

Módulo de seguridad de reconocimiento facial

Desarrollo Tecnológico

Erwing Forero Castro

1005336392

**UNIDADES TECNOLÓGICAS DE SANTANDER**

**FCNI**

**Ingeniería de sistemas**

**Bucaramanga**



Módulo de seguridad de reconocimiento facial

Desarrollo Tecnológico

Erwing Forero Castro

1005336392

Trabajo de Grado para optar al título de

Ingeniería de sistemas

**DIRECTOR**

Nombre completo del director

Grupo de investigación – SIGLA

**UNIDADES TECNOLÓGICAS DE SANTANDER**

**FCNI**

**Ingeniería de sistemas**

**Bucaramanga**

Nota de Aceptación

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Firma del Evaluador

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Firma del Director

**DEDICATORIA**

Nota mediante la cual los autores ofrecen su trabajo, en forma especial, a personas o entidades. Su presentación es opcional. Si se incluye no debe ser mayor a un párrafo por cada autor (máximo 14 líneas).

**AGRADECIMIENTOS**

Los autores expresan el reconocimiento hacia las personas y entidades que asesoran técnicamente, suministraron datos, financiaron total o parcialmente la investigación o contribuyeron significativamente al desarrollo del trabajo de grado. Es opcional y debe contener, además de la nota correspondiente, los nombres de las personas con sus respectivos cargos y nombres completos de las instituciones y su aporte al trabajo.

TABLA DE CONTENIDO

[RESUMEN EJECUTIVO 9](#_Toc25074334)

[INTRODUCCIÓN 10](#_Toc25074335)

[1. DESCRIPCIÓN DEL TRABAJO DE INVESTIGACIÓN 11](#_Toc25074336)

[1.1. PLANTEAMIENTO DEL PROBLEMA 11](#_Toc25074337)

[1.2. JUSTIFICACIÓN 12](#_Toc25074338)

[1.3. OBJETIVOS 12](#_Toc25074339)

[1.3.1. OBJETIVO GENERAL 12](#_Toc25074340)

[1.3.2. OBJETIVOS ESPECÍFICOS 13](#_Toc25074341)

[1.4. ESTADO DEL ARTE 13](#_Toc25074342)

[2. MARCO REFERENCIAL 14](#_Toc25074343)

[3. DISEÑO DE LA INVESTIGACION 15](#_Toc25074344)

[4. DESARROLLO DEL TRABAJO DE GRADO 16](#_Toc25074345)

[5. RESULTADOS 18](#_Toc25074346)

[6. CONCLUSIONES 19](#_Toc25074347)

[7. RECOMENDACIONES 20](#_Toc25074348)

[8. REFERENCIAS BIBLIOGRÁFICAS 21](#_Toc25074349)

[9. APENDICES 22](#_Toc25074350)

[10. ANEXOS 23](#_Toc25074351)

LISTA DE FIGURAS

[Figura 1. Tipos de Investigación 19](#_Toc443661245)

LISTA DE TABLAS

[Tabla 1. Fase 1 20](#_Toc443661246)

# RESUMEN EJECUTIVO

En el presente documento (de ahora en adelante PDSDT) se observa el desarrollo de un módulo de reconocimiento facial de seguridad, desarrollado en el lenguaje JavaScript para sistemas de servidor y web, para poder identificar posibles intrusos en un ambiente restringido.

El objetivo principal del proyecto es la creación de dicho modulo y la mantenibilidad del mismo, facilitando así una herramienta gratuita a la comunidad que pueda ser usada de forma sencilla en cualquier servidor de JavaScript. El proyecto también tiene el propósito de ser un referente en el área de seguridad visual y la visión computacional.

La seguridad es un factor inherente de cualquier sistema, además, el aumento del flujo masivo de personas en algunos de ellos, hace que el seguimiento individual por parte del grupo de seguridad sea una tarea difícil de realizar, por ello este modelo automatiza el proceso de selección entre usuarios conocidos y desconocidas, facilitando así el seguimiento solo de personas desconocidas.

El modelo implementado para desarrollar el proyecto es el Método Ágil RUP, se basa en un desarrollo incremental e iterativo (es decir, el proceso de planificación es evolutivo y se va detallando a medida que avanza el proyecto).

**Palabras clave**: Aprendizaje profundo, Visión por computadora, Reconocimiento facial, sistema de seguridad.

# INTRODUCCIÓN

El PDSDT muestra el desarrollo e implementacion de un modulo de seguridad, que contiene funciones en base a un modelo de aprendizaje profundo para indentificar rostros en un sistema cerrado de camaras, señalando potenciales usuarios desconocidos por el sistema, ademas de la trazabilidad de los usuarios para mantener un mejor control de situaciones anormales que se puedan presentar.

Ademas de ahondar en posibles dilemas de privacidad de forma parcial y objetiva, tambien se describen posibles situaciones generales donde el sistema deberia implementarse, y caracteristicas del sistema como latencia entre predicciones, funciones generales que se pueden usar, y una demostracion de como se puede implementar el sistema.

Para desarrollar el modulo se analizaron investigaciones previas en el area del reconocimiento facial, para optimizar el rendimiento en sistemas con caracteristicas minimas (que se veran mas adelante), para ello se usa TensorFlow como nucleo principal del modelo e implementacion en el lenguaje JavaScript.

Como metodologia se usa RUP, el cual es un proceso de fases, dentro de las cuales, se realizan pocas pero grandes y formales iteraciones en número variable, ademas se complementara con el metodo cientifico, para el desarrollo de pruebas unitarias.

# 

# DESCRIPCIÓN DEL TRABAJO DE INVESTIGACIÓN

## PLANTEAMIENTO DEL PROBLEMA

En la seguridad no se puede improvisar o dejar a azar tareas en las que está en juego la vida de las personas protegidas, compañeros y la de personas no involucradas. En algunas instituciones los sistemas de seguridad no son suficientes para proporcionar la seguridad suficiente, algunos componentes de un sistema cerrado, se ven implicitamente relacionados con sus acciones en comun, ademas de las politicas internas que se aceptan por estos, hace que sea poco probable realizar acciones anormales (aunque no siempre es asi).

Poder identificar factores relevantes de prevencion de situaciones problematicas, suele ser una tarea complicada cuando el personal es masivo o no se tiene un sistema lo suficientemente adaptado, esto provoca que algunas situaciones no puedan ser previstas, es por ello que el modulo prevee de herramientas, siendo el seguimimento de entidades desconocidas el principal, este proporciona un enfoque simple sobre entidades desconocidas facilitando la selección y accion sobre las mismas.

### Herramienta, no sistema

Un problema que puede preverse es intentar automatizar el modulo en su implementacion, esto puede malinterpretarse como un sistema automatizado de seguimiento, el cual no es el caso, ya que debe ser provista como una herramienta de apoyo al sistema de seguridad.

### Politica de privacidad

El modulo no es responsable de su implementacion, es por ello que al ser usado para realizar un sistema, se debe proveer de una politica de privacidad con los aspectos que conlleva manejar la informacion de los usuarios, asi como su imagen, esto puede traer un dilema de ¿hasta donde un sistema es privado?, abordar esto de forma objetiva, sin caer en las “areas grises legales”, suele ser complicado, ya que se puede caer en un problema selectivo, donde se esta a favor, ya que su implementacion fortalece un sistema de seguridad, y disminuyen sus costos, pero por otro lado, los usuarios pueden encontrarse “incomodos” o “inconformes”, sabiendo que su rostro este siendo usado por un sistema para ser etiquetados como conocidos u desconocidos, este tema es mas complejo de lo que aquí se puede intervenir, por ello se recomienda no tomar de forma generalizadora lo anteriormente mencionado.

### ¿Son los desconocidos los unicos problematicos?

La respuesta clara es no, dado que no se puede estigmatizar o generalizar el conocimiento de una persona con su conducta, pero establecer personal que no es generalmente interno, suele ser apropiado en el momento de aplicar acciones disciplinarias sobre acciones inapropiadas, ademas de mantener informacion relevante de la trazabilidad de usuarios conocidos y desconocidos, para tomar acciones en base a dicha informacion.

## JUSTIFICACIÓN

El presente proyecto se enfocara en la selección de entidades (cualquier tipo de persona) desconocidas en un sistema cerrado, esto permite que el seguimiento y la trazabilidad de los usuarios pueda ser selectivo solo en situaciones en las que intervengan desconocidos, el modulo proveera de herramientas que podran ser usadas principalmente para complementar la selección de los usuarios, para determinar parametros selectivos por quien lo implemente.

El modulo intentara solventar la problemática interviniendo en posibles situaciones internas al seleccionar las entidades que puedan haberse visto involucradas, y asi poder tomar acciones. Aunque el sistema puede ser usado en la toma de desciciones sobre la informacion trazabilidad de los usuarios, esto con el objetivo de ser usado sistemas robustos o debiles que se puedan apoyar de su implementacion, ademas de poder ofrecer a la comunidad de programadores un modulo de seguridad con un nucleo de aprendizaje profundo de alto nivel y modularidad de nivel intermedio.

## OBJETIVOS

### OBJETIVO GENERAL

Desarrollo de un modulo de seguridad para preveer de herramientas en la implementacion de un sistema de seguridad de seguimiento de desconocidos, para ello se usara el lenguaje JavaScript y la librería Tensorlow.

### OBJETIVOS ESPECÍFICOS

• Investigar implementaciones robustas de sistemas similares de reconocimiento facial y esquemas de modelos altamamente eficientes.

• Planear y diseñar la estructura de funciones que solventara en un posible sistema.

• Desarrollar el modulo de seguridad de reconocimiento facial.

• Realizar las pruebas unitarias.

• Publicar el ensayo investigativo sobre el modulo.

## ESTADO DEL ARTE

El estado del arte aplica para las modalidades de trabajo de grado de proyecto de investigación y desarrollo tecnológico. Para el caso de la modalidad monografía, en la propuesta no se requiere estado del arte. Cada cita del estado del arte/antecedentes debe estar referenciada, siguiendo la norma APA actualizada (*American Psychological Association*).

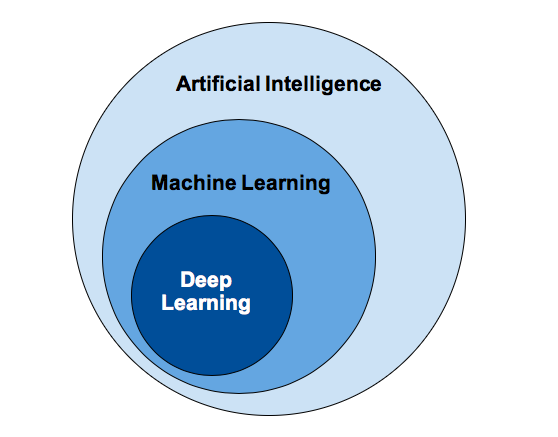
# 

# MARCO REFERENCIAL

## MARCO TEORICO

### Deep learning, Machine learning e inteligencia artificial

El Deep Learning, el Machine Learning y la Inteligencia Artificial, son conceptos que están íntimamente ligados, como sub conjuntos como se muestra en la figura 1 (Chollet,2018).



*Figure 1 Inteligencia Artificial, Machine Learning y Deep Learning*

Está claro que en la presente investigación nos centramos en el Deep Learning; sin embargo, es preciso conocer conceptos básicos del entorno conceptual de donde procede.

### Inteligencia artificial (IA)

Podemos definir a la Inteligencia Artificial como el proceso de simulación de la inteligencia humana mediante máquinas y sistemas informáticos especiales, que incluyen el aprendizaje, razonamiento y auto corrección (TutorialsPoint, 2018)

Es un campo de investigación muy amplio, donde las máquinas muestran cognitivas capacidades tales como conductas de aprendizaje, interacción proactiva con el medio ambiente, inferencia y deducción, visión por computadora, reconocimiento de voz, resolución de problemas, representación del conocimiento, percepción y muchos otros (Norvig, 2008). Más coloquialmente, la IA ve cualquier actividad donde las máquinas imitan comportamientos inteligentes típicamente mostrado por humanos. La inteligencia artificial se inspira en elementos de informática, matemática y estadística.

### Los temas fundamentales de la Inteligencia Artificial

Según (Ponce, 2014). el campo de la IA se compone de varias áreas de estudio, las más comunes e importantes son:

A. Búsqueda de soluciones

B. Sistemas expertos

C. Procesamiento del lenguaje natural

D. Reconocimiento de modelos

E. Robótica

F. Aprendizaje de las Máquinas (Machine Learning)

G. Lógica

H. Incertidumbre y “lógica difusa”

Como se destaca la investigación está dentro del área del Aprendizaje de las Máquinas o Machine Learning.

### Ramas de la Inteligencia Artificial

(Ponce, 2014), manifiesta que, existen varios elementos que componen la ciencia de la IA, dentro de los cuales se pueden encontrar tres grandes ramas:

A. Lógica difusa

B. Redes Neurales Artificiales

C. Algoritmos genéticos

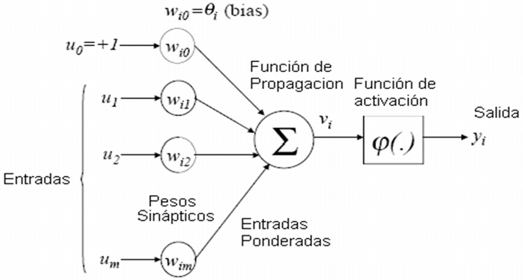
Dentro de estas ramas es notorio que la investigación está centrada en las Redes Neuronales Artificiales y más concretamente en Redes Neuronales Convolucionales, ya que éstas permiten el procesamiento de imágenes como se verá en temas siguientes.

### Redes Neuronales Artificiales (RNA)

(Ponce, 2014) afirma que las RNA se definen como sistemas de mapeos no lineales cuya estructura se basa en principios observados en los sistemas nerviosos de humanos y

animales.

La idea detrás de una Red Neuronal Artificial es simular el comportamiento de una red neuronal biológica. Para ello se emula con fórmulas matemáticas una neurona a la que le van a llegar señales de entrada con distintos pesos, que se sumarán, y se emitirá una señal de salida que dependerá de una determinada función de activación como se muestra en la Figura 2, Ponce.



*Figure 2Neurona artificial*

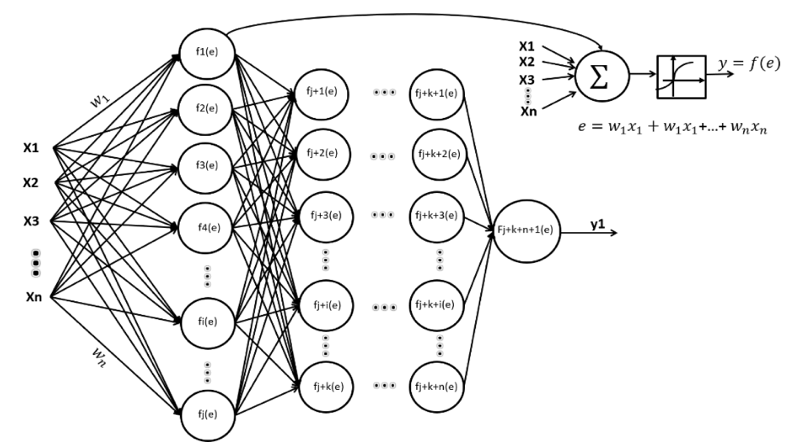
Existen diferentes tipos de funciones de activación las más relevantes para esta investigación son: Sigmoid (Sigmoide) y ReLU (Rectified Lineal Unit).

**Sigmoid: 𝑓(𝑥) = 2/1+𝑒−2𝑥 – 1**

**ReLU: 𝑓(𝑥) = max(0, 𝑥) = { 0 𝑓𝑜𝑟 𝑥 < 0 𝑥 𝑓𝑜𝑟 𝑥 ≥ 0 }**

Una red neuronal artificial estará formada por un conjunto de neuronas, y que se somete a un proceso de aprendizaje, para enseñarle a reconocer formas (clasificación) o hacer predicciones (Regresión).

La función ReLU se usa en las capas de entrada y ocultas; mientras que, en la capa de salida se usa la función Sigmoid para la identificación de personas.



*Figure 3Red neuronal artificial*

Cada unidad recibe entradas de otros nodos y genera una salida simple escalar que depende de la información local disponible, guardada internamente o que llega a través de las conexiones con pesos. Pueden realizarse muchas funciones complejas dependiendo de las conexiones.

### Machine Learning

El Machine Learning o Aprendizaje Automático es un tipo de inteligencia artificial (IA) que proporciona a las computadoras la capacidad de aprender, sin ser programadas explícitamente. El aprendizaje automático se centra en el desarrollo de programas informáticos que pueden cambiar cuando se exponen a nuevos datos (Gori, 2017)

Dentro del Machine Learning existen tres enfoques para aprender, el aprendizaje supervisado, aprendizaje no supervisado y aprendizaje por reforzamiento (Kirsch, 2018)

**A. Aprendizaje supervisado**

El aprendizaje supervisado generalmente comienza con un conjunto establecido de datos y una cierta comprensión de cómo se clasifican esos datos; por ejemplo, si le damos abundante información de imágenes de animales (perros y gatos), y etiquetamos cada imagen como perro o gato, entonces el sistema aprenderá a identificar un gato o un perro en otra imagen cualquiera distinta con la que fue entrenado (Kirsch, 2018)

**B. Aprendizaje no supervisado**

El aprendizaje no supervisado es más adecuado cuando el problema requiere una gran cantidad de datos sin etiqueta; por ejemplo, le damos abundante información de imágenes de (gatos y perros), pero no le decimos al sistema que son gatos o perros, por lo que la comprensión del significado detrás de estas imágenes, requiere algoritmos que pueden comenzar a comprender el significado de las imágenes para poder clasificar los “gatos o perros” en cualquier otra imagen (Kirsch, 2018).

**C. Aprendizaje por reforzamiento**

El aprendizaje por reforzamiento es un modelo de aprendizaje conductual, donde el algoritmo recibe retroalimentación del análisis de los datos para que el usuario sea guiado hacia el mejor resultado; es decir, se aprende con estímulos de ponderación alta si se acerca al objetivo o ponderaciones menores si comete errores

(Kirsch, 2018).

### Deep learning o aprendizaje profundo

El Deep Learning es un sub-campo del Machine Learning en el que los algoritmos en cuestión se inspiran en la estructura y función del cerebro llamadas redes neuronales artificiales (TutorialsPoint, 2018).

Según (al, 2016) se refieren al Deep Learning “como un enfoque de la Inteligencia Artificial, un tipo de aprendizaje automático que alcanza gran potencia y flexibilidad mediante el aprendizaje de la representación del mundo, a través de conceptos jerárquicamente anidados. Se trata de formar conceptos complejos mediante la extracción y concatenación de conceptos muy simples”. Para estos autores, el aprendizaje automático es el único enfoque viable, que permite construir sistemas de Inteligencia Artificial que pueden operar en los complicados ambientes del mundo en que vivimos.

La constante investigación que se ha tenido en el aprendizaje automático a través de los años, ha dado lugar a una gran cantidad de algoritmos y modelos, muchos relacionados entre sí y generando infinidad de aplicaciones en conjunto.

Según García (2015) el Deep Learning es un conjunto de técnicas y procedimientos algorítmicos basados en Machine Learning para lograr que una máquina aprenda de la misma forma que lo haría un ser humano. Siendo más precisos, hablamos de una familia de algoritmos cuyo propósito es simular el comportamiento que lleva a cabo nuestro cerebro para reconocer imágenes, palabras o sonidos. Son algoritmos que funcionan en base a “un proceso por capas”. El aprendizaje profundo simula el funcionamiento básico del cerebro, que se realiza a través de las neuronas.

### Principales algoritmos del Deep Learning

Dependiendo del tipo de aplicación que se trate, hay que emplear el tipo de algoritmo más adecuado para ello. Según (Yu, 2014), el tipo de aprendizaje, de acuerdo a su arquitectura y a su finalidad que persiguen los clasifican en tres grupos:

1) Redes profundas para aprendizaje no supervisado o generativo

En estas redes, el propósito principal es el análisis de patrones, la síntesis de los datos observados, o bien una agrupación, sin que se tenga una etiqueta para cada clase de

patrón u objetivo.

2) Redes profundas para aprendizaje supervisado

En estas redes, se cuenta con patrones conocidos y bien categorizados, con el fin de clasificar de forma directa.

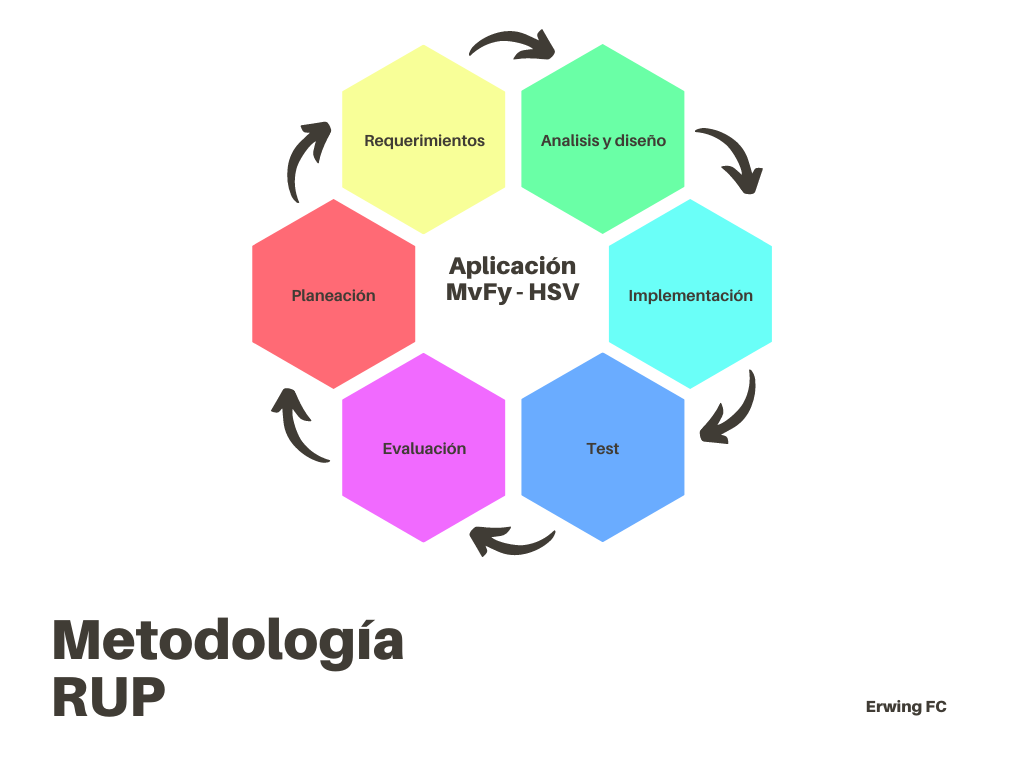
3) Redes profundas híbridas

Es una mezcla de las anteriores, con la meta de poder tener la capacidad de discriminar, auxiliado del aprendizaje no supervisado. Y esto podría llevar a un mejor performance que las redes supervisadas.

# 

# DISEÑO DE LA INVESTIGACION

El desarrollo del presente proyecto esta basado en la metodologia RUP, dicho proceso consta de 6 fases las cuales describen las actividades que se realizaran.



**Fase 1 ( Planeación )**

En esta fase se realizaran las reuiniones necesarias para describir las problematicas e identificar de forma general la necesidad del proyecto, de forma especifica esta fase cuenta con:

* **Esquematizacion de las reuniones:**  Se realizara un esquema principal de las reuniones que se haran en las semanas posteriores.
* **Estudio de viabilidad:** Se realizara un estudio para determinar la viabilidad del proyecto, proporcionando una estadistica de una encuesta hecha a posibles clientes.

**Fase 2 ( Requerimientos)**

En esta fase se realizara una recoleccion de requerimientos necesarios que debe cubrir el software, pára ello se hara:

* **Recopilacion de requerimientos:** Se realizaran un grupo de charlas y reuniones con el cliente para determinar los requerimientos y plasmarlos en un documento para su posterior uso

**Fase 3 ( Analisis y Diseño )**

Para esta fase se realizara un diseño del modulo, asi como su arquitectura, para ello se realizara:

* **Diseño de la arquitectura:**  se realizara un diseño del seguimiento del uso de la funcion principal del modulo, asi como los diagramas de caso de uso.
* **Investigacion:** para la realizacion del proyecto se deben tener en cuenta proyectos similares que puedan servir de apoyo en la creacion del modulo.
* **Creación de la documentacion:**  se plasmara de forma documental todos los aspectos necesarios que solidifiquen la implementacion del proyecto, el presente documento es dicho anexo de ello.

**Fase 4 ( Implementacion )**

En esta fase se realizara la creacion del modulo, para ello se realizara lo siguiente:

* **Desarrollo del modulo:** Se desarrollara el sistema, asi como las pruebas unitarias necesarias para la validacion del correcto funcionamiento del mismo.

**Fase 5 ( Test )**

Esta fase es crucial a la hora de validar el funcionamiento del modulo, este proporcionara la validacion de que el sistema esta funcionando de forma correcta antes de la fase posterior, para ello se realizara:

* **Plan de prueba:** Se realizara un plan de las pruebas a realizar.
* **Pruebas:**  se realizaran las pruebas unitarias y de integracion.
* **Solucion de problemas:**  si dichas pruebas anteriormente mencionadas resultan de forma negativa, se realizaran las correcciones respectivas y se validaran de nuevo las pruebas.

**Fase 6 ( Evaluacion )**

Esta fase tiene como objetivo la verificacion del cumplimiento de los requerimientos, se realizo lo siguiente:

* **Validacion:**  se le realizara un recorrido a las funcionalidades del modulo para validar los requerimientos recopilados.

# DESARROLLO DEL TRABAJO DE GRADO

## Análisis y esquematización del sistema

### Problema

En la seguridad no se puede improvisar o dejar a azar tareas en las que está en juego la vida de las personas protegidas, compañeros y la de personas no involucradas. En algunas instituciones los sistemas de seguridad no son suficientes para proporcionar la seguridad suficiente, algunos componentes de un sistema cerrado, se ven implícitamente relacionados con sus acciones en común, además de las políticas internas que se aceptan por estos, hace que sea poco probable realizar acciones anormales (aunque no siempre es así).

Poder identificar factores relevantes de prevención de situaciones problemáticas, suele ser una tarea complicada cuando el personal es masivo o no se tiene un sistema lo suficientemente adaptado, esto provoca que algunas situaciones no puedan ser previstas, es por ello que el módulo provee de herramientas, siendo el seguimiento de entidades desconocidas el principal, este proporciona un enfoque simple sobre entidades desconocidas facilitando la selección y accion sobre las mismas.

### Esquema del sistema

El sistema debe poder funcionar en un ambiente amplio de situaciones es por ello que se tuvieron en cuenta aspectos principales, los cuales son:

o Tiempo necesario para que el sistema pueda seleccionar una entidad como “Desconocida”

o El tipo de modelo de reconocimiento de rostros (optimizado o preciso).

o El tipo de archivo en donde se guardará el registro.

El modulo funcionaria de forma asíncrona en el servidor mientras se le envía la información de una cámara RGB 2D, se esperaría que el ambiente proporcione una alta resolución para la detección de rostros a larga distancia, además de proporcionar un flujo de imágenes de más de 15 FPS.

### Búsqueda de datos

El núcleo principal del sistema (reconocimiento de rostros), no necesito ser creado desde el comienzo por ello no requirió de información externa al ser implementado, mas que la API “face-api.js” y OpenCv.js.

Pero dado que el sistema requería de mayor robustez, se implemento un modelo de detección de vida, el cual implementa las capas CNN de [Keras](https://keras.io/), y para ello se necesito de un dataset de rostros proporcionado por (leokwu, 2018) y fue complementado con el dataset de (Mironică, 2019).

## Desarrollo del modulo

### Clase principal

Para proporcionar una implementación sencilla del módulo se desarrolló una clase que seria el punto principal de conexión con el servicio en su implementación, al instanciarse dicha clase se le pedirá al usuario los siguientes campos:

|  |  |
| --- | --- |
| Parámetro | Tipo |
| name | String |
| name\_file | String |
| Video\_label | Object HTMLElement |
| min\_date\_knowledge | String |
| file\_extension | String |
| features | String |
| time\_system | String |

Dichos parámetros serian los fundamentales para la instancia de dicha clase, proporcionaría un esquema inicial que puede ser llamado para empezar a iniciar el sistema.

Este módulo implementa la API “face-api.js”, esta proporciona los métodos necesarios para la detección de los rostros además de proporcionar el reconocimiento de rostros implementando la diferencia euclidiana entre dos imágenes de rostros, para ello el usuario podrá seleccionar entre ssdMobilenetv1 o tinyFaceDetector.

### Modelo CNN Liveness net

Usando el detector se puede evitar las falsificaciones y la suplantación anti-cara en el sistema.

Para crear el detector de vida se uso OpenCv, Deep Learning y Python.

El primer paso fue reunir nuestro conjunto de datos real vs. Para llevar a cabo esta tarea, nosotros:

Primero se usaron los datos obtenidos de (leokwu, 2018) y (Mironică, 2019), se ajustaron los datos de los rostros para mantener un tamaño similar, y se seleccionó cuales era falsificaciones y cuáles no, se hicieron transformaciones para mantener la media RGB y la inversión de la matriz de los tres canales a GBR.

Después de crear nuestro conjunto de datos implementamos, "LivenessNet", una CNN Keras. Esta red es deliberadamente superficial, asegurando que:

Reducimos las posibilidades de sobreajuste en nuestro pequeño conjunto de datos. El modelo en sí es capaz de ejecutarse en tiempo real (incluyendo en la Raspberry Pi). En general, nuestro detector de vida fue capaz de obtener 99% de precisión en nuestro conjunto de validación.

Para demostrar la canalización completa de detección de vida en acción, creamos un script Python + OpenCV que cargó nuestro detector de vivacidad y lo aplicó a secuencias de vídeo en tiempo real.

# RESULTADOS

Realizando pruebas de implementación el sistema reconoce rostros y es capaz de clasificar de forma correcta etiquetando a los usuarios de forma independiente y generando un registro individual, que posteriormente podría proporcionar información crucial y necesaria para la institución.

|  |  |
| --- | --- |
| Sistema | Precisión |
| Face-api.js | 85% |
| CNN (liveness net) | 90% |
| Deep face-detector | 75% |

# 

# CONCLUSIONES

En base a los resultados obtenidos logramos distinguir que el modulo puede depender de factores en las instituciones, pero de forma general se puede implementar de forma correcta y puede mantener una escalabilidad y dispone de forma sencilla de un apoyo en sistemas poco robustos donde se puedan integrar.

# 

# RECOMENDACIONES

Para la realización de trabajos futuros con base en el presente trabajo de investigación, se recomienda:

1. Se recomienda cambios en el apartado de seguridad, para mejorar el rendimiento de dicho apartado sobre todo si se piensa implementar en producción.
2. Se recomienda añadir funcionalidades para mejorar la interoperabilidad entre el módulo y sistemas de seguridad complejos que no se hayan tenido en cuenta.
3. Se sugiere que al ser implementado tal cual se encuentra el sistema, se proporcione una alerta al cliente indicando que dicho sistema es semiautomatizado y requiere de la intervención humana.
4. Se recuerda al lector que dicho artículo es una versión inicial, que contiene problemas y contenido no citado, no debe ser publicado ya que no refleja de forma completa el desarrollo del módulo propuesto.

# 

# REFERENCIAS BIBLIOGRÁFICAS

|  |  |
| --- | --- |
| [1] | A. Anjos, J. Komulainen, S. Marcel, A. Hadid, and M. Pietikainen.¨ Face anti-spoofing: Visual approach. In Handbook of Biometric Anti-Spoofing, pages 65–82. Springer, 2014. |
| [2] | A. Anjos and S. Marcel. Counter-measures to photo attacks in face recognition: A public database and a baseline. In IJCB, 2011. |
| [3] | S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh. Face anti-spoong via motion magnication and multifeature videolet aggregation. Technical report, 2014. Available at https://repository.iiitd.edu.in/jspui/ handle/123456789/138. |
| [4] | Z. Boulkenafet, J. Komulainen, and A. Hadid. Face spoofing detection using colour texture analysis. IEEE TIFS, PP(99):1–1, 2016. |
| [5] | C.-C. Chang and C.-J. Lin. LIBSVM: A library for support vector machines. ACM TIST, 2:27:1–27:27, 2011. Software available at http://www.csie.ntu.edu.tw/ ˜cjlin/libsvm. |
| [6] | G. Chetty and M. Wagner. Multi-level liveness verification for face-voice biometric authentication. In Biometric Consortium Conference, pages 1–6, Sept 2006. |
| [7] | I. Chingovska, A. Anjos, and S. Marcel. On the effectiveness of local binary patterns in face anti-spoofing. In BIOSIG, pages 1–7, Sept 2012. |
| [8] | T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel. Lbp- top based countermeasure against face spoofing attacks. In ACCV 2012 Workshops, pages 121–132. Springer, 2012. |
| [9] | T. de Freitas Pereira, J. Komulainen, A. Anjos, J. M. De Martino, A. Hadid, M. Pietikainen, and S. Marcel. Face liveness detection using dynamic texture. EURASIP JIVP, 2014:2, Jan. 2014. |
| [10] | T. Dhamecha, A. Nigam, R. Singh, and M. Vatsa. Disguise detection and face recognition in visible and thermal spectrums. In ICB, pages 1–8, June 2013. |
| [11] | N. Erdogmus and S. Marcel. Spoofing 2d face recognition systems with 3d masks. In BIOSIG, pages 209–216, 2013. |
| [12] | N. Erdogmus and S. Marcel. Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect. In IEEE BTAS, pages 1–6, Sept 2013. |
| [13] | N. Erdogmus and S. Marcel. Spoofing face recognition with 3d masks. IEEE TIFS, 9(7):1084–1097, July 2014. |
| [14] | J. Galbally and S. Marcel. Face anti-spoofing based on general image quality assessment. In 22nd ICPR, pages 1173– 1178, Aug 2014. |
| [15] | J. Galbally, S. Marcel, and J. Fierrez. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. IEEE TIP, 23(2):710–724, 2014. |
| [16] | A. Hadid, N. Evans, S. Marcel, and J. Fierrez. Biometrics systems under spoofing attack: An evaluation methodology and lessons learned. IEEE SPL, 32(5):20–30, Sept 2015. |
| [17] | R. Haralick, K. Shanmugam, and I. Dinstein. Textural features for image classification. IEEE TSMC, 3(6):610–621, Nov 1973. |
| [18] | L. Hua and J. E. Fowler. |
| Technical report, 2001. |  |
| [19] | K. Kollreider, H. Fronthaler, and J. Bigun. Evaluating liveness by face images and the structure tensor. In IEEE Workshop on Automatic Identification Advanced Technologies, pages 75–80, Oct 2005. |
| [20] | N. Kose and J.-L. Dugelay. Countermeasure for the protection of face recognition systems against mask attacks. In IEEE FG, pages 1–6, April 2013. |
| [21] | S. Marcel, M. S. Nixon, and S. Z. Li. Handbook of Biometric Anti-Spoofing: Trusted Biometrics Under Spoofing Attacks. Springer Publishing Company, 2014. |

# 

# APENDICES

Si aplica, se anexan: formato de encuestas entrevistas, chek list, en general las herramientas o instrumentos utilizados en la investigación. Se enumeran con letras mayúsculas de la A - Z, si la cantidad es mayor se enumeran con números arábigos. Fuente y títulos en Normas APA.

# ANEXOS

La sección de anexos será usada para presentar información que los autores y el director consideren importante, como el caso de: manuales de usuario, hojas de datos, guías de laboratorio, demostraciones matemáticas, diseños esquemáticos, cartografía, entre otros.

Cada Anexo debe estar identificado por una letra(A –Z), la cual será usada para diferenciar las figuras, tablas y ecuaciones que se encuentren en estas secciones.

**Instructivo General[[1]](#footnote-1)**

Apreciado Estudiante: Lea cuidadosamente este instructivo general y elimínelo una vez termine de elaborar el informe final.

Estilo: APA, 6ta edición, como se describe a continuación

Tamaño del papel: Carta (letter) / papel 21.59 cm x 27.94 cm (8 1/2” x 11”).

Márgenes: 2.54 en cada borde. El formato ya está configurado con estos márgenes. Por favor no los modifique.

Sangría: Cinco (5) o 0,5cm desde la pestaña diseño de Word, solo al inicio de cada párrafo y al inicio de las notas al pie de página.

Importante que en todas las páginas quede igual la sangría, para ello se sugiere usar tabulador. No lleva sangría:

• El texto correspondiente al resumen,

• El texto del Abstract

• Las citas en bloque

• Los títulos y encabezados

• Los títulos y notas de tablas

• Los pies de figuras o gráficas, ilustraciones, mapas

Fuente: Arial, tamaño: 12, en todo el documento, desde la portada hasta las referencias bibliográficas y los anexos.

Numeración de páginas

(Paginación): La paginación se inicia desde la portada, en forma consecutiva hasta el final. Se incluye en la esquina superior derecha de la hoja. La plantilla ya está numerada, no la modifique.

Texto: Justificado (APA sugiere alineado a la izquierda, pero se adopta justificado).

Interlineado: 1.5 en párrafos (APA sugiere 2.0, pero se adopta 1.5).

Listas especiales: **Tablas:** La American Psychological Association (p. 130), sugiere cuando sea conveniente diseñar tablas para incluir en el documento, es importante definir y estructurar los datos que los interesados en el tema, requerirán para comprender la explicación.

**Figuras:** “se pueden utilizar muchos tipos de figuras” (Manual de la APA, 2010, p. 153). Los más comunes son: gráficas, diagramas, Mapas. Dibujos y fotografías. Se incluyen, cada figura, en una página separada, al final del documento, después de las tablas o después de las referencias ( <https://apastyle.apa.org/manual/new-7th-edition>)).

Las tablas, imágenes y figuras: Todas elaboradas, bajo APA

Apéndice: Los apéndices son una sección opcional del trabajo en donde se incluye información o documentación que permite complementar y que no se puede incorporar en el cuerpo del trabajo. Esta sección se ubica al final de del manuscrito antes de los anexos.

Anexos: Los anexos serán usados para presentar información que los autores y el director consideren importante, como el caso de: manuales de usuario, hojas de datos, guías de laboratorio, demostraciones matemáticas, diseños esquemáticos, cartografía, entre otros. Esta sección se ubica al final de todo el manuscrito y es allí donde se pueden incorporar materiales de estímulo, tablas y/o figuras (Manual APA 6ª (sexta) edición. Disponible en http://www.apastyle.org/ y https://normasapa.net/tablas-figuras-y-apendices/

Textos escritos en gris: Se sobre escribe sobre éste en color negro la información solicitada, cuando se refirieren al título o datos de la portada o contraportada. Si se trata de una instrucción se elimina y se escribe el contenido que corresponda.

Texto escrito en negro

(en la plantilla): No se modifica. Se dejan como están.

Páginas de Dedicatoria y

Agradecimientos: Son opcionales.

Hoja de Aceptación: Se debe diligenciar completamente por los jurados (evaluadores, directores).

Recomendación: Por favor no modificar el formato de la plantilla y aplicar correctamente la norma APA.

**Referencias**

American Psychological Association. *APA Style*. Recuperado de <http://www.apastyle.org/>.

American Psychological Association (2010). *Manual de Publicaciones* (3a. ed.). México:

Nota: No olvide eliminar este instructivo y entregar solo el informe en la plantilla inicial de este documento

**AYUDAS PARA LA PRESENTACIÓN DEL DOCUMENTO**

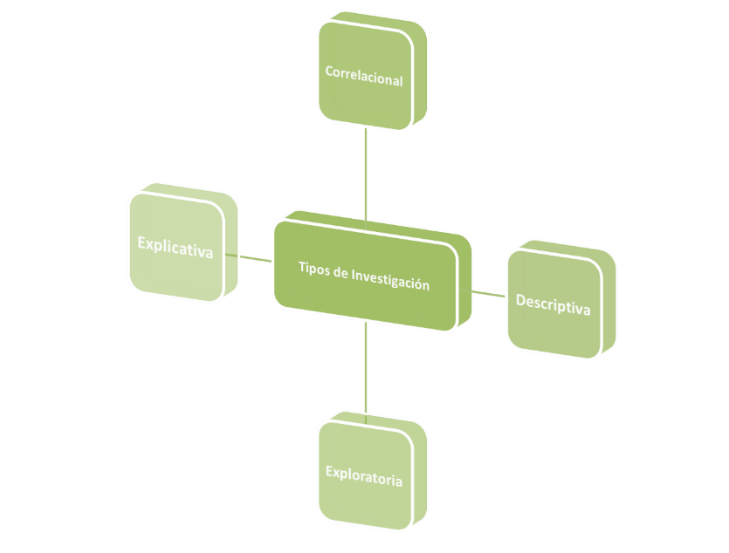
Esta sección del documento es de orientación para la elaboración del documento, **debe eliminarla** cuando genere la versión final. De igual manera, **debe eliminar** todas las instrucciones que contiene esta plantilla, que por lo general las encontrará como texto en color gris.

Recuerde que se debe tener especial cuidado en la redacción del texto del documento, este se debe redactar de manera formal en **tercera persona** y no en primera persona o de manera informal, no se permiten textos como: "nosotros esperamos que", en su lugar se debe usar: “se espera por parte de los autores que…”, igualmente sebe evitar el uso de gerundios, por ejemplo: estudiando el tema, en su lugar: estudiado el tema.

Las tablas, figuras, gráficas, esquemas, entre otros, deben tener nombre y fuente, a continuación, se presenta el ejemplo:

**Ejemplo de imagen**

***Figura 1***. Tipos de Investigación



Fuente: Autor

**Ejemplo de tabla**

Para el texto en el interior de la tabla deberá utilizarse fuente tipo Arial a 10 puntos con interlineado sencillo. Utilice el mismo formato para todas las tablas para dar uniformidad al documento.

***Tabla 1***.

*Descripción de la primera fase del estudio metodológico para construir un software en lenguaje Java*

|  |  |
| --- | --- |
| Tipo | Elementos |
| Actividades | * Actividad 1 * Actividad 2 * Actividad 3 * Actividad 4 |
| Recursos | * Sitio de trabajo   Conexión a internet   * Computador * Programas del computador * Navegador Web * Word * Excel |
| Resultados | Conocimiento y fortalecimiento del paradigma de la programación orientada a objetos, sus características, alcance, técnicas de desarrollo, métodos y funciones entre otros campos vinculados con esta misma. |

Nota: Tabla elaborada por el autor a partir de análisis sobre diseño de software.

1. Información tomada del Manual APA 6ª (sexta) Edición. Para complementar información se recomienda consultar en la página de la organización http://www.apastyle.org/ [↑](#footnote-ref-1)