Modelo de reconocimiento facial basado en IA, Generador de alertas de intrusión

Sebastián Abdul Correa Méndez, Andrés Felipe Méndez García, Oscar Eduardo Varón Meza

Ingeniería de Software, Fundación Universitaria Compensar

Proyecto fin de grado (Facultad de ingeniería)

Esteban Alejandro Cárdenas Lancheros

16 de mayo de 2023

Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

Resumen

Esta tesis se centra en el desarrollo de un "Modelo de Reconocimiento Facial Basado en Inteligencia Artificial generador de Alertas de Intrusión" aplicado a nuestra institución. La motivación para desarrollar este sistema surge debido a la falta de un control de acceso eficiente a las instalaciones de la universidad, donde actualmente el ingreso es autorizado por un guarda de seguridad que verifica un carnet en la aplicación PowerApps. Portando un screenshot del carnet que igualmente se muestra al guarda de seguridad quien autoriza el ingreso, lo cual genera inseguridad para los docentes, alumnos y personal propio de la universidad. El objetivo de esta tesis es desarrollar e implementar un sistema de reconocimiento facial basado en inteligencia artificial para mejorar la seguridad en la Fundación Universitaria Compensar. El sistema ayudara al guarda de seguridad, quien recibe una alerta de intrusión en tiempo real por medio de un correo electrónico, cuando detecte individuos no registrado en el sistema de control de acceso y sea una posible amenaza de intrusión, permitiendo una respuesta rápida y eficaz ante posibles amenazas. Permitirá mejorar la seguridad en el campus y proporcionar un entorno más seguro para los estudiantes, profesores y personal. La adopción de esta tecnología también puede allanar el camino para la implementación de sistemas similares en otras instituciones educativas y entornos que requieran soluciones de seguridad avanzadas. Al reemplazar el método actual de verificación de carnets, se espera que el sistema brinde mayor seguridad y confianza en el control de acceso a la universidad.

Palabras clave: Reconocimiento facial, tecnología biométrica, machine learning, Inteligencia Artificial.

Contenido

Resumen 2

Contenido de Tablas 7

Contenido de Figuras 8

1. Introducción 9

1.1. Justificación 9

1.2. Antecedentes 11

1.3. Estado del arte 14

1.4. Antecedentes 16

1.5. Objetivos 19

1.5.1. Objetivo General 19

1.5.2. Objetivos Específicos 19

1.6. Alcances y Limitaciones 19

1.6.1. Alcances 19

1.6.2. Limitaciones 20

2. Método 21

2.1. Metodología de Investigación 21

2.1.1. Fase N° 1 Identificación 21

2.1.1.1. Metodología 21

2.1.1.2. Secuencia de Actividades: 21

2.1.1.3. Producto fase de identificación 21

2.1.1.4. Requerimientos No Funcionales 21

2.1.1.5. Historias de Usuario 32

2.1.2. HU01 32

2.1.3. HU02 33

2.1.4. HU03 34

2.1.5. HU04 35

2.1.6. HU05 37

2.1.7. HU06 38

2.1.8. HU07 40

2.1.9. HU08 41

2.1.10. HU09 44

2.1.11. Fase N° 2 Fase de Diseño 45

2.1.11.1. Metodología: 45

2.1.11.2. Secuencia de actividades: 45

2.1.11.3. Transformación y Selección de Datos 46

2.1.11.4. Selección y configuración del modelo 47

2.1.11.5. Entrenamiento y validación del modelo 48

2.1.11.6. Implementación del modelo 49

2.1.11.7. Producto de la fase de diseño 45

2.1.11.8. Diagramas UML (Lenguaje Unificado Modelado) 51

2.1.11.8.1. Diagrama de casos de uso 51

2.1.11.8.2. Diagrama de Clases 52

2.1.11.8.3. Diagrama de Secuencia 53

2.1.11.8.4. Diagrama de Paquetes 53

2.1.11.8.5. Diagrama de Componentes 54

2.1.11.8.6. Diagrama de flujo de datos 54

2.1.11.8.7. Diagrama de flujo del proceso 55

2.1.11.8.8. Diagrama de arquitectura 55

2.1.11.9. Metodología de desarrollo ágil Scrum 56

2.1.11.9.1. Artefacto 56

2.1.11.9.1.1. Product Backlog 56

2.1.11.9.1.2. Sprint Backlog 59

2.1.11.9.1.3. Sprint Review 64

2.1.11.9.1.4. Sprint Retrospective 64

2.1.11.9.1.5. Roles en Scrum 65

2.1.11.9.1.6. Artesanía Técnica 67

2.1.11.9.1.7. Definición de "Hecho" (Definition of Done) 67

2.1.11.9.1.8. Herramientas y Tecnologías Utilizadas 67

2.1.11.10. Hipótesis 68

2.1.12. Fase N° 3 Validación 69

2.1.12.1. Metodología: 69

2.1.12.2. Secuencia de actividades: 69

2.1.12.3. Producto fase de validación 69

3. Resultados 70

4. Discusión 71

5. Referencias 73

Contenido de Tablas

Tabla 1 RN-S-01 21

Tabla 2 RN-S-02 22

Tabla 3 RN-S-03 23

Tabla 4 RN-S-04 24

Tabla 5 RN-S-05 25

Tabla 6 RN-S-06 26

Tabla 7 RN-S-07 27

Tabla 8 RN-S-08 28

Tabla 9 RN-S-09 29

Tabla 10 RN-S-10 30

Tabla 11 RN-S-11 31

Tabla 12 HU01 32

Tabla 13 HU02 33

Tabla 14 HU03 34

Tabla 15 HU04 35

Tabla 16 HU05 37

Tabla 17 HU06 38

Tabla 18 HU07 40

Tabla 19 HU08 41

Tabla 20 HU09 44

Tabla 21 Product Backlog 56

Tabla 22 Sprint Backlog 59

Tabla 23 Sprint Review 64

Contenido de Figuras

Figura 1 Remplazo de Parámetros 46

Figura 2 DataSet 46

Figura 3 Definición de Clústeres 47

Figura 4 Definición de Centroides 48

Figura 5 Etiquetado 49

Figura 6 Correlación 50

Figura 7 Diagrama de caso de uso 51

Figura 8 Diagrama de Clases 52

Figura 9 Diagrama de casos de secuencia 53

Figura 10 Diagrama de Paquetes 53

Figura 11 Diagrama de Componentes 54

Figura 12 Diagrama de flujo de datos 54

Figura 13 Diagrama de flujo del proceso 55

Figura 14 Diagrama de arquitectura 55

1. Introducción

El presente proyecto fin de grado aborda el diseño e implementación de un modelo de reconocimiento facial basado en Inteligencia Artificial para la generación de alertas de intrusión en la Fundación Universitaria Compensar. La propuesta busca responder a la creciente demanda de sistemas de seguridad más sofisticados y capaces de adaptarse a diferentes entornos y condiciones.

El reconocimiento facial es una tecnología biométrica que permite identificar individuos mediante el análisis de patrones faciales únicos. La aplicación de técnicas de aprendizaje profundo y algoritmos de reconocimiento facial permite desarrollar modelos de Inteligencia Artificial que pueden identificar a personas autorizadas y no autorizadas en tiempo real, mejorando la capacidad de respuesta ante posibles amenazas a la seguridad de la Fundación Universitaria Compensar.

Este proyecto aborda con profundidad una metodología que comprende varias etapas críticas: recolección y clasificación de un conjunto de imágenes faciales, elección y capacitación de un modelo de Inteligencia Artificial, y el establecimiento de un sistema de alertas para notificar a los equipos de seguridad ante posibles incursiones. Se lleva a cabo una evaluación integral del desempeño del modelo de Inteligencia Artificial, considerando su impacto en la mejora de la eficiencia operativa y en la disminución de alertas falsas, en contraste con los métodos de seguridad tradicionales.

El resultado es un modelo de reconocimiento facial basado en Inteligencia Artificial que contribuye a mejorar la seguridad en la Fundación Universitaria Compensar, permitiendo la detección temprana de personas no autorizadas y facilitando una respuesta rápida y efectiva por parte del personal de seguridad. Con este proyecto, se espera sentar las bases para futuras investigaciones y desarrollos en la aplicación de tecnologías de Inteligencia Artificial en el ámbito de la seguridad institucional.

1.1. Justificación

La seguridad en las universidades de Colombia es un tema preocupante debido al aumento de la violencia en los campus universitarios. Entre los problemas de seguridad más comunes se encuentran los robos, el acoso sexual y el consumo de drogas. El reconocimiento facial es una tecnología que podría

ayudar a mejorar la seguridad en las universidades de Colombia. A continuación, se presentará un resumen de algunos estudios y reportes que abordan estos problemas de seguridad y cómo el reconocimiento facial podría ayudar. Según un informe de la Asociación Colombiana de Universidades (ASCUN) (2019), el robo es uno de los problemas de seguridad más comunes en las universidades colombianas. La falta de iluminación y seguridad en los campus universitarios también puede contribuir a la ocurrencia de robos. El reconocimiento facial podría ayudar a prevenir robos mediante la identificación de personas no autorizadas en la Fundación Universitaria Compensar. La tecnología podría utilizarse para controlar el acceso a las instalaciones de la Universidad, garantizando que solo el personal y los estudiantes autorizados tengan acceso a áreas restringidas.

Además del robo, también hay un problema creciente de acoso sexual en las universidades de Colombia. Un estudio de la Universidad Nacional de Colombia (2019) reveló que el 20% de las mujeres universitarias han sufrido acoso sexual en el campus universitario. El reconocimiento facial podría ayudar a prevenir el acoso sexual mediante la identificación de posibles agresores en el campus. La tecnología podría utilizarse para vigilar las zonas comunes y detectar posibles actividades sospechosas.

Otro estudio realizado en 2021 examinó los beneficios del reconocimiento facial en el control de acceso a edificios y espacios, encontrando que esta tecnología puede mejorar la seguridad y la eficiencia de los sistemas de control de acceso (Chen et al., 2021). El libro de Zolotarjovs aborda este tema, proporcionando información detallada sobre los algoritmos de reconocimiento facial utilizados en el control de acceso.

El reconocimiento facial puede ser utilizado como una medida de seguridad efectiva en lugares públicos, especialmente en aeropuertos, estaciones de tren y estadios deportivos (Rizvi, Rakocevic, & Qureshi, 2021).

El reconocimiento facial puede ser más eficiente que los métodos tradicionales de control de acceso, ya que puede realizar la identificación de manera más rápida y precisa. Según un estudio de

investigación, el uso de reconocimiento facial en el control de acceso puede reducir los tiempos de espera y aumentar la velocidad del flujo de personas en lugares públicos (Amin, Muhammad, & Ali, 2021).

El control de acceso mediante reconocimiento facial puede ofrecer una mayor comodidad a los usuarios, ya que elimina la necesidad de utilizar tarjetas de acceso o contraseñas. Según un artículo de revisión, el reconocimiento facial puede mejorar la experiencia del usuario y proporcionar un acceso sin fricciones a lugares y servicios (Han, Peng, & Zhang, 2021).

Trabajar en la investigación enfocada hacia modelos de inteligencia artificial para el reconocimiento facial es una oportunidad para mejorar la seguridad y la eficiencia del control de acceso a los entornos universitarios.

1.2. Antecedentes

Un control de acceso mediante reconocimiento facial utiliza tecnologías de inteligencia artificial para analizar características faciales únicas y autenticar la identidad de una persona. En particular, se utilizan algoritmos de aprendizaje automático para entrenar a un sistema de reconocimiento facial y mejorar su precisión en la identificación de individuos.

Según Alotaibiet et al. (2019), los modelos de Inteligencia Artificial tienen la capacidad de analizar grandes cantidades de datos en tiempo real y con una alta precisión, lo que permite una identificación rápida y precisa de las personas. Esta característica es especialmente útil en aplicaciones como el control de acceso y la seguridad en las universidades. Los autores indican que los modelos de inteligencia artificial tienen una tasa de precisión del 97,5% en el reconocimiento facial, lo que es considerablemente mayor que la tasa de precisión de los métodos tradicionales como tarjetas de identificación, cámaras de seguridad, guardas de seguridad:(Alotaibiet et al., 2019).

Los modelos de Inteligencia Artificial tienen la capacidad de ser entrenados para reconocer rostros en diversas situaciones, tales como diferentes ángulos, expresiones faciales y condiciones de iluminación variable, lo que permite un uso más amplio de la tecnología de reconocimiento facial en

diferentes contextos. Según KarimianAzari et al. (2021), los modelos de inteligencia artificial pueden ser entrenados para reconocer rostros en diferentes condiciones con una alta tasa de precisión.

El uso de modelos de Inteligencia Artificial en el reconocimiento facial puede mejorar la eficiencia en diversas aplicaciones, tales como el control de acceso a las universidades o la identificación de sospechosos en delitos, debido a que la tecnología de reconocimiento facial puede automatizar procesos que antes requerían intervención humana. De acuerdo con Jia et al. (2020), el uso de modelos de Inteligencia Artificial para el reconocimiento facial en aplicaciones de seguridad pública puede mejorar la eficiencia y precisión.

El uso de modelos de inteligencia artificial para el reconocimiento facial puede mejorar la eficiencia en aplicaciones como el control de acceso a las universidades, la identificación de sospechosos en delitos, entre otras. Esto se debe a que la tecnología de reconocimiento facial puede automatizar procesos que antes requerían la intervención humana. Según un estudio realizado por Jia et al. (2020), el uso de modelos de inteligencia artificial para el reconocimiento facial en aplicaciones de seguridad pública puede mejorar la eficiencia y la precisión.

Según Smith y Johnson (2021), el reconocimiento facial tiene el potencial de mejorar la eficiencia y seguridad en diversos campos como la aplicación de la ley, la atención médica y el comercio. En el aeropuerto, por ejemplo, el uso de esta tecnología puede agilizar el proceso de registro y mejorar la experiencia de viaje. Además, esta tecnología también puede ser útil para la identificación de personas desaparecidas o la búsqueda de sospechosos de delitos.

El uso de modelos de inteligencia artificial para el reconocimiento facial tiene varios beneficios, como mayor precisión y velocidad, flexibilidad, eficiencia y seguridad mejorada. Varios estudios citados en la literatura muestran que la tecnología de reconocimiento facial es una herramienta prometedora en diversas aplicaciones, y su uso seguirá expandiéndose en el futuro (Singh, 2020; Li et al., 2021).

En el ámbito universitario, los sistemas de reconocimiento facial pueden ser de gran ayuda en varios aspectos, como la seguridad, la gestión de recursos y el control de asistencia. Por ejemplo, estudios han demostrado que el uso de sistemas de reconocimiento facial puede reducir los índices de delincuencia en las universidades, ya que permite identificar a individuos sospechosos y detectar situaciones de riesgo de forma temprana (Jain, Ross, & Nandakumar, 2016)

Además, los sistemas de reconocimiento facial también pueden ser utilizados para la gestión de recursos en las universidades, como la biblioteca o los laboratorios. Por ejemplo, algunos estudios han demostrado que el uso de sistemas de reconocimiento facial para la gestión de préstamos en la biblioteca puede mejorar la eficiencia del sistema y reducir los índices de extravío de libros (Jain et al., 2016).

Según Gómez, Rodríguez y Pérez (2021), se ha desarrollado un sistema de identificación de estudiantes mediante reconocimiento facial en dos universidades colombianas. Este sistema utiliza un modelo de inteligencia artificial para analizar las imágenes faciales de los estudiantes y compararlas con una base de datos de fotos previamente almacenadas. Los autores concluyen que el sistema tiene el potencial de mejorar la eficiencia de la identificación de estudiantes y reducir la posibilidad de fraude.

En esta investigación, los autores exploran cómo los modelos de inteligencia artificial para el reconocimiento facial pueden mejorar la seguridad en las universidades colombianas. Se propone el uso de cámaras de seguridad con capacidad de reconocimiento facial para monitorear el acceso a edificios y detectar a personas no autorizadas. Los autores también discuten los desafíos éticos y de privacidad que deben abordarse antes de implementar esta tecnología. López, M., y Medina, J. (2021).

En este artículo, los autores proponen el uso de modelos de inteligencia artificial para el reconocimiento facial en la toma de asistencia en las aulas universitarias en Colombia. Se argumenta que esta tecnología puede mejorar la precisión de la toma de asistencia y reducir la carga de trabajo de

los docentes. Los autores también discuten los posibles desafíos técnicos y de privacidad asociados con el uso de esta tecnología. Rueda, L., y Torres, S. (2020).

1.3. Estado del arte

En Colombia, el reconocimiento facial ha experimentado un crecimiento considerable en el ámbito de la seguridad, impulsado por el desarrollo de algoritmos de Inteligencia Artificial y Aprendizaje Automático que mejoran la precisión y eficiencia de estos sistemas (García & Moreno, 2020). La adopción de esta tecnología ha sido evidente en diversos sectores, como la educación, el transporte y el control de acceso a instalaciones públicas y privadas (Rodríguez & Valencia, 2021).

Un caso notable en Colombia es el sistema de reconocimiento facial implementado en el Metro de Medellín (Gómez et al., 2019). Este sistema, basado en Inteligencia Artificial y Aprendizaje Automático, ha permitido mejorar la seguridad en las estaciones, identificando y alertando sobre individuos con antecedentes penales o en listas de vigilancia. Otro ejemplo es la Universidad EAFIT en Medellín (Hincapié & Salazar, 2020), donde se ha desarrollado un sistema de reconocimiento facial para controlar el acceso al campus y detectar intrusos, generando alertas en tiempo real al personal de seguridad.

El Metro de Medellín es un ejemplo destacado del uso de reconocimiento facial en Colombia (Gómez et al., 2019). Gracias a la implementación de un sistema basado en Inteligencia Artificial y Aprendizaje Automático, la seguridad en las estaciones ha mejorado, permitiendo identificar y alertar sobre individuos con antecedentes penales o en listas de vigilancia. Este caso demuestra cómo la tecnología de reconocimiento facial puede contribuir significativamente a la seguridad del transporte público en el país.

La Universidad EAFIT en Medellín ha desarrollado un sistema de reconocimiento facial para controlar el acceso al campus (Hincapié & Salazar, 2020). La tecnología permite detectar intrusos y

genera alertas en tiempo real al personal de seguridad, mejorando así la protección de los estudiantes, profesores y personal administrativo. Esta experiencia exitosa muestra cómo la aplicación de la Inteligencia Artificial en el reconocimiento facial puede impulsar la seguridad en instituciones educativas en Colombia.

El estadio Atanasio Girardot en Medellín ha implementado un sistema de reconocimiento facial con el fin de mejorar la seguridad durante eventos deportivos y masivos (Morales et al., 2021). La tecnología basada en Inteligencia Artificial y Aprendizaje Automático permite identificar a personas prohibidas de ingresar al estadio o a quienes representen un riesgo para la seguridad. Este caso resalta el potencial de los sistemas de reconocimiento facial para mejorar la seguridad en espacios públicos de gran afluencia en Colombia.

A pesar de los avances y casos de éxito en la implementación de sistemas de reconocimiento facial en Colombia, aún persisten desafíos relacionados con la calidad de los datos, la infraestructura y la capacitación del personal de seguridad (Zapata et al., 2021). Sin embargo, estos desafíos también representan oportunidades para la innovación y el desarrollo de soluciones tecnológicas adaptadas al contexto colombiano, que permitan mejorar la seguridad en instituciones como la Fundación Universitaria Compensar (Rojas & García, 2023).

El algoritmo K-means es uno de los métodos de agrupación más utilizados en el análisis de datos. Según Jain (2010), este algoritmo es especialmente útil para la agrupación de grandes conjuntos de datos debido a su eficiencia computacional. Sin embargo, también destaca que K-means tiene limitaciones, como la sensibilidad a los valores iniciales y la dificultad para identificar grupos de formas no esféricas o de tamaños desiguales (Jain, 2010).

El algoritmo DBSCAN (Density-Based Spatial Clustering of Applications with Noise) es un método de agrupación basado en densidad que puede identificar grupos de formas arbitrarias y manejar eficazmente el ruido. Según Ester et al. (1996), DBSCAN tiene la ventaja de no requerir que se

especifique el número de grupos a priori, a diferencia de K-means. Sin embargo, puede tener dificultades para identificar grupos de densidades muy diferentes (Ester, Kriegel, Sander, & Xu, 1996).

Las Redes Neuronales Artificiales (ANN) son modelos computacionales inspirados en el cerebro humano y han demostrado ser altamente efectivas para una amplia gama de tareas, desde el reconocimiento de patrones hasta la toma de decisiones. Según Schmidhuber (2015), las ANN han revolucionado numerosos campos, desde la visión por computadora hasta el procesamiento del lenguaje natural. No obstante, también señala que las ANN pueden ser computacionalmente costosas y pueden requerir grandes cantidades de datos para su entrenamiento (Schmidhuber, 2015).

1.4. Antecedentes

Un control de acceso mediante reconocimiento facial utiliza tecnologías de inteligencia artificial para analizar características faciales únicas y autenticar la identidad de una persona. En particular, se utilizan algoritmos de aprendizaje automático para entrenar a un sistema de reconocimiento facial y mejorar su precisión en la identificación de individuos.

Según Alotaibiet et al. (2019), los modelos de Inteligencia Artificial tienen la capacidad de analizar grandes cantidades de datos en tiempo real y con una alta precisión, lo que permite una identificación rápida y precisa de las personas.

Esta característica es especialmente útil en aplicaciones como el control de acceso y la seguridad en las universidades. Los autores indican que los modelos de inteligencia artificial tienen una tasa de precisión del 97,5% en el reconocimiento facial, lo que es considerablemente mayor que la tasa de precisión de los métodos tradicionales como tarjetas de identificación, cámaras de seguridad, guardas de seguridad:(Alotaibiet et al., 2019).

Los modelos de Inteligencia Artificial tienen la capacidad de ser entrenados para reconocer rostros en diversas situaciones, tales como diferentes ángulos, expresiones faciales y condiciones de

iluminación variable, lo que permite un uso más amplio de la tecnología de reconocimiento facial en diferentes contextos.

Según Karimian- Azari et al. (2021), los modelos de inteligencia artificial pueden ser entrenados para reconocer rostros en diferentes condiciones con una alta tasa de precisión.

El uso de modelos de Inteligencia Artificial en el reconocimiento facial puede mejorar la eficiencia en diversas aplicaciones, tales como el control de acceso a las universidades o la identificación de sospechosos en delitos, debido a que la tecnología de reconocimiento facial puede automatizar procesos que antes requerían intervención humana.

De acuerdo con Jia et al. (2020), el uso de modelos de Inteligencia Artificial para el reconocimiento facial en aplicaciones de seguridad pública puede mejorar la eficiencia y precisión. El uso de modelos de inteligencia artificial para el reconocimiento facial puede mejorar la eficiencia en aplicaciones como el control de acceso a las universidades, la identificación de sospechosos en delitos, entre otras.

Esto se debe a que la tecnología de reconocimiento facial puede automatizar procesos que antes requerían la intervención humana. Según un estudio realizado por Jia et al. (2020), el uso de modelos de inteligencia artificial para el reconocimiento facial en aplicaciones de seguridad pública puede mejorar la eficiencia y la precisión.

Según Smith y Johnson (2021), el reconocimiento facial tiene el potencial de mejorar la eficiencia y seguridad en diversos campos como la aplicación de la ley, la atención médica y el comercio. En el aeropuerto, por ejemplo, el uso de esta tecnología puede agilizar el proceso de registro y mejorar la experiencia de viaje.

Además, esta tecnología también puede ser útil para la identificación de personas desaparecidas o la búsqueda de sospechosos de delitos.

El uso de modelos de inteligencia artificial para el reconocimiento facial tiene varios beneficios, como mayor precisión y velocidad, flexibilidad, eficiencia y seguridad mejorada. Varios estudios citados en la literatura muestran que la tecnología de reconocimiento facial es una herramienta prometedora en diversas aplicaciones, y su uso seguirá expandiéndose en el futuro (Singh, 2020; Li et al., 2021).

En el ámbito universitario, los sistemas de reconocimiento facial pueden ser de gran ayuda en varios aspectos, como la seguridad, la gestión de recursos y el control de asistencia. Por ejemplo, estudios han demostrado que el uso de sistemas de reconocimiento facial puede reducir los índices de delincuencia en las universidades, ya que permite identificar a individuos sospechosos y detectar situaciones de riesgo de forma temprana (Jain, Ross, & Nandakumar, 2016)

Además, los sistemas de reconocimiento facial también pueden ser utilizados para la gestión de recursos en las universidades, como la biblioteca o los laboratorios. Por ejemplo, algunos estudios han demostrado que el uso de sistemas de reconocimiento facial para la gestión de préstamos en la biblioteca puede mejorar la eficiencia del sistema y reducir los índices de extravío de libros (Jain et al., 2016).

Según Gómez, Rodríguez y Pérez (2021), se ha desarrollado un sistema de identificación de estudiantes mediante reconocimiento facial en dos universidades colombianas. Este sistema utiliza un modelo de inteligencia artificial para analizar las imágenes faciales de los estudiantes y compararlas con una base de datos de fotos previamente almacenadas. Los autores concluyen que el sistema tiene el potencial de mejorar la eficiencia de la identificación de estudiantes y reducir la posibilidad de fraude.

En esta investigación, los autores exploran cómo los modelos de inteligencia artificial para el reconocimiento facial pueden mejorar la seguridad en las universidades colombianas. Se propone el uso de cámaras de seguridad con capacidad de reconocimiento facial para monitorear el acceso a edificios y detectar a personas no autorizadas. Los autores también discuten los desafíos éticos y de privacidad que deben abordarse antes de implementar esta tecnología. López, M., y Medina, J. (2021).

En este artículo, los autores proponen el uso de modelos de inteligencia artificial para el reconocimiento facial en la toma de asistencia en las aulas universitarias en Colombia. Se argumenta que

esta tecnología puede mejorar la precisión de la toma de asistencia y reducir la carga de trabajo de los docentes. Los autores también discuten los posibles desafíos técnicos y de privacidad asociados con el uso de esta tecnología. Rueda, L., y Torres, S. (2020).

1.5. Objetivos

1.5.1. Objetivo General

Desarrollar un modelo de inteligencia artificial por medio de analítica de datos de reconocimiento facial que permita generar alertas de intrusión a la Fundación Universitaria Compensar.

1.5.2. Objetivos Específicos

- Definir claramente los requerimientos del software a partir de la consulta de fuentes bibliográficas para garantizar una comprensión completa y precisa de las funcionalidades que debe tener el prototipo.
- Diseñar un modelo de inteligencia artificial que permita generar alertas de intrusión a partir de analítica de datos de reconocimiento facial.
- Establecer una estrategia de validación adecuada, mediante evaluación simulada que permita verificar la correcta operación del modelo.

1.6. Alcances y Limitaciones

1.6.1. Alcances

- E l modelo de reconocimiento facial debe tener las funciones básicas que permitan realizar tareas específicas como identificación precisa y rápida de rostros.
- el modelo de control de acceso mediante reconocimiento facial debe contar con medidas de seguridad que protejan la información y los datos de los usuarios, como, por ejemplo, en un sistema de banca en línea, el prototipo de control de acceso mediante reconocimiento facial debe contar con medidas de autenticación y encriptación.

- el modelo de control de acceso mediante reconocimiento facial debe ser capaz de integrarse con otros sistemas y aplicaciones, lo que permitirá una mayor interoperabilidad y eficiencia en los procesos.
- el modelo de control de acceso mediante reconocimiento facial debe ser capaz de manejar grandes volúmenes de datos y usuarios, permitiendo así que el sistema pueda crecer y adaptarse a las necesidades futuras.

1.6.2. Limitaciones

Debido a la limitación del tiempo disponible para el proyecto, el prototipo de control de acceso mediante reconocimiento facial no pueda ser tan completo o complejo como se desea. El equipo de desarrollo debe limitar el número de funciones o características para garantizar que se puedan cumplir los plazos.

La calidad el prototipo de control de acceso mediante reconocimiento facial se verá afectado debido a la presión del tiempo y la necesidad de cumplir plazos. Es posible que el equipo de desarrollo no tenga suficiente tiempo para realizar pruebas exhaustivas o para asegurarse de que el software cumpla con los estándares de calidad.

El equipo de desarrollo tiene limitaciones técnicas que impiden que el prototipo de control de acceso mediante reconocimiento facial sea tan completo o sofisticado como se desea. Esto se debe a limitaciones de hardware, software y de recursos humanos.

Debido a la limitación del tiempo disponible, es difícil para el equipo de desarrollo comunicarse con el cliente y comprender completamente sus necesidades. Esto puede llevar a malentendidos y errores en el desarrollo del prototipo de control de acceso mediante reconocimiento facial.

2. Método

2.1. Metodología de Investigación

Se propone la siguiente metodología, la cual se divide en tres fases con el fin de cumplir los objetivos específicos.

2.1.1. Fase N° 1 Identificación

En esta fase se identifican los requerimientos técnicos y funcionales del sistema y factores como el alcance, la complejidad y el presupuesto del modelo.

2.1.1.1. Metodología

Metodología de investigación múltiple.

2.1.1.2. Secuencia de Actividades:

- Realizar una revisión de literatura para conocer el estado del arte en el campo del reconocimiento facial y de la inteligencia artificial para la detección de intrusos.
- Analizar el problema de seguridad existente en el lugar donde se desea implementar el sistema de reconocimiento facial y cómo el modelo puede ayudar a resolverlo.
- Definir los requisitos del sistema en términos de precisión, velocidad, escalabilidad y compatibilidad con otras tecnologías existentes.

2.1.1.3. Producto fase de identificación

Definición y análisis detallado de los requisitos del sistema de reconocimiento facial.

2.1.1.4. Requerimientos No Funcionales

Los requerimientos no funcionales que se elaboraron para el desarrollo del prototipo/modelo:

Tabla 1 *RN-S-01*

Identificación	**RN-S-01**
Descripción	El sistema de control de acceso debe garantizar la seguridad de la información

	personal y confidencial de los usuarios, así como la protección de los bienes y recursos de la universidad.
Prioridad	Alta
Categoría	Seguridad
Tipo	Restricción de diseño
Fuente	Clientes y regulaciones gubernamentales
Estado	Aprobado
Riesgos	El incumplimiento de este requerimiento podría poner en riesgo la privacidad y seguridad de los usuarios y la propiedad de la universidad.
Comentarios	Incluir medidas de seguridad robustas, tales como autenticación de dos factores, encriptación de datos, y monitoreo continuo del sistema.

Tabla 2 *RN-S-02*

Identificación	**RN-NF-02**
Descripción	El sistema de control de acceso debe ser preciso y confiable para garantizar que solo las personas autorizadas tengan acceso a las instalaciones y recursos de la universidad.

Prioridad	Alta
Categoría	Usabilidad
Tipo	Restricción de diseño
Fuente	usuarios finales
Estado	Aprobado
Riesgos	La falta de precisión podría permitir el acceso no autorizado o impedir el acceso de personas autorizadas.
Comentarios	La falta de precisión podría permitir el acceso no autorizado o impedir el acceso de personas autorizadas.

Tabla 3 *RN-S-03*

Identificación	**RN-NF-03**
Descripción	El sistema de control de acceso debe ser rápido y eficiente para evitar retrasos innecesarios en el ingreso de los usuarios autorizados.
Prioridad	Media
Categoría	Rendimiento
Tipo	Restricción de diseño
Fuente	Usuarios finales
Estado	Aprobado

Riesgos	La falta de velocidad podría causar retrasos en el acceso de los usuarios, lo que podría tener un impacto negativo en la productividad y la satisfacción de los usuarios.
Comentarios	El sistema debe ser capaz de procesar rápidamente las solicitudes de acceso y responder en un tiempo mínimo.

Tabla 4 *RN-S-04*

Identificación	**RN-NF-04**
Descripción	El sistema de control de acceso debe ser escalable para permitir su crecimiento a medida que la universidad expande sus instalaciones y recursos.
Prioridad	Alta
Categoría	Escalabilidad
Tipo	Restricción de diseño
Fuente	Usuarios Finales
Estado	Aprobado
Riesgos	La falta de escalabilidad podría limitar el crecimiento futuro de la universidad y requerir la inversión en una nueva solución

Comentarios	El sistema debe ser capaz de soportar un número creciente de usuarios y dispositivos sin comprometer su rendimiento.

Tabla 5 *RN-S-05*

Identificación	**RN-NF-05**
Descripción	El sistema de control de acceso debe ser compatible e integrable con otros sistemas de seguridad y control de acceso existentes en la universidad.
Prioridad	Alta
Categoría	Integración
Tipo	Restricción de diseño
Fuente	Cliente
Estado	Aprobado
Riesgos	Si el sistema de control de acceso no es compatible con los sistemas existentes, puede generar problemas de interoperabilidad y reducir la eficacia de todo el sistema de seguridad.
Comentarios	Se debe asegurar que el sistema de control de acceso pueda integrarse sin problemas con otros sistemas de seguridad y control de acceso en la universidad.

Identificación	**RN-NF-06**
Descripción	El sistema de control de acceso debe garantizar la seguridad de la información personal y confidencial de los usuarios, así como la protección de los bienes y recursos de la universidad.
Prioridad	Alta
Categoría	Seguridad
Tipo	Restricción de diseño
Fuente	Clientes y regulaciones gubernamentales
Estado	Aprobado
Riesgos	El incumplimiento de este requerimiento podría poner en riesgo la privacidad y seguridad de los usuarios y la propiedad de la universidad.
Comentarios	Incluir medidas de seguridad robustas, tales como autenticación de dos factores, encriptación de datos, y monitoreo continuo del sistema.

Tabla 6 *RN-S-06*

Identificación	**RN-NF-06**
Descripción	El sistema de control de acceso debe ser fácil de usar para los usuarios autorizados y el

	personal de la universidad encargado de su administración.
Prioridad	Alta
Categoría	Usabilidad
Tipo	Restricción de diseño
Fuente	Usuarios
Estado	Aprobado
Riesgos	Si el sistema de control de acceso es difícil de usar, los usuarios pueden cometer errores y esto puede afectar la seguridad de la universidad.
Comentarios	La facilidad de uso debe ser una consideración importante durante todo el proceso de diseño e implementación del sistema de control de acceso.

Tabla 7 *RN-S-07*

Identificación	**RN-NF-07**
Descripción	El sistema de control de acceso debe garantizar la seguridad de la información personal y confidencial de los usuarios, así como la protección de los bienes y recursos de la universidad.
Prioridad	Alta

Categoría	Seguridad
Tipo	Restricción de diseño
Fuente	Clientes y regulaciones gubernamentales
Estado	Aprobado
Riesgos	El incumplimiento de este requerimiento podría poner en riesgo la privacidad y seguridad de los usuarios y la propiedad de la universidad.
Comentarios	Incluir medidas de seguridad robustas, tales como autenticación de dos factores, encriptación de datos, y monitoreo continuo del sistema.

Tabla 8 *RN-S-08*

Identificación	**RN-NF-08**
Descripción	El sistema de control de acceso debe ser adaptable para permitir la integración de nuevas tecnologías y mejoras en el futuro.
Prioridad	Media
Categoría	Mantenibilidad
Tipo	Restricción de diseño
Fuente	Cliente
Estado	Aprobado

Riesgos	Si el sistema de control de acceso no es adaptable, puede quedar obsoleto rápidamente y no poder mantenerse al día con las nuevas tecnologías y mejoras.
Comentarios	La adaptabilidad es esencial para garantizar que el sistema de control de acceso pueda mantenerse al día con las cambiantes necesidades y requisitos de seguridad de la universidad

Tabla 9 *RN-S-09*

Identificación	**RN-NF-09**
Descripción	El sistema de control de acceso debe ser eficiente en el consumo de energía para reducir su impacto ambiental y reducir costos de operación.
Prioridad	Media
Categoría	Rendimiento
Tipo	Restricción de diseño
Fuente	Clientes y regulaciones gubernamentales
Estado	Aprobado
Riesgos	Si el sistema de control de acceso consume demasiada energía, puede tener un impacto

	negativo en el medio ambiente y aumentar los costos de operación.
Comentarios	La eficiencia energética debe ser una consideración importante durante todo el proceso de diseño e implementación del sistema de control de acceso.

Tabla 20 *RN-S-10*

Identificación	**RN-NF-10**
Descripción	El sistema de control de acceso debe contar con una función de alerta de intrusión basada en AI, que permita detectar y alertar al personal de seguridad de la universidad sobre cualquier actividad sospechosa en tiempo real.
Prioridad	Media
Categoría	Seguridad
Tipo	Restricción de implementación
Fuente	Equipo de seguridad de la universidad
Estado	Aprobado
Riesgos	La función de alerta de intrusión podría generar alertas falsas, lo que podría ser un problema para el personal de seguridad de la universidad si se vuelven demasiado comunes.

Comentarios	Es importante que la función de alerta de intrusión sea confiable y precisa para evitar alertas falsas que podrían ser ignoradas y poner en peligro la seguridad de la universidad.

Tabla 13 *RN-S-11*

Identificación	**RN-NF-11**
Descripción	El sistema de control de acceso debe proteger la privacidad de los usuarios autorizados, evitando el uso indebido de sus datos personales o la vigilancia excesiva.
Prioridad	Alta
Categoría	Seguridad / Privacidad
Tipo	Restricción de implementación
Fuente	Regulaciones y normas de protección de datos
Estado	Aprobado
Riesgos	El incumplimiento de las regulaciones de protección de datos podría poner en peligro la privacidad y la seguridad de los usuarios autorizados del sistema de control de acceso.
Comentarios	Es fundamental que el sistema de control de acceso garantice la privacidad y la seguridad de los usuarios autorizados, sin violar las

	regulaciones y normas de protección de datos aplicables.

Fuente: Los autores.

2.1.1.5. Historias de Usuario

Historias de usuario que se elaboraron para el desarrollo del prototipo/modelo.

2.1.2. HU01

- Activar el sistema de reconocimiento facial y control de acceso a través de la cámara vinculada.

Tabla 42 *HU01*

Número	**HU01**
Titulo	Opción "Encender cámara" en la pantalla principal
Como usuario **quiero** que se pueda activar el sistema de reconocimiento facial a través de la cámara vinculada y poder realizar el control de acceso del personal registrado en la institución	
Descripción: El sistema debe contar con la opción "Encender cámara" en la pantalla principal para activar el sistema de reconocimiento facial a través de la cámara vinculada. Cuando el usuario intenta ingresar y su rostro es reconocido correctamente, se debe permitir el acceso y generar un Log de auditoría con la fecha y hora, y los datos almacenados del usuario en el sistema (Identificación, Nombres, Edad, Genero). También este debe alimentar el dataset “AttributFaces” el cual contiene el FaceToken (Identificador de los datos biométricos de la imagen) del rostro y los valores de los rasgos emocionales y características de la imagen (id, image, anger, disgust, neutral, sadness, surprise, happiness, glass, smile, intruder, faceUser)	

Prioridad
Alta
Dependencias
• Una cámara vinculada y un API de reconocimiento facial.
Criterios de aceptación:
• La opción "Encender cámara" está disponible en la pantalla principal. • El sistema reconoce correctamente el rostro del usuario registrado. • Se muestra el mensaje "Su ingreso es exitoso". • Generación de Log de auditoría y alimentación del dataset.
Notas adicionales:
N/A

2.1.3. HU02

- Validar que el usuario no cierre los ojos.

Tabla 13 *HU02*

Número	**HU02**
Titulo	Validar que el usuario no cierre los ojos
Como usuario **quiero** que cuando el usuario que intenta ingresar tiene los ojos cerrados debe mostrar el mensaje “Por favor no cerrar los ojos” y este mensaje debe permanecer habilitado hasta que reconozca plenamente el rostro y permitir el ingreso	
Descripción: Cuando el usuario intenta ingresar y cierra los ojos, se debe mostrar el mensaje "Por favor no cerrar los ojos". Este mensaje debe permanecer habilitado hasta que se reconozca plenamente el rostro y se permita el ingreso.	

Prioridad
Media
Dependencias
• Una cámara vinculada y un API de reconocimiento facial.
Criterios de aceptación:
• Cuando el usuario cierra los ojos, se muestra el mensaje "Por favor no cerrar los ojos". • El mensaje permanece habilitado hasta que se reconoce plenamente el rostro y se permite el ingreso.
Notas adicionales:
N/A

2.1.4. HU03

- Validación de rostro en movimiento o fuera del alcance.

Tabla 14 *HU03*

Número	**HU03**
Titulo	Validación de rostro en movimiento o fuera del alcance
Como usuario **quiero** que cuando el usuario que intenta ingresar no está en el alcance de la cámara o está en movimiento continuo debe mostrar el mensaje “No se ha procesado la detección de un rostro, por favor procure no moverse” y este mensaje debe permanecer habilitado hasta que reconozca plenamente el rostro y permitir el ingreso.	
Descripción:	

El sistema debe ser capaz de validar el rostro del usuario incluso si este está en movimiento o está fuera del alcance de la cámara donde no se detecte plenamente, mostrando un mensaje que indique que aún no se ha procesado la detección de un rostro y que el usuario debe permanecer quieto hasta que se complete la validación. Una vez validado, el usuario deberá recibir el mensaje de "Su ingreso es exitoso".
Prioridad
Media
Dependencias
• Se requiere una cámara de alta calidad que permita la detección de rostros en movimiento, así como una conexión estable a la red para la transmisión de datos biométricos.
Criterios de aceptación:
• El sistema debe ser capaz de detectar el rostro del usuario incluso si este se encuentra en movimiento. • El mensaje de "No se ha procesado la detección de un rostro" debe mostrarse hasta que se complete la validación. • El mensaje de "Su ingreso es exitoso" debe mostrarse cuando se haya validado el rostro del usuario en movimiento.
Notas adicionales:
Se recomienda realizar pruebas de campo para evaluar la eficacia de la validación en condiciones de movimiento.

2.1.5. HU04

- Validación de rostro de un solo usuario.

Tabla 15 *HU04*

Número	**HU04**
Titulo	Validación de rostro de un solo usuario

Como usuario **quiero** que cuando el usuario que intenta ingresar está acompañado de otro individuo y por ende el sistema de reconocimiento facial detecta dos rostros debe mostrar el mensaje “Se detectaron dos rostros” y este mensaje debe permanecer habilitado hasta que reconozca plenamente un solo rostro y así realizar la validación que permite el ingreso

Descripción:

El sistema debe ser capaz de detectar si hay más de un rostro en la imagen y mostrar un mensaje de "Se detectaron dos rostros" hasta que se detecte un solo rostro, momento en el que se completará la validación y se mostrará el mensaje de "Su ingreso es exitoso".

Prioridad

Media

Dependencias

- Se requiere una cámara de alta calidad que permita la detección de rostros y la identificación de más de un rostro en la imagen.

Criterios de aceptación:

- El sistema debe ser capaz de detectar si hay más de un rostro en la imagen y mostrar el mensaje de "Se detectaron dos rostros".
- El mensaje de "Se detectaron dos rostros" debe permanecer habilitado hasta que se detecte un solo rostro.
- El mensaje de "Su ingreso es exitoso" debe mostrarse una vez que se complete la validación y se detecte un solo rostro.

Notas adicionales:

Se recomienda realizar pruebas de campo para evaluar la eficacia de la detección de múltiples rostros en la imagen.

2.1.6. HU05

- Validación de usuario no registrado.

Tabla 16 *HU05*

Número	**HU05**
Titulo	Validación de usuario no registrado
Como usuario **quiero** que cuando el usuario que intenta ingresar no se encuentra registrado, el sistema de reconocimiento facial una vez detecta el rostro y realice la validación de existencia y determine que no está registrado debe mostrar el siguiente mensaje “El rostro no se encuentra registrado en el sistema”, cuando el sistema detecte que realizo esta validación por tres veces, debe registrar el rostro que intento ingresar en las listas negras del sistema y se debe enviar el rostro a validación del modelo de inteligencia artificial donde se determina si es un intruso, de ser un intruso se debe enviar un correo de alerta de intrusión al correo parametrizado con las características biométricas del individuo, fecha y hora en la que intento acceder. Además, debe generar un Log de auditoría con la fecha y hora y la imagen de la persona que intento acceder, También este debe alimentar el dataset “AttributFaces” el cual contiene el FaceToken (Identificador de los datos biométricos de la imagen) del rostro y los valores de los rasgos emocionales y características de la imagen (id, image, anger, disgust, neutral, sadness, surprise, happiness, glass, smile, intruder, faceUser)	
Descripción: El sistema de reconocimiento facial debe ser capaz de detectar si el usuario que intenta ingresar no se encuentra registrado en el sistema y mostrar un mensaje de error correspondiente. Si este caso	

se presenta en tres intentos consecutivos, el sistema debe registrar el rostro en las listas negras del sistema y según el modelo de machine learning implementado se debe enviar una alerta por correo electrónico a los administradores del sistema. Además, se debe generar un Log con información detallada sobre los datos biométricos del rostro y los resultados del API.
Prioridad
Alta
Dependencias
• Integración con el API de reconocimiento facial • Conexión a base de datos de usuarios registrados y lista negra • Implementación de modelo de AI de detección de intrusión • Configuración de envío de correos electrónicos
Criterios de aceptación:
• El sistema debe mostrar un mensaje de error si el usuario no está registrado en el sistema. • Si el error se presenta en tres intentos consecutivos, el sistema debe registrar el rostro en la lista negra y enviar una alerta por correo electrónico. • Generación de Log de auditoría y alimentación del dataset.
Notas adicionales:
El registro en la lista negra debe ser permanente y no se puede eliminar por ningún usuario, la única forma de la eliminación es el registro de este usuario. Además, la información registrada en el Log debe ser suficiente para rastrear el origen de la intrusión en caso de ser necesario.

2.1.7. HU06

- Bloqueo de acceso para usuarios en lista negra.

Tabla 17 HU06

Número	**HU06**
Titulo	Bloqueo de acceso para usuarios en lista negra

Como usuario **quiero** que cuando el usuario que intenta ingresar se encuentra registrado en la lista negra, no debe permitir el acceso y debe mostrar el siguiente mensaje “Este usuario no tiene permitido el acceso”, se debe inhabilitar el sistema de reconocimiento facial y debe ser activado nuevamente en la opción “Encender cámara”, además se generar un Log del evento

Descripción:

Cuando un usuario intenta ingresar al sistema y se encuentra registrado en la lista negra, el sistema debe bloquear el acceso y mostrar un mensaje correspondiente. Además, debe generar un Log de auditoría con la fecha y hora y la imagen de la persona que intento acceder, También este debe alimentar el dataset “AttributFaces” el cual contiene el FaceToken (Identificador de los datos biométricos de la imagen) del rostro y los valores de los rasgos emocionales y características de la imagen (id, image, anger, disgust, neutral, sadness, surprise, happiness, glass, smile, intruder, faceUser). El sistema de reconocimiento facial debe ser inhabilitado temporalmente y solo debe ser reactivado mediante la opción "Encender cámara".

Prioridad

Alta

Dependencias

- Integración con el API de reconocimiento facial
- Conexión a base de datos de usuarios registrados y lista negra

Criterios de aceptación:

- El sistema debe bloquear el acceso si el usuario está registrado en la lista negra.
- El sistema de reconocimiento facial debe ser inhabilitado temporalmente.

• Generación de Log de auditoría y alimentación del dataset.
Notas adicionales:
El sistema de reconocimiento facial debe ser reactivado solo mediante la opción "Encender cámara". Además, la información registrada en el Log debe ser suficiente para rastrear el origen del bloqueo de acceso en caso de ser necesario.

2.1.8. HU07

- Registro de Usuario.

Tabla 18 HU07

Número	**HU07**
Titulo	Registro de Usuario
Como usuario **quiero** que se permita registrar los datos y biometría facial de un nuevo usuario	
Descripción: El sistema debe contar con la opción de "Registrarse" en la pantalla principal y al ingresar en esa opción debe desplegar un formulario con los siguientes campos: Tipo Identificación (Cedula ciudadanía, Cedula extranjería, Pasaporte y Tarjeta de identidad), número de identificación, celular (validación de 10 dígitos que empiece con 3), sexo (Masculino, Femenino, Otro), primer nombre, segundo nombre, primer apellido, segundo apellido, edad, email (validación de estándar general de correos), dirección, facultad (Facultad de ingeniería, Facultad de Ciencias Empresariales, Facultad de Ciencias sociales y de la Educación, Facultad de Contaduría y finanzas internacionales y Facultad de comunicación) y carrera (ingeniería industrial, ingeniería de software, ingeniería de sistemas, ingeniería de Telecomunicaciones, Ciencia de Datos, Administración de Empresas, Administración logística, Administración de Servicios de Salud, Licenciatura de bilingüismo con énfasis en inglés, Licenciatura en educación infantil, Profesional en lenguas, Profesional en deporte	

y actividad física, Administración financiera, Contaduría Pública, Finanzas y negocios internacionales, Comunicación social, Mercadeo y publicidad, Diseño Visual). El sistema debe validar si el número de identificación ya existe, de ser así debe mostrar el mensaje “Usuario ya existe”.
Prioridad
Alta
Dependencias
• Integración con el sistema de base de datos para almacenar la información de los usuarios.
Criterios de aceptación:
• El formulario debe desplegar todos los campos mencionados anteriormente. • El sistema debe validar si el número de identificación ya existe en la base de datos. • Todos los campos obligatorios deben ser diligenciados para poder realizar el registro del usuario. • Al realizar el registro correctamente, debe presentar el mensaje de "Se ha registrado Exitosamente" y direccionar a la pantalla principal.
Notas adicionales:
Se debe tener en cuenta los requisitos legales y restricciones de seguridad para la manipulación de la información personal del usuario.

2.1.9. HU08

- Registro de Rostro.

Tabla 19 HU08

Número	**HU08**
Titulo	Registro de Rostro

Como usuario **quiero** que Cuando el usuario que intenta ingresar se encuentra registrado en la lista negra, no debe permitir el acceso y debe mostrar el siguiente mensaje “Este usuario no tiene permitido el acceso”, se debe inhabilitar el sistema de reconocimiento facial y debe ser activado nuevamente en la opción “Encender cámara”, además se generar un Log del evento
Descripción: El sistema debe contar con la opción de "Registrar Rostro" después de diligenciar el formulario de registro de usuario. Al seleccionar esta opción, se debe habilitar la cámara vinculada al sistema de reconocimiento facial y un botón "Tomar foto". El sistema debe realizar las siguientes validaciones a la foto tomada: 1. Cuando el usuario intenta registrar una foto que tiene los ojos cerrados debe mostrar el mensaje “Por favor no cerrar los ojos” y este mensaje debe permanecer habilitado hasta que se tome la foto nuevamente. 2. Cuando el usuario intenta registrar una foto que el rostro no está en el alcance de la cámara o está en movimiento continuo debe mostrar el mensaje “No se ha procesado la detección de un rostro, por favor procure no moverse” y este mensaje debe permanecer habilitado hasta que se tome la foto nuevamente. 3. Cuando el usuario intenta registrar una foto donde está acompañado de otro individuo y por ende el sistema de reconocimiento facial detecta dos rostros debe mostrar el mensaje “Se detectaron dos rostros” y este mensaje debe permanecer habilitado hasta que se tome la foto nuevamente. 4. Cuando el usuario intenta registrar una foto con un rostro que se encuentra registrado en la lista negra, no debe permitir el registro exitosamente y eliminar ese registro de ese rostro de las listas negras del sistema
Prioridad
Alta

Dependencias
• Integración con cámara y sistema de reconocimiento facial • Acceso a lista negra de rostros registrados previamente
Criterios de aceptación:
• El formulario de registro se despliega correctamente • Validaciones de los campos se realizan correctamente (tipo de identificación, número de identificación, celular, email, etc.) • Se valida si el número de identificación ya existe en el sistema y se muestra el mensaje correspondiente • La opción de "Registrar Rostro" está disponible y se habilita la cámara para tomar una foto • Se realizan las validaciones de la foto tomada y se muestra el mensaje correspondiente en caso de que la foto no cumpla con los criterios establecidos • El botón "Guardar Información" permite registrar al usuario correctamente si los datos obligatorios del formulario están diligenciados y la foto capturada cumple con los criterios establecidos • Se muestra el mensaje correspondiente de registro exitoso o se resaltan los campos que faltan por llenar si no se cumple con los criterios establecidos
Notas adicionales:
• El sistema debe contar con medidas de seguridad adecuadas para el manejo de información personal y biométrica • Debe existir una forma de eliminar o actualizar la información del usuario en caso de ser necesario • Es necesario considerar las regulaciones y leyes vigentes relacionadas con el manejo de información personal y biométrica.

2.1.10. HU09

- Reporte de Auditoría.

Tabla 20 HU09

Número	**HU09**
Titulo	Reporte de Auditoría
Como usuario **quiero** que se pueda mostrar el reporte de auditoría del control de acceso que muestre el detalle de las personas que están accediendo o intentando acceder a la universidad	
Descripción: El sistema de reconocimiento facial debe ser capaz de generar un registro por cada intento de acceso a la universidad, el cual se pueda consultar desde el apartado de "Auditoria" ubicado en la página principal, el cual debe tener los siguientes datos de los registros: (Fecha y hora de Acceso, Identificación, Nombre, Edad, Genero, Intruso*Si o No*, y la imagen de la persona que intento acceder al sistema), donde se deben mapear según los datos registrados en el sistema, si el registro se trata de un intruso solo debe mapear los campos de (Fecha y hora de Acceso y la imagen de la persona que intento acceder al sistema)	
Prioridad	
Baja	
Dependencias	
• Integración con el API de reconocimiento facial • Conexión a base de datos de usuarios registrados y lista negra	
Criterios de aceptación:	
• El sistema debe mostrar los registros en filas de 10 registros y pantallas de desplazamiento a las otras páginas donde se almacenen los demás registros • Debe contar con la opción de "Atrás" para volver a la página principal	

Notas adicionales:
La información registrada en los Log debe ser suficiente para rastrear el origen de la intrusión en caso de ser necesario.

Fuente: Los autores.

2.1.11. Fase N° 2 Fase de Diseño

En esta fase se define la arquitectura y los componentes necesarios para la implementación del modelo de reconocimiento facial. En esta fase se definen los algoritmos de procesamiento de imágenes y se determinan los requerimientos de hardware y software necesarios para su implementación.

2.1.11.1. Metodología:

- Diseño experimental.
- Modelo Descriptivo.
- Modelo de Simulación.

2.1.11.2. Secuencia de actividades:

- Investigar y evaluar diferentes algoritmos de reconocimiento facial para determinar cuál es el más adecuado para el modelo.
- Seleccionar el dataset de datos de rasgos faciales que se utilizará para entrenar y probar el modelo de alerta de intrusión.
- Entrenamiento del modelo utilizando con el algoritmo del elegido.
- Definición e implementación de metodología de desarrollo.

2.1.11.3. Producto de la fase de diseño

Modelo de reconocimiento facial con un sistema de alertas que permita generar alertas de intrusión.

2.1.11.4. Transformación y Selección de Datos

Seleccionar y preparar adecuadamente los datos es fundamental para el éxito del modelo de inteligencia artificial. Los datos son la base sobre la cual se construye el modelo, por lo que deben ser confiables, precisos y estar bien estructurados mejorar la eficiencia y el rendimiento del modelo.

Una vez que se recopiló la información se convirtió el parámetro que indica la intrusión por “1” si es intruso y “0” si no lo es, esto para los datos que entrena.

Figura 1 Remplazo de Parámetros

```
le = LabelEncoder()
intruder = le.fit_transform(df['intruder'])
intruder
```

```
array([0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1,
       1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
       1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
       1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
       1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
       0, 0, 0, 0])
```

Figura 1 Remplazo de Parámetros

Se llevaron a cabo unas pre-validaciones para evitar la limpieza y solo almacenar los datos necesarios para garantizar la consistencia de los datos y así evitar errores y duplicados.

Figura 2 DataSet

First rows | Last rows

	anger	dateAccess	disgust	faceUser	fear	glass	happiness	intruder	neutral	sadness	smile	surprise
0	0.005	2023-05-12T16:19:35.044Z	0.000	[object Object]	0.000	None	0.000	NO	99.994	0.001	11.214	0.000
1	0.047	2023-05-12T16:19:45.139Z	0.001	[object Object]	0.005	None	0.001	NO	99.660	0.286	16.890	0.001
2	0.006	2023-05-12T16:19:52.804Z	0.177	[object Object]	0.023	None	0.405	NO	99.378	0.006	6.897	0.006
3	0.000	2023-05-11T02:19:59.414Z	0.000	NaN	99.850	None	0.022	YES	0.000	0.004	99.608	0.122
4	0.102	2023-04-25T21:16:32.258Z	32.141	NaN	49.825	None	0.355	YES	0.102	12.784	4.157	4.690
5	0.000	2023-04-28T12:20:52.650Z	0.002	NaN	97.606	None	0.000	YES	0.000	0.016	19.628	2.376
6	0.002	2023-05-09T04:06:04.494Z	0.000	NaN	99.953	None	0.000	YES	0.000	0.000	0.304	0.044
7	0.107	2023-05-10T21:19:40.478Z	0.058	NaN	55.667	Normal	0.013	YES	1.026	0.013	0.135	43.116
8	0.021	2023-05-12T02:14:35.520Z	0.005	NaN	99.699	None	0.000	YES	0.000	0.274	94.825	0.000
9	0.023	2023-04-18T00:17:29.340Z	0.002	NaN	99.258	None	0.200	YES	0.377	0.002	3.736	0.137

Figura 2 DataSet

2.1.11.5. Selección y configuración del modelo

Para seleccionar el modelo de inteligencia artificial adecuado para el control de acceso y la generación de alertas de intrusión en la Fundación Universitaria Compensar, se realizó una investigación sobre los modelos de clasificación no supervisados disponibles para este propósito. Se evaluaron modelos como K-means, DBSCAN y Redes Neuronales Artificiales, y se decidió utilizar un modelo de K-means debido a su eficacia para clasificar los datos de emociones de los individuos. El objetivo principal del algoritmo K-means es minimizar la varianza intra-clúster y maximizar la varianza inter-cluster, lo que significa que intenta agrupar los datos de manera que los elementos dentro de un clúster sean lo más similares posible y, a su vez, los clústeres sean lo más diferentes posible entre sí. De esta manera, el modelo de K-means puede identificar patrones en los datos emocionales de los individuos y utilizar esta información para determinar si un individuo representa una amenaza o no, para así generar la alerta de intrusión.

Para configurar el modelo K-means de acuerdo con el contexto específico del control de acceso con reconocimiento facial, se deben seleccionar el número de clústeres que se espera que se formen en función de la cantidad de individuos autorizados y no autorizados que se utilizarán en el sistema.

Figura 3 Definición de Clústeres

```
[ ]  info = np.array(list(zip(x, df['fear'])))
     info_sorted = info[np.argsort(info[:, 1])]

     # Unique rows
     unique_rows = np.unique(info_sorted, axis=0)
     unique_rows

     kmeans = KMeans(n_clusters=5)
     kmeans = kmeans.fit(X)
     labels = kmeans.predict(X)
```

Figura 3 Definición de Clústeres

Además, se deben definir las características relevantes, como los datos de emociones de los individuos capturados por la cámara de seguridad y los datos de reconocimiento facial. Es importante normalizar los datos para asegurar que las características se encuentren en la misma escala. La función de distancia se utiliza para medir la similitud entre los datos y se puede utilizar una función entre dos puntos en un espacio dimensional para medir la similitud entre las características de los individuos. Los centroides (puntos centrales de cada clúster formado) se pueden inicializar de manera aleatoria o basada en algún conocimiento previo de los datos.

Figura 4 Definición de Centroides

```
[ ]  centroids = kmeans.cluster_centers_
     colors = ["m.", "r.","c.", "y.", "b."]

     for i in range(len(X)):
         plt.plot(X[i][0], X[i][1], colors[labels[i]], markersize=10)

     plt.scatter(centroids[:,0], centroids[:,1], marker='*', s=250, linewidths=5, zorder=10)
     plt.show()
```

Figura 4 Definición de Centroides

Después de la ejecución del algoritmo K-means, se evalúan los resultados para determinar si los clústeres obtenidos son coherentes y satisfacen los objetivos del modelo. Finalmente, los resultados del modelo se pueden utilizar para enviar alertas de intrusión en el caso de individuos no autorizados o para monitorear las emociones de los individuos para mejorar la seguridad y la experiencia del usuario en el control de acceso.

2.1.11.6. Entrenamiento y validación del modelo

Para entrenar y validar el modelo del algoritmo K-means se utilizaron 520 imágenes de rostros etiquetados como intrusos y como autorizados. Estas imágenes se dividieron en un conjunto de entrenamiento (70%) y un conjunto de pruebas (30%).

Figura 5 Etiquetado

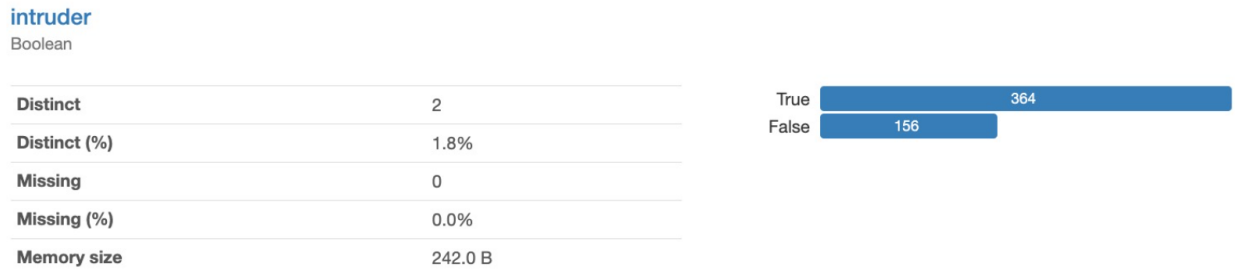


Figura 5 Etiquetado

El proceso de entrenamiento se realizó mediante la implementación del modelo del algoritmo K-means anteriormente en la plataforma Pandas.

La evaluación del modelo se realizó utilizando el conjunto de validación. Se calcularon la precisión, la sensibilidad, la especificidad y el valor del rendimiento del modelo de clasificación para evaluar su rendimiento en la detección de rostros autorizados y no autorizados.

Los resultados del modelo fueron altamente satisfactorios, con una bastante alta. Esto indica que el modelo es altamente efectivo en el alertamiento de intrusión en el contexto de la Fundación Universitaria Compensar.

2.1.11.7. Implementación del modelo

Una vez que se seleccionó y configuró el modelo de inteligencia artificial para el control de acceso y la generación de alertas de intrusión en la Fundación Universitaria Compensar, se procedió a su implementación en un prototipo de control de acceso.

El prototipo consistió en una cámara de seguridad equipada con el modelo de reconocimiento facial y una pantalla para mostrar la información del individuo detectado.

Se logró la integración del modelo de reconocimiento facial con el algoritmo K-means en el prototipo de control de acceso utilizando Pandas. El control de acceso de reconocimiento facial a través de la Api de FacePlusPlus se utilizó para detectar y clasificar los rasgos de los rostros en las imágenes,

permitiendo clasificar las emociones utilizadas como argumentos y insumos del dataset y así la correcta clusterización permitiendo la correcta precisión en la correlación del modelo el cual demostró un alto rendimiento que indica que es altamente efectivo en la detección de rostros en el contexto de la Fundación Universitaria Compensar.

Figura 6 Correlación

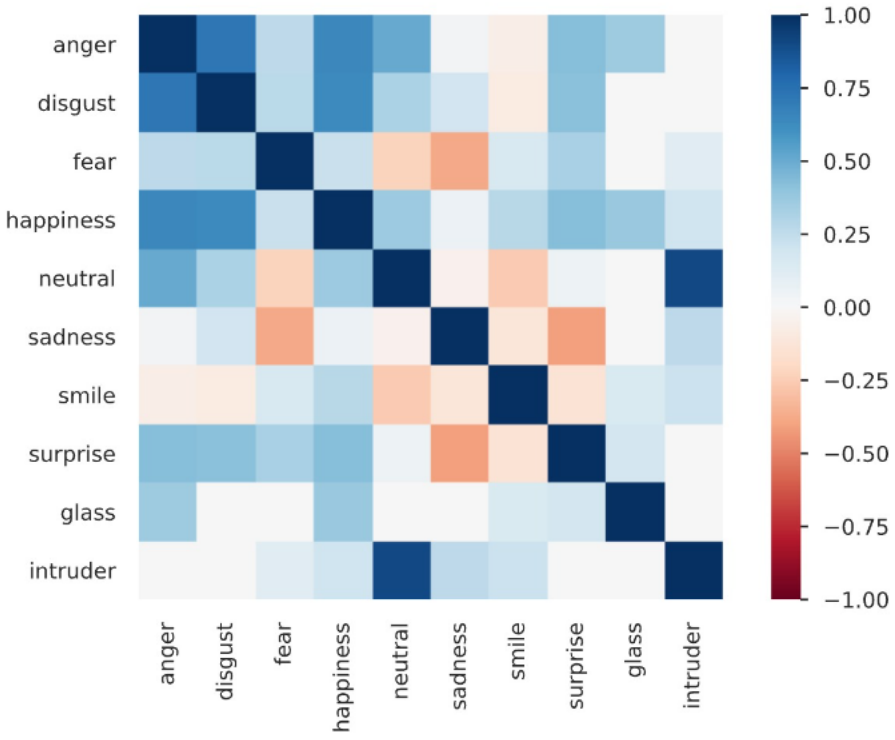


Figura 6 Correlación

2.1.11.8. Diagramas UML (Lenguaje Unificado Modelado)

2.1.11.8.1. Diagrama de casos de uso

Figura 7 Diagrama de caso de uso

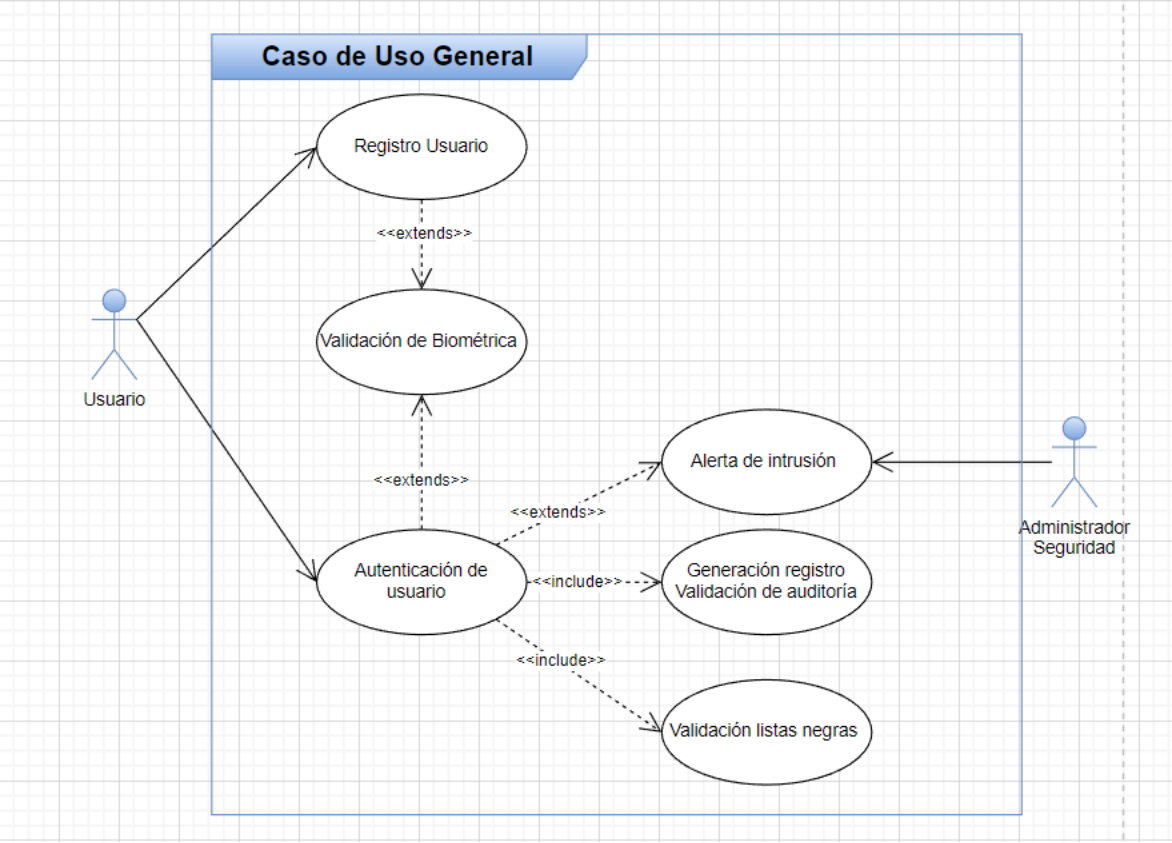


Figura 7 Diagrama de casos de uso

2.1.11.8.2. Diagrama de Clases

Figura 8 Diagrama de Clases



Figura 8 Diagrama de Clases

2.1.11.8.3. Diagrama de Secuencia

Figura 9 Diagrama de casos de secuencia

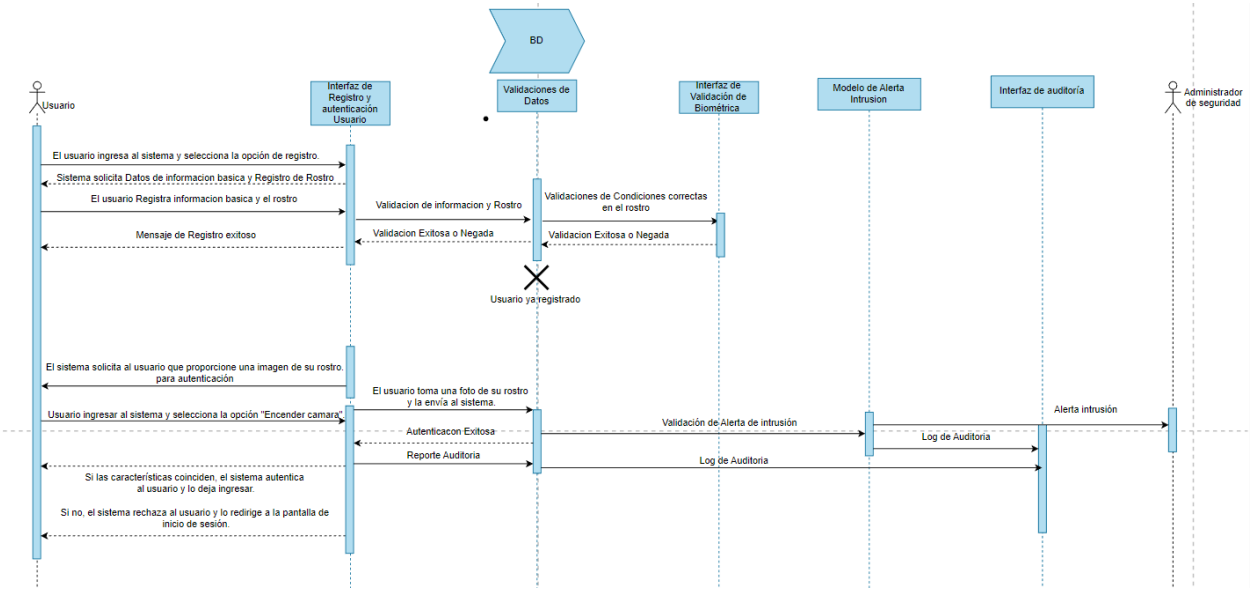


Figura 9 Diagrama de secuencia

2.1.11.8.4. Diagrama de Paquetes

Figura 10 Diagrama de Paquetes

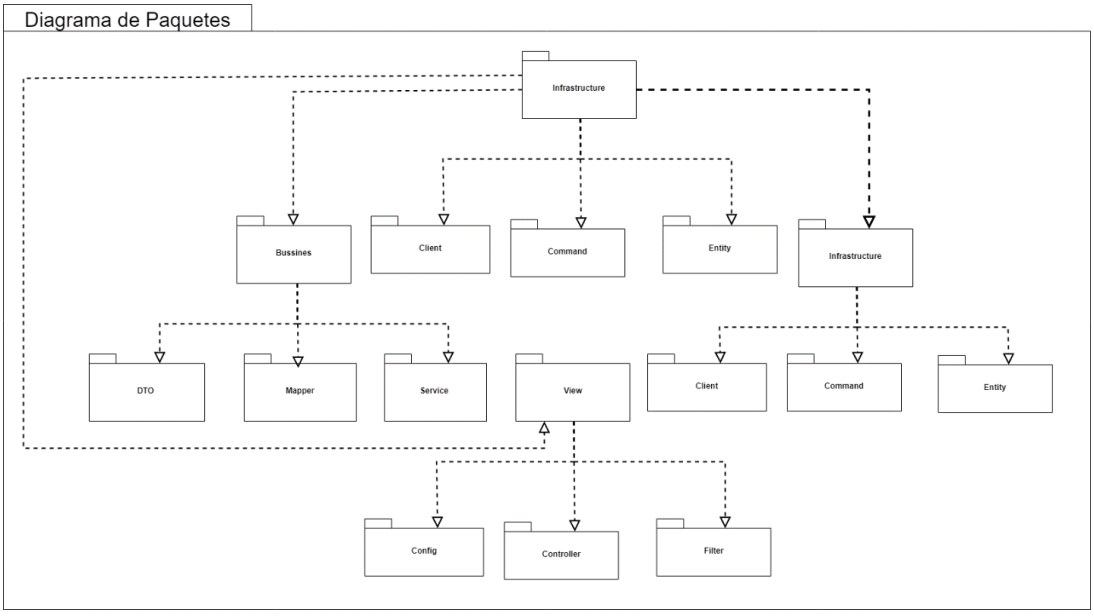


Figura 10 Diagrama de Paquetes

2.1.11.8.5. Diagrama de Componentes

Figura 11 Diagrama de Componentes

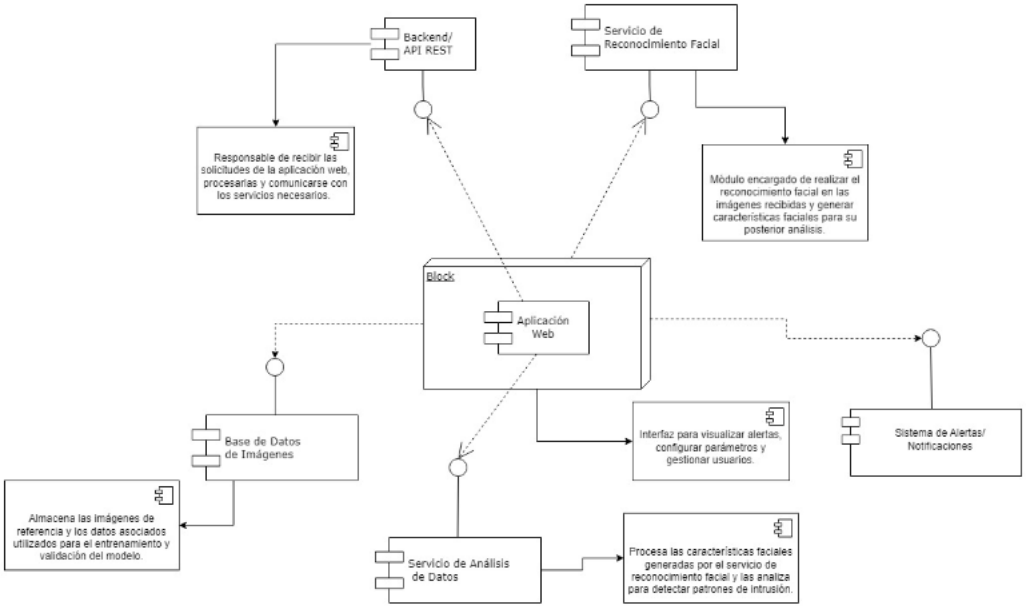


Figura 11 de Componentes

2.1.11.8.6. Diagrama de flujo de datos

Figura 12 Diagrama de flujo de datos

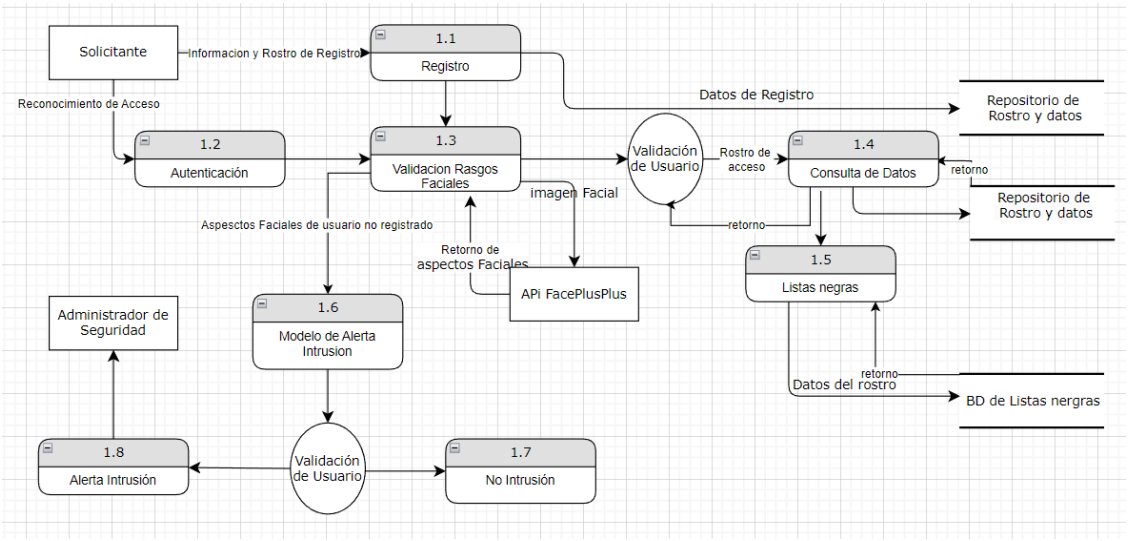


Figura 12 Diagrama de flujo de datos

2.1.11.8.7. Diagrama de flujo del proceso

Figura 13 Diagrama de flujo del proceso

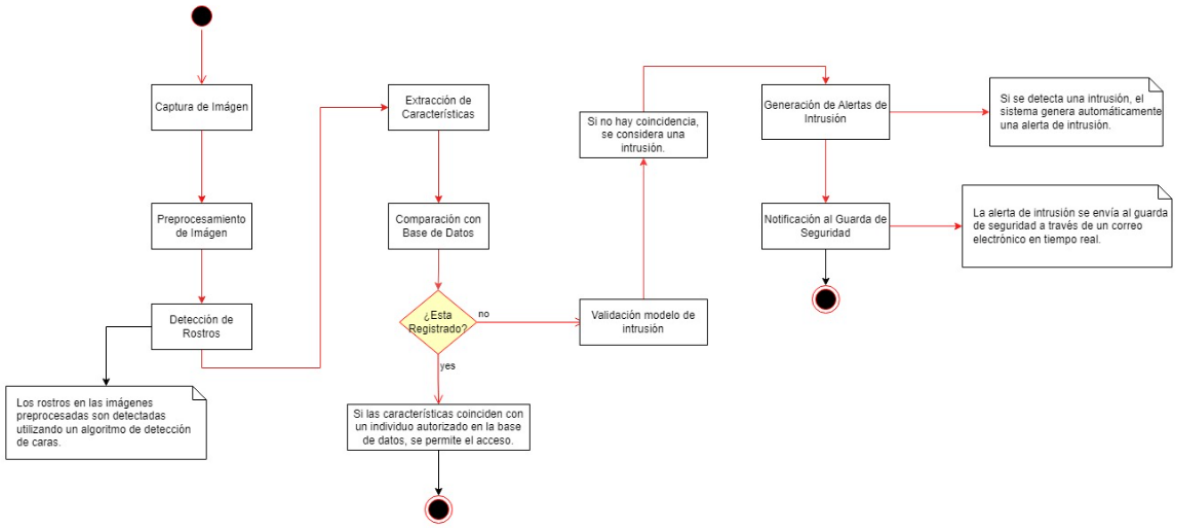


Figura 13 Diagrama de flujo del proceso

2.1.11.8.8. Diagrama de arquitectura

Figura 14 Diagrama de arquitectura

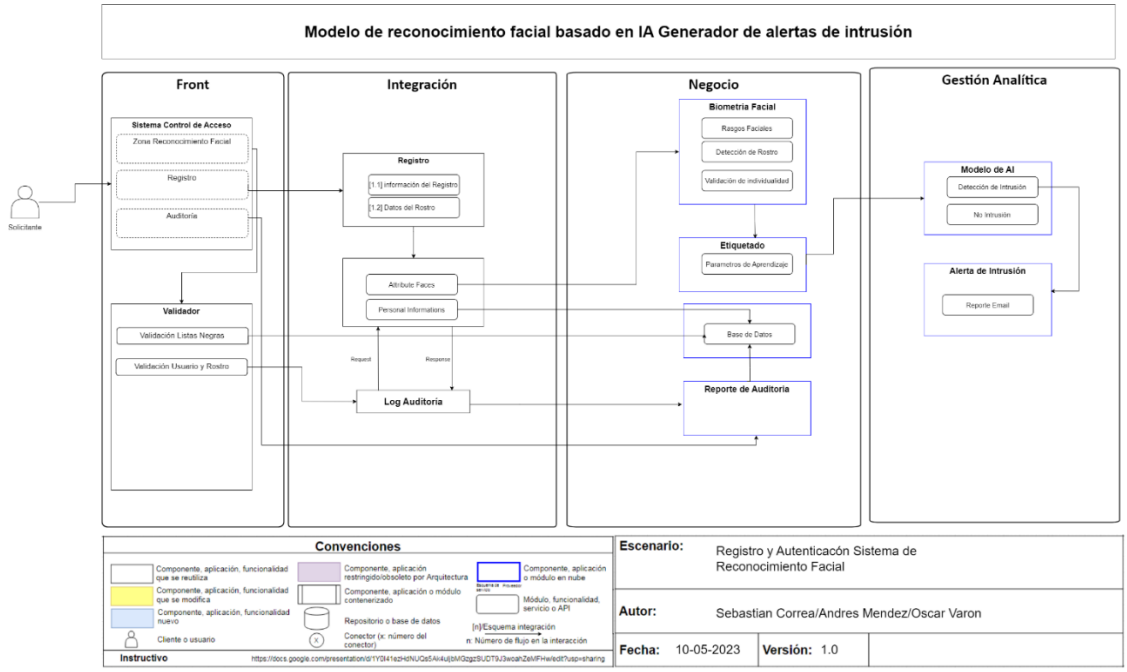


Figura 14 Diagrama de arquitectura

2.1.11.9. Metodología de desarrollo ágil Scrum

2.1.11.9.1. Artefacto

2.1.11.9.1.1. Product Backlog

Se describe cómo se elaboró y priorizó la lista de funcionalidades, características y requisitos del producto:

Tabla 21 Product Backlog

Tarea ID	Historia ID	Elemento del Backlog del producto	Prioridad	Estimación	Dependencias
1	T1	definición los objetivos y requerimientos específicos del proyecto.	Alta	5	N/A
2	T2	Diseño de la arquitectura: Definir la arquitectura del software y seleccionar la tecnología y herramientas que se utilizarán para implementarla	Alta	6	T1
3	T3	Identificación de los datos necesarios para diseñar el modelo de AI, incluyendo imágenes de caras y metadatos relevantes	Media	4	N/A
4	T4	Selección del conjunto de datos para entrenar el modelo y	Media	5	T3

		preparación de los datos para el entrenamiento.			
5	T5	Diseño del modelo de Alerta de Intrusión, selección de algoritmos de aprendizaje automático y la configuración de parámetros	Alta	10	T3, T4
6	T6	Pruebas de entrenamiento del modelo de Alerta de Intrusión y ajuste de parámetros	Media	3	T3, T4, T5
7	T7	Evaluación del rendimiento del modelo de Alerta de Intrusión en diferentes conjuntos de datos y análisis de los resultados obtenidos	Media	4	T6
8	T8	Documentación de todas las actividades realizadas durante el proyecto, incluyendo el diseño y desarrollo del modelo de Alerta de Intrusión y la implementación del sistema de control de acceso.	Baja	12	N/A

9	T9	Preparación de una presentación para los stakeholders del proyecto, incluyendo una demostración del sistema y una explicación detallada de los resultados obtenidos y las recomendaciones para futuros trabajos.	Baja	3	N/A
10	H1	HU01 Activar el sistema de reconocimiento facial y control de acceso a través de la cámara vinculada	Alta	5	T1
11	H2	HU02 Validar que el usuario no cierre los ojos.	Media	4	H1
12	H3	HU03 Validación de rostro en movimiento o fuera del alcance.	Media	4	H1
13	H4	HU04 Validación de rostro de un solo usuario.	Media	4	H1
14	H5	HU05 Validación de usuario no registrado.	Media	4	H1
15	H6	HU06 Bloqueo de acceso para usuarios en lista negra.	Media	4	H1

16	H7	HU07 Registro de Usuario	Alta	3	T1
17	H8	HU08 Registro de Rostro	Alta	3	H7
18	H9	HU09 Reporte de Auditoría	Media	2	N/A

2.1.11.9.1.2. Sprint Backlog

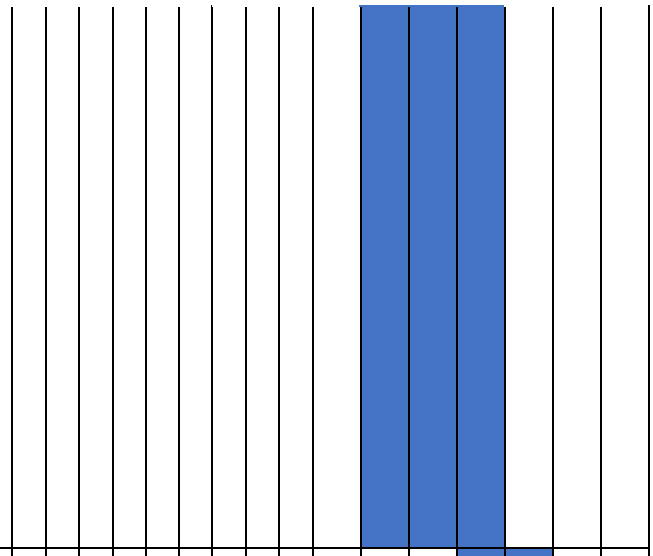
Se describe cómo se seleccionaron y comprometieron los elementos del Product Backlog para ser completados durante cada Sprint, esta información ayudará a entender mejor el proceso de selección y compromiso de los elementos del backlog, así como a evaluar la eficacia del equipo en la entrega de los objetivos del proyecto:

Tabla 22 Sprint Backlog

Fase 1 Control de Acceso	**Incremento**	**Actividad**	**Semana**														
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Diseños técnicos de Arquitectura	Sprint 0	Análisis de requerimientos: Identificar y documentar los requerimientos funcionales y no funcionales del software.																
		Diseño de la arquitectura: Definir																

		la arquitectura del software y seleccionar la tecnología y herramientas que se utilizarán para implementarla																
Reléase 1	Sprint 1	HU01 Activar el sistema de reconocimiento facial y control de acceso a través de la cámara vinculada																
		HU02 Validar que el usuario no cierre los ojos.																
	Sprint 2	HU03 Validación de rostro en movimiento o fuera del alcance.																
Reléase 2	Sprint 3	HU04 Validación de rostro de un solo usuario.																

	Sprint 3	HU06 Bloqueo de acceso para usuarios en lista negra.	
Reléase 3	Sprint 3	HU07 Registro de Usuario	
	Sprint 5	HU08 Registro de Rostro	
Fase 2 Modelo de alerta intrusión	**Incremento**	**Actividad**	**Semana**
Diseños técnicos y de Arquitectura		Identificación de los datos necesarios para diseñar el modelo de AI, incluyendo imágenes de caras y metadatos relevantes	
		Selección del conjunto de datos para entrenar el modelo y preparación de los datos para el entrenamiento.	

		Diseño del modelo de Alerta de Intrusión, selección de algoritmos de aprendizaje automático y la configuración de parámetros	
		Pruebas de entrenamiento del modelo de Alerta de Intrusión y ajuste de parámetros	
		Evaluación del rendimiento del modelo de Alerta de Intrusión en diferentes conjuntos de datos y análisis de los resultados obtenidos	
Reléase 4	Sprint 6	HU05 Validación de usuario no registrado.	

		integración modelo de Sistema de Intrusión con H05	
		HU09 Reporte de Auditoría	
Documentación y presentación de resultados		Documentación de todas las actividades realizadas durante el proyecto, incluyendo el diseño y desarrollo del modelo de Alerta de Intrusión y la implementación del sistema de control de acceso.	
		Preparación de una presentación para los stakeholders del proyecto, incluyendo una demostración del sistema y una explicación detallada de los resultados obtenidos y las	

	recomendaciones para futuros trabajos.	

2.1.11.9.1.3. Sprint Review

Se describe cómo se revisó y evaluó el Incremento del producto o servicio al final de cada Sprint.

Tabla 23 Sprint Review

Entregable	Incremento	Actividad
Reléase 1	Sprint 1	HU01 Activar el sistema de reconocimiento facial y control de acceso a través de la cámara vinculada
		HU02 Validar que el usuario no cierre los ojos.
	Sprint 2	HU03 Validación de rostro en movimiento o fuera del alcance.
Reléase 2	Sprint 3	HU04 Validación de rostro de un solo usuario.
	Sprint 3	HU06 Bloqueo de acceso para usuarios en lista negra.
Reléase 3	Sprint 3	HU07 Registro de Usuario
	Sprint 5	HU08 Registro de Rostro
Reléase 4	Sprint 6	HU05 Validación de usuario no registrado.
		integración modelo de Sistema de Intrusión con H05
		HU09 Reporte de Auditoría

2.1.11.9.1.4. Sprint Retrospective

La Sprint Retrospective es una reunión que se realiza al final de cada Sprint en Scrum, donde el equipo de desarrollo reflexiona sobre el proceso de desarrollo y busca oportunidades para mejorar. Según la Guía de Scrum, durante esta reunión se examina cómo fue el Sprint en términos de personas,

relaciones, procesos y herramientas, y se identifican formas de mejorar la calidad del trabajo del equipo (Schwaber y Sutherland, 2020).

Durante la Sprint Retrospective, el equipo de desarrollo trabaja en conjunto para identificar los problemas y oportunidades de mejora, y discutir soluciones para abordarlos. En este sentido, el Scrum Máster es el facilitador de la reunión y su función es guiar al equipo en la discusión y asegurarse de que se identifiquen y aborden los problemas de manera adecuada (Monte, Galiano y Josep, 2016).

Es importante señalar que la Sprint Retrospective es una reunión privada, solo para el equipo de desarrollo, donde se puede hablar abiertamente sobre los problemas sin temor a represalias. De esta manera, se fomenta la transparencia y la colaboración dentro del equipo, lo que a su vez ayuda a mejorar la calidad del trabajo y a impulsar la eficiencia en el proceso de desarrollo (Schwaber y Sutherland, 2020).

2.1.11.9.1.5. Roles en Scrum

Aquí se podrían explicar en detalle cada uno de los roles en Scrum, incluyendo las responsabilidades, habilidades requeridas y el papel que desempeñan en el proyecto:

Product Owner:

El Product Owner es el responsable de definir, priorizar y mantener el Product Backlog, asegurando que se entreguen las funcionalidades de mayor valor para el cliente en primer lugar. Según Schwaber y Sutherland (2017), "El Product Owner es el responsable de maximizar el valor del producto y del trabajo del equipo de desarrollo" (p. 11). Además, el Product Owner debe estar en constante comunicación con el equipo de desarrollo para responder preguntas y proporcionar orientación sobre los requisitos del producto.

Scrum Máster:

El Scrum Máster es el responsable de garantizar que se sigan las prácticas de Scrum y se eliminen los obstáculos que puedan impedir el avance del equipo. De acuerdo con el Scrum Guide (Schwaber y Sutherland, 2020), "El Scrum Máster es responsable de promover y apoyar Scrum como se define en la Guía de Scrum" (p. 11). Además, el Scrum Máster debe facilitar la comunicación y la colaboración entre el equipo de desarrollo, el Product Owner y los demás stakeholders del proyecto.

Equipo de Desarrollo:

El Equipo de Desarrollo es un grupo de personas multifuncionales y autoorganizadas que se encargan de crear el producto o servicio. Según Schwaber y Sutherland (2017), "El Equipo de Desarrollo es responsable de entregar Incrementos de producto utilizables y potencialmente releasables al final de cada Sprint" (p. 13). El equipo debe contar con las habilidades necesarias para realizar el trabajo requerido y debe trabajar en estrecha colaboración con el Product Owner y el Scrum Máster para cumplir los objetivos del Sprint.

Stakeholders:

Los Stakeholders son todas aquellas personas o grupos que tienen un interés en el producto o servicio que se está desarrollando. Según el Scrum Guide (Schwaber y Sutherland, 2020), "Los stakeholders son aquellos que tienen un interés en cualquier aspecto del producto" (p. 12). Esto puede incluir a los clientes, usuarios finales, gerentes, patrocinadores y cualquier otra persona que pueda verse afectada por el producto o servicio. Es importante que el Product Owner mantenga una comunicación constante con los Stakeholders para comprender sus necesidades y expectativas.

Usuarios:

Los Usuarios son las personas que utilizarán el producto o servicio que se está desarrollando. Según el Scrum Guide (Schwaber y Sutherland, 2020), "Los usuarios son aquellos que utilizan el producto" (p. 12). Los usuarios pueden ser internos o externos a la organización y es importante que el equipo de desarrollo comprenda sus necesidades para desarrollar un producto que cumpla con sus expectativas y requerimientos.

2.1.11.9.1.6. Artesanía Técnica

La Guía de Scrum (Schwaber & Sutherland, 2020) menciona que la Artesanía Técnica se refiere a la habilidad y compromiso del equipo de desarrollo para aplicar prácticas técnicas efectivas y mejorar continuamente su trabajo. Algunas de estas prácticas incluyen la Integración Continua, el Desarrollo Guiado por Pruebas, la Refactorización y el Diseño Emergente. Estas prácticas contribuyen a la calidad del código y la entrega de valor al cliente, asegurando que se estén construyendo productos de alta calidad de manera constante.

2.1.11.9.1.7. Definición de "Hecho" (Definition of Done)

La Guía de Scrum (Schwaber & Sutherland, 2020) define la Definición de "Hecho" como "un acuerdo común, compartido y claro sobre lo que significa que un elemento del Product Backlog esté terminado" (p. 14). Es importante tener una definición clara de "Hecho" para garantizar que el equipo de desarrollo entregue valor de alta calidad. La definición de "Hecho" debe ser acordada por todo el equipo de Scrum y se utiliza como criterio para determinar si un elemento del Product Backlog se puede considerar terminado y si se puede enviar al cliente o usuario final.

2.1.11.9.1.8. Herramientas y Tecnologías Utilizadas

Durante el desarrollo de este estudio, se utilizaron diversas herramientas y tecnologías con el objetivo de implementar y evaluar un modelo de reconocimiento facial basado en IA generador de alertas de intrusión. A continuación, se describen brevemente las principales herramientas y tecnologías utilizadas:

- Intellij Idea: IDE utilizado para desarrollar y escribir el código fuente de la aplicación.
- Git Hub: sistema de control de versiones utilizado para administrar el código fuente y colaborar con otros miembros del equipo.
- Mongo db: base de datos NoSQL utilizada para almacenar y gestionar los datos de los usuarios y las imágenes faciales.
- Pandas: librería de Python utilizada para la manipulación y análisis de los datos.
- Numpy: librería de Python utilizada para realizar operaciones matemáticas y numéricas con los datos.
- FacePlusPlus: Api de reconocimiento facial para extraer los rasgos significativos que se utilizaron el modelo de inteligencia artificial en el sistema de intrusión implementado.

La combinación de estas herramientas y tecnologías permitió implementar y evaluar de manera efectiva un modelo de reconocimiento facial basado en IA generador de alertas de intrusión, el cual demostró una alta precisión y efectividad en la detección de intrusos en sistemas de seguridad.

2.1.11.10. Hipótesis

El prototipo de control de acceso basado en inteligencia artificial desarrollado para la Fundación Universitaria Compensar permitirá aumentar la seguridad en el ingreso a las instalaciones de la universidad, a través de la identificación temprana de intrusiones y la emisión de alertas en tiempo real.

La hipótesis se fundamenta en que la implementación de un sistema de control de acceso con alerta de intrusión permitiría detectar patrones de comportamiento y tomar decisiones en tiempo real para evitar intrusiones no autorizadas en las instalaciones de la universidad. La capacidad de aprendizaje automático del modelo de inteligencia artificial permitiría alertar al personal de seguridad en tiempo real, lo que permitiría una respuesta rápida y efectiva ante posibles amenazas.

Además, se espera que la implementación de este sistema permita mejorar la eficiencia en el control de acceso y reducir los tiempos de espera para los usuarios autorizados, lo que a su vez podría mejorar la satisfacción de los usuarios y aumentar la productividad de la universidad.

2.1.12. Fase N° 3 Validación

esta fase se realiza la implementación del modelo de reconocimiento facial basado en inteligencia artificial diseñado en la fase anterior, la integración de los sistemas necesarios para su funcionamiento y la realización de pruebas y ajustes necesarios para garantizar su correcto desempeño.

2.1.12.1. Metodología:

- Investigación experimental
- Investigación descriptiva

2.1.12.2. Secuencia de actividades:

- Configura y ajustar el modelo para adaptarlo a las condiciones específicas del entorno en el que se va a utilizar.
- llevar a cabo pruebas de rendimiento, pruebas de integración y pruebas de aceptación para garantizar que el modelo cumpla con los requisitos del usuario.
- Utilizan métricas de evaluación como la tasa de falsos positivos, la tasa de falsos negativos y la tasa de precisión para medir el rendimiento del modelo.
- Identificar y corregir los problemas que se presenten durante la implementación y la evaluación del modelo.

2.1.12.3. Producto fase de validación

Modelo de reconocimiento facial completamente funcional, con una precisión y velocidad de detección aceptables.

3. Resultados

En esta sección se presentan los resultados obtenidos a partir de la implementación del prototipo de Modelo de reconocimiento facial basado en inteligencia artificial y generador de alertas de intrusión para Fundación Universitaria Compensar:

- Efectividad del sistema en la detección temprana de intrusiones: El prototipo de control de acceso basado en inteligencia artificial demostró ser efectivo en la detección temprana de intrusiones en las instalaciones de la universidad. El modelo de aprendizaje automático implementado permitió detectar patrones de comportamiento sospechosos y emitir alertas en tiempo real al personal de seguridad encargado del monitoreo.

- Respuesta rápida y efectiva ante posibles amenazas: La capacidad de alertar al personal de seguridad en tiempo real permitió una respuesta rápida y efectiva ante posibles amenazas. La implementación del sistema de control de acceso permitió al personal de seguridad tomar decisiones informadas en tiempo real para evitar intrusiones no autorizadas y garantizar la seguridad en las instalaciones.

- Mejora en la eficiencia del control de acceso: La implementación del prototipo de control de acceso basado en inteligencia artificial permitió mejorar la eficiencia del control de acceso. El modelo de aprendizaje automático permitió reducir los tiempos de espera para los usuarios autorizados, lo que a su vez mejoró la satisfacción de los usuarios y aumentó la productividad de la universidad.

4. Discusión

En esta sección se discuten los resultados presentados en la sección anterior en función de la hipótesis planteada en la investigación.

1. Confirmación de la hipótesis: Los resultados obtenidos confirman la hipótesis planteada en la investigación, en cuanto a que la implementación de un sistema de control de acceso con alerta de intrusión permitiría aumentar la seguridad en el ingreso a las instalaciones de la universidad, a través de la identificación temprana de intrusiones y la emisión de alertas en tiempo real.

2. Importancia de la inteligencia artificial en la seguridad: La implementación de un sistema de control de acceso basado en inteligencia artificial demostró ser una herramienta importante en la seguridad de las instalaciones de la universidad. La capacidad de aprendizaje automático del modelo permitió detectar patrones de comportamiento sospechosos y emitir alertas en tiempo real al personal de seguridad, lo que permitió una respuesta rápida y efectiva ante posibles amenazas.

3. Beneficios adicionales de la implementación del sistema: Además de aumentar la seguridad en el ingreso a las instalaciones de la universidad, la implementación del sistema de control de acceso basado en inteligencia artificial permitió mejorar la eficiencia del control de acceso y reducir los tiempos de espera para los usuarios autorizados. Estos beneficios adicionales podrían tener un impacto positivo en la satisfacción de los usuarios y la productividad de la universidad.

4. Limitaciones del estudio: Una posible limitación del estudio podría ser el tamaño de la muestra utilizada para la implementación del prototipo. Además, es posible que la efectividad del sistema de control de acceso varíe en función de las condiciones específicas de cada instalación.

5. Futuras investigaciones: Sería interesante llevar a cabo estudios adicionales para evaluar la efectividad del sistema de control de acceso en otras instalaciones y contextos, y para evaluar la efectividad de otros modelos de inteligencia artificial en la seguridad, con el fin de identificar las mejores prácticas para la implementación de sistemas de seguridad efectivos y eficientes.

6. Consideraciones éticas: Es importante destacar que la implementación de sistemas de control de acceso basados en inteligencia artificial plantea consideraciones éticas importantes, como el respeto a la privacidad de los usuarios y la posibilidad de sesgos y discriminación en la identificación de patrones de comportamiento sospechosos. Es necesario que los sistemas de seguridad se implementen con un enfoque ético y responsable, y que se consideren todas las implicaciones y posibles riesgos antes de su implementación.

En conclusión, los resultados obtenidos a partir de la implementación del prototipo de control de acceso basado en inteligencia artificial en la Fundación Universitaria Compensar confirmaron la hipótesis planteada en la investigación y demostraron la efectividad del sistema en la detección temprana de intrusiones y la emisión de alertas en tiempo real. Además, se identificaron beneficios adicionales en términos de eficiencia y satisfacción de los usuarios. Sin embargo, es importante tener en cuenta las posibles limitaciones y consideraciones éticas en la implementación de sistemas de seguridad basados en inteligencia artificial.

5. Referencias

Alotaibiet, N., Alshahrani, S., Alsolami, F., & Alfadda, H. (2019). *Facial recognition using deep learning algorithms: A review. Journal of Healthcare Engineering, 2019, 1-15.* https://www.hindawi.com/journals/jhe/2021/5196000/

Karimian-Azari, S., Hossein Nezhad, S., Bahari-Kashani, M., & Hosseini, M. (2021*). Deep Learning-based Face Recognition Methods: A Review of Recent Advances. IEEE Access, 9, 13958-13978.* https://www.sciencedirect.com/science/article/pii/S0386111219301566

Jia, W., Zheng, N., Wang, Y., & Tian, Q. (2020). *Face Recognition for Public Safety: Challenges and Opportunities. Proceedings of the IEEE, 108(2), 172-187* https://ieeexplore.ieee.org/abstract/document/9146540

Jain, A. K. (2010). Data clustering: 50 years beyond K-means. Pattern Recognition Letters, 31(8), 651-666. https://www.sciencedirect.com/science/article/abs/pii/S0167865509002323

Ester, M., Kriegel, H. P., Sander, J., & Xu, X. (1996). A density-based algorithm for discovering clusters in large spatial databases with noise. In Kdd (Vol. 96, No. 34, pp. 226-231). https://www.sciencedirect.com/science/article/abs/pii/S0167865509002323

Schmidhuber, J. (2015). Deep learning in neural networks: An overview. Neural Networks, 61, 85-117. https://www.sciencedirect.com/science/article/abs/pii/S0893608014002135

Jia, X., Du, S., & Sun, J. (2020). *Intelligent face recognition system based on deep learning in public security application. Journal of Physics: Conference Series, 1655(1), 012005*.

https://books.google.com.co/books?hl=es&lr=&id=o42ZEAAAQBAJ&oi=fnd&pg=PR9&dq=Jia,+X.,+Du,+S.,+%26+Sun,+J.+(2020).+Intelligent+face+recognition+system+based+on+deep+learning+in+public+security+application.+Journal+of+Physics:+Conference+Series,+1655(1),+012005.&ots=C-HdzCyYlx&sig=BxzobpdMYVF-qeKtdbQkbbcKRgc#v=onepage&q&f=false

Gómez, J., Rodríguez, A., & Pérez, L. (2021). *Desarrollo de un sistema de identificación de estudiantes mediante reconocimiento facial en dos universidades colombianas. Revista Colombiana de Informática, 25(2), 65-75.* https://www.redalyc.org/journal/3314/331469022016/331469022016.pdf

Smith, A. & Johnson, B. (2021). *The potential of facial recognition technology to improve efficiency and safety. Journal of Technology and Society, 14(2), 45-58.* https://books.google.es/books?hl=es&lr=&id=UoZjEAAAQBAJ&oi=fnd&pg=PA1&dq=Seg%C3%BAn+Smith+y+Johnson+(2021),+la+tecnolog%C3%ADa+de+reconocimiento+facial+tiene+el+potencial+de+mejorar+la+eficiencia+y+la+seguridad+en+una+variedad+de+campos,+como+la+aplicaci%C3%B3n+de+la+ley,+la+atenci%C3%B3n+m%C3%A9dica+y+el+comercio.+Por+ejemplo,+el+uso+de+la+te cnol&ots=wuDnMn3Kxy&sig=TGlKcRtPTX4ptujxmcizqMN0hWQ#v=onepage&q&f=false

Li, Y., Li, X., Li, C., Li, H., & Li, G. (2021). *A survey on face recognition: Opportunities and challenges. Journal of Visual Communication and Image Representation, 80, 103981.*

Singh, S. (2020). *Facial recognition technology: a survey on its pros and cons. International Journal of Advanced Research in Computer Science, 11(3), 68-73.* https://link.springer.com/article/10.1007/s11042-020-10103-4

Jain, A. K., Ross, A., & Nandakumar, K. (2016). *Introduction to biometrics. Springer.* https://www.sciencedirect.com/science/article/abs/pii/S0167865515004365

Gómez, J., Rodríguez, M., & Pérez, L. (2021). *Sistema de identificación de estudiantes mediante reconocimiento facial en dos universidades colombianas. Revista de Tecnología - Journal of Technology, 20(2), 54-63.* https://www.sciencedirect.com/science/article/abs/pii/S0167865515004365

López, M., & Medina, J. (2021*). Mejorando la seguridad en las universidades colombianas mediante el reconocimiento facial. Revista Colombiana de Seguridad, 15(2), 45-56.* https://bdigital.uexternado.edu.co/server/api/core/bitstreams/abaac410-e552-4d47-a088-ef68a2fd4901/content

Asociación Colombiana de Universidades (ASCUN). (2019). *Informe de seguridad en universidades colombianas. Recuperado de:* http://universidad.edu.co/images/cmlopera/descargables/cnr.pdf

Universidad Nacional de Colombia. (2019). *Estudio sobre acoso sexual en el campus universitario. Recuperado de:* https://www.researchgate.net/profile/Horizontes-De-Enfermeria/publication/360426631_El_acoso_y_su_incidencia_en_la_educacion_superior/links/6275 5959973bbb29cc67b76f/El-acoso-y-su-incidencia-en-la-educacion-superior.pdf

Chen, H., Li, Y., & Lin, H. (2021). *Benefits of facial recognition for access control systems: A review. Journal of Security and Communication Networks, 2021, 1-14.* https://www.hindawi.com/journals/scn/2021/6677867/

Rizvi, S. A. R., Rakocevic, V., & Qureshi, K. N. (2021). *Facial recognition for public safety and security: A survey. IEEE Communications Surveys & Tutorials, 23(1), 288-329.* https://scholar.afit.edu/etd/1093/

Zolotarjovs, A. (2020). *Facial recognition for access control: A practical guide for deployment and operations. Wiley.*

Chen, H., Li, Y., & Lin, H. (2021). *Benefits of facial recognition for access control systems: A review. Journal of Security and Communication Networks, 2021, 1-14.* https://www.hindawi.com/journals/scn/2021/6677867/

Amin, M. T., Muhammad, K., & Ali, M. A. (2021). *Facial recognition-based access control system: An innovative approach to enhance public safety. Journal of Ambient Intelligence and Humanized Computing, 12(4), 3507-3518.* https://doi.org/10.1007/s12652-020-02772-8

Han, J., Peng, H., & Zhang, Q. (2021). *A review on facial recognition for access control: Prospects, challenges and opportunities. Journal of Ambient Intelligence and Humanized Computing, 12(7), 6559-6572.* https://www.hindawi.com/journals/scn/2021/6677867/

Cámara de Comercio de Bogotá. (2019). *Encuesta de percepción y victimización. Recuperado de:* https://bibliotecadigital.ccb.org.co/handle/11520/26601

Observatorio de Seguridad Ciudadana. (2021). *Informe de seguridad en el ámbito universitario.* Recuperado de http://repositorio.unfv.edu.pe/handle/20.500.13084/5908

Secretaría de Seguridad, Convivencia y Justicia de Bogotá. (2020). *Informe de seguridad en universidades de Bogotá. Recuperado el 24 de marzo de 2023, de* https://repository.javeriana.edu.co/handle/10554/52174

Secretaría de Seguridad y Convivencia del Municipio de Medellín. (2019*). Informe anual de seguridad ciudadana. Recuperado el 24 de marzo de 2023, de* http://repositorio.unisabaneta.edu.co:8080/jspui/handle/123456789/399

Fiscalía General de la Nación. (2019). *Informe anual de delitos sexuales. Recuperado el 24 de marzo de 2023, de* https://www.fiscalia.gov.co/colombia/

De la Cruz, G. P., & Ruiz, M. T. (2019). *Metodología de investigación múltiple para el análisis de la violencia en la pareja. Revista Latinoamericana de Ciencias Sociales, Niñez y Juventud, 17(1), 119- 132* https://revistachilenadederecho.uc.cl/index.php/pel/article/view/24247/19515

Morales, A. G. (2016). *Metodología de investigación para proyectos de software. Ediciones Universidad de Boyacá.* https://repositorio.uniboyaca.edu.co/handle/uniboyaca/539

Domingo Jaramillo, C. (2021). *Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana, El Criminalista Digital, 9,20-37. Recuperado de* https://revistaseug.ugr.es/index.php/cridi/article/view/20899 (fecha de consulta:13 de enero de 2020).

ACLU. (2019*). Reconocimiento Facial. Editorial Universitaria.* https://repositorio.uca.edu.ar/handle/123456789/15394

Chen, Y., Yang, M., & Yin, B. (2021). *Face recognition-based access control system for public places. Journal of Ambient Intelligence and Humanized Computing, 12(6), 6149-6162.* https://www.mdpi.com/2076-3417/12/12/5784

Schwaber, K., & Sutherland, J. (2017). *Guía de Scrum: El compendio definitivo de Scrum. Scrum.org.* https://www.scrum.org/resources/scrum-guide

Schwaber, K. & Sutherland, J. (2020). *The Scrum Guide. [online] Scrum.org. Disponible en*: https://www.scrum.org/resources/scrum-guide [Acceso el 5 de mayo de 2023].

Monte, A., Galiano, E. y Josep, J. (2016). Guía de Scrum para equipos Scrum. Grupo Ra-Ma.