de valorar su pertinencia técnica, funcionalidad operativa y su potencial aplicación institucional en el contexto colombiano. El trabajo realizado permitió consolidar un prototipo funcional que simula el proceso de bloqueo y desbloqueo del documento de identidad mediante el uso del número CARD ID y la autenticación biométrica facial, mecanismos diseñados para fortalecer los procesos de verificación de identidad y reducir el riesgo de suplantación.

El sistema se estructuró sobre una arquitectura cliente-servidor distribuida en tres capas: presentación, lógica de negocio y almacenamiento de datos. Esta estructura favorece la interoperabilidad entre el ciudadano, la plataforma y la base de datos simulada del Archivo Nacional de Identificación (ANI). Para ello, se desarrollaron diagramas técnicos, flujogramas, esquemas de navegación y un diagrama de secuencia UML, todos orientados a describir con precisión el comportamiento del sistema y sus mecanismos de validación. Asimismo, se

diseñaron mensajes informativos y preventivos con enfoque pedagógico y de seguridad, garantizando una experiencia de usuario clara, coherente y orientada a la confianza digital.

Durante el proceso de evaluación, se constató el cumplimiento de los objetivos específicos planteados en la propuesta inicial. Se logró diseñar e implementar un prototipo web funcional con capacidad de simular el flujo completo de gestión del documento de identidad. Se integraron mecanismos de validación doble, datos personales validados con el ANI y autenticación biométrica facial, mediante herramientas de simulación, dada la restricción de acceso a plataformas oficiales. También se habilitó la consulta del estado del documento por parte del usuario y se desarrollaron pruebas piloto orientadas a evaluar la usabilidad, accesibilidad y percepción de seguridad del sistema. Estas pruebas reflejaron una alta aceptación por parte de los usuarios, así como oportunidades de mejora que fueron integradas en las iteraciones finales del diseño.

No obstante, el desarrollo del prototipo enfrentó ciertas limitaciones técnicas propias de un entorno académico. Entre ellas se destacan la imposibilidad de acceder a la base de datos oficial del ANI y al sistema real de autenticación biométrica de la Registraduría Nacional del Estado Civil, así como la carencia de un entorno estatal de pruebas para realizar validaciones reales. Estas restricciones obligaron a trabajar con simulaciones técnicas y bases de datos estructuradas en formato JSON, sin comprometer la legalidad ni la confidencialidad de la información. A pesar de ello, la plataforma logró replicar con fidelidad los flujos y procesos esperados en una implementación institucional real.

El valor del proyecto radica en su propuesta de solución tecnológica aplicada a una problemática social creciente como lo es la suplantación de identidad. La plataforma no solo representa una herramienta de prevención, sino también un avance en la transformación digital del servicio público. Permite al ciudadano gestionar de manera autónoma y segura el estado de su documento físico, y a las instituciones contar con un mecanismo actualizado de verificación

documental. Su enfoque se alinea con los principios del gobierno digital, la interoperabilidad y la protección de datos personales.

Análisis de Costos

El análisis de costos evidencia la viabilidad técnica, operativa y económica de la solución propuesta, basada en una estructura financiera equilibrada y diseñada bajo principios de sostenibilidad, eficiencia y alto impacto institucional. La Registraduría Nacional del Estado Civil, además de ser la entidad beneficiaria, cumple un papel clave en la ejecución del sistema, ya que cuenta con áreas técnicas especializadas que pueden apoyar los procesos de desarrollo, implementación y mantenimiento. Adicionalmente, posee las bases de datos que constituyen los pilares del funcionamiento de la plataforma, como el sistema de biometría, el Archivo Nacional de Identificación (ANI) y el número CARD ID. Esto permite optimizar los recursos disponibles, reducir los costos de integración y garantizar que la solución se desarrolle sobre una infraestructura estatal ya existente, segura y controlada.

Costos directos

Incluyen todos los recursos necesarios para el diseño, desarrollo y ejecución del sistema, entre ellos:

Capacidad de desarrollo (mano de obra técnica):

Comprende la contratación de desarrolladores backend y frontend, DevOps, QA testers, diseñadores UX/UI, analistas funcionales y gestores de proyecto. Estos perfiles son fundamentales para garantizar el cumplimiento de los requerimientos funcionales, técnicos y de experiencia de usuario de la plataforma. $466.200.000

Licencias de software:

Considera la adquisición de APIs de reconocimiento facial, herramientas de desarrollo

colaborativo, motores de base de datos, licencias SSL y software de seguridad, necesarios para garantizar la interoperabilidad, integridad y protección de los datos del sistema. $115.000.000 COP

Datacenter, hosting y almacenamiento:

Cubre el uso de servidores en centros de datos seguros, alojamiento en la nube y servicios de respaldo de información. Este componente garantiza la disponibilidad, escalabilidad y continuidad operativa de la plataforma. $25.500.000 COP

Mantenimiento del sistema:

Incluye soporte técnico, aplicación de parches, monitoreo del rendimiento, mejoras funcionales y actualizaciones necesarias durante el primer año de operación. $200.000.000 COP

Coordinación del proyecto:

Se refiere a la planificación, control y supervisión técnica del desarrollo, incluyendo gestión de cronogramas, cumplimiento de hitos y articulación entre los equipos de trabajo. $35.000.000 COP

Comunicaciones internas y externas:

Incluye reuniones de seguimiento, uso de plataformas de colaboración, documentación técnica y canales de comunicación entre los diferentes actores del proyecto. $12.500.000 COP

Desarrollo del prototipo:

Consiste en el diseño y construcción del modelo funcional de la plataforma, con pruebas preliminares de integración con las bases de datos simuladas del ANI y del sistema de

biometría, para validar su viabilidad técnica antes de la implementación definitiva.

$85.000.000 COP

Implementación del sistema:

Cubre el despliegue de la solución en el entorno institucional, pruebas reales con las bases de datos oficiales y configuración final para su entrada en funcionamiento.

$35.000.000 COP

Subtotal costos directos: $841.700.000 COP

Costos fijos y gastos generales

Estos costos, aunque no se presentan como una categoría separada, están integrados dentro de los rubros anteriores, principalmente en mantenimiento, coordinación y comunicaciones. Incluyen servicios institucionales, soporte administrativo, infraestructura física y operación logística básica.

Costos de inversión indirectos

Imprevistos:

Fondo de reserva para cubrir ajustes técnicos, emergencias, licencias complementarias o requerimientos normativos que puedan surgir durante el desarrollo del sistema.

$50.000.000 COP

Capital de trabajo

Capital de trabajo inicial:

Recursos destinados a cubrir la operación del sistema en sus primeros meses de funcionamiento, incluyendo soporte al usuario, pagos operativos puntuales y gastos logísticos mientras se estabiliza el uso de la plataforma. $50.000.000 COP

Tabla 9.Resumen de Inversión

Tipo de costo	Valor estimado (COP)
Costos directos	$ 841.700.000
Costos indirectos	$ 50.000.000
Capital de trabajo	$ 182.500.265
Total del proyecto	**$ 1.074.200.265**

A continuación, se presenta la tabla con la propuesta de costos del proyecto, en la cual se especifican las categorías presupuestales, sus respectivos valores y las justificaciones asociadas. Estas explicaciones permiten comprender la función que cumple cada componente dentro del proyecto, evidenciando su pertinencia y relación directa con los objetivos funcionales, técnicos y operativos de la plataforma.

Tabla 10.Propuesta Costos Proyecto

Categoría	Costo estimado (COP)	Justificación
Capacidad de desarrollo (Mano de obra técnica)	**$ 466.200.000**	Desarrollador Backend (Senior) Desarrollador Frontend (Mid) Diseñador UI/UX QA / Tester DevOps / Infraestructura Project Manager / Scrum Master Analista funcional / BA

Categoría	Costo estimado (COP)	Justificación
Licencias de software	$ 115.000.000	Uso de APIs de reconocimiento facial, herramientas de desarrollo y motor de base de datos, licencias ssl, equipos de computo
Datacenter, Hosting y almacenamiento	$ 25.500.000	Costo promedio de servidores en datacenter y almacenamiento en nube (anual).
Mantenimiento del sistema	$ 200.000.000	Horas técnicas para soporte y actualizaciones mensuales (anual).
Coordinación del proyecto	$ 35.000.000	Supervisión técnica y planificación del proyecto.
Comunicaciones internas y externas	$ 12.500.000	Costos asociados a reuniones, software colaborativo y documentación.
Desarrollo del prototipo	$ 85.000.000	Diseño inicial del sistema, pruebas y documentación técnica.
Implementación del sistema	$ 35.000.000	Despliegue final en entorno institucional con pruebas reales.
Imprevistos	$ 50.000.000	Reserva para problemas técnicos o necesidades emergentes.
Capital de trabajo	$ 50.000.000	Fondo inicial para recursos operativos menores o soporte inicial.

Enfoque de Rentabilidad Institucional

El análisis de costos de la solución propuesta permite evidenciar su viabilidad técnica, operativa y económica dentro del contexto institucional de la Registraduría Nacional del Estado Civil. La plataforma digital para el bloqueo y desbloqueo del documento de identidad, diseñada con base en la validación del número CARD ID, autenticación biométrica facial y conexión con el sistema ANI, responde a una necesidad crítica del Estado colombiano relacionada con la prevención de la suplantación de identidad y el fortalecimiento de los mecanismos de verificación ciudadana. Si bien esta propuesta no está concebida como un producto comercial ni se proyecta para generar ingresos directos a través de su uso, su valor institucional es

significativo, tanto en términos de eficiencia operativa como de fortalecimiento de la seguridad documental y de la confianza en los servicios públicos.

En ese sentido, la inversión estimada para el desarrollo e implementación de la plataforma asciende a $1.074.200.265 COP, monto que incluye tanto los costos directos asociados al desarrollo técnico (como la contratación de perfiles especializados, licencias de software, infraestructura de almacenamiento, mantenimiento del sistema y gestión del proyecto), como los costos indirectos relacionados con posibles imprevistos legales o técnicos, y los recursos asignados como capital de trabajo para su puesta en marcha. Aunque tradicionalmente los análisis de costos se enfocan en establecer una tasa de retorno financiera, en proyectos como el presente, cuyo objetivo es institucional y social, el enfoque debe centrarse en el valor público generado por la solución y no en utilidades comerciales. En este contexto, se sugiere aplicar una tasa social mínima aceptable de retorno del 9 % anual, recomendada por entidades como el Departamento Nacional de Planeación (DNP) para proyectos estatales orientados al fortalecimiento del servicio público. Esta tasa no representa rentabilidad financiera, sino la eficiencia del gasto frente al valor generado en términos de mejora del servicio, protección de derechos y optimización de recursos institucionales.

Considerando esta lógica, es razonable proyectar que la implementación de la plataforma podría generar ahorros anuales estimados en más de $1.500 millones, como resultado de la reducción de fraudes por suplantación, litigios, rectificaciones y trámites operativos que actualmente representan una carga significativa para la Registraduría. Estos beneficios, comparados con la inversión proyectada, indican que la rentabilidad institucional y social del sistema es no solo aceptable, sino también altamente favorable.

Adicionalmente, es importante tener en cuenta que la Registraduría Nacional del Estado Civil ya presta actualmente el servicio de consulta al Archivo Nacional de Identificación (ANI) mediante convenios y contratos con entidades públicas y privadas, a través de los cuales se

generan ingresos sostenibles. En el año 2024, se realizaron 108.057.238 consultas al ANI, con un valor unitario de $98,41 COP por consulta, lo que representó ingresos superiores a los $10.635 millones. En este escenario, la plataforma desarrollada introduce una funcionalidad adicional de alto valor: la validación del estado físico del documento (activo o bloqueado), función especialmente útil para entidades como notarías, bancos, EPS y otras instituciones que requieren verificar no solo la identidad del ciudadano, sino también la vigencia del documento físico que porta.

Por lo tanto, si se proyectara un ajuste mínimo de $10 COP adicionales por consulta ANI, como resultado de incluir esta funcionalidad dentro del servicio actual, y se mantuviera el mismo volumen de consultas, se generarían ingresos complementarios por un valor aproximado de $1.080.572.380 COP anuales. Este valor supera la inversión estimada para la implementación de la plataforma, lo que demuestra que, más allá de su impacto operativo y social, la solución también representa una oportunidad real de optimizar y ampliar los servicios institucionales existentes sin necesidad de crear nuevos modelos de negocio ni incrementar significativamente los costos para el usuario final.

Desde esta perspectiva, la sostenibilidad del sistema se fortalece no solo por su capacidad de generar valor social y reducir riesgos, sino también por su potencial para consolidarse como una herramienta estratégica que aporta eficiencia, seguridad y modernización a los procesos de verificación ciudadana. A esto se suma el hecho de que la Registraduría ya cuenta con las bases de datos necesarias (ANI, CARD ID y biometría facial), así como con las competencias técnicas y jurídicas para llevar a cabo la integración real del sistema, lo cual minimiza significativamente los costos de operación a largo plazo y hace del proyecto una iniciativa integralmente viable, tanto desde el punto de vista económico como institucional.

Plan de Implementación

El presente plan tiene como propósito guiar la puesta en marcha del sistema Cédula Segura en la Registraduría Nacional del Estado Civil, transitando de un entorno académico simulado a una solución operativa real. La plataforma permitirá al ciudadano bloquear y desbloquear su cédula en caso de pérdida o hurto, usando el número CARD ID y la autenticación biométrica facial.

La implementación del proyecto *Cédula Segura* está concebida como un proceso progresivo que parte de una validación institucional y técnica hasta llegar al despliegue oficial del sistema en los canales digitales de la Registraduría Nacional del Estado Civil. En primer lugar, se contempla una etapa de validación institucional y análisis de viabilidad, en la que se socializa el proyecto ante las áreas técnicas, jurídicas y tecnológicas de la entidad. En esta fase inicial se evalúa la compatibilidad del sistema con las bases de datos existentes como el Archivo Nacional de Identificación (ANI), la base del número CARD ID y el sistema de biometría facial, se determina la viabilidad legal del uso del CARD ID como identificador para activar o desactivar el documento de identidad. Con base en este análisis, se espera obtener una aprobación preliminar que permita asignar un equipo técnico conjunto para acompañar las siguientes fases.

Superada esta etapa, se da paso a un proceso de desarrollo técnico y ajustes operativos, en el cual se revisa la arquitectura del prototipo, se adapta el código fuente a los entornos institucionales y se establecen los mecanismos de integración con las plataformas de validación facial y de consulta del ANI. También se rediseñan algunos aspectos visuales de la interfaz de usuario para alinearla con la imagen institucional de la Registraduría y se incorpora un módulo de trazabilidad que registre las acciones realizadas por cada ciudadano, garantizando control y auditoría en tiempo real.

Posteriormente, se ejecuta una fase de pruebas piloto controladas, que permite poner a prueba el sistema en un entorno real pero restringido. En esta etapa participan tanto usuarios internos de la Registraduría como ciudadanos voluntarios, quienes acceden a la plataforma para realizar procesos de bloqueo y desbloqueo de manera simulada. Esta fase permite evaluar la estabilidad de la herramienta, los tiempos de respuesta del sistema, la efectividad de la validación biométrica y la comprensión del flujo de uso por parte del ciudadano. A partir de los resultados obtenidos, se recogen incidentes, observaciones y sugerencias para la mejora continua.

Con base en dicha retroalimentación, se avanza hacia una etapa de ajustes post-piloto e integración definitiva. En esta fase se corrigen los errores detectados durante la prueba piloto, se refuerzan los mecanismos de seguridad de la información como el cifrado de datos personales y las validaciones cruzadas y se entrena al personal técnico y de soporte que estará a cargo de la operación del sistema una vez esté en funcionamiento. Esta preparación es clave para garantizar una respuesta eficiente a posibles incidencias ciudadanas.

Finalmente, el proyecto culmina con el lanzamiento oficial y despliegue progresivo de la plataforma. Esta etapa contempla la publicación del sistema en los canales oficiales de la Registraduría, acompañada de una campaña de divulgación digital que eduque a la ciudadanía sobre cómo utilizar la herramienta, cuándo aplicarla y qué beneficios ofrece. Al mismo tiempo, se inicia la integración progresiva con las entidades públicas y privadas que ya utilizan la consulta al ANI, permitiéndoles visualizar no solo si un ciudadano está identificado correctamente, sino también si el CARD ID consultado corresponde a un documento activo o ha sido reportado como bloqueado. Este despliegue se acompaña de un monitoreo permanente de transacciones y de la disposición de un canal de soporte técnico para atender inquietudes o fallos operativos.

Ilustración 18. Plan de Implementación de Cédula Segura en la RNEC

Elaboración Propia

Recursos Necesarios

Para garantizar una implementación exitosa de la plataforma Cédula Segura, es necesario disponer de recursos estratégicos que abarquen los aspectos técnicos, humanos, tecnológicos, logísticos y comunicacionales del proyecto. La siguiente tabla resume los recursos requeridos para la puesta en marcha y operación del sistema dentro del ecosistema tecnológico de la Registraduría Nacional del Estado Civil:

Tabla 11. Recursos Requeridos

Categoría	Descripción del recurso necesario
Talento humano	Equipo interdisciplinario conformado por desarrolladores, diseñadores UX/UI, expertos en ciberseguridad, profesionales jurídicos y personal de soporte técnico.
Tecnología	Servidores seguros, certificación SSL, APIs de autenticación biométrica facial, y conectores para la interoperabilidad con los sistemas ANI y CARD ID.
Infraestructura	Alojamiento en la nube institucional o en centros de datos de la Registraduría, con alta disponibilidad, escalabilidad y respaldo.
Comunicación	Desarrollo de materiales pedagógicos, tutoriales interactivos, videos explicativos y campañas digitales de sensibilización ciudadana.
Formación y soporte	Capacitación a funcionarios encargados de la operación y atención al usuario, manuales internos y protocolos de respuesta técnica.

Actores Involucrados y sus Responsabilidades

La implementación de Cédula Segura requiere la articulación de diversos actores institucionales y técnicos que, desde sus competencias, contribuyan al éxito del proyecto. Cada uno desempeña un rol específico en la planeación, desarrollo, operación y apropiación ciudadana de la plataforma.

Tabla 12. Actores Involucrados y Responsabilidades

Actor	Responsabilidad
Registraduría Nacional del Estado Civil	Gestión del entorno institucional y coordinación del proyecto.
Equipo de desarrollo	Adaptación técnica, pruebas, mejoras e integración.
Entidades con convenio ANI	Validación y consulta del CARD ID para prevenir fraudes.
Ciudadanos usuarios	Uso adecuado del sistema y retroalimentación en su fase operativa.

Conclusiones

El desarrollo del presente proyecto de grado permitió dar una respuesta concreta y viable a la pregunta formulada en la etapa inicial del trabajo: ¿Cómo la implementación de una plataforma digital para bloquear documentos de identificación física extraviados o hurtados, mediante el número único de identificación (CARD ID), puede contribuir a reducir significativamente los riesgos de suplantación de identidad física en Colombia? A través del diseño, simulación y validación del prototipo Cédula Segura, se logró demostrar que el uso del CARD ID como identificador único del plástico, complementado con un proceso de validación biométrica facial y una interfaz ciudadana accesible, constituye una herramienta efectiva para disminuir las oportunidades de uso fraudulento de documentos perdidos o robados.

Uno de los principales aportes de esta solución es que responde a una necesidad real y urgente que actualmente no está cubierta en el país: el bloqueo digital del documento de identidad físico en caso de pérdida o hurto. En la actualidad, el ciudadano no cuenta con un mecanismo oficial que le permita desactivar el plástico de su cédula, lo que deja una ventana de vulnerabilidad entre el momento de la pérdida y la posible utilización fraudulenta del documento. El único soporte que muchas personas utilizan es el denuncio de pérdida ante la Policía Nacional, que, si bien antes era obligatorio, ya no lo es desde la entrada en vigor de la Ley Anti trámites. Esta normativa eliminó la exigencia de presentar denuncio para la mayoría de los trámites, lo que ha provocado que muchos ciudadanos no lo realicen, dejando como único rastro un soporte informal que carece de valor vinculante ante entidades públicas o privadas. En este contexto, Cédula Segura ofrece un canal oficial, trazable y en tiempo real, que podría reemplazar al denuncio como prueba de la pérdida del documento, fortaleciendo la protección de la identidad ciudadana.

La solución permite al ciudadano bloquear temporalmente su cédula de ciudadanía desde una plataforma digital, generando una alerta inmediata que marca el documento como

inactivo. Esto rompe con la brecha institucional actual y previene que el plástico extraviado sea utilizado en trámites presenciales como apertura de cuentas bancarias, compras a crédito, retiros financieros o firmas fraudulentas. Asimismo, permite el desbloqueo en caso de recuperación del documento dentro de un plazo de 24 horas, otorgando al titular el control directo sobre su documento.

Una de las principales fortalezas del proyecto radica en que la solución no requiere crear nuevas bases de datos o sistemas externos, sino aprovechar al máximo la infraestructura ya existente en la Registraduría Nacional del Estado Civil. Actualmente, esta entidad dispone del Archivo Nacional de Identificación (ANI), que almacena datos biográficos; del número CARD ID, que identifica de forma única cada plástico físico expedido; y del sistema de biometría facial, que permite validar la identidad del ciudadano de manera segura. El proyecto Cédula Segura se enfoca en articular estos recursos a través de una interfaz amigable y accesible, promoviendo la interoperabilidad institucional y generando mayor valor público a partir de bases de datos que ya están en operación.

Adicionalmente, se identificó un beneficio estratégico para las entidades que actualmente consultan el ANI como servicio: las entidades del Estado (de forma gratuita) y las empresas privadas (mediante convenio de pago). Estas organizaciones podrían mejorar sus procesos de verificación documental si, además del número de cédula, pudieran consultar el CARD ID vigente. Esto permitiría confirmar no solo que un ciudadano está identificado correctamente, sino que el documento físico presentado no ha sido reportado como bloqueado, lo cual fortalecería los mecanismos de prevención de fraude y suplantación en sectores como el financiero, notarial, educativo, entre otros.

En cuanto al cumplimiento de los objetivos, el proyecto logró con éxito el diseño e implementación de un prototipo funcional, con capacidad de simular el flujo completo de registro, autenticación, bloqueo, desbloqueo y consulta del estado del documento. La validación

con el ANI se emuló mediante estructuras locales, se integró un sistema de autenticación biométrica facial simulado y se realizaron pruebas piloto que evidenciaron altos niveles de comprensión y aceptación por parte de los usuarios.

Desde el punto de vista metodológico, se optó por un enfoque proyectivo con diseño no experimental, lo cual permitió construir una solución aplicable a un problema real. Las simulaciones técnicas utilizadas suplieron las limitaciones de acceso a entornos oficiales, sin comprometer la lógica funcional ni la coherencia del diseño. Las principales restricciones fueron de tipo técnico y legal, como la imposibilidad de acceder directamente a los entornos del ANI y del sistema biométrico oficial. No obstante, estas limitaciones fueron previstas y gestionadas adecuadamente dentro del marco académico.

En un país donde la identidad es el pilar de acceso a derechos, servicios y oportunidades, Cédula Segura se configura como un proyecto con profundo impacto social, ya que coloca al ciudadano en el centro de la solución, brindándole control, autonomía y protección frente a una amenaza real como lo es la suplantación de identidad. Además, es un proyecto sostenible, en tanto aprovecha la infraestructura tecnológica ya existente en la Registraduría Nacional del Estado Civil sin generar sobrecostos, y promueve el uso eficiente de los recursos públicos. Este trabajo demuestra cómo la ingeniería industrial, desde su enfoque integral y sistémico, puede contribuir significativamente a la innovación institucional, no solo optimizando procesos, sino también desarrollando soluciones tecnológicas viables que transformen la experiencia ciudadana. La construcción de esta plataforma permitió aplicar conocimientos de gestión de proyectos, análisis de procesos, diseño de sistemas y experiencia de usuario, con el propósito de generar un bien público que trascienda el aula y pueda integrarse en la vida cotidiana de los colombianos.

Finalmente, las proyecciones del proyecto son amplias. Cédula Segura puede integrarse a la plataforma de servicios digitales de la Registraduría Nacional del Estado Civil y

ampliarse a su uso en dispositivos móviles. Su funcionalidad puede ser adaptada para brindar soporte a procesos de verificación en tiempo real ante otras entidades del Estado, o ser adoptada por instituciones privadas que requieran validar la vigencia del documento físico. También puede servir como base para futuras investigaciones relacionadas con identidad digital, interoperabilidad y ciberseguridad.

En conclusión, el proyecto Cédula Segura representa una propuesta innovadora, técnicamente viable y socialmente necesaria, que puede contribuir de manera significativa a cerrar una brecha actual en el sistema de identificación colombiano. Su implementación fortalecería la confianza institucional, reduciría los casos de suplantación de identidad física, y mejoraría la protección de los derechos de los ciudadanos frente al uso indebido de sus documentos personales.

Recomendaciones Futuras para la Implementación Institucional

A partir de los resultados obtenidos y la viabilidad funcional demostrada a lo largo del desarrollo de este proyecto, se considera que la plataforma Cédula Segura tiene el potencial de ser implementada de manera oficial por la Registraduría Nacional del Estado Civil. Para ello, se sugiere que, como primer paso, se formalice una fase de prueba piloto institucional que permita validar el prototipo en un entorno real, bajo la supervisión de las áreas técnicas y jurídicas de la entidad. Esta fase debería incluir la integración directa con los sistemas de autenticación biométrica existentes, el servicio de validación de datos del Archivo Nacional de Identificación (ANI) y la base oficial del número CARD ID, con el fin de evaluar la interoperabilidad y seguridad en condiciones reales de operación.

Es indispensable que la plataforma se adapte a los lineamientos de seguridad de la información exigidos por la entidad, cumpliendo con las disposiciones establecidas por la Ley 1581 de 2012 y los marcos técnicos de referencia como la norma ISO 27001. En este sentido, la aplicación deberá someterse a pruebas de penetración, validación de vulnerabilidades y revisión de políticas de cifrado de datos personales, especialmente en los procesos que involucran captura de datos biométricos. Paralelamente, sería pertinente considerar la ampliación del campo de validación a las entidades que ya cuentan con convenios de consulta con la Registraduría, permitiéndoles verificar no solo la validez del número de cédula, sino también si el documento físico consultado se encuentra activo o ha sido reportado como bloqueado. Esta funcionalidad adicional sería de gran utilidad para prevenir fraudes en sectores como la banca, las notarías, las EPS y otras entidades que dependen de procesos presenciales de validación de identidad.

En términos institucionales, sería recomendable gestionar alianzas con entidades como el Ministerio TIC, la Superintendencia de Industria y Comercio y la Policía Nacional, con el fin de garantizar el respaldo normativo y operativo del sistema, y su reconocimiento como un canal

legítimo de protección de la identidad ciudadana. Asimismo, la Registraduría podría adoptar una estrategia de inclusión digital que facilite el acceso a la plataforma en zonas rurales o con baja conectividad, por medio de kioscos digitales o aplicativos móviles de bajo consumo.

Para fortalecer la cobertura del sistema, se sugiere también explorar mecanismos biométricos alternativos, como la validación por huella digital, para ampliar la accesibilidad del servicio a personas que puedan presentar limitaciones en el reconocimiento facial. Finalmente, sería pertinente evaluar la posibilidad de incorporar este procedimiento de bloqueo como una medida formalmente reconocida por la Registraduría, a través de un acto administrativo que establezca su validez legal como soporte en caso de pérdida o suplantación, permitiendo que el ciudadano tenga un respaldo institucional más allá del simple denuncio ante la Policía, el cual dejó de ser obligatorio con la Ley Anti trámites.

La implementación de estas recomendaciones permitirá que Cédula Segura no solo evolucione de un prototipo académico a una solución institucional efectiva, sino que también represente un avance tangible en la modernización del sistema de identificación colombiano, en línea con los principios de seguridad, eficiencia y servicio al ciudadano.

Referencias Bibliográficas

Aguirre, M. A. (2018). Legislación comparada sobre protección de datos biométricos en América Latina y Europa. *Revista de Derecho y Tecnología*, 25(1), 45–63.

Aratek. (s.f.). *How biometrics is improving security in Africa*. https://www.aratek.co/es/news/how-biometrics-is-improving-security-in-africa

Ardito, L., Messeni Petruzzelli, A., Dezi, L., & Castellano, S. (2021). Transformación digital e innovación sostenible: una revisión. *Sostenibilidad*, 13(19), 10727. https://doi.org/10.3390/su131910727

Bernal Torres, C. A. (2016). *Metodología de la investigación: administración, economía, humanidades y ciencias sociales*.

Bieser, J. C., & Hilty, L. M. (2018). Evaluación de los efectos ambientales indirectos de las tecnologías de la información y la comunicación (TIC): Una revisión sistemática de la literatura. *Sustainability*, 10(8), 2662. https://doi.org/10.3390/su10082662

Biometría Aplicada. (s.f.). *Estos países han adoptado el uso de datos biométricos*. https://biometriaaplicada.com/estos-paises-han-adoptado-el-uso-de-datos-biometricos

Congreso de la República de Colombia. (2022). *Proyecto de ley sobre suplantación de identidad en Colombia*.

Cruz, N. (2001). *Métodos de diseño: estrategias para el diseño de productos*.

Dijin. (2020). *Informe sobre delitos cibernéticos y suplantación de identidad en Colombia*. Dirección de Investigación Criminal e Interpol.

El País. (2025, marzo 25). México implementará la CURP con foto y huellas dactilares para facilitar la búsqueda de personas desaparecidas. https://elpais.com/mexico/2025-03-25/mexico-implementara-la-curp-con-foto-y-huellas-dactilares-para-facilitar-la-busqueda-de-personas-desaparecidas.html

Flórez Rojas, M. L., & Camelo Pimienta, A. M. (2023). Tecnologías de reconocimiento facial en Colombia: Análisis comparativo en relación con la protección de datos. *Revista Ius et Praxis*, 29(1), 3–26.

Galvis, L. F. (2023). Prevención de la suplantación de identidad con huellas de látex en productos digitales del sector bancario en Colombia. Universidad de los Andes.

García Salazar, W. A., Rodríguez Montero, P. A., & Torres Figueroa, D. S. (2014). Identificación biométrica de patrones faciales en multiplataforma bajo arquitectura cliente-servidor. Universidad Piloto de Colombia.

García Silva, C. E., & Mazón Loaiza, J. D. (2024). El reconocimiento facial como instrumento de investigación y prevención del delito. *Anatomía Digital*, 7(2.2), 274–291. https://doi.org/10.33262/anatomiadigital.v7i2.2.3255

Gimeno Hernández, R. (2010). *Estudio de técnicas de reconocimiento facial*. Departamento de Procesado de Señal y Comunicaciones, Barcelona.

Golembiewski, B., & Sick, N. (2020). La digitalización como motor de una economía circular más sostenible: Evidencia de Alemania. *Journal of Cleaner Production*, 123, 127061. https://doi.org/10.1016/j.jclepro.2020.127061

Hincapié, C. A. (2023). Suplantación de identidad: Una mirada desde el derecho comparado. Universidad Nacional de Colombia.

IEEE. (2022). *Estudios en ciberseguridad y protección de identidad: Implementaciones en América Latina*. Transacciones IEEE sobre seguridad de la información.

Ley 1581 de 2012. (31 de agosto). Por la cual se dictan disposiciones generales para la protección de datos personales. *Diario Oficial*, n.° 48.587.

Lerma Kirchner, A. E. (2017). *Desarrollo de productos: una visión integral*.

Martínez, R. J. (2021). La evolución de la biometría facial y su impacto en la seguridad digital. *Revista de Innovación Tecnológica*, 34(2), 78–91.

Monastersky, R., & Salimbeni, H. (2020). *Introducción al robo de identidad*. Editorial Jurídica Panamericana.

Organización de las Naciones Unidas (ONU). (2022). *Monitor mundial de residuos electrónicos 2022*. https://ewastemonitor.info

Pardo Morcote, J. D. (2020). Reconocimiento facial en tiempo real orientado a videollamadas o live stream para autenticar identidades durante una audiencia legal. Universidad Santo Tomás Seccional Tunja.

Pedroza Manga, R. E. (2019). Diseño e implementación de un sistema de biometría facial para la búsqueda e identificación de personas desaparecidas en Colombia. Universidad de Cartagena.

Registro Nacional de Identificación y Estado Civil (RENIEC). (2015). *Identidad digital: La identificación desde los registros parroquiales al DNI electrónico*. RENEC.

Saavedra, R., & Astolfi, M. (2015). *Modernización de los registros civiles y estrategias de gobierno electrónico en Latinoamérica*. Editorial Universitaria del Perú.

Torres, A., & Vargas, M. (2019). Suplantación de identidad digital, una realidad económica en Colombia. Universidad Javeriana.

Yrivarren, J. (2015). *Identidad digital y el desarrollo del DNI electrónico en Latinoamérica*. RENIEC.

Manual del Ciudadano: Plataforma Digital Cédula Segura

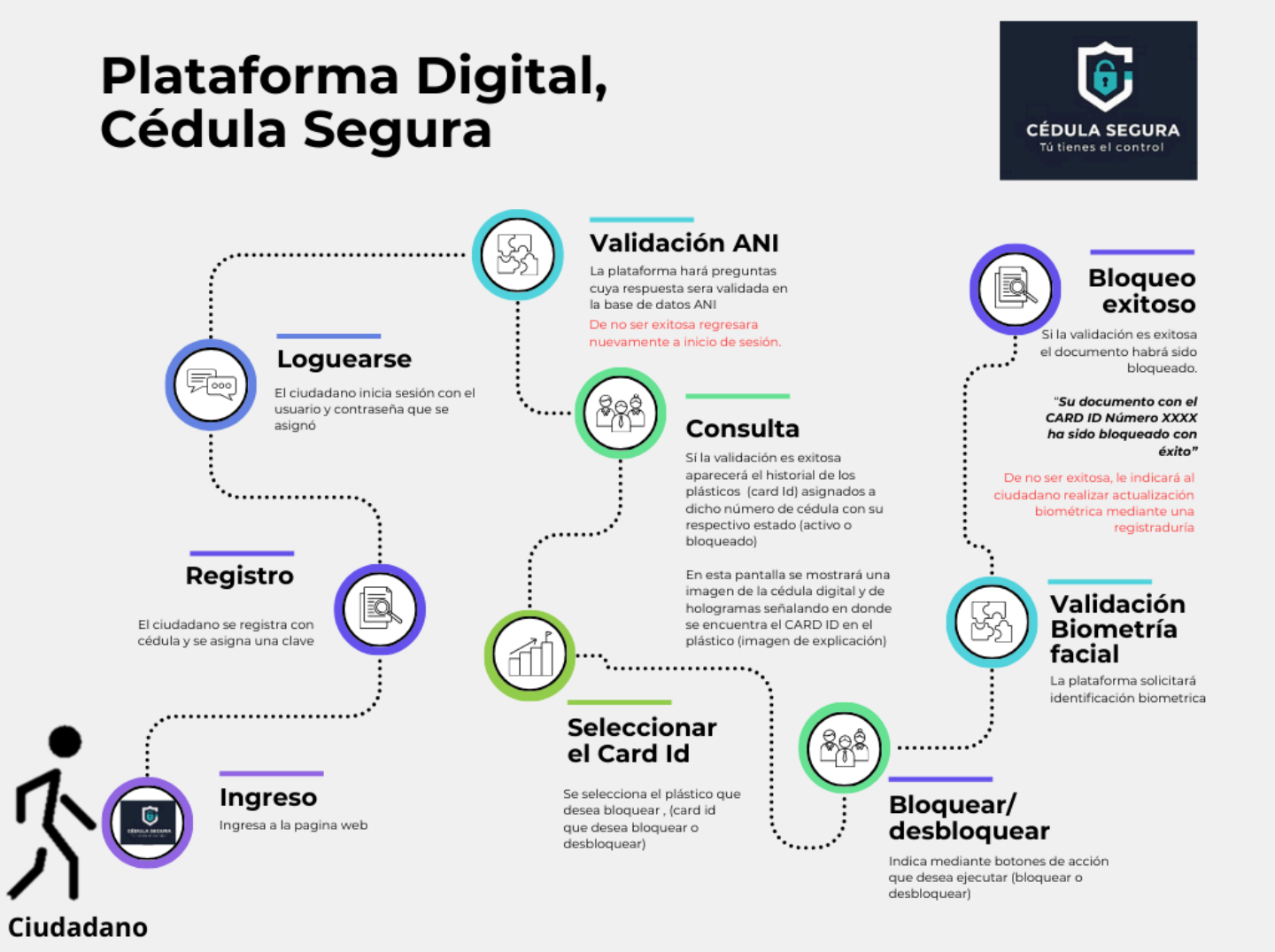
Propósito del Manual

Este manual tiene como objetivo guiar al ciudadano en el uso de la plataforma Cédula Segura, una herramienta oficial diseñada para permitir el bloqueo y desbloqueo de la cédula de ciudadanía en caso de pérdida o hurto. Protege tu identidad mediante la validación con el Archivo Nacional de Identificación (ANI) y la autenticación biométrica facial.

Requisitos para acceder

- Acceso a internet desde dispositivo móvil o computador.
- Número de cédula y fecha de expedición.
- Conocimiento del número CARD ID (ubicado en la cédula física).
- Cámara habilitada para autenticación facial.

Flujo del uso ciudadano



1. Ingreso a la plataforma

Accede a través del portal oficial: [www.cedulasegura.gov.co] desde tu navegador, ya sea en computador o celular.

2. Registro inicial

Ingresa tu número de cédula y fecha de expedición.

- ✅ **Si los datos coinciden con el ANI:** podrás crear tu contraseña.
- ❌ **Si fallas 3 veces:** se bloqueará el registro y verás el mensaje: "La información no coincide con nuestros registros. Por favor acérquese a una sede de la Registraduría para validar su identidad."

3. Inicio de sesión

Ingresa con tu cédula y contraseña.

- 🔁 **¿Olvidaste tu contraseña?** Haz clic en "¿Olvidó su contraseña?" y recibirás una temporal para ingresar.

4. Ubicación del CARD ID

Antes de ver tus documentos, se te mostrará cómo identificar el CARD ID:

- 🟡 **Cédula de hologramas:** debajo del código de barras.
- 🔵 **Cédula digital:** sobre la foto fantasma, en orientación vertical.

5. Consulta de documentos y estados

Verás una tabla con:

- Tipo de documento
- CARD ID
- Estado (Activo / Bloqueado)

Introduce el texto aquí

📝 **Mensaje destacado:** “Si bloqueas tu cédula, estará inactiva durante 24 horas. Si no la desbloqueas en ese lapso, deberás solicitar un duplicado en la Registraduría.”

6. Selección de acción

Selecciona la opción que deseas:

- 🔒 **Bloquear**
- 🔓 **Desbloquear**

Confirma tu decisión con los botones Sí o No.

7. Validación biométrica facial

Mensaje mostrado: “Queremos asegurarnos de que eres tú. Realizaremos una validación facial para continuar con el bloqueo o desbloqueo de tu documento.” Sigue las instrucciones para permitir el acceso a tu cámara.

8. Resultado del proceso

- ✅ **Si es exitoso:** “La verificación biométrica se realizó correctamente. Tu documento con CARD ID N.º XXX ha sido bloqueado/desbloqueado con éxito.”
- ❌ **Si falla tras 3 intentos:** “No fue posible confirmar tu identidad. Debes acudir a una sede de la Registraduría para actualizar tus datos biométricos.”

9. Retorno al listado

Verás nuevamente tus documentos y sus estados actualizados en tiempo real.

Soporte al ciudadano

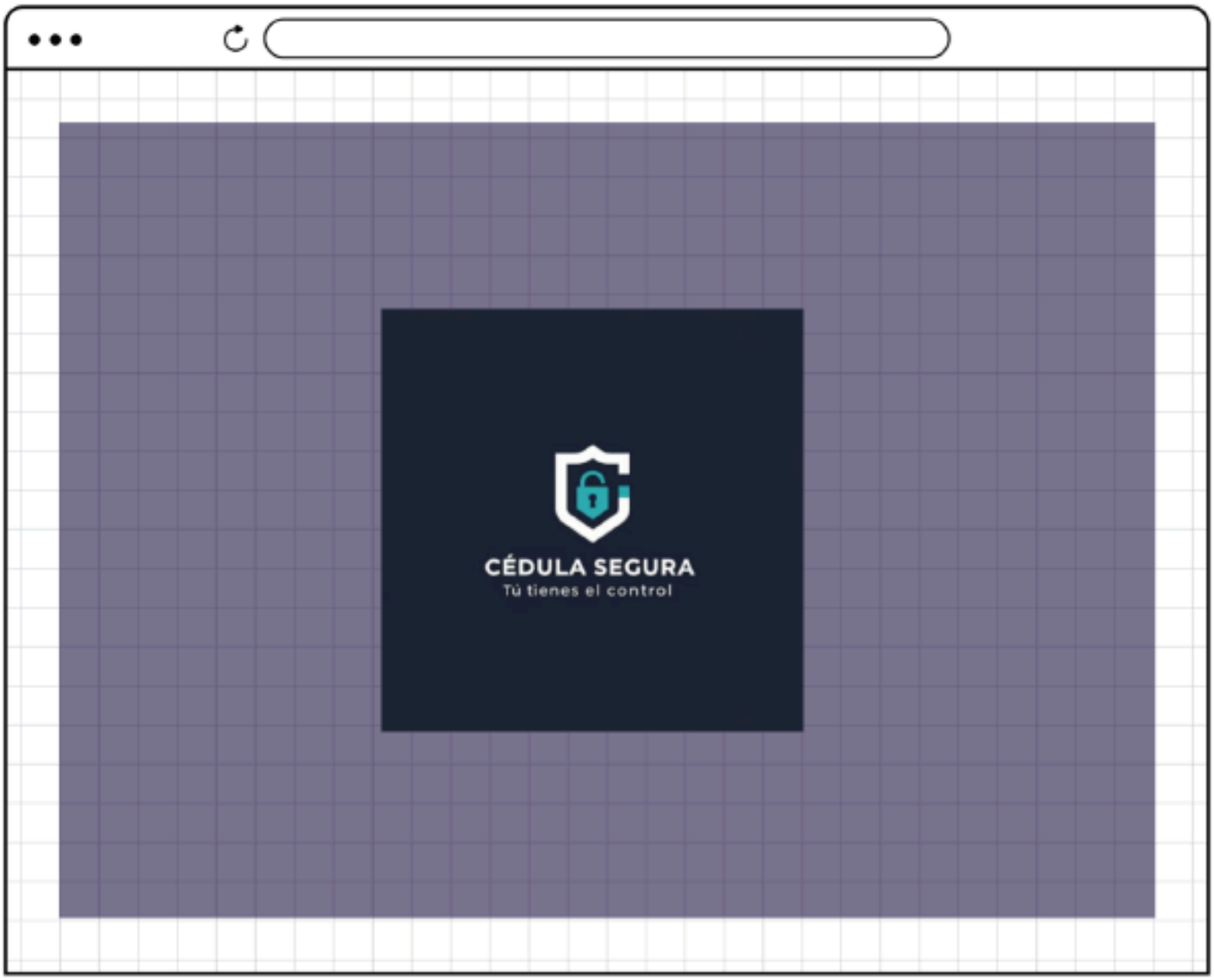
Si tienes inconvenientes, comunícate con:

- **Línea gratuita nacional:** 01 8000 123 456
- **Correo:** soporte@cedulasegura.gov.co

Recomendaciones de seguridad

- Nunca compartas tu contraseña.
- Realiza el bloqueo inmediatamente al extraviar tu cédula.
- Mantén actualizados tus datos biométricos en la Registraduría.

Anexo B. Mockups del Prototipo Funcional



Formulario de registro

Número de cédula

Email

Contraseña

Fecha de expedición

27 | Enero | 1981

Registrarse

ANI

SI LA INFORMACIÓN NO COINCIDE NO PODRA GENERAR CONTRASEÑA (3 intentos)

Por motivos de seguridad, la información ingresada no coincide con nuestros registros oficiales. Para proteger su identidad, debe presentarse personalmente en una sede de la Registraduría para realizar la validación correspondiente

Formulario de registro

Número de cédula

Email

Contraseña

Fecha de expedición

27 | Enero | 1981

Registrarse

ANI

SI LA INFORMACIÓN NO COINCIDE NO PODRA GENERAR CONTRASEÑA (3 intentos)

Por motivos de seguridad, la información ingresada no coincide con nuestros registros oficiales. Para proteger su identidad, debe presentarse personalmente en una sede de la Registraduría para realizar la validación correspondiente

Iniciar sesión

Número de cédula

Contraseña

Expedition date

27 Enero 1981

Iniciar sesión

Olvido su contraseña

"A continuación le explicamos cómo ubicar el **CARD ID** en su cédula de holograma
En el reverso del documento, justo **debajo del código de barras**, encontrará el número **impreso en negrilla**. Este código es fundamental para identificar y validar el documento que desea bloquear o desbloquear.

"

A continuación, le explicamos cómo ubicar el **CARD ID** en su cédula digital
En el reverso del documento, justo arriba de su fotografía, encontrará el número **impreso de forma vertical.** Este código es fundamental para identificar y validar el documento que desea bloquear o desbloquear.

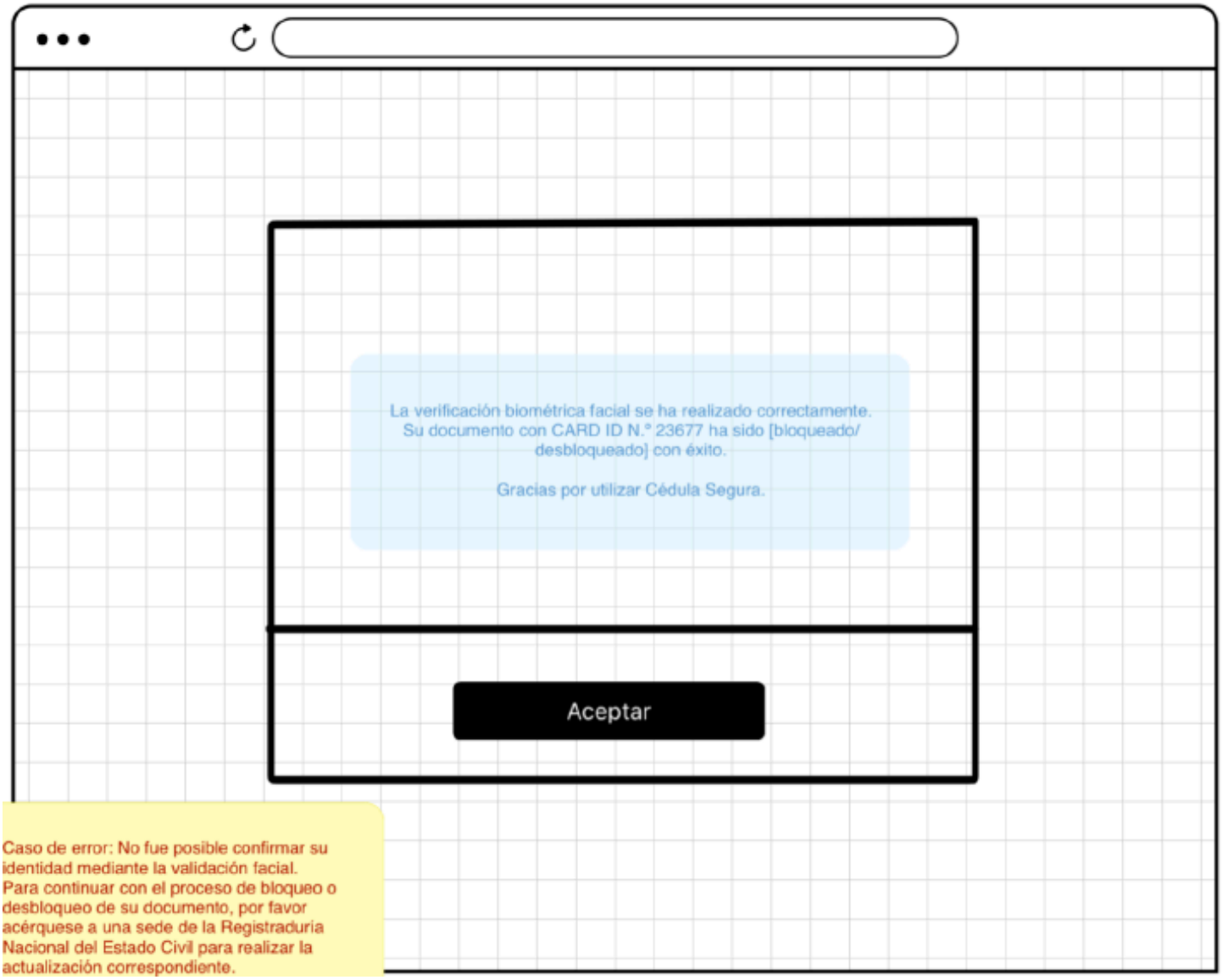
Pedro Pérez

Mis documentos **Bloquear / Desbloquear**

Tipo	**Card ID**	
Cédula de hologramas	23654	
Cédula digital	22353	
Cédula de hologramas	23677.	

"Al bloquear su cédula, esta quedará inactiva temporalmente para evitar suplantaciones. Tendrá un plazo máximo de 24 horas para desbloquearla en caso de encontrarla. Pasado este tiempo, si no realiza el desbloqueo, deberá solicitar la expedición de un duplicado ante la Registraduría Nacional del Estado Civil.

"Queremos asegurarnos de que realmente eres tú. A continuación, realizaremos una validación biométrica para que puedas bloquear o desbloquear tu documento de forma segura.



Caso de error: No fue posible confirmar su identidad mediante la validación facial. Para continuar con el proceso de bloqueo o desbloqueo de su documento, por favor acérquese a una sede de la Registraduría Nacional del Estado Civil para realizar la actualización correspondiente.

Pedro Pérez

Mis documentos **Bloquear / Desbloquear**

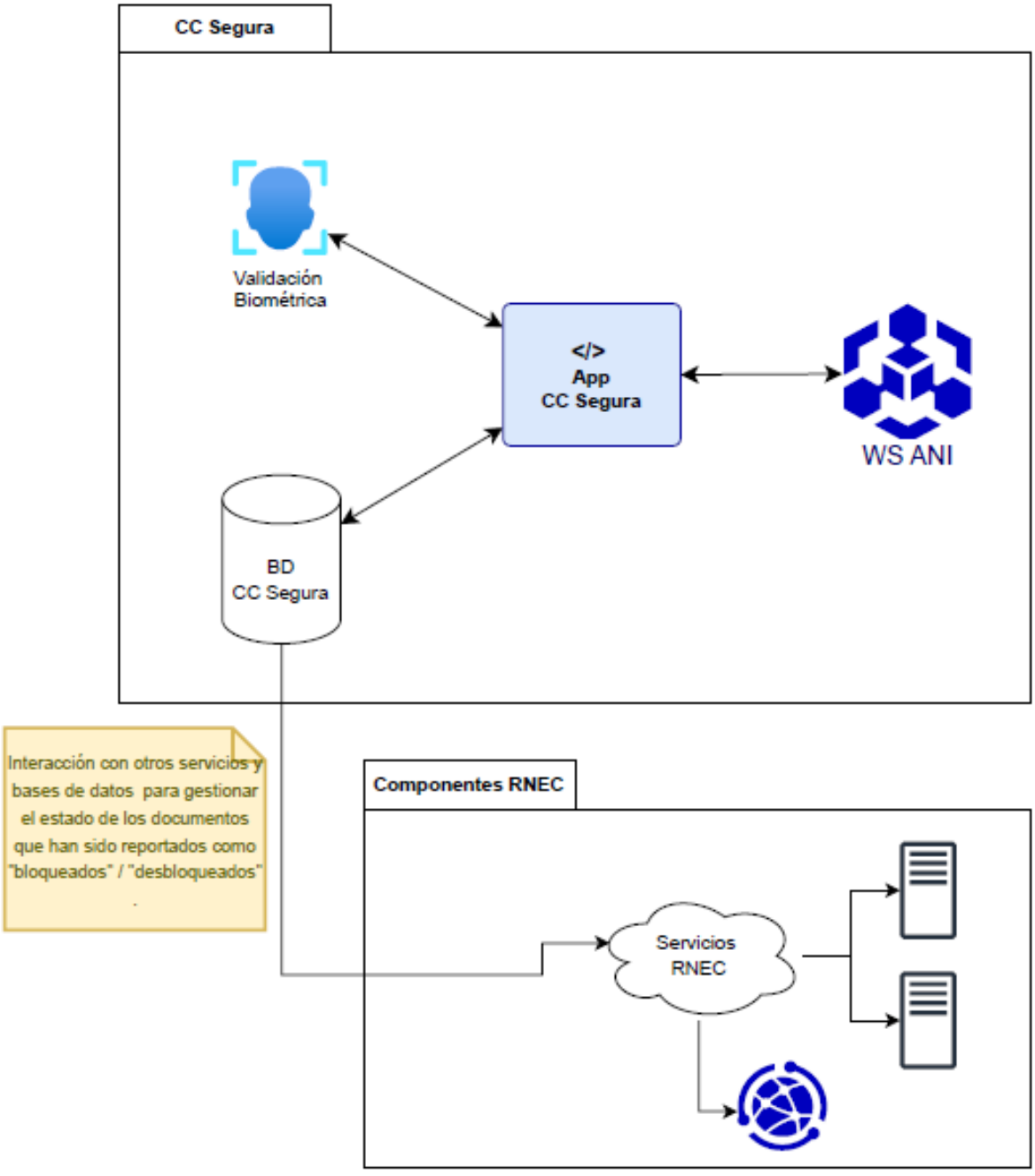
Tipo	Card ID	
Cédula de hologramas	23654	
Cédula digital	22353	
Cédula de hologramas	23677	

La verificación biométrica facial se ha realizado correctamente.

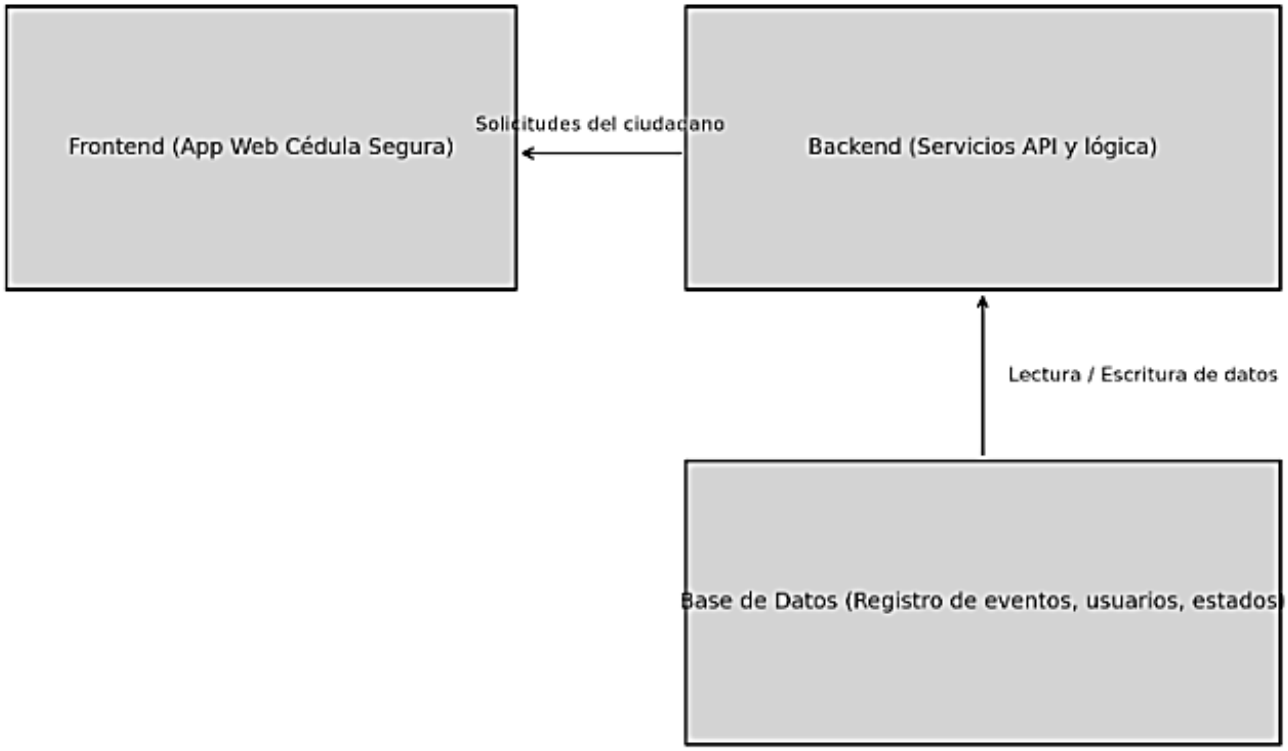
Su documento con CARD ID N.° 23677 ha sido [bloqueado/desbloqueado] con éxito.
Gracias por utilizar Cédula Segura.

De lo contrario: (3 intentos)
No fue posible confirmar su identidad mediante la validación facial.
Para continuar con el proceso de bloqueo o desbloqueo de su documento, por favor acérquese a una sede de la Registraduría Nacional del Estado

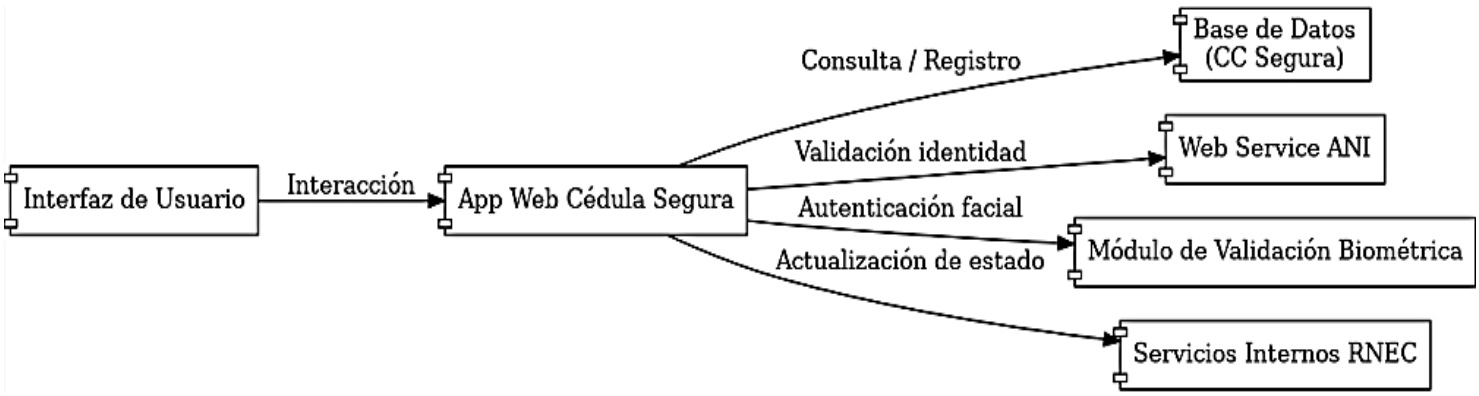
Anexo C. *Diagrama de Contexto (C4) – Plataforma Cédula Segura*



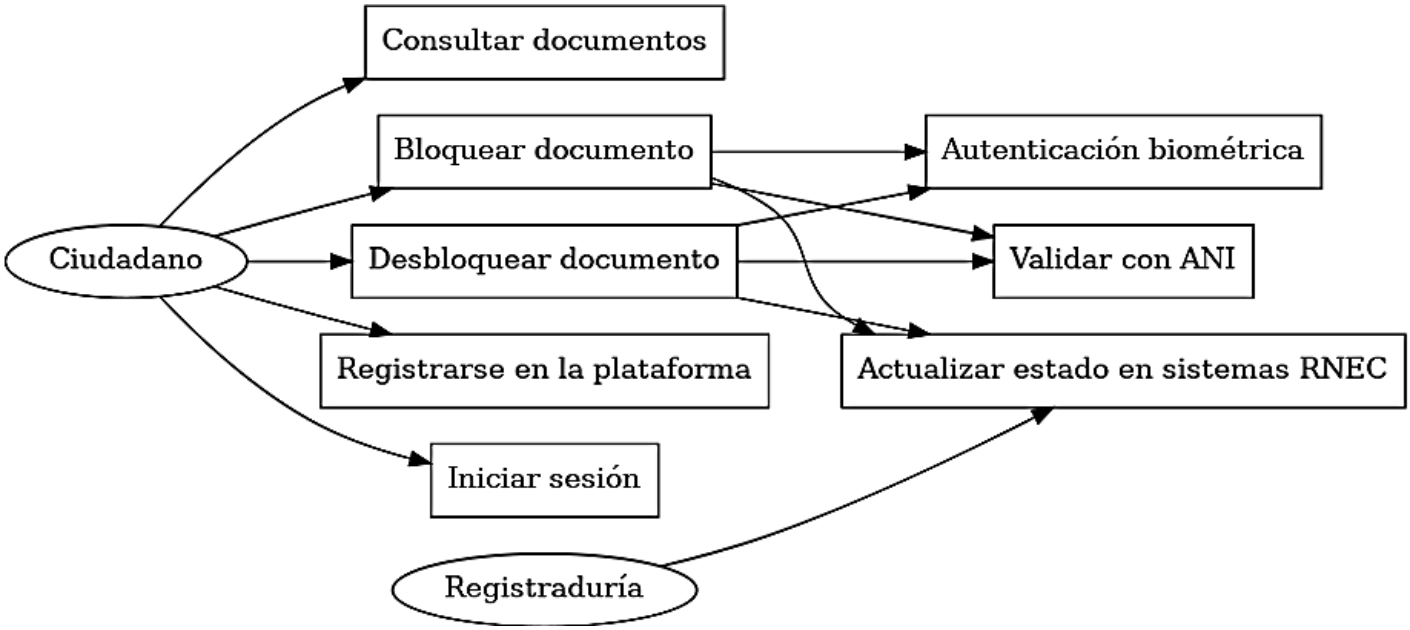
Anexo D. *Diagrama de Contenedores (C4) – Plataforma Cédula Segura*



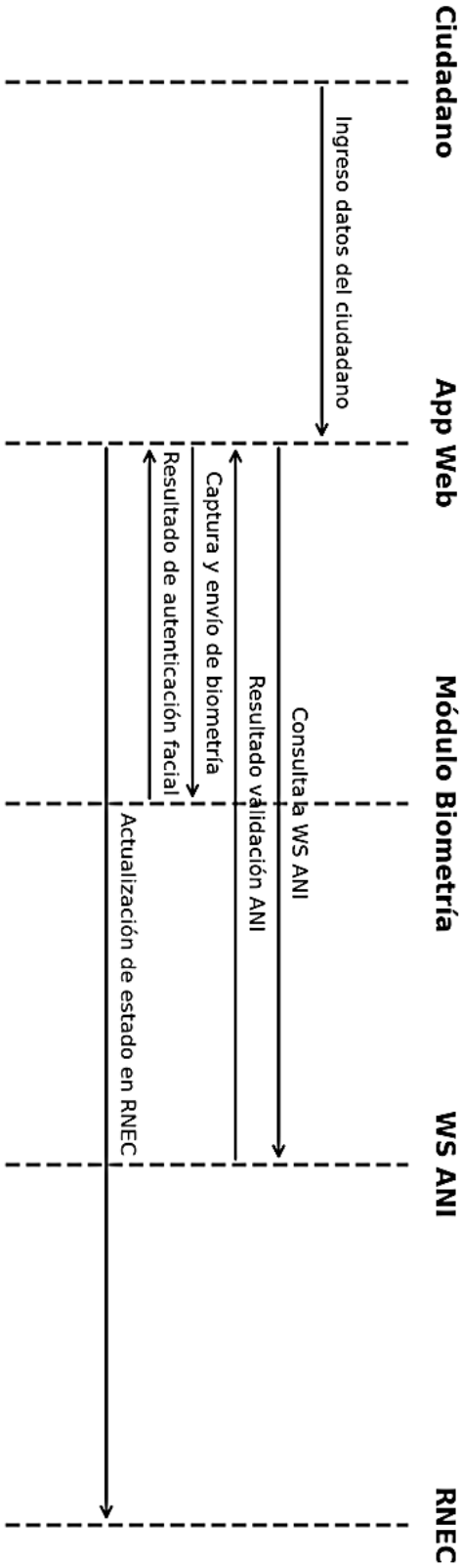
Anexo E. *Diagrama de Componentes (C4) – Plataforma Cédula Segura*



Anexo F. *Diagrama de Casos de Uso UML*



Anexo G. *Diagrama de Secuencia UML*



Anexo H. *Diccionario de Datos – Plataforma Cédula Segura*

Nombre del Campo	Tipo de Dato	Longitud	Descripción	Origen	Módulo/Función	Requerido
cedula usuario	Numérico	10	Número de cédula del ciudadano	Usuario	Registro / Validación ANI	Sí
fecha expedición	Fecha	10	Fecha de expedición de la cédula	Usuario	Validación ANI	Sí
contraseña	Texto	64	Contraseña creada por el usuario (hash en BD)	Usuario	Registro / Inicio Sesión	Sí
token_sesion	Texto	128	Token único generado para sesión segura	Sistema	Seguridad / Login	Sí
resultado validación	Texto	15	Resultado de la validación ANI (válido / inválido)	WS ANI	Validación ANI	Sí
imagen biométrica	BLOB	-	Imagen facial capturada para autenticación	Usuario	Autenticación facial	Sí
resultado biometría	Texto	15	Resultado del análisis biométrico	Módulo biométrico	Validación de identidad	Sí
estado documento	Texto	20	Estado del documento: bloqueado / desbloqueado	Usuario / Sistema	Actualización estado	Sí
fecha actualización	FechaHora	-	Fecha y hora del último cambio de estado	Sistema	Auditoría / Registro	Sí
ip_dispositivo	Texto	45	IP del dispositivo usado por el ciudadano	Sistema	Seguridad / Auditoría	No
email_usuario	Texto	100	Correo electrónico asociado a la cuenta	Usuario	Recuperación de cuenta / Contacto	Sí
codigo_verificacion	Numérico	6	Código temporal enviado por email o SMS	Sistema	Verificación / Recuperación	Sí
intentos fallidos	Numérico	2	Cantidad de intentos fallidos de acceso	Sistema	Seguridad / Login	No
motivo bloqueo	Texto	100	Motivo declarado por el usuario para el bloqueo	Usuario	Gestión de bloqueos	No
historial bloqueo	Texto	-	Registro de bloqueos/desbloqueos con fecha	Sistema	Auditoría / Historial	No

Anexo I. *Bitácora de Pruebas Funcionales y Validación de Usuario*

Fecha	Escenario de prueba	Resultado esperado	Resultado obtenido	Observaciones
20/05/2025	Registro con cédula y fecha válidas	El sistema valida con el ANI simulado y permite la creación de contraseña	La validación fue exitosa, se habilitó el campo para asignar contraseña	Se confirmó que el primer filtro de verificación funciona correctamente
21/05/2025	Ingreso de datos erróneos tres veces	Sistema bloquea el intento de registro y muestra mensaje indicando que debe acudir a una sede	Tras el tercer intento fallido, el flujo fue cerrado con mensaje preventivo	El bloqueo funciona correctamente como medida de seguridad
22/05/2025	Acceso al sistema y visualización de documentos	El ciudadano visualiza los documentos asociados, el estado y el CARD ID	La tabla se cargó correctamente con datos simulados	Flujo adecuado, se confirma que el sistema puede manejar múltiples documentos por usuario
23/05/2025	Bloqueo de documento con validación biométrica facial	El sistema solicita reconocimiento facial y actualiza el estado a 'Bloqueado'	Autenticación facial simulada fue exitosa y el estado cambió correctamente	Se validó el flujo completo con interacción de múltiples módulos
24/05/2025	Desbloqueo sin autenticación biométrica	El sistema deniega la acción e informa que se requiere validación facial previa	El intento fue rechazado con mensaje preventivo	Se confirmó que no es posible ejecutar acciones sensibles sin validación previa

Anexo J. *Plan de Implementación Gráfico – Fases de Integración Cédula Segura*

Anexo K. *Flujograma del Ciudadano – Navegación Funcional de la Plataforma*