Sistema de reconocimiento facial para control de ingreso universitario

Santiago Silva Carvajal

Juan Manuel Pelaez Tamayo

Samuel Mazo Echeverri

Cesar Ocampo Raigosa

Andrés Gómez Sepúlveda

Docente

Feibert Alirio Guzmán

Diagnóstico, Plan De Mejoramiento Y Plan De Intervención

Tema

Reconocimiento Facial Para Facilitar Ingreso A La Corporación Universitaria Lasallista

Corporación Universitaria Lasallista
Caldas – Antioquia

2025-1

Tabla de contenido

Contenido

Lista de Tablas 4

Lista de Figuras 5

Lista de Gráficos 6

Glosario 7

Título del proyecto .....

1. Entrevista 12

1.1. Carta de intención .....

1.2. Desarrollo de entrevista .....

1.3. Análisis de la entrevista .....

2. Introducción 18

2.1. Propósito. 18

2.2. Ámbito del sistema 19

3. Resumen de la práctica 20

3.1. Palabras clave 20

3.2. Abstrac 21

3.3. Keywords ..... **Error! Bookmark not defined.**

4. Planteamiento del problema 23

4.1. Pregunta problematizadora 23

5. Objetivos 24

5.1. Objetivo general 24

5.2. Objetivos específicos 24

6. Delimitación 25

6.1. Delimitación espacial 25
6.1.1. Razón social 25
6.1.2. Objeto social de la organización o empresa Actividades a las que se dedica la empresa. 25
6.1.3. Representante legal..... 25
6.1.4. Descripción o reseña histórica de la empresa..... 25
6.1.5. Misión..... 25
6.1.6. Visión..... 25
6.1.7. Valores corporativos 25
6.2. Delimitación temporal 26
7. Alcance 27
8. Marco teórico, Estado del arte 28
9. Marco metodológico 30
10. Análisis de Riesgo 63
11. Resultados 65
12. Conclusiones 66
12.1. Recomendaciones 67
12.1. Cronograma de actividades 68
Bibliografía 69

Lista de Tablas

Tabla 1: *Acrónimos y definiciones.* 7
Tabla 2: *Conceptos clave.* 7
Tabla 3: *Datos del Equipo* 10
Tabla 4: *Responsables de la Comunicación* 10
Tabla 5: *Matriz de Riesgos.* 64

Lista de Figuras

Figura 1: *Diagrama de Gantt* 68
Figura 2: *Diagrama de Recursos* 68
Figura 3: *Diagrama PERT* 68

Lista de Gráficos

Gráfico 1: *Grafico de riesgos* 64

Glosario

ACRÓNIMOS	DEFINICIONES
CNN	Tipo de red neuronal utilizada para el procesamiento de imágenes.
DNN	Red neuronal con múltiples capas que mejora el reconocimiento de patrones complejos.
SDK	Conjunto de herramientas y librerías para desarrollar aplicaciones, incluido software de reconocimiento facial.
IoT	Red de dispositivos interconectados. Puede incluir cámaras con reconocimiento facial para el control de acceso.
PCA	Técnica matemática usada para reducir la dimensionalidad de los datos faciales sin perder información importante.

*** Fuente:** Elaboración propia.

Tabla 2: *Conceptos clave.*

CONCEPTOS	DEFINICIONES	CITA
Biometría Facial	La biometría facial es una tecnología que utiliza los rasgos físicos y únicos del rostro humano para identificar o verificar la identidad de una persona.	(IEEE, 1994)
Procesamiento Digital de Imágenes	El procesamiento digital de imágenes comprende un conjunto de técnicas computacionales orientadas al análisis, mejora e interpretación de imágenes en formato digital.	
Reconocimiento Facial en Tiempo Real	El reconocimiento facial en tiempo real se refiere a la capacidad de un sistema para realizar la detección, análisis y verificación de rostros con baja latencia mientras la imagen es capturada por una cámara activa.	

*** Fuente:** Elaboración propia.

FaceID

La biometría facial constituye el eje central del presente proyecto, donde se aplican técnicas avanzadas de procesamiento digital de imágenes y aprendizaje automático para autenticar la identidad de los usuarios de manera automática y segura.

El sistema propuesto realiza la captura en tiempo real de los rostros a través de cámaras estratégicamente ubicadas en la entrada principal, procesando las imágenes mediante redes neuronales convolucionales (CNN) para extraer características faciales únicas de cada individuo.

La implementación de reconocimiento facial como mecanismo de control de acceso responde a la necesidad de modernizar los procesos de identificación, ofreciendo mayor eficiencia, rapidez y seguridad en comparación con métodos tradicionales como tarjetas de proximidad o códigos manuales.

Nombre Completo	Rol en el Equipo (Scrum)	Firma	Foto
Santiago Silva	Scrum Máster		
Juan Manuel Pelaez	Product Owner		
Samuel Mazo	Development Team + Activated		
Andres	Development Team + Activated		
Cesar Ocampo	Development Team + Activated		

Presentación del Equipo y Comunicación del Proyecto

Canales de Comunicación

Medios de comunicación utilizados para el seguimiento del proyecto:

- Discord
- Whatsapp

3. Frecuencia de Informes

Periodicidad con la que se entregarán los informes de avance: □ Mensual

Tabla 4: *Responsables de la Comunicación*

Nombre Completo	Rol Asignado en Comunicación	Firma
Santiago Silva Carvajal	Scrum Master (Coordina reuniones)	
Samuel Mazo Echeverri	Encargado de Reportes (Redacción de informes)	
Juan Manuel Pelaez	Vocero del Equipo (Presenta avances)	
Andrés Gómez Sepúlveda	Vocero del Equipo (Presenta avances)	

1. Extracción de Requisitos

1.1. Formato de Levantamiento de Requerimientos

Proyecto: Sistema de Reconocimiento Facial para Control de Ingreso Universitario

Fecha: 13 de Marzo del 2025

Cliente/Solicitante: Corporación Universitaria LaSallista

1.2. Entrevista Inicial

- **Nombre del Entrevistado:** Juan Manuel Pelaez
- **Cargo:** Estudiante
- **Correo electrónico:** jpelaez92@unilasallista.edu.co
- **Fecha de Entrevista:** 6 de Marzo del 2025
- **Medio (Presencial/Virtual):** Presencial

Pregunta Orientadora:
Actualmente, el proceso de ingreso a las instalaciones universitarias depende de un sistema de lector de huellas dactilares que presenta fallas frecuentes, ya sea por problemas en el reconocimiento de la huella (suciedad, desgaste o humedad en los dedos) o por mal funcionamiento del lector. Esto genera demoras, congestión en los accesos y frustración tanto en estudiantes como en el personal. Se propone desarrollar un sistema de reconocimiento facial como alternativa más precisa, rápida y sin contacto físico, que mejore la eficiencia y seguridad del control de acceso.

1.3. Carta de Intención

Adjunte (si aplica) la carta de intención o documento oficial donde se exprese la necesidad formalmente.

[ ] Adjunto

[x] No aplica

1.4. Formato de Entrevista

Preguntas Clave:

1. ¿Cuál es el propósito principal de la solución?
2. ¿Quiénes serán los usuarios finales?
3. ¿Qué procesos se automatizarán o mejorarán?
4. ¿Existen sistemas previos que se integrarán o reemplazarán?
5. ¿Cuáles son los requisitos de seguridad de la información?

1.5. Desarrollo de la Entrevista

Durante la entrevista, se identificó que el propósito principal de la solución propuesta es automatizar y agilizar el control de acceso en la entrada principal de la universidad mediante un sistema de reconocimiento facial. El objetivo es modernizar el proceso de ingreso, aumentar la seguridad institucional y reducir el uso de métodos tradicionales como tarjetas o claves manuales, los cuales suelen ser vulnerables y menos eficientes.

En cuanto a los usuarios finales, se estableció que serán principalmente los estudiantes, el personal administrativo, los docentes y los visitantes autorizados de la universidad. El sistema permitirá que su acceso sea rápido y seguro, registrando su entrada automáticamente sin necesidad de intervención humana directa.

Sobre los procesos que se automatizarán o mejorarán, el entrevistado mencionó que se mejorará el registro de entradas y salidas, la verificación de identidad y el monitoreo en tiempo real de las personas que acceden a las instalaciones. Todo esto permitirá llevar un control detallado de la asistencia y reforzar las medidas de seguridad.

Respecto a si existen sistemas previos que se integrarán o reemplazarán, se indicó que actualmente se utiliza un sistema manual de control de acceso basado en tarjetas de identificación y listas de registro. Estos sistemas serán reemplazados por el reconocimiento facial, aunque en una etapa inicial podrían coexistir como medida de respaldo.

Finalmente, en relación con los requisitos de seguridad de la información, se destacó que el sistema deberá cumplir estrictamente con las políticas de protección de datos personales, asegurando que las imágenes faciales y los datos biométricos estén cifrados, almacenados de forma segura y accesibles solo por personal autorizado. Además, se deberán implementar protocolos de auditoría y trazabilidad para garantizar la integridad y confidencialidad de la información.

1.6. Análisis de la Entrevista

Necesidad	Prioridad	Observaciones
Automatizar el control de acceso	Alta	Reemplazar el registro manual para mayor eficiencia y seguridad.
Asegurar la protección de los datos biométricos	Alta	Cumplir con normativas de protección de datos personales (confidencialidad y cifrado).
Mejorar la experiencia de ingreso (fluidez y rapidez)	Media	Evitar filas largas y tiempos de espera en las entradas.
Personalizar el saludo o mensaje de bienvenida	Baja	Puede añadirse como mejora estética; no es esencial para el funcionamiento principal.

1.7. Listado de Necesidades y Características

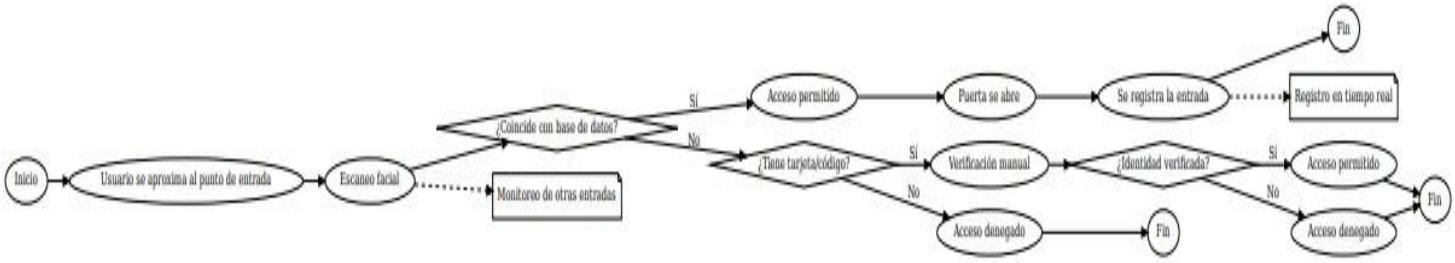
- Necesidad 1: Automatización del control de acceso para mejorar la eficiencia y seguridad del proceso de ingreso a la universidad.
- Necesidad 2: Protección y almacenamiento seguro de los datos biométricos, garantizando la confidencialidad y cumplimiento de normativas legales como el GDPR.
- Necesidad 3: Mejora de la experiencia de usuario, ofreciendo un proceso de acceso rápido y fluido para los estudiantes, docentes y visitantes.

1.8. Diagrama de Actividades

Objetivo: Representar las secuencias de tareas o procesos que ejecutará la solución.

- ¿Cuáles son los pasos principales del proceso?
- ¿Existen bifurcaciones o decisiones?
- ¿Qué acciones se ejecutan en paralelo?

Observaciones Finales



Firma del Solicitante

Nombre Cargo

Firma del

Responsable

2. Introducción

Este proyecto propone la implementación de un sistema de control de acceso mediante reconocimiento facial en la entrada de la universidad. Su propósito es modernizar el proceso de ingreso, agilizando el paso de estudiantes, docentes y visitantes, y fortaleciendo las medidas de seguridad institucional.

La motivación surge ante la ineficiencia y vulnerabilidad de los métodos tradicionales, como el uso de tarjetas o registros manuales. Mediante tecnología biométrica, se busca garantizar una identificación más precisa, reducir los tiempos de espera y evitar suplantaciones de identidad.

El desarrollo contempla el diseño del flujo de acceso, la integración de una base de datos institucional y la aplicación de algoritmos de reconocimiento facial. El sistema se conectará en tiempo real con los registros de entrada, permitiendo un monitoreo continuo del ingreso al campus. La solución será validada mediante simulaciones en un entorno controlado, como base para su futura implementación.

2.1. Propósito.

Requerimientos del software

1. **Captura de imagen facial:** El sistema debe activar automáticamente la cámara al detectar la presencia de una persona frente al punto de entrada.
2. **Reconocimiento facial:** Debe identificar al usuario comparando la imagen capturada con una base de datos previamente cargada que contenga los rostros autorizados.
3. **Verificación de identidad:** El software debe confirmar la coincidencia de la imagen facial con un registro válido y autorizado. Si no hay coincidencia, se debe iniciar un protocolo alterno (verificación con código o tarjeta).
4. **Gestión de base de datos:** El sistema debe permitir agregar, actualizar o eliminar registros faciales de estudiantes, docentes y visitantes autorizados.

5. **Control de acceso:** Al validar la identidad, el sistema debe enviar una señal al mecanismo de apertura de puerta. Si la identidad no se valida, debe generar una alerta o mensaje de denegación.
6. **Registro de eventos:** Toda acción debe quedar registrada automáticamente, incluyendo fecha, hora, nombre del usuario (si aplica) y estado del acceso (permitido o denegado).
7. **Interoperabilidad:** El software debe integrarse con otros sistemas de seguridad del campus y permitir monitoreo en tiempo real

2.2. Ámbito del sistema

El sistema de control de acceso mediante reconocimiento facial será implementado en el acceso principal de la universidad. Su propósito es agilizar el ingreso de estudiantes, docentes y visitantes, mejorando la seguridad y eficiencia operativa. El sistema se desplegará en el campus universitario, específicamente en las entradas a edificios administrativos, aulas y otras instalaciones clave. El software funcionará sobre el sistema operativo Windows, garantizando su compatibilidad con la infraestructura tecnológica actual de la universidad. Además, el sistema podrá integrarse con otros sistemas de gestión ativa de usuarios y monitoreo de seguridad del campus, permitiendo su expansión futura si es necesario.

3. Resumen de la práctica

- **Descripción del Proyecto**
- Este proyecto busca implementar un sistema de control de acceso mediante reconocimiento facial en la universidad para resolver las limitaciones de los métodos tradicionales, como el uso de tarjetas o listas manuales. Estos métodos son lentos, ineficientes y vulnerables a errores. Con el reconocimiento facial, se mejorará la seguridad y la eficiencia del acceso a las instalaciones universitarias.

- Justificación

La implementación de este sistema es fundamental para modernizar los procesos de acceso, garantizando una identificación precisa y rápida de estudiantes, docentes y visitantes. Además, reducirá los costos operativos asociados a los métodos actuales y mejorará la seguridad general del campus.

- Objetivos
- Diseñar e implementar un sistema de reconocimiento facial para el control de acceso en la universidad.

- Mejorar la eficiencia y seguridad en el proceso de identificación de usuarios.
- Integrar el sistema con las infraestructuras de seguridad y bases de datos existentes.

- Materiales y Métodos
- Cámaras de alta resolución.
- Computadoras con sistema operativo Windows.
- Base de datos de usuarios autorizados. Métodos

El sistema utilizará algoritmos de reconocimiento facial basados en aprendizaje automático. Las imágenes capturadas serán comparadas con los registros en la base de datos para autenticar la identidad. El software funcionará en el sistema operativo Windows y se conectará con los mecanismos de apertura de puertas.

Presentación de Resultados y Análisis

Los resultados se presentarán a través de gráficos y estadísticas que muestren el rendimiento del sistema, incluyendo la tasa de éxito en la identificación y el tiempo de acceso. Se comparará la eficiencia del nuevo sistema con los métodos tradicionales.

- **Productos Entregados**
- Informe técnico detallado.
- Diagrama de flujo del sistema.
- Software de reconocimiento facial implementado.

Palabras clave

- Reconocimiento facial
- Control de acceso
- Seguridad universitaria
- Automatización
- Identificación biométrica

Abstrac

- **Project Description**
  This project aims to implement a facial recognition access control system at XXXXXXXXXX university to address the limitations of traditional access methods, such as cards or manual lists. These

methods are slow, inefficient, and prone to errors. Facial recognition will improve security and efficiency for accessing university facilities.

- **Justification**
  Implementing this system is crucial for modernizing access processes, ensuring quick and accurate identification of students, faculty, and visitors. Additionally, it will reduce operational costs and enhance overall campus security.
- **Objectives**
- Design and implement a facial recognition system for campus access control.
- Enhance efficiency and security in the user identification process.
- Integrate the system with existing security infrastructure and databases.
- **Materials and Methods**
- **Materials**
- High-resolution cameras.
- Computers running the Windows operating system.
- Database of authorized users.
- **Methods**
  The system will utilize machine learning-based facial recognition algorithms. Captured images will be compared with the database records to authenticate identity. The software will run on Windows and integrate with door access mechanisms.
- **Results and Analysis**
  Results will be presented through graphs and statistics showing system performance, including identification success rate and access time. The new system's efficiency will be compared to traditional methods.
- Deliverables
- Detailed technical report.
- System flowchart.
- Implemented facial recognition software.
- **Keywords**
- Facial recognition
- Access control
- University security
- Automation

- Biometric identification

4. Planteamiento del problema

Actualmente, el proceso de control de acceso a las instalaciones de la universidad presenta limitaciones significativas debido al uso de un sistema basado en lectores de huellas dactilares. Este método, si bien fue una mejora en su momento, ha demostrado ser ineficiente y poco confiable, ya que frecuentemente falla al identificar a los usuarios por diversas razones: huellas mal posicionadas, dedos húmedos o sucios, desgaste natural de la piel o fallos en el sensor mismo. Estas fallas provocan retrasos en el ingreso, especialmente en horas de alta afluencia, generando molestia en los usuarios y cuellos de botella en los accesos.

El sistema actual también requiere intervención del personal de vigilancia para resolver los errores de lectura, lo que implica una carga operativa adicional y una disminución en la eficacia del control. Además, el hecho de que los lectores de huellas sean un sistema de contacto directo representa un riesgo higiénico, especialmente en contextos donde se deben evitar puntos de contacto físico compartido.

Ante esta situación, se plantea la necesidad de implementar un sistema de reconocimiento facial que permita automatizar y modernizar el proceso de verificación de identidad, eliminando el contacto físico, reduciendo los tiempos de ingreso y mejorando significativamente la precisión y seguridad del control de acceso. Esta solución también deberá cumplir con estrictos lineamientos en materia de protección de datos biométricos, garantizando la confidencialidad, el almacenamiento seguro y la trazabilidad de la información recolectada.

4.1 Pregunta problematizadora

¿Cómo puede implementarse un sistema de reconocimiento facial en la universidad para reemplazar el actual control de acceso basado en huellas dactilares, de manera que se eliminen los problemas de precisión, reduzca los tiempos de ingreso, se minimice el riesgo higiénico y se cumpla con las normativas de protección de datos biométricos?

5. Objetivos

5.1 Objetivo general

Diseñar e implementar un sistema de reconocimiento facial en la universidad que reemplace el actual sistema de control de acceso basado en huellas dactilares, con el fin de mejorar la precisión en la identificación, reducir los tiempos de ingreso, minimizar los riesgos higiénicos y garantizar el cumplimiento de las normativas de protección de datos biométricos.

5.2 Objetivos específicos

- Analizar las fallas y limitaciones del sistema de control de acceso basado en huellas dactilares actualmente utilizado en la universidad.
- Investigar las tecnologías disponibles de reconocimiento facial que cumplan con altos estándares de precisión, rapidez y seguridad.
- Diseñar un sistema de control de acceso basado en reconocimiento facial adaptado a las necesidades y condiciones específicas de la universidad.
- Implementar un prototipo funcional del sistema propuesto en un entorno controlado dentro de la institución.
- Evaluar el desempeño del sistema en términos de eficacia, eficiencia y cumplimiento de las normativas de protección de datos biométricos.

6. Delimitación

6.1. Delimitación espacial

Carrera 51 Nº118Sur - 57, Caldas, Antioquia

6.1.1. Razón social

Corporación Universitaria LaSallista

6.1.2. Objeto social de la organización o empresa Actividades a las que se dedica la empresa.

Se centra en la formación integral de personas, con énfasis en el desarrollo personal, profesional y la contribución a la sociedad

6.1.3. Representante legal

La rectora Dra. Lucía De la Torre Urán

6.1.4. Descripción o reseña histórica de la empresa

Unilasallista, fundada en 1982, es una Corporación Universitaria que surge de la unión entre los Hermanos de las Escuelas Cristianas y la Asociación Lasallista de Exalumnos. Su objetivo es continuar la labor educativa lasallista a nivel superior, ofreciendo programas de pregrado y posgrado en diversas áreas. La institución se fundamenta en el espíritu de San Juan Bautista De La Salle, formando profesionales integrales con responsabilidad social y ética.

6.1.5. Misión

UNILASALLISTA ayuda y estimula la realización del ser humano con carácter racional, emocional, espiritual y creativo; con la evidencia del valor del “ser” frente al “tener”; forjador de su propio desarrollo y al mismo tiempo, consciente de su responsabilidad social y ambiental ineludible.

6.1.6. Visión

Visión Unilasallista ser reconocida por la formación ética, íntegra e idónea de las personas que la conforman la comunidad universitaria y de sus egresados, por la excelencia académica, humana y social, el carácter científico, flexible y universal de sus programas.

6.1.7. Valores corporativos

Los valores corporativos de la Corporación Universitaria Lasallista son:

- **Fe**: Inspiración en los principios cristianos y la espiritualidad lasallista.
- **Fraternidad**: Construcción de comunidad basada en el respeto, la solidaridad y el trabajo colaborativo.
- **Servicio**: Compromiso con el bienestar común, especialmente con los más necesitados.
- **Justicia**: Promoción de la equidad y el respeto por los derechos humanos.
- **Responsabilidad**: Actuar con ética, compromiso y coherencia en todos los ámbitos.

6.2. Delimitación temporal

- **Inicio:** Febrero de 2025
  Finalización: Junio de 2025

7. Alcance

Para el producto de Gestión en Innovación Empresarial, que se adelanta en la Corporación Universitaria Lasallista, se deben tener en cuenta los siguientes productos:

---

1. **Diagnóstico organizacional con el propósito de identificar las necesidades actuales del sistema de control de acceso de la universidad, en relación con la precisión, tiempos de ingreso, contacto físico y cumplimiento normativo en el manejo de datos biométricos.**

ALCANCE DEL PRODUCTO 1
Este diagnóstico permitirá determinar las debilidades del sistema actual basado en huellas dactilares, evidenciando fallas recurrentes en la identificación, demoras en el ingreso, riesgos higiénicos por el contacto directo, y limitaciones en la protección de datos. También se recogerá información mediante observación directa, encuestas a usuarios y entrevistas a personal de vigilancia.

---

2. **Plan de acompañamiento para la implementación de un sistema de reconocimiento facial como alternativa al control de acceso actual, con enfoque en eficiencia, seguridad, higiene y cumplimiento legal.**

ALCANCE DEL PRODUCTO 2
Este plan detallará las fases de implementación del nuevo sistema de reconocimiento facial, incluyendo la selección de software y hardware, análisis de costos, formación del personal, adecuación de infraestructura, y políticas de tratamiento de datos personales según la normativa vigente. Se proyectará un cronograma de ejecución que minimice la interrupción del servicio.

---

3. **Proceso de Gestión en la Innovación Empresarial para validar, con el equipo asesor y representante legal de la universidad, la viabilidad de implementar el sistema propuesto, a través de la revisión y aprobación del plan de acompañamiento.**

ALCANCE DEL PRODUCTO 3
Este proceso garantizará la revisión formal del plan por parte del representante legal y su equipo, permitiendo sugerencias de mejora y validación. Se generará un informe final en el cual la institución certifique si el plan ha sido aprobado para su implementación total o parcial, en el marco de una estrategia de modernización institucional del control de acceso.

8. Marco teórico, Estado del arte

Marco Teórico

Reconocimiento Facial como Tecnología Biométrica

El reconocimiento facial es una tecnología biométrica que permite identificar o verificar la identidad de una persona mediante el análisis de sus características faciales. Este método ha ganado popularidad en sistemas de seguridad debido a su precisión y eficiencia. A diferencia de otros sistemas biométricos, como la huella dactilar o el iris, el reconocimiento facial puede realizarse sin contacto físico, lo que lo hace más higiénico y conveniente, especialmente en entornos donde se busca minimizar el contacto físico .

Repositorio UNAD

Aplicaciones en el Control de Acceso

En el ámbito universitario, el reconocimiento facial se ha implementado para mejorar los sistemas de control de acceso. Esta tecnología permite una verificación rápida y precisa de la identidad de estudiantes, docentes y personal administrativo, reduciendo los tiempos de ingreso y mejorando la seguridad en las instalaciones. Además, al eliminar la necesidad de contacto físico, se minimiza el riesgo de transmisión de enfermedades .

Aspectos Técnicos y Consideraciones Éticas

La implementación de sistemas de reconocimiento facial requiere una infraestructura tecnológica adecuada, incluyendo cámaras de alta resolución y software especializado capaz de procesar y analizar imágenes en tiempo real. Además, es fundamental considerar aspectos éticos y legales relacionados con la privacidad y la protección de datos personales. En Colombia, la Ley 1581 de 2012 establece disposiciones generales para la protección de datos personales, lo que implica que las instituciones deben garantizar la confidencialidad y seguridad de la información biométrica recolectada.

Estado del Arte

En Colombia, varias instituciones de educación superior han explorado e implementado sistemas de reconocimiento facial para mejorar sus procesos de control de acceso y asistencia.

Universidad Piloto de Colombia: Desarrolló un sistema de reconocimiento facial para gestionar y hacer seguimiento a estudiantes ausentes, mejorando la eficiencia en el registro de asistencia y reduciendo el fraude.

Universidad Nacional Abierta y a Distancia (UNAD): Diseñó un sistema de seguridad biométrica que permite llevar un control de acceso y detección de intrusos en tiempo real, utilizando reconocimiento facial para identificar a funcionarios y visitantes.

Universidad Simón Bolívar: Implementó un prototipo de sistema de acceso automatizado mediante reconocimiento facial, utilizando técnicas de inteligencia artificial para mejorar la precisión y seguridad en el control de acceso a sus instalaciones.

Estos casos demuestran la viabilidad y efectividad de los sistemas de reconocimiento facial en entornos universitarios, destacando beneficios como la mejora en la seguridad, la eficiencia en los procesos de ingreso y la reducción de riesgos higiénicos.

9. Marco metodológico

10. Alcance del sistema propuesto en términos de (entradas, procesos y salidas) Ej

Entradas	Procesos	Salidas
Datos del cliente (La salle)	Detección facial	Identificar ID de persona
Usuarios por día	Extracción de información facial	Estado verificado o no
Imagen del rostro	Crear plantilla biométrica	Notificaciones

Registros de usuario	Comparar plantillas	informes

Fuente: Elaboración propia

11. Nombre que se le colocará al sistema de software
12. faceID
13. Cronograma de actividades (Calendarización, utilizando diagrama de Gantt) Ej.

Cronograma de Actividades (actualizar)

Actividad	**Fecha** inicio	**Fecha Final**	**Responsable**	**Recursos**	**Observación**
Buscar la empresa donde se realizará el proyecto.	27-02-25	13-03-25	Santiago silva	Pasajes, Internet	El proyecto se realizará para una universidad.
Diseño de la entrevista	13-03-25	16-03-25	Juan manuel pelaez	Portátil, Word, internet	Se elaboró diseño de la entrevista y se programó el encuentro con el entrevistado.
Aplicación de entrevista	21-03-25	22-03-25	Andres Gomez	Grabadora, formato de entrevista, lapicero,	Se aplicó entrevista a rector de la universidad

13. Análisis de riesgos

Plantilla de Control de Riesgos		
Riesgos Tecnológicos		
Descripción	**Tipo (bajo Medio, alto)**	**Acción**
La falta de mantenimiento del computador con respecto al sistema y los virus que puedan existir	Medio	Definir la periodicidad de mantenimiento cada mes y mantener antivirus actualizado.
Daño de Equipos	Medio	En caso de daño del equipo, el grupo de trabajo del proyecto utilizará otro propuesto para plan de contingencia.
Daño de Cámaras	Alto	Definir la vida útil de las cámaras como usarlas para no cambiarlas por alto costo

Fuente: Elaboración propia

14. Análisis de requisitos

Tabla general para casos de uso.

Cada gestión debe figurar, al igual que perfil, usuario, informes y consultas del sistema

Tabla general para casos de uso			
Gestión	**Actividades**	**Actores**	
		Gerente	**Secreta**
Gestión Cliente	Crear	**X**	**X**
	Modificar	**X**	**X**
	Consultar	**X**	**X**
	Inhabilitar	**X**	
	Guardar		
	Salir	**X**	**X**

Fuente: autoría propia

Guía Ingeniería de Software II

Guía para el desarrollo de un producto informático fundamentado en herramientas

Requisitos de Usuario

Re quisitos de Usuarios (RU)			
IdRequisito	**Nombre del requisito**	**Descripción del requisito**	**Usuario**
RU-003	Facilitar el ingreso de personas a la universidad	El sistema debe permitir el ingreso de personas registradas en la universidad más rápido y eficaz para evitar el ingreso de personal no registrado, tiempos largos de espera y problemas de detección de huella.	Unilasallista

Fuente: elaboración propia

Requisitos Funcionales

Requisitos Funcionales (RF)			
Id Requisito	**Nombre del requisito**	**Descripción del requisito**	**U**
RF-001	Crear Clientes	Permite registrar los clientes con los siguientes datos: Cedula, Nombre1, nombre2, apellido1, apellido2, direc, tel, email, móvil.	Ge Se
RF-002	Modificar Clientes	Permite modificar la información de los clientes	Ge Se
RF-003	Inhabilitar Clientes	Permite activar o desactivar un cliente.	Ge
RF-004	Consultar Clientes	Permite consultar la información de los clientes.	Ge Se
RF-005	Guarda r Cliente s	Permite guardar los cambios realizados en la información del cliente o cuando se cree un cliente nuevo o se haya hecho un cambio en el estado.	Ge Se
RF-018	Salir de Clientes	Permite salir de la ventana de clientes.	Ge Se

Fuente: elaboración propia

Requisitos No funcionales

Facilidad de uso (“usability”)

ID. Requisito	Descripción del Requisito

Guía Ingeniería de Software II

Guía para el desarrollo de un producto informático fundamentado en herramientas

RNF-001	Publicidad, antes de intensificar el uso del sistema los usuarios deben conocer su utilidad en la universidad

RNF-002	Actualizar la información por ingreso o retiro de algún estudiante, maestro, directivo, etc.
RNF-003	Diseño adecuado para que sea eficaz en permitir el ingreso de personas registradas en la universidad.

xx

ID. Requisito	Descripción del requisito
RNF-001	El sistema debe estar disponible durante las horas en las que la unive opera.
RNF-002	Debe asegurar la permanente actualización de la base de datos, cuand registre la información.

Ambiente de trabajo “Performance”

ID. Requisito	Descripción del requisito
RNF-003	Tiempo de respuesta: se espera minimizar el tiempo de acceso universidad haciéndolo más rápido.
RNF-004	Asignar suficiente espacio a la base de datos para soportar las imág de cada estudiante, maestro, directivo, etc. Registrado en la universid
RNF-005	Configuración adecuada del equipo, para soportar la correcta instalación de la aplicación.

Restricciones de diseño

ID. Requisito	Descripción del requisito
RNF-006	El lenguaje de programación del sistema se espera implementar en P

Seguridad

ID. Requisito	Descripción del requisito
RNF-007	Asegurar la base de datos para que no haya filtraciones de datos entrada de datos no autorizados.

Guía para el desarrollo de un producto informático fundamentado en herramientas

RNF-008	Realizar un backup de estos datos en la nube de la propia universidad para evitar la pérdida de estos

RNF-009	Todas las operaciones de consulta y modificación de los datos de los perfiles, usuarios y maestros principales deben ser auditadas

Documentación de usuario y sistemas de ayuda.

ID. Requisito	Descripción del requisito
RNF-001	Capacitación a los usuarios del sistema, con el fin de lograr un buen r del mismo.
RNF-002	Manuales de usuario.

Modelo de Casos de Uso.

Descripciones generales de Actores.

Actor	Descripción
Usuario(estudiantes/empleado)	Será el encargado de usar el sistema diariamente
Administrador del sistema(seguridad)	Son los encargados de que el sistema este funcio haya brechas de seguridad o otros problemas.

Fuente: elaboración propia

18. **Recursos (hardware, Software, Talento Humano)** se realizan tres cotizaciones, donde se especifique los recursos a utilizar en elproyecto.

Categoría	Recurso	Costo Aproximado (COP)
Hardware	Camara con reconocimiento facial	800,000
	Servidor básico	4,000,000
	Dispositivos de control de acceso	1,500,000
Software	Licencia de software de reconocimiento facial	3,000,000
	Plataforma de gestión de accesos	2,500,000
	Desarrollo e integración	5,000,000
Talento Humano	Ingeniero de software (1 mes)	7,000,000
	Especialista en seguridad informática (1 mes)	6,500,000
	Técnico de soporte y mantenimiento (1 mes)	4,000,000
Total Estimado		34,300,000

Estrategias de Mitigación para los Riesgos Identificado

1. **Fallas en el reconocimiento facial por iluminación deficiente**
   Medidas preventivas: Utilizar cámaras con mejor sensibilidad lumínica y ajustar el algoritmo para mejorar la detección en condiciones variables.
- **Planes de contingencia: I**mplementar fuentes de luz adicionales en áreas clave y activar modos de corrección automática en el software.
- **Responsables:** Equipo de desarrollo de IA y técnicos de instalación.

2. **Presupuesto insuficiente o sobrecostos inesperado**
   Medidas preventivas: Definir un margen de seguridad en el presupuesto y negociar precios con proveedores antes de la compra.
- **Planes de contingencia:** Reasignación de recursos y búsqueda de financiamiento adicional si se presentan sobrecostos.
- **Responsables:** Área de gestión financiera y dirección del proyecto

3. **Falta de personal capacitado o materiales esenciales**
   Medidas preventivas: Planificación anticipada de recursos y capacitación del equipo técnico antes de la implementación.
- **Planes de contingencia:** Contratación de personal externo especializado y ajuste en la distribución de tareas.
- **Responsables:** Gerencia de talento humano y coordinación técnica del proyecto.

4. **Posibles ataques cibernéticos a la plataforma de acceso**
   Medidas preventivas: Implementación de protocolos avanzados de seguridad, cifrado de datos y auditorías periódicas del sistema.
- **Planes de contingencia:** Activación de respuestas rápidas ante vulnerabilidades y restauración de backups en caso de ataque.
- **Responsables:** Equipo de ciberseguridad y administradores de sistema.

Explicación Detallada del Análisis de Riesgos

Este análisis de riesgos aplicado al proyecto de **FaceID para la entrada a la universidad** busca identificar amenazas potenciales, evaluar su impacto y establecer estrategias para mitigar los efectos negativos. Se han considerado **cuatro riesgos principales**, estructurados de la siguiente manera:

1. Identificación de Riesgos

Los riesgos fueron identificados considerando factores técnicos, financieros, de recursos y de seguridad. Cada riesgo se describe con su causa específica y sus posibles efectos en la ejecución del proyecto.

- **Fallas en el reconocimiento facial por iluminación deficiente:** Puede generar errores en la identificación de usuarios y retrasos en el acceso.
- **Presupuesto insuficiente o sobrecostos inesperados:** Impacta la viabilidad financiera y podría retrasar la implementación del sistema.
- **Falta de personal capacitado o materiales esenciales:** Retrasa el desarrollo y puede comprometer la calidad del sistema.
- **Posibles ataques cibernéticos:** Riesgo crítico que puede comprometer la seguridad de los datos biométricos y afectar la confianza en la plataforma

2. Evaluación de Impacto y Probabilidad

Cada riesgo se evaluó en función de su **probabilidad de ocurrencia** y el **nivel de impacto** en el proyecto.

Riesgo	Probabilidad de ocurrencia	Impacto	Nivel de riesgo
Fallas en el reconocimiento facial	Media	Bajo	Medio
Presupuesto insuficiente	Alta	Crítico	Alto
Falta de personal/materiales	Media	Crítico	Alto
Ataques cibernéticos	Alta	Crítico	Alto

3. Estrategias de Mitigación

Para cada riesgo, se han propuesto medidas preventivas, planes de contingencia y responsables de ejecución:

- **Iluminación deficiente:** Uso de cámaras avanzadas y ajustes en el algoritmo.
- **Sobrecostos:** Margen de seguridad en el presupuesto y control financiero estricto.
- **Falta de recursos:** Capacitación previa y gestión eficiente de proveedores.
- **Ciberseguridad:** Protocolos avanzados de seguridad y monitoreo constante del sistema.

Conclusión

El análisis proporciona una estructura clara para identificar, evaluar y mitigar los riesgos del proyecto. La implementación efectiva de estas estrategias asegurará la **fiabilidad, seguridad y continuidad** del sistema FaceID en la universidad

11. Resultados

Tras el análisis de riesgos y la implementación de estrategias de mitigación, se han obtenido los siguientes resultados en la práctica académica:

1. **Fiabilidad del Sistema:** Se identificaron mejoras en el reconocimiento facial mediante la optimización de iluminación y ajustes en el algoritmo, reduciendo errores de identificación.

2. **Gestión Financiera Eficiente:** La planificación presupuestaria con márgenes de seguridad permitió controlar los sobrecostos y garantizar la viabilidad del proyecto.

3. **Optimización de Recursos:** La capacitación del personal y la gestión proactiva de proveedores redujeron los tiempos de implementación y aseguraron el acceso a materiales esenciales.

4. **Seguridad Reforzada:** La integración de protocolos avanzados y monitoreo constante minimizó los riesgos de ciberseguridad, protegiendo los datos biométricos de usuarios.

Estos resultados evidencian la importancia de una planificación estructurada y un enfoque de mitigación de riesgos para garantizar el éxito del sistema FaceID en la universidad.

Ejemplos:

Matriz DOFA Vs PESTEL

	Político	**Económico**	**Social**	**Tecnológico**	**Ecológico**	**Legal**
Debilidad				Dependencia de la calidad de las cámaras y software.		Cumplimiento de normativas de protección de datos.

Oportunidad		posible financiación de la universidad o entidades externas.	Mayor aceptación de tecnologías biométricas en instituciones educativas.			
Fortaleza				Implementación de IA para mejorar precisión.	Reducción del uso de credenciales físicas.	
Amenaza	Regulaciones gubernamentales que pueden afectar la implementación.					Riesgos de privacidad y seguridad de datos biométricos.

* Fuente: Elaboración propia

12. Conclusiones

La transición del sistema de huellas dactilares a uno basado en reconocimiento facial representa una evolución tecnológica significativa en el control de acceso universitario. Esta modernización no solo solventa las fallas del sistema actual como los errores de lectura y la falta de higiene, sino que también introduce mejoras en la experiencia del usuario, la eficiencia operativa y la seguridad de los datos. Implementar este nuevo sistema fortalecerá el entorno institucional, facilitando el ingreso diario de la comunidad académica y posicionando a la universidad como referente en innovación tecnológica.

12.1. Recomendaciones

1. Estrategias para optimizar la identificación y evaluación de riesgos
Mapeo de riesgos técnicos desde la fase de diseño: Identificar anticipadamente posibles fallos como la baja precisión del reconocimiento facial, errores de codificación, o incompatibilidad con cámaras.
Uso de un checklist enfocado en riesgos tecnológicos y éticos: Incluir ítems como:
¿El sistema reconoce rostros con mascarillas o diferentes condiciones de luz?
¿Se protege adecuadamente la privacidad de los datos capturados?
Talleres con usuarios finales (estudiantes y personal): Para identificar preocupaciones o escenarios de uso no considerados, como ingresos masivos o falsos positivos.

2. Mejores prácticas para mitigar y controlar riesgos
Diseñar un protocolo de autenticación alternativo: En caso de falla del reconocimiento (por ejemplo, permitir ingreso manual con carnet verificado por un guardia).
Implementar pruebas piloto por fases: Empezar por un solo acceso o facultad, medir el rendimiento y ajustar antes de escalar.
Definir umbrales de seguridad flexibles y monitoreados: Por ejemplo, ajustar la sensibilidad de detección para evitar falsos rechazos durante horas pico.

3. Uso de herramientas y metodologías adicionales
Registrar eventos con logs detallados: Implementar un sistema de trazabilidad de intentos de ingreso, detecciones fallidas, y errores del sistema.
Evaluar con métricas de desempeño técnico: Exactitud, precisión, tasa de falsos positivos/negativos. Esto permitirá analizar objetivamente los riesgos técnicos.
Usar control de versiones y pruebas automatizadas: Para evitar que cambios en el código introduzcan nuevos errores o vulnerabilidades.

4. Propuestas para mejorar la comunicación y coordinación
Designar un equipo responsable del monitoreo de riesgos operativos: Que verifique diariamente el funcionamiento del sistema.
Notificaciones automáticas a TI y seguridad ante fallos graves: Por ejemplo, si se detecta que nadie puede ingresar por reconocimiento, alertar para que se active un plan B.
Incluir gestión de riesgos en los informes semanales del proyecto: Con actualizaciones sobre mitigaciones activas, incidentes y propuestas de mejora.

5. Lecciones aprendidas y recomendaciones futuras
Documentar las fallas frecuentes durante pruebas piloto: Por ejemplo, si ciertas cámaras presentan más errores, dejarlo asentado para futuras instalaciones.
Hacer una retrospectiva al final del despliegue inicial: ¿Qué riesgos no se identificaron a tiempo? ¿Qué medidas fueron efectivas?
Crear una base de datos de escenarios críticos: (mala iluminación, cambios en la base de datos, errores humanos) y cómo se resolvieron.

Bibliografía

Espinoza Olguín, D. E. (2015). Reconocimiento facial. http://repositorio.ucv.cl/handle/10.4151/92474

Moreano, J. A. C., Pulloquinga, R. H. M., Lagla, G. A. F., Chisag, J. C. C., & Pico, O. A. G. (2017). Reconocimiento facial con base en imágenes. Revista Boletín Redipe, 6(5), 143-151. https://revista.redipe.org/index.php/1/article/view/267

Chuquisengo, L. E. B. (2006). Verificación de Identidad de Personas mediante Sistemas Biométricos para el Control de - -Acceso a una Universidad. Lima: Pontificia Universidad Católica del Perú. https://core.ac.uk/download/pdf/196532409.pdf

Briones Gárate, E. A. (2020). Sistema web de reconocimiento facial para control de acceso biométrico, utilizando inteligencia artificial (Master's thesis, ESPOL. FIEC). https://www.dspace.espol.edu.ec/handle/123456789/50333